

## System reliability of jack-up structures based on fatigue degradation

N. Shabakhty & H. Boonstra

*Delft University of Technology, Marine Technology, Mekelweg, Delft, The Netherlands*

P. Van Gelder

*Delft University of Technology, Civil Engineering Faculty, Stevinweg, Delft, The Netherlands*

**ABSTRACT:** In recent years there has been considerable development in the area of system reliability assessments of offshore structures except for jack-up platform. However, since the reliability of jack-up platform is a crucial aspect with regard to the safety of the structure during its service time and possibly beyond the predicted lifetime, there is significant demand from the offshore industry to investigate system reliability of this type of offshore structure. This paper therefore presents a methodology to estimate the system reliability of jack-up structures by considering sequence of fatigue failure. First, component reliability of this structure based on fatigue limit state function is derived, and then the branch and bound technique has been used to identify an important sequence of section failure leading to system collapse. The structural failure is therefore regarded as the event at which one of these important sequences occurs. The result determined for a jack-up structure shows a significant systems effect and that the probability of structural failure is larger than the probability of failure for an individual section.

### 1 INTRODUCTION

Jack-up structures are generally used for production drilling and exploration of hydrocarbons. Their combination of mobility and the behavior as fixed structures in operational conditions have made them important in the offshore industry over the last 40 years.

When these types of platforms have been in operation for a great part of their original design-life and the intention is to extend their utilization beyond the predicted lifetime, considerable research into assessing the safety of structures regarding to degradation agents like fatigue is needed. In accordance with code philosophy, most of this work is on the safety of individual sections in terms of fatigue limit state function. However, jack-up structures have redundancy and failure of individual section does not lead to structural collapse. Hence, a procedure is needed to investigate system reliability of jack-up structure due to fatigue degradation.

Several investigations have been carried out in last decade on system reliability of jacket structure due to fatigue, extreme environmental loads or combination of these two failure modes, (Karamchandani et al., 1991, Shetty, 1992, Dalane, 1993, Onoufriou, 1999, Pillai & Pradad, 2000). However, regarding to jack-up platforms, this has been only restricted to component

level e.g. Jensen et al. (1991) and Shabakhty et al. (2001) and system effect under extreme environmental loads without considering fatigue degradation, e.g. Karunkaran (1993) and Daghigh (1997).

This paper presents a specific approach to estimate system reliability of jack-up platforms under fatigue degradation. First, probability of failure of each component of platform is calculated by using fatigue limit state function. The probability of failure of second element is therefore determined by extending fatigue limit state function for subsequent failure. Important sequences of failure are then identified by utilizing branch and bound technique and finally the system reliability through combination of important failure paths leading to system failure has been calculated.

The advantage of this method is that the FORM or SORM technique can be used to compute each failure path individually and finally determine system reliability based on combination of significant failure paths identified in branch and bound search technique.

### 2 FORMULATION OF FATIGUE DAMAGE

To predicate crack growth due to fatigue, the growth of crack per stress cycle at any points along the crack

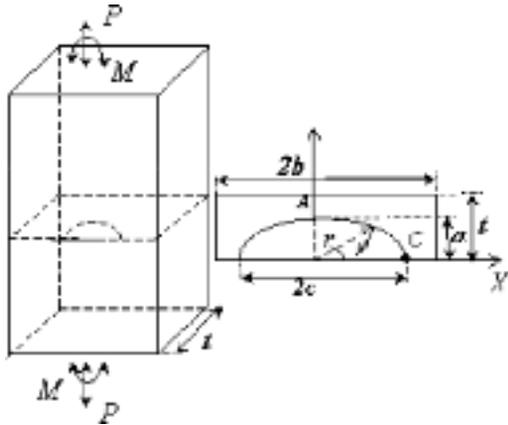


Figure 1. Crack-growth due to fatigue.

front is supposed to follow the Paris-Erdogans equation. In addition, to simplify the problem, the fatigues cracks shape is assumed to be initially semielliptic, and to remain semi-elliptic during propagation of crack. As is clear from figure (1), characteristics of crack front can be sufficiently described with two parameter of crack depth ( $a$ ) and crack length ( $2c$ ). Based on Paris-Erdogans equation, the increment of crack size  $dr(\phi)$  during a load cycle  $dN$ , at a specific point along the crack front can be related to stress intensity factor,  $\Delta K_r(\phi)$  with the following expression

$$\frac{dr(\phi)}{dN} = C_r(\phi)(\Delta K_r(\phi))^m, \Delta K_r(\phi) > 0 \tag{1}$$

when  $C_r(\phi)$  and  $m$  are two material parameters for specific points along the crack front, and  $\phi$  is location angle. However, this differential equation must satisfy at all points along the crack front.

The consequence is the following differential equation for deepest point of crack, point  $A$ , (see figure 1)

$$\frac{da}{dN} = C(\Delta K)^m, a(N_0) = a_0 \tag{2}$$

The general expression for the stress intensity factor is  $K = YS\sqrt{\pi a}$ , where the geometry function  $Y$  accounts for the effect of all boundaries, i.e. width, thickness, crack front curvature, etc.

Raju & Newman (1986) proposed an empirical equation for the stress intensity factor,  $\Delta K(\phi)$ , of a surface crack in a finite plate subjected to remote tension and bending loads. This equation has been fitted on finite element results for two types of remote tension and bending loads applied to surface cracked-plate. The

derived stress intensity equation from this research is

$$\begin{aligned} \Delta K_{plate}(\phi) &= (S_t + S_b) \sqrt{\pi a} (1/Q)^{1/2} \frac{1 + HS_b/S_t}{1 + S_b/S_t} F\left(\frac{a}{t}, \frac{c}{b}, \phi\right) \\ &= S \sqrt{\pi a} Y_{plate} \end{aligned} \tag{3}$$

where  $S_t$  and  $S_b$  are remote tension and bending stress ranges, respectively.  $Q$  is shape factor and two parameters  $F$  and  $H$  characterize the boundary-correction factor.

In the welded joints, such as tubular member in jack-up platforms, the non-linearity in stress field arising from local stress concentration at the weld toe is important and should be considered. Smith & Hurworth (1984) therefore recommended applying the following correction to stress intensity factor to consider this non-linearity.

$$M_K = 1 + 1.24 \exp(-22.1 a/t) + 3.17 \exp(-357 a/t) \tag{4}$$

The final geometry function used for tubular joints can therefore multiplied by this correction factor,  $Y = Y_{plate} M_K$ . Now by substituting this geometry function in the stress intensity factor,  $(\Delta K)^m = S^m Y(a)^m (\pi a)^{m/2}$  and integrating differential equation of propagation of crack, the following expression is between propagation of crack and stress range derived.

$$\int_{a_0}^{a_t} \frac{da}{C \delta_Y^m Y(a)^m (\sqrt{\pi a})^m} = \sum_{i=1}^{N_t} S_i^m \tag{5}$$

In which  $\delta_Y$  is a random variable to model uncertainty introduced in the geometry function. As is clear, the left hand side of this equation depend only on fatigue and material characteristics, and right hand side on loading, therefore we term them fatigue strength function,  $\Psi_R(a)$ , and fatigue loading function,  $\Psi_L(T)$ , respectively.

Since each stress range in equation (5) has random characteristic, the summation will be random. For a large amount of stress range,  $N_t$ , the coefficient of variation of stress range is relatively small and can therefore be replaced by its expected value.

Furthermore, the fatigue degradation is combination of damage of structural elements in long-term due to stress range of several sea-states. The fatigue loading function for combination of long-term stress distribution can be determined by following expression, Shetty (1992).

$$\Psi_L(T) = \sum_{i=1}^{N_t} S_i^m = E[N(T)] E[S^m] = \nu_p^m T E^I[S^m] \tag{6}$$

Where  $v_p^l$  is long-term average peak-frequency of stress-cycle and  $E^l[S^m]$  is long-term expected stress range power  $m$ . We can determine long-term distribution of stress range by combining stress distribution in each sea-state that the structure may experience in its lifetime. This can be carried out by multiplying stress distribution with weighting factor,  $\omega$ , and probability of occurrence of each sea-state

$$F_S(s) = \int_{H_s} \int_{T_z} \int_{\theta} \omega_{h_s, t_z, \theta} F_S(s | h_s, t_z, \theta) f_{H_s, T_z}(h_s, t_z | \theta) f_{\theta}(\theta) d\theta dt_z dh_s \quad (7)$$

In which  $f_S(s | h_s, t_z, \theta)$  is short term stress range distribution,  $f_{H_s, T_z}(h_s, t_z | \theta)$  is conditional distribution function of the sea-state in direction  $\theta$ , and  $f_{\theta}$  is directional distribution of wave.  $\omega$  is the weighting factor, which expresses the relative rate of response peaks within each short-term sea-state to the long-term response peak.

When the stress process is narrow banded, the average peak of response will be almost the same as average zero crossing. However, in jack-up structure, this case is not correct and original peak-frequency derived from stress distribution is used here. The weighting factor can therefore be determined for each sea state with the following expression

$$\omega_{h_s, t_z, \theta} = v_p(h_s, t_z, \theta) / v_p^l \quad (8)$$

when  $v_p(h_s, t_z, \theta)$  is the average peak-frequency of stress-cycle in specific sea-state and  $v_p^l$  is long-term average zero-frequency of stress-cycle, which can be determined with the following equation.

$$v_p^l = \int_{H_s} \int_{T_z} \int_{\theta} v_p(h_s, t_z, \theta) f_{H_s, T_z}(h_s, t_z | \theta) f_{\theta}(\theta) d\theta dt_z dh_s \quad (9)$$

Since close form integration of equation (7) is not possible and in fatigue reliability, we need an analytical expression for long-term distribution function of stress range, it is important to fit a specific available distribution function on simulation results. If the stress process followed Gaussian process, the distribution of stress range according to bandwidth parameters will vary between Rayleigh and Gaussian distribution, Farens (1990). The non-linearity in stress process due to drag term in calculation of hydrodynamic loads, variability in submergence section of structure when wave passing from structure and finally  $p$ - $\delta$  effects in jack-up platform deviates the stress process from Gaussian and using a proper distribution is therefore very important.

The two-term Weibull distribution is found to fit appropriately on long-term stress range distribution determined in simulation results and selected for its

simplicity and ability to resemble Rayleigh distribution, Farens (1990). Hence, by calibrating two-term Weibull distribution on the outcome of simulation results, the long-term distribution of stress range can be specified with

$$F_S(s) = 1 - \exp\left[-\left(\frac{s}{A}\right)^B\right] \quad (10)$$

where  $A$  and  $B$  is scale and shape parameter of Weibull distribution and can be calculated by using non-linear least square methods. In computing stress range, some uncertainties in the hydrodynamic load, stress calculation and stress concentration in a specific hot spot are existed and should be accounted. To take into account these uncertainties, the final stress range determined with Weibull model has been therefore multiplied by three random variables,  $\delta_F$ ,  $\delta_S$  and  $\delta_{SCF}$  which each one represent uncertainty in hydrodynamic load, stress calculation and stress concentration factor in specific hot-spot respectively, Dalan (1993). Consequently, the final expression of fatigue loading function is

$$\psi_L(T) = v_p^l E^l[S^m] T = v_p^l \delta_F^m \delta_S^m \delta_{SCF}^m A^m \Gamma\left(1 + \frac{m}{B}\right) T = \eta T \quad (11)$$

and time required for propagation of crack through the thickness of the tubular elements can be calculated with the following expression.

$$T_{th} = \frac{\psi_R(a_{th})}{\eta} = \frac{1}{v_p^l \delta_F^m \delta_S^m \delta_{SCF}^m A^m \Gamma\left(1 + \frac{m}{B}\right)} \int_{a_0}^{a_{th}} \frac{da}{C \delta_f^m Y(a)^m (\sqrt{\pi a})^m} \quad (12)$$

According to fatigue damage, development of through the thickness cracks may not cause section failure and before the final failure occurs the crack should propagation significantly along the circumference of tubular section. The time to develop such crack will be larger than the time to develop through the thickness and this should be taken into account in our formulation. Hanna & Karsan (1989) revealed the time to failure could be related to the time of the first through the thickness crack with

$$T_f = \delta_{if} T_{th} \quad (13)$$

when multiplication factor,  $\delta_{if}$  is the random correction factor. Furthermore, the test data in this research demonstrated that the correction factor is independent of the stress parameter and lognormal distribution can appropriately be fitted on the results with mean value 1.5 and standard deviation 0.5.

### 3 FAILURE PROBABILITY BASED ON SEQUENCE OF JOINTS FAILURE

In reliability analysis, we need to specify the limit state function, which separate safe and failure domain and determine the probability of failure. The time-to-failure derived for specific joint based upon equation (13) has random characteristics since it depend on other random variables. Applying modification factors mentioned in last section, the random time-to-failure of joint e.g.  $J_1$  can therefore be determined by

$$T_{fJ1} = \frac{\delta_{fJ1}}{\sqrt[p_{F1}]{\delta_{F1}^m \delta_{S1}^m \delta_{SCF1}^m C_{J1} A_{J1}^m \Gamma(1 + \frac{m}{B_{J1}})}} \int_{a_{J1}}^{a_{J1}'} \frac{d\alpha}{\alpha^m \gamma(\alpha)^m (\sqrt{m\alpha})^m} \quad (14)$$

If this random time-to-failure becomes less than the expected lifetime of joint  $J_1$ , the fatigue failure will be expected to occur in this joint and vice versa if it is greater than the expected lifetime it means the joint can appropriately functioning. Therefore, the limit state function required in the reliability analysis based on fatigue failure of the first joint, e.g.  $J_1$  can be expressed by

$$g_{J1} = T_{fJ1} - T_{life} \leq 0 \quad (15)$$

and its probability of failure determined with the following expression.

$$P_f = P[g_{J1} \leq 0] = P[T_{fJ1} - T_{life} \leq 0] = P[T_{fJ1} \leq T_{life}] \quad (16)$$

Furthermore, for each joints in the structure, we can extend and determine their probability of failure with an expression like equation (16). The highest probability determined in this way would therefore be related to the joint with the maximum probability of occurrence of failure. It means the joint with the highest failure probability likely to be the first failure joint. However, it is not general cases and other possibilities might be suggested. The branch and bound technique in this situation can help us to specify the most important failure sequence of joints under fatigue.

The next step in reliability calculation would be to establish a formulation for next failure joint when the first failure joint is known. In this regards, suppose the first joint, which fails due to fatigue degradation is  $J_1$ , the next failure joints might be joints as well as  $J_2$ . In term of linear damage accumulation model for fatigue, this joint has fatigue strength function like equation (5) but the fatigue loading function is the combination of two terms. The first one is fatigue loading function in joint  $J_2$  when the joint  $J_1$  is in intact state and reaches

to failure,  $\Psi_{LJ2}(T_{J1})$ , and next one from failure of joint  $J_1$  to  $J_2$ ,  $\Psi_{LJ2/J1}$ .

$$\Psi_L(T_{J2}) = \Psi_{LJ2}(T_{J1}) + \Psi_{LJ2/J1}(T_{J2} - T_{J1}) \quad (17)$$

The total time to reach the sequence failure of joint  $J_2$  follow by joint  $J_1$  is therefore divided to the time when the first joint is in intact state and reaches to failure,  $T_{J1}$ , and the time of failure of joint  $J_2$  followed by  $J_1$ ,  $(T_{J2/J1} - T_{J1})$ .

By substituting equation (17) in equation (5) and apply same modification factors to consider uncertainty in hydrodynamic load, stress concentration factor and time to failure, the following expression can be generated to relate the fatigue strength function and loading function.

$$\begin{aligned} \delta_{fJ2} \int_{a_{J2}}^{a_{J2}'} \frac{d\alpha}{\alpha^m \gamma(\alpha)^m (\sqrt{m\alpha})^m} &= \sqrt[p_{F2}]{\delta_{F2}^m \delta_{S2}^m \delta_{SCF2}^m C_{J2} A_{J2}^m \Gamma(1 + \frac{m}{B_{J2}})} T_{J1} \\ &+ \sqrt[p_{F2/J1}]{\delta_{F2/J1}^m \delta_{S2/J1}^m \delta_{SCF2/J1}^m C_{J2/J1} A_{J2/J1}^m \Gamma(1 + \frac{m}{B_{J2/J1}})} (T_{J2/J1} - T_{J1}) \end{aligned} \quad (18)$$

As noted from equation (18), the first expression is the strength of the joint and next expression shows the total fatigue loading at failure time. The modification  $\delta_{fJ2}$  is applied to the first expression to represents uncertainty in the strength. This modification is then modeled independent of the loading function i.e. does not change when the fatigue loading function changed.

The time to failure of  $J_2$  followed by  $J_1$  is therefore expressed by rearranging equation (18) as

$$T_{J2/J1} = \frac{\delta_{fJ2} \int_{a_{J2}}^{a_{J2}'} \frac{d\alpha}{\alpha^m \gamma(\alpha)^m (\sqrt{m\alpha})^m} - \sqrt[p_{F2}]{\delta_{F2}^m \delta_{S2}^m \delta_{SCF2}^m C_{J2} A_{J2}^m \Gamma(1 + \frac{m}{B_{J2}})} T_{J1}}{\sqrt[p_{F2/J1}]{\delta_{F2/J1}^m \delta_{S2/J1}^m \delta_{SCF2/J1}^m C_{J2/J1} A_{J2/J1}^m \Gamma(1 + \frac{m}{B_{J2/J1}})}} + T_{J1} \quad (19)$$

and the probability of failure of sequence  $J_2$  followed by  $J_1$  can be calculated with

$$P_{fJ2/J1} = P[(g_{J2/J1} \leq 0) \cap (g_{J1} \leq 0)] = P[(T_{J2/J1} \leq T_{life}) \cap (T_{J1} \leq T_{life})] \quad (20)$$

The same approach can be used to determine an expression for higher sequence failure e.g., joint  $J_n$  when  $J_1, J_2, \dots, J_{n-1}$  have respectively failed,

$$\Psi_L(T_n) = \Psi_{LJn}(T_n) + \Psi_{LJn/J1}(T_{Jn} - T_{J1}) + \dots + \Psi_{LJn/J2 \dots J_{n-1}}(T_{Jn/J2 \dots J_{n-1}} - T_{Jn/J2 \dots J_{n-2}}) \quad (21)$$

By substitute this equation in equation (5) and apply the same modification factors to represents uncertainty in the strength, hydrodynamic load and stress concentration factor, the following general equation can be

derived for the time to failure of joint  $J_n$  when failure of joints  $J_1, J_2/J_1, J_3/J_2, J_1, \dots, J_{n-1}/J_{n-2}, J_{n-3}, \dots, J_2, J_1$  occur respectively.

$$T_{J_1/J_2, \dots, J_k} = \frac{\int_{t_0}^{t_{\infty}} \frac{dt}{\delta_{F_1}^m(\alpha)^m (\pi a)^m} \sum_{i=1}^{n-1} \delta_{F_i}^m(\alpha)^m C_{F_i}^m A_{J_i}^m \Gamma(1 + \frac{m}{B_{J_i, n, \dots, k}})}{\int_{t_0}^{t_{\infty}} \delta_{F_1}^m(\alpha)^m C_{F_1}^m A_{J_1}^m \Gamma(1 + \frac{m}{B_{J_1, n, \dots, k}}) + \dots + T_{J_{k-1}/J_{k-2}, \dots, J_2}} \quad (22)$$

where the fatigue loading function for this sequence failure of joints can be obtain with the following expression

$$\psi_{L, J_1/J_2, \dots, J_k} = \int_{t_0}^{t_{\infty}} \delta_{F_1}^m(\alpha)^m C_{F_1}^m A_{J_1}^m \Gamma(1 + \frac{m}{B_{J_1, n, \dots, k}}) \quad (23)$$

Hence, the final failure probability of the sequence of  $k$  joints failure i.e.  $J_1, J_2, J_3, \dots, J_k$  should be calculated with intersection of all these component failures i.e.,

$$P_{f, J_1/J_2, \dots, J_k} = P\left[\bigcap_{i=1}^k (S_{J_i, n, \dots, k} \leq 0)\right] = P\left[\bigcap_{i=1}^k (T_{J_i, n, \dots, k} \leq T_{t_{i/c}})\right] \quad (24)$$

#### 4 SEARCH TECHNIQUES TO IDENTIFY DOMINANT FAILURE SEQUENCE

In redundant offshore structure, innumerable failure sequences can be expected to occur but only some of them contribute significantly to collapse or system failure and others have very low probability of occurring.

In system reliability, identification of these important sequences is essential and several methods have been developed to distinguish dominant failure sequence. These methods can be generally classified into two categories, deterministic and probabilistic approaches.

Incremental loading and plastic mechanism analysis are two examples of deterministic method. In the incremental lading, the random variables are fixed at their mean values and a deterministic analysis is performed to identify the sequence of section failure leading to structural collapse. By assuming a proportional loading condition, the load factor is gradually increased to cause sequence of element failure. To determine additional failure sequence, value of some variables can be modified and deterministic analysis repeated to specify a new failure sequence. This method basically uses a deterministic search strategy and obtain important failure path without so many repetitions of structural analysis, but can not ensure all the probabilistically dominant failure paths are identified, Moses (1982).

In plastic mechanism, an ideal plastic behavior of a material is considered and based on this model analytical formulation for plastic limit state function is extended. Hence, the final plastic mechanism leading to structural collapse is identified using  $\beta$ -unzipping method in connection with basic plastic mechanisms. Which, it is not possible to guarantee that the  $\beta$ -unzipping method identifies all significant mechanisms but it may gives reasonable good results. Since some of plastic mechanisms are excluded in this method, the reliability index determined in this approach is therefore an upper bound of the correct generalized system reliability index, Thof-Christensen & Murotsu (1986).

The simulation-based and branch and bound methods are two main models of probabilistic approaches. The simulation-based is constructed on Monte Carlo simulation technique and is an expensive tool for reliability assessment of large structures. The structural analysis needs to repeat several times for each sampling point and taking into account numbers of leading to failure of structure. Furthermore, to increase the efficiency and reduce the simulation, the importance sampling technique in combination with directional simulation technique can be employed, Warrts & Vrouwenvelder (1998).

The more robust method to specify system failure is branch and bound technique, Thof-Christensen & Murotsu (1986). In this approach, the failure sequence is identified based on the sequences in decreasing order of importance. This means the first failure sequence belongs to the largest probability of failure which has maximum probability of occurrence of corresponding damaged state and the second one to the second largest and so on. Therefore, the first step will be to compute the failure probability of each joint using equation (16).

The calculated failure probabilities show the first branches in failure tree. Let the joint  $J_1$  has the largest failure probability i.e. the most likely to occur damage state, now focus shift to this joint and the probability of failure leading to next joint failure which represent new damage state in the failure tree and can be calculated with equation such as equation 20.

Note that the probability of occurrence of this damage state is the probability of joint  $J_1$  fails in intact state and joint  $J_2$  fails subsequently if the second joint failure is  $J_2$ . However, this can be extended for other joints to determine their failure probability. Hence, the sequence with maximum probability of failure in the second branches leads us to the next damage state with maximum probability of occurrence. This process continues to reach the damage state, which constitutes collapse of system. The sequence of failure leading to this damage state is the-most-likely-to-occur sequence. Since the focus was on the most-likely-to-occur damage state with maximum probability of occurrence, the collapse state reached in this way is the most

important one and is named the collapse state with the highest probability of occurrence.

System collapse can happen in the sequence other than expected already; the contribution of other collapse sequence in system reliability should therefore be taken into account. To establish different system collapse, we need to consider other scenarios that might occur and lead to system collapse.

The system collapse based on maximum probability of occurrence is the system with the highest failure probability but it is possible to shift focus in branch tree to the next failure sequence which has the second highest probability i.e. on the next most-likely-to-occur damage state. If this is not the collapse state, continues the search technique until the damage states under study constitute the system collapse. The sequence leading to this collapse state is the second most important failure sequence. If this process is continued for other failure sequences i.e. third, fourth, etc., most-likely-to-occur damage states, it will be possible to identify several collapse states and their probability of occurrence. Since some of these collapse states are not disjoint, the total system probability should be computed based on the union of these collapse sequences. In this research, the branch and bound technique has been used to identify sequences leading to collapse of system and system reliability is determined based on union of these collapse failure.

## 5 JACK-UP MODEL AND PROBABILISTIC DESCRIPTION OF RANDOM VARIABLES

To illustrate the procedure of determining system reliability based on sequence of fatigue failure, the Neka jack-up platform is considered in this research. This platform operates in water depth 95 m with three retractable legs, see figure (2).

The system reliability of this platform due to extreme environmental loads has been already investigated by Daghigh (1997). In this research, system failure was represented based on series system of parallel subsystem when failures of elements constitute subsystem. The system reliability is evaluated by using simple upper bound on series system and incremental loading approach used to identify failure of elements in parallel system.

To determine stochastic response of jack-up platform, two approaches can generally be used in structural analysis, frequency and time domain method. The frequency domain is applicable when structure behaves linearly.

The stochastic time domain analysis is preferred and used in this research because the stress processes show high non-linearity due to drag term in wave loading, variation in submergence sections of structural and finally  $p$ - $\delta$  effects in jack-up platform.

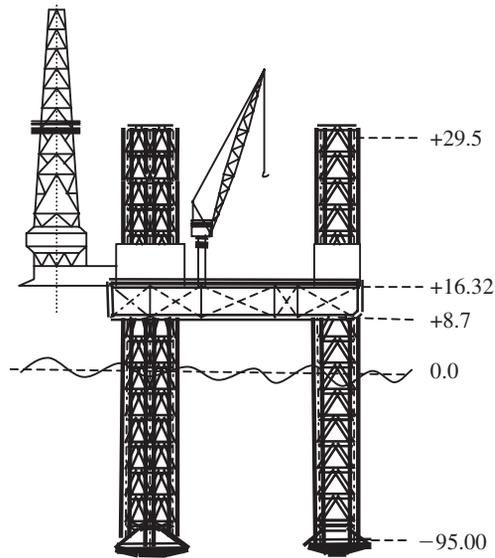


Figure 2. Neka jack-up platform.

By using Morison equation and P-M spectra, the hydrodynamic loads in combination with wind and functional loads are calculated for several sea-state for each 0.25 second of time step. In addition, to take into account the wave kinematics above mean water level, the Wheeler stretching method is applied in this research.

The short-term stress distributions are determined for each element and each sea-state in scatter diagram using the time history of stress response computed for one hour simulation of each sea-state, figure (3).

To determine the long-term distribution of stress range, we need to calculate the integral of equation (7). Since calculation of this integral is difficult and impossible in close form, the Monte Carlo Simulation (MCS) technique is preferable to other numerical integration because this technique is less rigorous on the analytical properties of the function to be integrated and can be used even for the block-block system of scatter diagram. The long-term stress distribution is determined by using MCS and the results are fitted on a two-term Weibull distribution for each element in structure.

Due to computer memory restriction, we cannot use the full details of the three legs. In addition, the simulation results showed that the critical hot-spot stress usually occur in the first leg for several sea states thus we shift our focus to detailed models of the first leg and suppose the failure of this leg cause the failure of structure, figure (3). However, the present approach in this research can be used for full detail model of legs.

The fatigue failure usually occurs at welded joint. Hence, for each member in the structure two potential

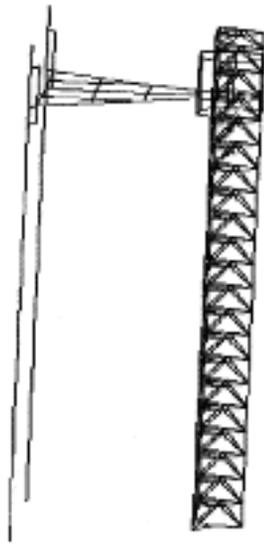


Figure 3. Finite element model of Neka Jack-up platform used for stress calculation.

of failures can be expected at the ends of member joints. Element fails and separate from structure if each failure in the ends of element joints occurs. However, this member retains in structure for wave load calculation. In this investigation, structural collapse is assumed to occur if any two members fail or if a leg member fails.

For the jack-up model under investigation the fatigue characteristic,  $C$ , is modeled as a random variable by lognormal distribution in which the mean value and coefficient of variation of its logarithm are respectively  $-29.84$  and  $0.55$  for joints in air and for joint in seawater  $-31.01$  and  $0.77$ , respectively. These values are selected based on DNV (1984) specification. Other fatigue characteristic i.e.,  $m$ , is equal to  $3.1$  for joints in air and  $3.5$  for joint in sea-water based on this specification and in this research is considered deterministic.

Based on review on available data for initial crack, Bokalrud & Karlsen (1981) showed the exponential distribution with mean value  $0.11$  and coefficient of variation equal  $1.0$  can appropriately be used to specify randomness in the initial crack size,  $a_0$ . However, Moan's (2001) later investigation on crack data derived from under-water inspection of jacket platforms indicated mean value equal  $0.19$  mm would be sufficient.

To represent uncertainty in stress analysis, three random variables  $\delta_F$ ,  $\delta_S$  and  $\delta_{SCF}$  are used to represent uncertainty in hydrodynamic load; stress calculation and stress concentration factor in specific hot spot, respectively. Since there is not any statistical information for these variables in jack-up structure, we used the same values recommended by Dalan (1993) for

hydrodynamic load and stress concentration factor and higher coefficient of variation for stress calculation due to using one leg detail model. Therefore, each of these variables is log-normally distributed with mean value  $1$  and coefficient of variation  $0.1$ ,  $0.15$  and  $0.1$  respectively and independent from each other.

The statistical characteristics of two random variables  $\delta_F$  and  $\delta_{SCF}$  are assumed the same in all sea-states and damage states. However, the stress calculation uncertainty,  $\delta_S$  is dependent from joint to joint and as the structure state changed.

In this research, since the time history of each sea state are available, the correlation coefficient of each pair of joints can be determined by integration of correlation coefficient of these joints in each sea-state with regarding to weighting function presented by equation (8).

## 6 RESULTS

By using the limit state function and random variables explained and presented in the last section, a computer program has been written to determine probability of failure of each element and sequence of failure based on FORM method.

The result of branch and bound technique is illustrated in figure (4). As is clear, the most likely to failure element is 295 with a failure probability  $0.0026175$ . The most likely of collapse sequence is 295 followed by 169 with the occurrence probability  $0.00174543$ . The probability of any section failure in the intact structure is  $0.0107317$ , while the probability of system failure is  $0.00727$  based on the ten important sequences of failure. It is important to note that inclusion of additional sequences did not cause significant increase in the probability of system failure. This result shows that here is a significant system impact on failure probability.

It is important to note that the probability of system failure is quite larger than the individual first element failure. The reason to the difference can be explained by redundancy effect. Usually, the first failure occurs in the bracing elements, see figure (5). Thus, failure of this element cause the load transmitted by frame action and stress increase suddenly in other elements. Probability of failure of second element increases and causes to increase probability of system failure. This fact can be clearly observed from figure (4) for element 169 when the failure probability of this element increases from  $0.00020737$  for the first failure to  $0.00174543$  for subsequent failure.

This result is in contrary to result determined for jacket type platform, Karamchandani et al. (1991) showed the probability of total structure failure for jacket type platform is much smaller than the probability of an individual section failure. The reason to this

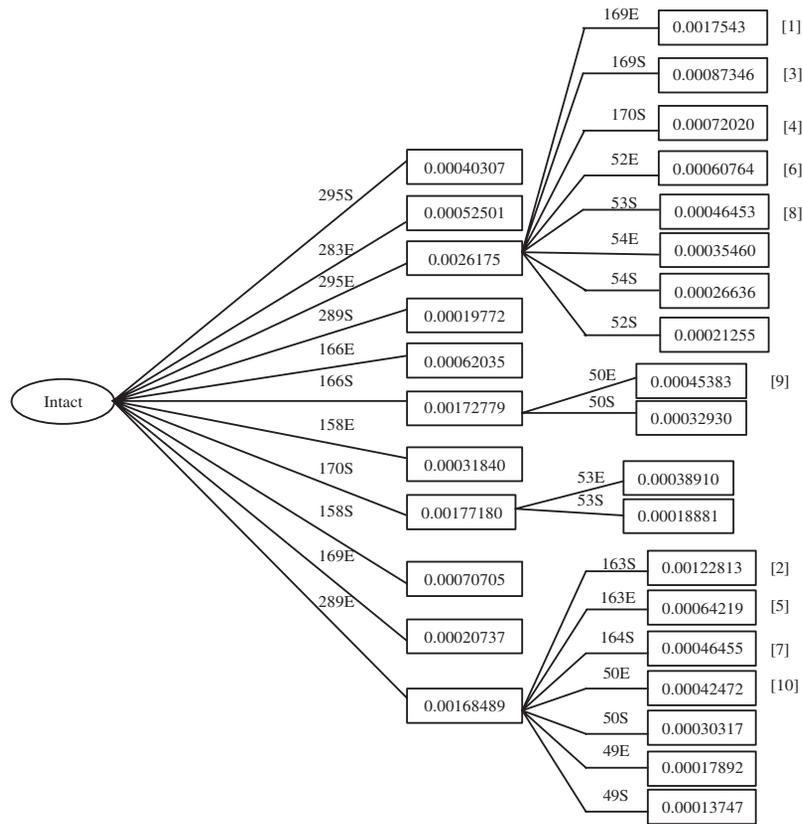


Figure 4. Failure sequence in branch and bound (E stand for End and S for Start of element).

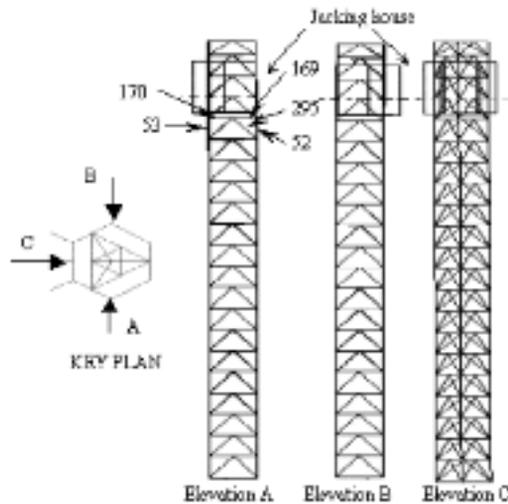


Figure 5. Schematic representation of jack-up structure.

difference between these two platforms, jacket and jack-up, can be explained by this fact that the jacket platform under investigation showed more redundancy than the K bracing jack-up platform here. Therefore, when the first failure occurs in jacket structure, the increasing of stress parameter is not too large and some additional time is required before the next section fail.

### 7 CONCLUSION

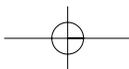
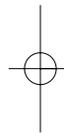
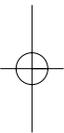
An approach to determine system reliability of jack-up structure is presented in this research. This approach can account change of stress distribution in jack-up structure when the elements fail and allow using detailed probabilistic model. In addition, the important or major advantage of this approach is that it allows using the first order reliability methods, which make better and easier calculation of the probability of failure.

This approach is used to estimate the system reliability of jack-up structure. The result shows there is

significant system effect and probability of structural collapse is much larger than the probability of failure of the first element in contrary to jacket type platforms. This difference is explained by redundancy of structure and revealed this factor is important and should be considered in reliability analysis.

## REFERENCES

- Bokalrud, T. & Karlsen, A. 1981. A probabilistic Fracture Mechanics Evaluation of Fatigue from Weld Defects, *Proceeding of Conference on Fitness for Purpose Validation of Welded Constructions*, No. 8, London, UK.
- Daghighi, M., Hengst, S., Vrouwenvelder, A. & Boonstra H. 1997. System reliability analysis of jack-up structures under extreme environmental conditions., *Proceeding of the Behavior of Offshore Structure*, BOSS97, pp. 127–143.
- Dalan, J.I. 1993. System reliability in design and maintenance of fixed offshore structures, *Ph.D. thesis*, Department of Marine Structures, The Norwegian institute of Technology, Trondheim, Norway, May.
- DNV, 1984. *Fatigue strength analysis for Mobile offshore units*, classification notes, No. 30.2, August.
- Farnes, K.A. 1990. Long term statistics of response in non-linear marine structures, Div. of Marine structure, The Norwegian Inst. of Tech., MTA-Rep, 1990: 74.
- Hanna, S.Y. & Karsan, D.I. 1989. Fatigue modeling for reliability based inspection and repair of welded tubular offshore structure, *Eight Offshore Mechanics and Arctic Engineering Conference*, The Hague, Netherlands, pp. 657–666.
- Jensen, J.J., Mansour, A.E. & Pedersen, T. 1991. Reliability of Jack-up platforms against overturning, *Marine structures*, No. 4, pp. 203–229.
- Karamchandani, A.K. Dalane, J.I. & Bjerager, P. 1991, System reliability of offshore structures including fatigue and extreme wave loading, *Marine structures*, No. 4, pp. 353–379.
- Karunkaran, D.N. 1993. Nonlinear dynamic response and reliability analysis of drag-dominated offshore platforms, *Ph.D. thesis*, Department of Marine Structures, The Norwegian institute of Technology, Trondheim, Norway, November.
- Moan, T., Zhong, W. & Vardal, O.T. 2001. Initial Crack Depth and POD Data based on Underwater Inspection of Fixed Steel Platforms, *Proc. Of the Eighth International Conference on Structural Safety and Reliability*, ICOS-SAR2001, June, Newport Beach, California, USA.
- Moses, F. 1982. System reliability developments in structural engineering, *Structural Safety*, 1 (1), p.p. 3–13.
- Onoufriou, T. 1999. Reliability based inspection planning of offshore structures, *Marine structures*, No. 12, p.p. 521–539.
- Pillai, T.M.M. & Prasad A.M. 2000, Fatigue reliability analysis in time domain for inspection strategy of fixed offshore structures, *Ocean Engineering*, No. 27, p.p. 167–186.
- Raju, I.S. & Newman, J.C. 1986. Stress Intensity Factor for Circumferential Surface Crack in pipes and rods under bending and tension loads, *Fracture Mechanics*, ASTM, Vol.17, pp. 709–805.
- Shabakhty, N. Van Gelder, P. & Boonstra, H. 2002. Reliability analysis of Jack-up platforms based on fatigue degradation, *Proceeding of 21st International Conference on Offshore Mechanics and Arctic Engineering*, OMAE 2002, June, Oslo, Norway.
- Shetty, N. 1992. System reliability of fixed offshore structures under fatigue deterioration, *Ph.D. thesis*, Department of Civil Engineering, Imperial College of Science, Technology and Medicine, London, April.
- Smith, I.J. & Hurworth, S.J. 1984. The effect of geometry changes upon the predicted fatigue strength of welded joints, *Res. Report No. 244*, Welding Inst, Cambridge, England.
- Thoft-Christensen, P. & Murotsu Y. 1986. Application of structural system reliability theory, ISBN 0-387-16362-X, Springer-Verlag, Berlin.
- Waarts, P.H. & Vrouwenvelder, A. 1998. The use of directional sampling in structural reliability, *The Eighth IFIP WG 7.5 Conference on reliability and optimization of structural systems*, Krakow, Poland.



## Correlation in probabilistic safety assessment uncertainty analysis

Z. Šimić, I. Vuković, V. Mikuličić

*University of Zagreb, Faculty of Electrical Engineering and Computing, Zagreb, Croatia*

**ABSTRACT:** Uncertainty analysis is essential part of every complete risk assessment. Increased usage of Probabilistic Safety Assessment (PSA) models for various practical applications in the nuclear industry makes uncertainty analyses even more important. Essential steps related to the PSA model uncertainty determination are: parameters uncertainty identification, uncertainty propagation, and uncertainty analysis. One special issue related to the PSA model uncertainty analysis is about parameter uncertainty correlation. PSA model parameters uncertainty might be correlated because of various different reasons (i.e., same data source, similar component design, same related function, same operating environment, etc.). There are two interesting and important questions related to the parameter uncertainty correlation: (1) how to determine correlation level? and (2) what is the influence of parameter correlation to the PSA model uncertainty? This paper discusses second question: assuming parameter correlation existence and various levels, the potential influence to the PSA results uncertainty is investigated.

### 1 INTRODUCTION

Uncertainty analysis is an important component of probabilistic safety assessment (PSA). It provides quantitative statement as to degree of uncertainty in the PSA results, and it can force careful consideration of the sources of uncertainty and clear thinking of PSA model itself.

Uncertainties can be grouped regarding their nature into two groups: aleatory and epistemic (U.S. NRC RG 1.1.74, 2002). The aleatory uncertainty is addressed that when the events or phenomena being modeled are characterized as occurring in a random manner (usually known as stochastic, type A or irreducible uncertainty). The epistemic uncertainty is that associated with the analyst's assessment confidence in the predictions of the PSA model (usually known as subjective, type B, reducible), thus reflecting how well PSA model represents the real system being modeled. This has been referred to as state-of-knowledge uncertainty. Aleatory uncertainty is a property of a system, whereas epistemic uncertainty is a property of the analysts performing the study and general level of knowledge about an event (Jordan Cizelj, R. et al. 2002). The aleatory uncertainty is built into the PSA model itself, so in this paper it is the epistemic uncertainty that is discussed.

On the other hand, there are three classes of uncertainty that impact the results of PSAs: parameter uncertainty, model uncertainty and completeness

uncertainty. Parameter uncertainties are those associated with the values of the basic parameters of the PSA model (e.g., component failure rate). Those parameters are defined by establishing their probability distributions, thus expressing the analyst's degree of belief in the values these parameters could take, based on his state of knowledge. For the PSA purposes the corresponding PSA tool must have adequate built-in capabilities to propagate the distributions representing parameter uncertainty in order to generate a probability distribution of the results (e.g., core damage frequency, fault tree top event probability). Model uncertainty reflects the fact that state of knowledge induces different opinions on how the model should be formulated. Completeness, which is not itself uncertainty, reflects an unanalyzed contribution and is very difficult to estimate its magnitude (U.S. NRC RG 1.1.74, 2002). Analysis carried out for this paper included only the analysis of the parameter uncertainty.

Random variables that exhibit aleatory uncertainties are considered to be independent and consequently without correlation. On the other hand, two variables with epistemic uncertainty that are derived from the same source are considered to be correlated.

This paper describes the procedure to determine the influence of correlation level between the uncertain input variables (parameters assigned to fault tree's basic event such as component failure rate, probability of failure per demand, unavailability due to test and

maintenance) on the uncertainty of the fault tree top event probability. Since correlation level is a-priori not known, the analysis has been done by changing its value. The procedure is applied to minimal cut-sets for a fault tree model from a plant-specific PSA. The propagation of uncertainties is performed using Monte Carlo simulation methodology.

## 2 GENERAL ABOUT CORRELATION

The experience has shown that input variables to Monte Carlo simulation are often not independent of one another. If two identical components are located side by side in a building there is a high response dependency and the responses of these components are correlated. This is called the correlation of response. Similarly, it is thought that capacities of two identical components are correlated what is called the correlation of capacity.

Physically, dependencies exist due to similarities in both response and capacity parameters. The structural capacities of two identical pumps, located side by side in a building, are highly correlated. Then, if one pump fails due to an earthquake, it is likely that the other pump will also fail (Reed, J.W. et al. 1985).

When the degree of correlation increases the probability of simultaneous failure of multiple components (intersection of component failures) increases and the occurrence probability of union of component failure decreases (Wantanabe, Y. et al. 2003).

A nuclear power plant (NPP) consists of redundant systems, with large number of components, and the failures of the systems and core damage represented by union of many intersections of component failures. Therefore, correlation might significantly influence failure probabilities of system and core damage frequency.

In PSA model of NPP uncertainty is mostly epistemic so the variables might be quite strongly correlated. The analysis must be done to correlate the sample values for different PSA elements from a group to which the same parameter value applies (the so-called state-of-knowledge dependency) (Apostolakis, G. & Kalan, S. 1981).

### 2.1 Definition of correlation

Mathematically, the strength (level) of correlation between two random variables  $X_i$  and  $X_j$  is expressed by correlation coefficient,  $\rho$ , defined by the following equation:

$$\rho = \frac{Cov(X_i, X_j)}{\sqrt{Var(X_i)Var(X_j)}} \quad (1)$$

where  $Cov(X_i, X_j)$  is covariance coefficient between  $X_i$  and  $X_j$ ,  $Var(X_i)$  is variance of  $X_i$  defined by the following equation:

$$Var(X_i) = E((X_i)^2) - (E(X_i))^2 \quad (2)$$

$$Cov(X_i, X_j) = E(X_i X_j) - E(X_i)E(X_j) \quad (3)$$

where  $E(X_i)$  and  $E(X_i, X_j)$  are defined by the following equation using probability density function  $f(X_i)$  and  $f(X_i, X_j)$ :

$$E(X_i) = \int_{-\infty}^{\infty} X_i f(X_i) dX_i \quad (4)$$

$$E(X_i X_j) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} X_i X_j f(X_i, X_j) dX_i dX_j \quad (5)$$

The value of  $\rho$  lies between  $-1$  (perfect negative correlation) and  $1$  (perfect positive correlation).

## 3 CASE STUDY

In order to demonstrate the influence of input parameter uncertainty correlation on the uncertainty of output variable of interest, fault tree top event was selected. PSA analysis tool, *Risk Spectrum Professional* (RS), was used to generate the minimal cut-sets (MCS) for selected fault tree top event. This tool can make uncertainty analysis (calculate a probability distribution for a top event result) only for two boundary cases (Berg, U. & Sardh, L. 1994):

- parameters are not correlated ( $\rho = 0$ ), and
- parameters are perfectly correlated ( $\rho = 1$ ).

First one is so-called Event Sampling simulation type, which means RS samples parameter values according to the uncertainty distribution assigned generating a new parameter for each basic event with a reference to the parameter. This is done for each sampling in Monte Carlo Simulation.

The second one is so-called Parameter Sampling, which means RS samples the parameter value according to the uncertainty distribution assigned and use this value for all basic events with a reference to the parameter (Olsson, A. 2000). This is also done for each sampling in the Monte Carlo simulation.

One important effect of simulating at the parameter level is that parameter dependencies (coupled failure data, state-of-knowledge dependence) are correctly taken into account.

Having this on mind, it is necessary to employ another tool for uncertainty analysis of correlated

uncertain parameters using some values from correlation coefficient range [0,1]. This was done using *Crystal Ball* software which has an executive interface with MS Excel.

Thus, for this paper's purpose, RS provides a list of minimal cut-sets and fault tree top event unavailability as a sum of minimal cut-sets each of which presented as a product of basic events.

### 3.1 Fault tree model and propagation of uncertain correlated parameters

In order to obtain a minimal cut-set list for further analysis, an existing fault tree model from a plant-specific PSA was selected as a case study. The fault tree was chosen after its initial minimal cut-set analysis showed that there were no minimal cut-sets which contribution was over dominant. Point-estimated top event probability was  $1.24E-4$ . Only first 100 minimal cut-sets out all 4460 minimal cut-sets (cut-off value was set to  $1E-12$ ) were selected for further analysis since the contribution of each other minimal cut-set was less than 0.1% of calculated value.

In *Crystal Ball*, probability distributions (referred to as "assumptions") are normally calculated independently of each other. *Crystal Ball* generates random numbers for each assumption without regard to how random numbers are generated for other assumptions.

However, because dependencies often do exist between variables in a system being modeled, *Crystal Ball* has a Correlated Assumptions feature that allows to build these dependencies into the model. When the values of two variables depend on each other in any way, they should be correlated to increase the accuracy of simulation's forecast results. When simulation with correlation is run, *Crystal Ball* does not alter the way that the random values are generated for each assumption. It merely rearranges the values to produce the desired correlation. In this way, the original distributions of the assumptions are preserved.

For the purpose of this paper, we have considered only the positive correlation. Anything in the range  $[-0.15, 0.15]$  could be noise and is unlikely to impact the results. It is rare to have correlation coefficients above 0.8 or below  $-0.8$  (Murtha, J. 2000). Having this in mind, the Monte Carlo simulation was run with a several values of correlation coefficient (0.25, 0.5,

and 0.75) beside two boundary cases (independent parameters  $-\rho = 0$  and perfectly correlated parameters  $-\rho = 1$ ). Correlations were established within specific failure modes (e.g. failure to start on demand, failure to operate, etc.) of components of the same generic types (e.g. air operated valves, motor-driven pumps, compressors, etc.).

### 3.2 Results

List of minimal cut-set were obtained for an existing fault tree model from a plant-specific PSA, selected as a case study, by employing RS.

Propagation of uncertainties in the fault tree was performed with Monte Carlo simulation using *Crystal Ball* software with ability to change arbitrary correlation level between uncertain input variable.

Number of trials was increasing as the correlation level increased equally in steps of 0.25 within range [0, 1] in order to achieve same results confidence level.

The results of analysis performed using different correlation levels are shown in Table 1.

Figure 1 presents visualization of most important results describing the uncertainty of the output value.

Another fault tree model (Example B) with higher result probability was analyzed in order to verify correlation influence to the result. Table 2 presents results for Example B. It is visible that correlation

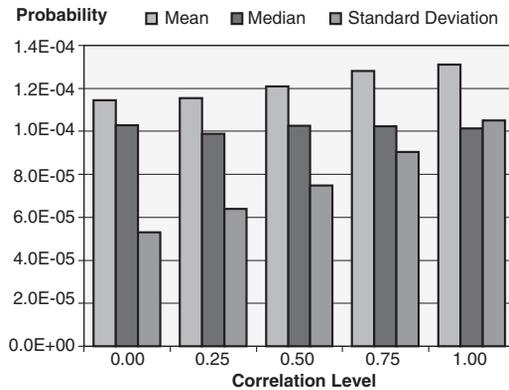


Figure 1. Correlation level and output variable uncertainty – Example A.

Table 1. Numerical results of the fault tree top event uncertainty analysis for five correlation levels – Example A.

Correlation statistics	0	0.25	0.50	0.75	1
Trials	2100	2950	3700	4850	6250
Mean	1.15E-04	1.15E-04	1.21E-04	1.28E-04	1.31E-04
Median	1.03E-04	9.89E-05	1.03E-04	1.02E-04	1.01E-04
St. deviation	5.31E-05	6.40E-05	7.49E-05	9.05E-05	1.05E-04
Coeff. of variability	0.46	0.55	0.62	0.71	0.80

Table 2. Numerical results of the fault tree top event uncertainty analysis for five correlation levels – Example B.

Correlation statistics	0	0.25	0.50	0.75	1
Trials	2100	2950	3700	4850	6250
Mean	5.32E-03	5.40E-03	5.52E-03	5.74E-03	5.92E-03
Median	4.72E-03	4.61E-03	4.62E-03	4.70E-03	4.64E-03
St. deviation	2.87E-03	3.05E-03	3.38E-03	4.05E-03	4.52E-03
Coeff. of variability	0.54	0.57	0.61	0.70	0.76

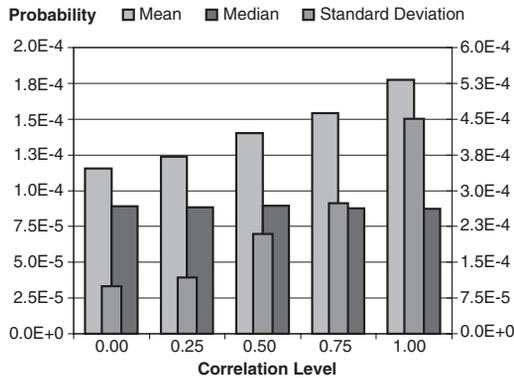


Figure 2. Correlation level and output variable uncertainty with higher level of input variable uncertainty – Example A.

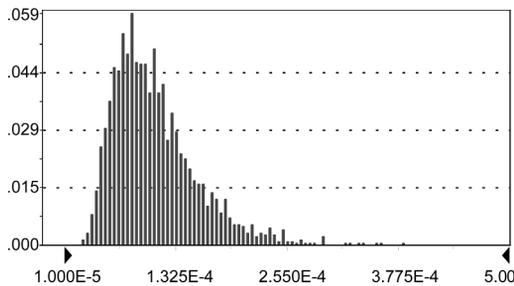


Figure 3. Probability density function of output variable uncertainty with no correlation – Example A.

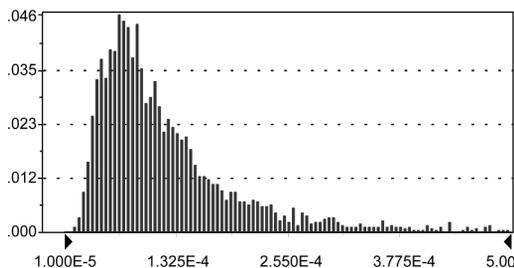


Figure 4. Probability density function of output variable uncertainty with perfect correlation – Example A.

influence to the result uncertainty is similar but little bit less significant as result probability increases.

Additional analysis has been done in order to see how increased uncertainty (error factor for log-normal distribution) of input parameters impact the uncertainty of output given the assumed correlation between parameter exists. Just for illustration, the results showed that correlation influence is then even more emphasized (Figure 2).

Finally as illustration probability density function is presented for two extreme correlation cases: without correlation (Figure 3) and with perfect correlation (Figure 4).

#### 4 CONCLUSION

Positive correlation between uncertain input parameters increased the mean value of the result. This is the consequence of a product model since the mean value of the output is not affected by correlation among the summands. PSA models are neither pure products nor pure sums, but rather complex algebraic combinations of the various inputs.

The influence of correlation on standard deviation of an output and coefficient of variability is more obvious and significantly has increased by increasing the correlation level. The median of the output is very weakly affected by correlation and remains almost the same with change of correlation level.

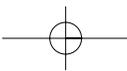
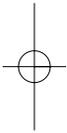
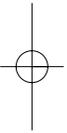
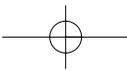
Input parameters correlation has increased effects on result uncertainty with higher degree of input parameter uncertainty and lower total result.

It seems important for the more precise result uncertainty and mean result value determination to investigate existence and level of correlation between input parameters. PSA model parameters uncertainty might be correlated because of various different reasons (i.e., same data source, similar component design, same related function, same operating environment, etc.).

#### REFERENCES

Apostolakis, G. & Kaplan, S. 1981. Pitfalls in risk calculation. Reliability Engineering, Vol. 2, pages 134–145.

- Berg, U. & Sårdh, L. 1994. Risk Spectrum Theory Manual. Relcon Teknik AB.
- Boissonnade, A. 1999. Modeling correlation in the treatment of uncertainty for catastrophic loss assessment, Risk Management Solutions Inc.
- Borgonovo, E. et al. 2003. Comparison of global sensitivity analysis techniques and importance measures in PSA. Reliability Engineering & System Safety, Issue 79, pages 175–185.
- Decisioneering, Inc. 2002. How to correlate dependent assumptions?, Web-site: [www.decisioneering.com](http://www.decisioneering.com)
- Jordan Cizelj, R. et al. 2002. Uncertainty analysis of fault tree parameters, *Proceedings of ANS International Topical Meeting on PSA., Detroit, MI, USA, 6–9 October 2002*, pages 450–455.
- Murtha, J. 2000. When does correlation matter? Risk Analysis for the Oil Industry. Pages 20–23.
- Olsson, A. 2000. The Probability of a parameter, RELCON AB, Risk Spectrum Magazine, Issue 2, Stockholm, Sweden, pages 8–9.
- Reed, J.W. et al. 1985. Analytical techniques for performing probabilistic seismic risk assessment of nuclear power plants. Proceedings of 4th International Conference on Structural Safety and Reliability.
- U.S. Nuclear Regulatory Commission 2002. Regulatory Guide 1.174 Revision 1. An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis. Washington, DC, USA.
- Wantanabe, Y. et al. 2003. Development of the DQMF method to consider the effect of correlation of component failures in seismic PSA of nuclear power plant. Reliability Engineering & System Safety, Issue 79 pages, 265–279.



## Experience with the use of risk assessment in IMO

Rolf Skjong

*Det Norske Veritas, Høvik, Norway*

**ABSTRACT:** In the maritime industry the International Maritime Organisation (IMO) is the UN organisation responsible for developing international safety and environmental protection regulations. IMO has recently developed the second version of “Guidelines for FSA for use in the IMO rule making process” available as circulars both from the Marine Safety Committee (MSC) and the Marine Environmental Protection Committee (MEPC). This standard is, as far as the author knows, the first risk assessment standard adopted in an UN organisation. As there have been some attempts to develop internationally accepted risk assessment and risk management standards, the paper try to describe some of the experience and lessons learned from implementing FSA in IMO.

The work with developing the guidelines is briefly reviewed. Some concepts used in the first version of the guidelines, e.g. the regulatory impact diagram resulted in a lot of controversies, and have subsequently been removed. Similarly the questions of risk acceptance and transparency have been subject to considerable debate and controversy.

Paralleling the development of the guidelines there have been a number of applications of the guidelines, recently focusing on bulk carrier safety. Relevant studies have been carried out by UK, by Japan, by Norway and International Confederation of Free Trade Unions (ICFTU), and by International Association of Classification Societies (IACS). These studies will be briefly reviewed with respect to methods used, assumptions made and conclusions drawn. The entire process from the initial terms of reference was formulated by IMO to the final decisions is briefly reviewed. The final decision making took place at the MSC meeting early in December 2002.

The main conclusion is that the maritime industry has made a lot of progress, quite fast in the use of risk assessment for use in the decision making process. This being the case, despite the many communication problems that arises in discussing risk issues in international forums. Furthermore, the FSA has helped balancing the often-conflicting interest of the flag states and non-governmental organisations present in IMO.

### 1 INTRODUCTION

#### 1.1 *General*

The application of risk analysis techniques is generally well established in most industries, both as a means for the owner/operator to manage their own risks and for the regulator to prioritize work on the development of rules and regulations.

Most risk analysis techniques have their origin in the nuclear industry, for which risk analysis became an important tool in the 1960s, and has now developed into living Probabilistic Safety Assessment (living-PSA). The living-PSA will be regularly updated, e.g. after upgrades, inspections, maintenance.

In the offshore industry the use of risk analysis has been required since 1981 in Norway and in the UK since 1992 as a consequence of the Piper Alpha disaster. The risk analysis is carried out on behalf of the

owner of the plant, and is to be documented. The document is called a Safety Case in the UK, which will be approved by the UK Health and Safety Executive. In Norway the authorities do not approve such documentation or any safety goals, but are allowed insight into the safety related decision making process of the individual enterprises, and can act on situation which are not considered acceptable.

On a generic policy level, most OECD countries require risk analysis as basis for regulation, e.g.: according to the US President Executive Order # 12866 on “Regulatory Planning and Review” for example the US Coast Guard has to base the rules and regulation on risk analysis and cost benefit evaluation. From OECD many nations have also received a tool called Regulatory Impact Assessment (RIA), and are implementing this in many areas of regulatory policies. RIA also refers to risk and costeffectiveness assessment.

Finally, it should be noted that both International Organization for Standardization (ISO) and CEN have most of their structural standards based on risk assessment.

### 1.2 *Shipping*

In the shipping industry, most of the statutory regulations in the past have been developed as a reaction to major accidents and disasters. However, in 1992, the "UK House of Lords Select Committee on Science and Technology" recommended a Safety Case Regime for shipping, similar to that already adopted in the oil and gas industries. It also recommended a move towards performance standards in place of prescriptive rules, and a concentration on the management of safety.

In 1993, during the 62nd session of the IMO MSC, the UK proposed a standard five step risk based approach, which was termed Formal Safety Assessment (FSA). In 1996 the IMO established a working group on FSA, and by 1997 a Circular on "Interim Guidelines on the Application of FSA to the IMO Rule-making Process" (IMO, 1997) had been developed, which was adopted by the MSC and MEPC the same year. Subsequently, a number of FSA trial applications and FSA studies were carried out and presented to IMO. In 2001, during the 74th session of the IMO MSC, the FSA Interim Guidelines were revised into "Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule- Making Process" (IMO, 2001).

### 1.3 *Purpose of FSA*

FSA has been developed as a tool for supporting the decision making process at IMO. It should make decision making procedures more rational and provide a proactive and holistic approach, thus reducing the number of ad-hoc proposals and implementations, and giving less room for politics in the decision making process.

FSA should also encompass both technical and operational aspects, taking into account the influence of human factors on accidents in shipping.

FSA should provide reliable information on hazards, risks, risk control options, their costs and benefits, in a rational, structured and auditable manner, in order to improve the decisions regarding the management of the risks identified.

### 1.4 *What is FSA?*

FSA is a risk based approach consisting of five inter-related steps:

1. Identification of hazards
2. Assessment of the risks arising from the hazards identified

3. Identification of options to control the risks
4. Cost/benefit assessment of the risk control options
5. Recommendations for decision making, based upon the information derived in the previous steps.

The safety of an issue under consideration is assessed by evaluating the risk associated with this issue, e.g. a specific system or operation. The decision upon the acceptability of that risk is done by referring to risk acceptance criteria. So far IMO has been reluctant to formulating explicit criteria. However, during the work with the bulk carrier safety references were made to criteria submitted by Norway (2000). The Norway paper argued that bulk carrier risk were in the ALARP region, and suggested cost effectiveness criteria of \$3 m per fatality averted to be used for decision making.

Compared to the current safety assessment approach there are several differences to be observed. Today, decision on regulatory changes at IMO is normally initiated as a reaction to an accident. The decision on safety requirements results from activities after the problem occurred, focusing on the question: What went wrong? The FSA approach is pro-active, by trying to find out before an accident occurs: What might go wrong?

In today's safety assessment approach the risk is normally not explicitly evaluated. The FSA approach tries to find out about the likelihood of scenarios, which may possibly develop from the hazards, and about the magnitude of their consequences in order to calculate the risk.

As today's safety assessment process is rather reactive to an accident rather than pro-active, decisions on how to improve matters are often carried out on an ad-hoc basis, influenced by public pressure or aspects like reputation. Quick fixes are therefore preferred and an assessment of the costs and the benefits of such solutions are normally not performed. The FSA approach, on the other hand, systematically analyses the different options which are available to control the risk, and also assesses both the costs and the benefits of those options should they be implemented. The final decision on safety requirements can therefore be made on the basis of an analysis.

The current reactive approach has led to a continuous amendment of already complex and sometimes inconsistent regulations. These regulations are often characterised as being prescriptive, leaving only limited room for other equivalent solutions to a safety problem than those prescribed. Especially in periods of rapid technology developments the pace of regulatory developments is too slow to cope with industrial needs and the principle of technical equivalence an obstruction to innovation. Specific safety objectives and functional requirements would be more useful, requiring safety goals/performances to be met both for technical and operational aspects.

## 2 THE FIRST FSAs

The first FSA studies were termed trial applications. There are a number of such studies, and it would be far beyond the scope of this paper to discuss all these submissions. They generally did not contain any recommendations for decision making, and therefore were not subject to much scrutiny at IMO. Their purpose was mainly to illustrate and educate.

There were some exceptions to this: The UK FSA on High Speed Crafts and the Norway/International Council of Cruise Lines (ICCL) study on helicopter landing areas. In addition IACS carried out a HAZID to communicate the safety problems generated by requiring ballast water exchange at sea, a requirement resulting from environmental considerations (IACS, 1998), thereby demonstrating that complete FSA studies are not always required.

The UK FSA on high speed craft was a large project, and a number of reports were submitted to IMO. A large number of questions were raised relating to the results of the analysis, some of which clearly indicating that many delegates were of the opinion that results were wrong and contradicted factual information. It was decided to review the reports, and a correspondence group was established, chaired by Italy. The terms of reference may be found in IMO (1998). The correspondence group concluded by stating "The Group appreciated both studies by the United Kingdom (for which the majority of comments were made) and Sweden, which were found to provide a great deal of insight into high-speed craft safety issues, although concerns were raised about the degree to which they should be used for decision making. Given the complexities of the FSA and the system under consideration, the analysis needs to be extremely open and clear in order for the utility of the study for decision making to be assessed" (Italy, 1999). The correspondence group analysed the situation and pointed to the use of regulatory impact diagrams, instead of fault and event trees as causing the problem, and stated "It may generate confusion and subjectivity rather than offer a valuable contribution to the FSA." The story ended with the new FSA Guidelines, where the regulatory impact diagrams have been removed (IMO, 2001).

The first FSA that was used for decision making was the Norway/ICCL FSA on helicopter landing areas for non-ro/ro passenger ships (Skjong et al. (1997)). Helicopter landing areas had been proposed as a safety measure for ro/ro passenger ships by the Panel of Experts in the aftermath of the Estonia tragedy in 1994 (Estonia, 1997). Some of the proposals by the Panel of Experts had been made mandatory for all passenger ships by IMO. The industry representatives (like ICCL), questioned the justification for the regulation, and Norway decided to carry out an analysis. The

FSA developed two different risk models. One model was rather reliant on review of historic accidents, and estimation of the benefits of helicopter landing areas for those accidents. The other model was more theoretical, and estimated helicopter response time, time to come to the scene of the accident, time to find and pick up personnel, etc. This was compared to the time available for successful search and rescue operations. Both models gave the same and very clear conclusion: The regulation was not justified based on cost and benefits of requiring helicopter landing areas for cruise ships. The cost of averting a fatality was estimated under optimistic assumptions relating to the effectiveness of helicopter landing areas to be larger than \$70 m. This was observed to be much higher than criteria used for safety interventions in any OECD country. Also this FSA was subject to detailed review. The terms of reference for the review can be found in IMO (1998). The review was first carried out in a correspondence group, reported in UK (1999) and concluded that "the methodology broadly followed the guidelines", "the scenarios selected for analysis are appropriate", and "the evaluation of risk are broadly valid". Still, the joint working group on FSA and the Human Element used the full MSC 70 meeting to review the FSA in further detail. The conclusion of the working group may be found in IMO (1999) stating "The Committee noted that the cost-effectiveness of a helicopter landing area, in terms of the cost of implementation divided by the expected number of additional lives saved (the implied cost of averting a fatality) is \$37 m and that, acknowledging the uncertainties in the evaluation of both risk benefit and cost, the group agreed that the Implied Cost of Averting a Fatality (ICAF) may range from about \$12 m to \$73,000 m." The working group noted that all assumptions made were optimistic on behalf of requiring helicopter landing areas. The conclusions were therefore robust, and the requirement was repeated.

## 3 FSA FOR BULK CARRIERS

### 3.1 *Initial studies*

The first FSA study on bulk carriers was carried out by DNV in 1997, and a paper was distributed to both the working group on Bulk Carrier Safety and the working group on FSA during the MSC meeting (DNV, 1997). The study represented the DNV's justification for supporting the IACS decision to strengthen the bulkhead between No.1 and No.2 cargo holds on existing bulk carriers. The justification was based on costs of averting a fatality between \$0.5 m and \$1.5 m for the various types of bulk carriers analyzed. This decision is therefore consistent with later decisions at IMO. The analysis was based on extensive

analysis of casualty data and rather simple risk modeling. The analysis was very easy to understand. The paper was widely distributed, and contributed to the understanding of FSA in the industry.

### 3.2 Bulk carrier FSA studies at IMO

An FSA on bulk carrier safety was proposed by UK (1998). The proposal was generally supported, although many delegates expressed concerns that the scope of the study was too broad. In the aftermath it may be observed that this concern was justified. Most of the risk control options adopted during MSC 76 in December 2002 related to fore-end watertight integrity – an issue put on the agenda prior to MSC 70 for urgent review. On this issue IACS submitted a HAZID report to MSC 71 (IACS, 1999) and a full FSA to MSC 74 (IACS, 2001). This study was carried out independently by IACS and reported to IMO. The study took about a year. The study uses standard risk assessment techniques involving fault and event trees and extensive analysis of accident data. However, to be able to quantify some of the risk reduction effects (e.g. strengthening of hatch covers), structural reliability methods (see Skjong et al. 1996) was developed based on detailed probabilistic modelling of strength, structural response and the marine environment.

Norway initiated the study on life saving appliances by preparing a document on risk acceptance criteria, as this was viewed as a preparatory step to an FSA. This document was submitted to MSC 72 (Norway, 2000). Individual and Societal risk for bulk carriers and other ship types are given in Figure 1 and Figure 2 are taken from this document.

The complete study was reported to MSC 74 (Norway & ICFTU, 2001). This study took less than a year, and is very detailed in the risk modelling as compared to other FSA submissions. The level of detail reflected the need to quantify risk control measures that affected probabilities at a detailed level. The study had to use human reliability data from other industries, as similar data did not exist for the maritime industry. The study was carried out independently.

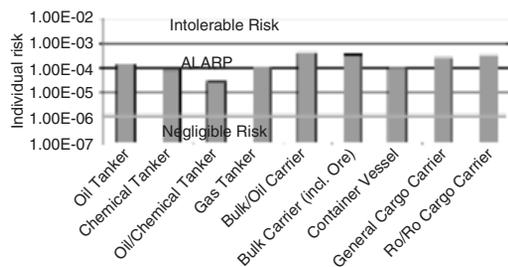


Figure 1. Individual (annual) risk per ship-type.

Also Japan was able to deliver their FSA after a one year project (Japan, 2001), but decided to update the study to MSC 75 (Japan, 2002a). The Japan study, much like the IACS study, is based on comprehensive assessment of accident statistics and rather limited risk modelling. Still, the study is sufficiently detailed for the decision making and relatively easy to follow. Also this study was carried out independently.

The international study was coordinated by UK based on terms of reference agreed during MSC 71 (IMO, 1999). Up to MSC 76 only progress reports were received by IMO. An implication was that during MSC 75 in May 2002 the committee short-listed the recommendations from all studies including the UK recommendation, but without any reported FSA study from UK. The main study was subsequently reported to MSC 76 (UK, 2002a). UK also submitted a large number of other papers on bulk carrier safety that was independent of the main FSA report, including a complete FSA carried out at Strathclyde (UK, 2002b) on the IACS unified requirement for hatch cover strength.

### 3.3 Decision making

The final decision making based on the FSA studies on bulk carrier safety was scheduled for MSC 76 (December 2002). As previously stated, the risk control options had already been short-listed at MSC 75, and the working group tried to structure the order in which decision were made. The reason is that decisions to implement one risk control option would affect the cost effectiveness of other risk control

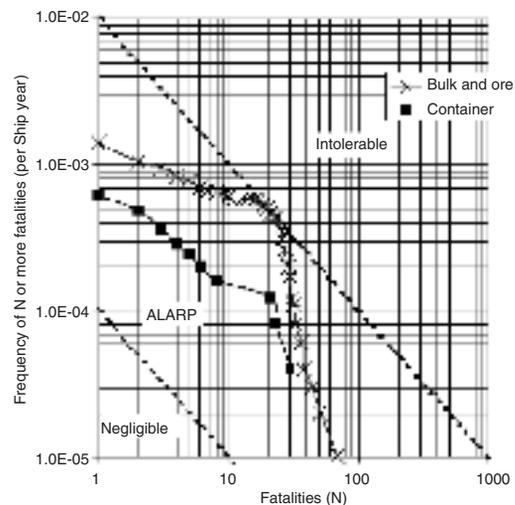


Figure 2. Societal risk of bulk carrier and container vessel accidents.

options as there would be “fewer to save”. Both Japan (2002a) and INTERCARGO (2002) submitted papers discussing this final decision making process, and it may be expected that the FSA working group will reconvene at a later MSC meeting to discuss and resolve these issues, as many delegates found the process difficult to grasp.

For a risk analyst it may be difficult to understand the problem as such recalculations are rather trivial, and the whole idea of waiting to make all decision relating to bulk carrier safety at the same time was that such dependencies between risk control options were unavoidable.

### 3.4 The risk control options and the decisions

The first and most important risk control option related to the side shell failures. These failures had been demonstrated by all studies to be a major contributor to bulk carrier casualties. The most comprehensive risk control option considered was to require *double side skin*. The quantification of costs and benefits were carried out by IACS (2001). The key data, from IACS, are given in Table 1. The decision parameters are now defined in the FSA guidelines as Gross and Net Cost of Averting a Fatality.

$$GCAF = \Delta Cost / \Delta PLL \quad (1)$$

$$NCAF = (\Delta Cost - \Delta Benefit) / \Delta PLL \quad (2)$$

PLL is the Potential Loss of Life,  $\Delta Cost$  is the additional cost of the risk control option, and  $\Delta Benefit$  is the economic benefits resulting from implementing the risk control option.

This rather clear recommendation, given an acceptance criterion of \$3m was later confirmed by UK (2002a). This study claimed many commercial benefits of double side skin in addition to the safety benefits. This made the NCAF value negative. Although the IACS study was conclusive, IACS did wait for MSC 76 to take the decision, and promised to develop the necessary unified requirements for double side skin bulk carriers (IMO, 2002).

IACS (2002) and UK (2002a) both had included *coating* in their assessment, and both studies produced

negative NCAFs. IACS summarized the situation in the working group by stating that the analysis confirmed that it is always in the owner's best interest to coat and to maintain coating. However, as explained by INTERCARGO, coating of cargo holds can not be easily be regulated, as appropriate coating depend on the cargo. However, the MSC noted that SOLAS regulation II-1/3-2 made the coating of dedicated ballast tanks mandatory for oil tankers and bulk carriers but extending that requirement to cargo holds could introduce serious problems, bearing in mind that cargos can react distinctly to different coatings. Therefore, MSC agreed that new ships, which would be of double side skin construction, should be required to have their dedicated seawater ballast tanks and void spaces within double hull spaces coated according to current SOLAS requirements for ballast spaces. Class and the ship-owner would address the coating of cargo holds. The MSC instructed the Design and Equipment (DE) Sub-Committee to develop international performance standards for coatings. With respect to existing ships, the Committee acknowledged that at present there was sufficient control over the condition of coatings through the enhanced survey programme and agreed that this risk control option should also be addressed by class and the ship-owner.

*Control standards of steel repair carried out at terminals*, was proposed by UK (2002a), and presented with negative NCAFs, but very small risk reducing effects, actually indication that this was mainly of commercial interest. The discussion disclosed that the problem could be associated with repair carried out without notifying the class society. The discussion was inspired by a detailed casualty investigation presented by Marshall Island (2002), where this problem was clearly identified. MSC agreed to request the DE Sub-Committee to prepare a draft MSC circular to remind ship owners and operators of their obligations and responsibilities under SOLAS regulation II-1/3-1, concerning the provision that ships shall be maintained in accordance with the structural requirements of recognized classification societies, and other related management obligations under the ISM Code. It is clear from the discussion that the FSA was not used as a significant contributor to this decision.

IACS did propose *Forecastle* and presented this as marginally cost effective for new building; see table 11 of IACS (2001) and Table 2.

MSC noted the information provided by IACS on the on-going development of Unified Requirement S28, requiring the fitting of a forecastle on bulk carriers contracted for construction on or after 1 January 2004 with the purpose of protecting foredeck fittings against green sea loads and minimizing the impact of such loads on fore hatch covers. The Committee also noted that, while the fitting of a forecastle as such was not an IMO requirement, draft Load Lines Protocol

Table 1. Double side skin for new bulk carriers.

	Cost \$	Risk reduction	NCAF \$m	GCAF \$m
Double side skin, new bulk carriers	131,000–182,000	41%	0.8–1.1	0.1–0.4

Table 2. Forecastle for new bulk carriers.

	Cost \$	Risk reduction	NCAF \$m	GCAF \$m
Capesize	54,000– 102,000	0.0211	2.2–4.5	2.6–4.8
Panamax	29,100– 54,000	0.0493	0.2–0.7	0.6–1.1
Handymax	15,600– 51,000	0.0933	–4.9–2.0	0.2–0.3

regulation 39 – “Minimum bow height and reserve buoyancy” would require additional reserve buoyancy forward consistent with the provision of some sheer and/or a forecastle. It seems as the FSA and the use of the same decision criteria by IMO and IACS lead IACS to the conclusion.

The MSC recognized that *replacing hatch covers* in existing ships would not be cost-effective, but agreed that more attention should be paid to hatch cover securing mechanisms and the issue of horizontal loads only, especially with regard to maintenance and frequency of inspection. The Committee agreed that ship owners and operators should be made aware of the need to implement regular maintenance and inspection procedures for closing mechanisms in existing bulk carriers in order to ensure proper operation and efficiency at all times, and instructed the DE Sub-Committee to develop standards for hatch cover securing arrangements for existing ships. The decision of not strengthening hatch covers on existing ships is not well documented. It may be noted that IACS (2001), in Table 12, lists this risk control option as cost effective. UK (2002b) also lists this as cost-effective. The reason for not implementing this risk control option may be found in Japan (2002c), table 1. This table shows that UK classified too many accidents as hatch cover related. A scrutiny of the data, which was made possible by the exchange of information between UK and Japan, resulted in an agreement to reduce the frequency of hatch cover failures in the models. This resulted in the conclusion that this risk control option was no longer cost effective.

Hold, ballast and dry space *water level detectors* was already scheduled for implementation in the new SOLAS regulation XII/12, both for new and existing bulk carriers. Both Norway/ICFTU (2000) and IACS (2000) demonstrated this risk control option to be cost effective. After the decision was made also UK (2002a) confirmed this. Close comparisons of the FSA studies shows that all risk models are different – still giving the same result. Earlier, at IMO, many delegates have stated skepticism on FSA by referring to some undocumented experience that an FSA can produce “any answer”. Hopefully the case of the water level detectors can prevent such skepticism to flourish.

Table 3. Ban Forecastle for new bulk carriers.

	Cost \$	Risk reduction	NCAF \$m	GCAF \$m
Panamax-new	54,000	0.0216	2.5	1.4
Panamax-existing	50,000	0.0120	4.2	2.8

UK (2002a) proposed to *ban alternate hold loading* for bulk carriers carrying heavy bulk cargo and presented Table 3. It should be clear from the information, if taken as unquestionable facts that this recommendation would be outside the criteria, when considering the other risk control options already implemented.

MSC decided to have DE look closer into this issue.

## 4 DISCUSSION

### 4.1 FSA work

Generally IACS, Japan and Norway/ICFTU demonstrated that rather extensive FSA studies may be carried out in about a year’s time. If well coordinated a comprehensive FSA study of a ship type may take two to three years. The reason is that many ship types are more complicated to analyse, more modelling work and search into reliability and incident data may therefore be required. Bulk carriers are particularly simple designs and there have been (too) many accidents that make up the experience base. Still FSA studies may be carried out within the time span that is normally available at IMO for such tasks – it is quite common that a dedicated work group need two to three years to complete the tasks.

### 4.2 FSA methods

Most FSA studies presented at IMO have used standard risk models using fault trees and event trees. Fault trees have not been large or detailed. When detailed fault trees have been prepared, e.g. by France (2002) as part of the UK/International project, the analysts have sometimes given up on populating the fault trees with relevant data. This happened with the UK/Int. study, which ended up without using fault trees except for splitting up the initiating events into causes. The result of this was that the UK/Int. study had no models for quantifying risk reduction based on risk models, but resorted to expert judgement of risk reducing effects for each event tree scenario.

Both IACS (2001) and Japan (2002) used rather detailed structural reliability models to be able to quantify risk reducing effects, and Norway/ICFTU (2001) used detailed fault and event trees populated by data from many sources.

From a method perspective it may be stated that the FSA studies have presented something good at something new. The problem is that what is new is not good (e.g. the regulatory impact diagrams), and what is good is not new. The maritime industry is just learning to use the standard methods.

#### 4.3 *Remaining controversies*

There are some issues that are still unresolved and subject to debate. For example there seems to be two different views on the use of NCAFs and GCAFs. When risk reduction is small and economic benefits are large, this may result in large negative NCAF. Some seem to conclude that such risk control options should be implemented in mandatory instruments, whilst others are of the opinion that there is no need to regulate, as it is reasonable to assume that the owner can take care of his own economic interest. At MSC 76, various questions relating to coating came in this category. All studies showed that it is in the owner's best interest to coat and maintain coating, and that this also have safety implications. Still it was decided not to regulate this at IMO level.

There are also controversies on how FSA studies should be verified. The verification of the FSA on helicopter landing areas for non-Ro/Ro passenger ships was a case of detailed verification. The international FSA on bulk carrier safety was not verified. The study was open to anyone, but there are no records of any independent verification. It is expected that verification of FSA studies will be on the agenda for future IMO meetings.

Finally, the risk acceptance criteria will be an issue of future discussions. On environmental risks there has not so far been any proposal on how to deal with this issue.

#### 4.4 *Risk acceptance criteria*

The FSA guidelines are sufficiently specific on the format of the risk acceptance criteria for safety relating to loss of life. Individual risk and societal risks are supposed to be analyzed, and societal risk should be presented as FN diagrams. The ALARP criterion is referred to, but no criteria have been given for intolerable risk or negligible risk. Still, during the FSA on bulk carriers safety the reasoning by Norway (2000) was adopted. This document concluding that most ship types (including bulk carriers) are in the ALARP area, and that cost effectiveness criteria should be used to reach a final recommendation. In the final decision making process at IMO referred only to this criterion and implemented all risk control options with a cost of averting a fatality less than \$3 m. This is the criterion suggested by Norway (2000) in cases where a fatality

is used an indicator which in addition to representing the fatality risk also represents injuries.

#### 4.5 *The FSA process*

Most risk analysts see the FSA process as a method to coordinate all activities relating to the decision making process. This is still not a widespread view in the maritime industry. A number of risk issues with large cost implications have been put on the agenda during the last couples of years, without considering FSA studies. For example, both security issues and large passenger ship safety issues have been considered without FSA.

Even during the decision making process for bulk carriers there were a number of risk control options implemented without FSA, for example issues relating to the revision of the Load Line Conventions or the UK proposal to strengthen all bulkheads on existing bulk carriers UK (2002c). Furthermore a large number of separate studies, e.g. model tests, were never integrated into the FSA studies, although some studies used structural reliability models that could easily include e.g. new hatch cover load distributions in the risk estimation and estimation of risk reduction.

## 5 CONCLUSIONS

It took the maritime industry seven years from the work with developing the first version of the FSA guidelines was initiated to the first major decisions were made based on the new decision making tool. There have been some failures with using the new tool, but the industry is learning relatively fast. Some attempts to make FSA something different from standard risk based decision making have failed, and focus seems now to be shifting towards educating more people to use the new tools, rather than "inventing the wheel" again.

There is still a lot to be done relating to verification, risk acceptance, data collection and methods for integrating all relevant knowledge. This is probably going to take many years.

The final decisions for bulk carrier safety seems as a good package of preventive and risk mitigating measures, and have a large risk reduction potential of some 60–70%, for new ships, according to the studies. This is a good achievement, and it is not likely that all these decisions would be possible without an FSA.

## ACKNOWLEDGEMENT

The work reported in this paper has been carried out under the DNV strategic research programmes. The

opinions expressed are those of the author and should not be construed to represent the views of DNV.

## REFERENCES

- Estonia (1997) "Final report on the capsizing on 28 September 1994 in the Baltic Sea of the Ro Ro Passenger vessel MV ESTONIA" The Joint Accident Investigation Commission of Estonia, Finland and Sweden.
- DNV (1997) "Cost benefit analysis of existing bulk carriers", Det Norske Veritas Paper series No. 97-P008.
- France (2002) "International collaborative study – Step 2 of FSA" MSC 75/5/5.
- IACS (1998) "HAZID of ballast water exchange at sea" MEPC 41/9/2 submitted by International Association of Classification Societies.
- IACS (1999) "Hazard identification on the watertight integrity of the fore end of bulk carriers" MSC 71/INF.7.
- IACS (2001) "Formal safety assessment – fore-end watertight integrity" MSC 74/5/4.
- IACS (2002) "Bulk carrier safety – side shell integrity evaluation of risk control options" MSC 76/INF.21.
- IMO (1997) "Interim Guidelines on the Application of Formal Safety Assessment (FSA) to the IMO Rule-making Process." MSC Circ.829/MEPC Circ.335.
- IMO (1998) "Report from MSC 69".
- IMO (1999) "Bulk carrier Safety – Report of the working Group" MSC 71/WP.3.
- IMO (2001) "Guidelines on the Application of Formal Safety Assessment (FSA) to the IMO Rule-making Process." MSC Circ.1023/MEPC Circ.392.
- IMO (2002) "Report from the Working Group on Bulk Carrier Safety" MSC 76/WP.16.
- INTERCARGO (2002) MSC 76/5/6 submitted by International Association of Dry Cargo Shipowners.
- Italy (1999) "Report of the correspondence group on trial applications of FSA to high speed crafts".
- Japan (2001) "Report on FSA study on bulk carrier safety" MSC 74/5/3.
- Japan (2002a) "Report on FSA study on bulk carrier safety" MSC 75/5/2.
- Japan (2002b) "Consideration on decision-making process from independent FSA Studies" MSC 76/5/12.
- Japan (2002c) "Investigation on Hatch-Cover related casualties" MSC 76/5/13.
- Marshall Island (2002) "Hull envelope structural failure of M/V LAKE CARLING" MSC 72/5/16.
- Norway (2000) "Decision parameters including risk acceptance criteria" MSC 72/16. (Authors: R Skjong and M Eknes).
- Norway & ICFTU (2001) "Formal Safety Assessment of Life Saving Appliances for Bulk Carriers FSA/LSA/ BC" MSC 74/5/5 (Authors: R Skjong and B.H Wentworth).
- Skjong, R, E Bitner-Gregersen, E Cramer, A Croker, Ø Hagen, G Korneliussen, S Lacasse, I Lotsberg, F Nadim and KO Ronold (1995) "Guidelines for Offshore Structural Reliability Analysis – General" Det Norske Veritas Report No 95 – 2018. The guidelines are available on the internet at <http://research.dnv.com/skj/OffGuide/SRAatHOME.pdf>.
- Skjong, R, P Adamcik, ML Eknes, S Gran and J Spouge (1997), "Formal Safety Assessment of Helicopter Landing Area on Passenger Ships as a Safety Measure" DNV Report 97-2053. (Public as IMO/COMSAR 3/2 and IMO/DE 41 documents).
- UK (1998) MSC 70/4/Add.1 and MSC 70/INF.14.
- UK (1999) "Report of the intersessional correspondence group on helicopter landing areas (HLAs)" MSC 70/14.
- UK (2002a) "International collaborative FSA study – final report" MSC 76/5/5.
- UK (2002b) "Effect of URS21 on existing hatch covers of bulk carriers" MSC 76/5/3.
- UK (2002c) "Comments on the international collaborative FSA study final report and review of proposals" MSC 76/5/17.

## Criteria for establishing risk acceptance

Rolf Skjong

*Det Norske Veritas, Høvik, Norway*

**ABSTRACT:** In the maritime industry the International Maritime Organization (IMO) is the UN organization responsible for developing international safety and environmental protection regulations. IMO has recently developed the “Guidelines for FSA for use in the IMO rule making process”. This standard is, as far as the author knows, the first risk assessment standard adopted in an UN organization.

Paralleling the development of the guidelines there have been a number of applications of the guidelines, recently focusing on bulk carrier safety. Bulk carrier safety has been a challenge for IMO and the industry, in particular after heavy losses in the early nineties. As the problems mainly relates to structural components, the FSA studies have to some extent applied Structural Reliability Analysis (SRA) in order to quantify the effect of Risk Control Options (RCOs) that have been proposed to mitigate the risk.

The paper briefly reviews FSA and SRA describing similarities and differences relating risk acceptance criteria.

The main point in the paper is that the traditional risk acceptance criteria established in SRA can not be used consistently in an FSA. Criteria based on the As Low As Reasonably Practicable (ALARP) principle and cost-effectiveness may play a more prominent role if the two methods shall be integrated.

The consequence of this change is exemplified with one of the few studies that are available. It is observed that the actual change of practice in terms of costs to the industry (e.g. structural material used) is limited.

The case studies are based on experiences from the maritime industry. However, it should be pointed out that SRA is used in many industries and that similar debates take place elsewhere. The proposed approach is expected to be more generally applicable.

### 1 INSTRUCTION

#### 1.1 *Target reliabilities in structural reliability analysis*

The tradition in structural reliability analysis is to base the target reliabilities on one of the following methods (Skjong et al., 1996; DNV, 1992):

- Calibration against well established codes that are judged acceptable or best practices for the same type of structures
- Calibration against well established codes that are judged acceptable or best practices for similar type of structures
- Calibration against tabulated values, using distribution assumptions that are judged to be (slightly) conservative

The first two methods adds costs to the use of SRA as the analysis has to identify implicit reliabilities in

current codes in addition to carrying out the probabilistic design or code calibration in question.

The problem with using the tabulated values, see Table 1, is that the calculated value of the reliability

Table 1. Annual target probabilities (and Target  $\beta_T$ ) from DNV classification Note 30.6.

Class of Failure	Consequence of failure	
	Less serious	Serious
I – Redundant structure	$P_F = 10^{-3}$ , $\beta_T = 3.09$	$P_F = 10^{-4}$ , $\beta_T = 3.71$
II – Significant warning before the occurrence of failure in a non-redundant structure	$P_F = 10^{-4}$ , $\beta_T = 3.71$	$P_F = 10^{-5}$ , $\beta_T = 4.26$
III – No warning before the occurrence of failure in a non-redundant structure	$P_F = 10^{-5}$ , $\beta_T = 4.26$	$P_F = 10^{-6}$ , $\beta_T = 4.75$

index is a function of the analysis methods used and distribution assumptions. Therefore, one should not directly compare reliability indices as obtained from different models and sources.

A calculation of  $\beta_{calculated}$  and  $\beta_{target}$  ( $\beta = -\phi^{-1}(P_F)$ , where  $\phi$  is the standard normal distribution and  $P_F$  is the failure probability) should be based on similar assumptions about distributions, statistical and model uncertainties. It is thus understood that  $\beta_{calculated} > \beta_{target}$  is not considered to be unique when using different distribution assumptions and computational procedures. The value of the target reliability level may be dependent on how the reliability is calculated. Generally, structural reliability analysis is based on a Bayesian interpretation of the probability concept, and the tradition by most practitioners is to include epistemic uncertainties in the models. Such uncertainties are not properties of the structures, but of our knowledge and will also result in probability estimation that is not reflected in a frequency interpretation.

It should also be noted that the industry is in a transition period from experience based to risk based design codes. As the physical models describing the failure mechanisms are improved and more calibration studies are carried out, the knowledge of implicit target reliabilities in existing codes will be improved. Today the inherent target level is not precisely known in many cases or it should hardly be presented without a number of assumptions used for its calculation due to lack of precise knowledge of physical models or lack of data. Furthermore, the reliability models are updated from time to time. If an author claims that the implicit target reliability in a specific code is  $\beta_{target}$  this will relate to the models used. Another model refined during the years would give a different  $\beta_{target}$ .

Owing to dependence on assumptions and analysis models used for reliability analysis the word “reliabilities” in a frequency interpretation of observed structural failures cannot be used in a narrow sense. Due to the unknown deviations from ideal predictions the computed failure probabilities are often referred to as nominal failure probabilities. This is due to the recognition that it is difficult to determine the absolute value of the inherent safety in e.g. design codes by reliability analyses. The requirements to absolute reliability levels may be avoided by performing analysis on a relative basis, i.e. a similar model and distributions are used for calculation of  $\beta_{target}$  as for  $\beta_{calculated}$ . By relating the reliability analysis to relative values it may be possible to use probabilistic analysis for design without a specific requirement to an absolute target reliability level. Such considerations are included in many documents. For the sake of exemplification the first NPD regulations accepting probabilistic analysis are quoted: “The design may be based on a more complete probabilistic analysis, provided it can be documented that the method is theoretically

suitable, and that it provides adequate safety in typical, familiar cases.” Reference is made to NPD (1994).

## 1.2 Risk acceptance criteria in FSA

In the same way as structural reliability analysis has two distinct types of uses, either as basis for design codes or for use in risk based (probabilistic) design, risk assessment is also used in two different ways. The risk assessment is either basis for approving individual objects (e.g. structures, platforms, and plants) or as a basis for deciding on implementing risk-reducing measures for a class of objects (e.g. cars and ships). For example in the offshore or nuclear sectors, risk assessment of the individual platforms or plants is on a license per license basis, whilst in shipping risk assessment is used to make decisions about all ships or all ships of a particular type, e.g. bulk carrier, tanker, or passenger vessel. The terms used for the two uses are risk based design and risk based rules or regulations.

The methods for defining acceptable risk are in practice quite different. For safety issues, both individual and societal risks are considered and risks are divided into three categories. Risks are intolerable, negligible or in the ALARP region. Intolerable risks must be reduced irrespectively of costs or a license to operate will not be given or withdrawn, for new or existing structures, respectively. Negligible risks are accepted and it is accepted that no further assessment is required. Risks that are in the ALARP region need to be reduced until further risk reduction can not be achieved unless excessive costs are involved. A decision is therefore based on the cost effectiveness of the risk reducing measure.

Figure 1 and Figure 2 are examples of individual and societal risks representing some ship types (Skjong and Eknes, 2000). The situation that most ship types are in the ALARP region may be expected to be true also for other existing objects (e.g. plants, platforms, and structures) as it should be expected that regulators acted on intolerable risk.

Based on the considerations above it may be expected that in most cases the risk acceptance criteria

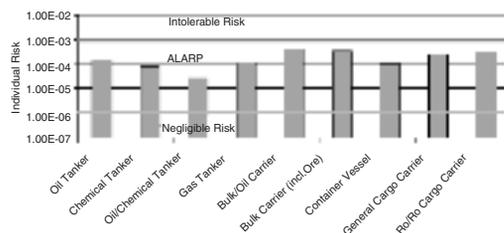


Figure 1. Individual fatality risk (annual) for crew of different ship types, shown together with a proposed individual risk evaluation criterion.

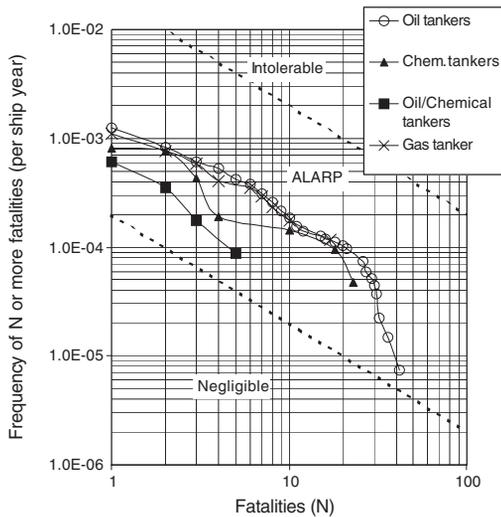


Figure 2. FN curves for different tankers, shown together with established risk evaluation curves. Data are from 1978 to 1998, from Lloyds Maritime Information System. The method for deriving the risk criteria is from Skjong and Eknes (2001, 2002).

of importance (dimensioning) will be the criteria based on cost effectiveness.

## 2 METHODS FOR DERIVING CRITERIA

The type of risk criteria proposed above may define a range within which the risks should be reduced ALARP. Cost effectiveness assessment is recommended used to select reasonably practicable measures.

### 2.1 Human capital method

Cost benefit assessment is discredited by its earlier uses by economists. In the human capital approach, some economists found “value of life” by estimating the value of man as a resource in an economic activity. The view was pursued in e.g. Rice (1966) and Lave and Seskin (1970). This approach is conflicting with ethical traditions. Most ethical systems would regard the wellbeing of man as the purpose of economic activity<sup>1</sup> rather than regarding man as a resource for use in economic activity. Early use of cost benefit assessment lead to such bizarre result that a child was worth next to nothing, because of the “low opportunity cost

<sup>1</sup>e.g. The “Homo Mensura” sentence was formulated by Protagoras (485–415 BC).

of replacement”. The resulting acceptance criteria are given for some countries in Figure 5.

### 2.2 Well informed decisions

Cost effectiveness assessment presents a ratio of costs to benefits, and avoids putting a value to the benefit (e.g. life saved). The value judgment is left to the decision-maker when deciding which risk control options to implement. Sometimes such decisions are made by the responsible regulatory body, based on risk and cost effectiveness studies. After a decision is made on which risk control options to implement and not implement the criterion is revealed and may be used in later studies. Such a judgment was made at IMO by the Marine Safety Committee when deciding which risk control options to implement from the Formal Safety Assessment studies carried out for bulk carriers. The criterion used was \$3 m to avert a fatality.

### 2.3 Comparing to previous decisions

Society spends large sums (some 20% of Gross Domestic Product in some countries) on safety (including the health sector). Such use of resources cannot be justified in order to optimize economic production (the human capital approach). However, resources are limited and society needs to put some limit to how much resources could be used for safety, and thus a cost effectiveness criterion may be proposed.

The valuation of fatality risks is a critical step in this process, and modern risk assessment practice is to highlight this issue by expressing the results in the form of a Gross Cost of Averting a Fatality (GCAF) if a risk control option were to be adopted, i.e. by cost effectiveness assessment.

$$GCAF = \Delta Cost / \Delta Risk \quad (1)$$

$\Delta Cost$  is the marginal (additional) cost of the risk control option, whilst  $\Delta Risk$  is the reduced risk in terms of fatalities averted. If the regulators could avoid implementing risk control options with high GCAFs and implement those with low GCAFs, more lives would be saved for the same budget (Condition of Pareto optimality), see e.g. Tengs et al. (1995), Ramberg and Sjøberg (1997).

An alternative cost-effectiveness measure is given by Net Cost of Averting a Fatality (NCAF), where the economic benefits of the investigated RCOs are accounted for. Economic benefits (or risk reduction) may also include the economic value of reduced pollution. The consequence of pollution may be established from clean-up costs or comparing to previous decisions. For example the OPA 90 regulations represent

a cost of \$10,000 per barrel of oil pollution averted (see Lloyds List May 18th 2001).

$$NCAF = (\Delta Cost - \Delta Benefit) / \Delta Risk \quad (2)$$

Large studies have revealed large inconsistencies in safety policy. The most well known and largest study is that of Tengs et al. (1995) carried out in the US. Table 2 presents the average values. These figures represent willingness to pay in actual decisions. Assuming that a fatality corresponds to 35 lost life-years, the median value corresponds to \$1.47 m. By

Table 2. Results from Tengs et al. (1995).

"Five hundred life-saving interventions and their cost effectiveness"	
Number of measures studied	587
Range of cost effectiveness	Negative to \$10 billion/life year saved
Median Value	\$42,000/life year
Median for Medical Interventions	\$19,000/life year
Median for Injury Prevention	\$48,000/life year
Median for toxic control	\$2.8 million/life year

reallocating resources and implementing only the most cost effective measures, but allocating the same total budget some 40,000 additional lives could be saved annually in the US.

### 2.4 Social indicators

It is also possible to derive evaluation criteria expressed as NCAF from compound aggregated social indicators, see UNDP (1990) and Lind (1996), Skjong and Ronold (1998, 2002), Ditlevsen (2003). The Life Quality Index Criterion for acceptable risk implies that an option is preferred or accepted as long as the change in the Life Quality Index owing to the implementation of the option is positive. The Life Quality Index contains such indicators as GDP/capita and life expectancy at birth. As a risk control option changes these two, an optimum acceptable NCAF may be derived, and as GDP and life expectancy varies between countries there are variations in the evaluation criteria. Within OECD member countries with sustained memberships (representing some 95% of the global GDP), the variation is not very large, see Figure 3.

Based on the above, a NCAF criterion of \$3 m may be proposed for use for international regulations, in cases where fatalities in addition to representing fatality risk also represent an indicator of risk of

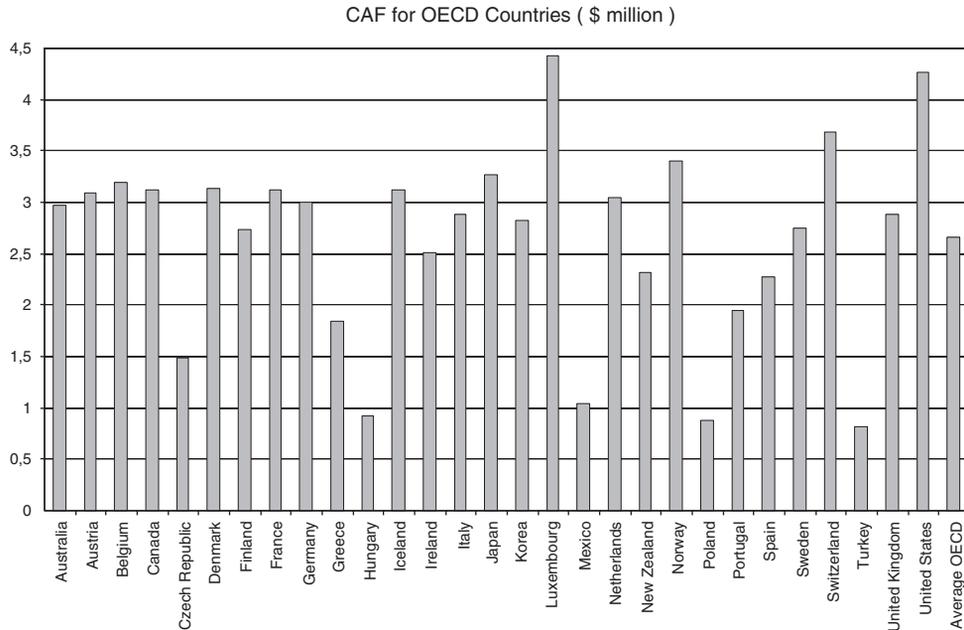


Figure 3. Acceptance criterion in terms of cost of averting a fatality for OECD member countries. Data are for 1999, from Skjong and Ronold (2002).

injuries and ill health. The NCAF criterion may be updated every year according to the average risk free rate of return (some 5%), or if data is available by use of the formula derived by societal indicators, see Skjong and Ronold (1998, 2002). Higher values may be justified for risks that are just tolerable.

From the ideas presented, it should be evident that rational arguments exist for using specific criteria for cost effectiveness. Still, in practice it may be difficult to argue against proposals for increasing the safety of structures if a hazard is identified that may be avoided by increasing the structural dimension.

### 2.5 Voluntary measures

It is well known from the research literature over many years that there is a relationship between purchasing power and life expectancy. The life expectancy increases with increasing purchasing power. This effect is well known from demographic studies, and most people have probably seen results from such studies comparing, for example, east and west in their own hometown. The effect exists despite the fact that the same safety regulations and health services are offered regardless of purchasing power. If a causal effect can be established the result is interesting, because it would then indicate that individuals will be safer without any safety regulations if their purchasing powers increase. As the implementation of mandatory safety regulations also implies expenses, there will be a limit to the cost effectiveness of such expenses at which decisions by individuals are more cost effective. It may therefore be stated that a mandatory regulation that is less cost effective actually has a net negative result (net killers).

In a similar way as the NCAF value derived from the societal indicators indicates how much a regulator should spend on life saving interventions the NCAF value derived from voluntary investment in safety, should be regarded as an upper limit for implementing safety measures.

Keeney (1990) formalized this idea and Lutter and Morrall (1994) and Lutter et al. (1999) formulated a theoretical relationship for linking mortality and income. To derive this relationship, a model was established by which individuals reduce their risk of death through self-protective measures and increase their risk of death with increases in risky behavior such as smoking, consumption of alcohol and overweight. A causal relation was established with 99% confidence and the question of whether good health results in high income or vice versa was given an answer. Keeney (1994) also discusses a number of practical and ethical implications.

Figure 4 from Skjong and Ronold (2002), shows the global relationship between life expectancy and purchasing power using 190 data-points (countries)

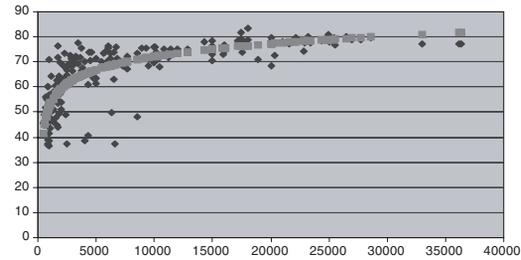


Figure 4. Life expectancy (years) as function of annual purchasing power (US\$). The data represent 190 countries.

from CIA(2001). Among a number of tested functions, the following function was found to honour the data the best:

$$e = a \ln(p - b) + c \quad (3)$$

in which  $e$  is the life expectancy at birth and  $p$  is the annual purchasing power (in \$US/year). The coefficients of the best fit to the data are  $a = 7.1874$ ,  $b = 371.5$  and  $c = 6.2075$ .

The derivative of the function is

$$\partial e / \partial p = a / (p - b) \quad (4)$$

Again, consider the prevention of one fatality. As in Skjong and Ronold (1998, 2002) it is assumed that the number of years saved by averting one fatality in a population is  $\Delta e = e/2$ . To "buy" this additional number of life years requires an increase in annual purchasing power per capita

$$\Delta p = \partial p / \partial e \cdot \Delta e = (p - b) / a \cdot e / 2 \quad (5)$$

With duration of one life expectancy, the implication of this is that the net cost of averting a fatality by voluntary investment is

$$NCAF(Voluntary) = (p - b) / a \cdot e^2 / 2 \quad (6)$$

A country like India is at \$2,200 annual purchasing power (CIA, 2001), corresponding to  $NCAF(Voluntary) = \$0.46$  m. The number estimated by Hahn et al. (2000) based on data from Pritchett and Summers (1996) for averting a child mortality in India is \$0.3 million. As previously indicated the methods are different but the results are similar and within the variability range in Figure 4. However, it should be noted that a child fatality should count as the loss of  $e$  and not  $e/2$ , which is used herein to represent the loss associated with an arbitrary accidental fatality.

For a wealthy country like the US, Lutter et al. (1999) derive a  $NCAF(Voluntary)$  of \$15 m (with an uncertainty range between \$10 m and \$50 m). Keeney

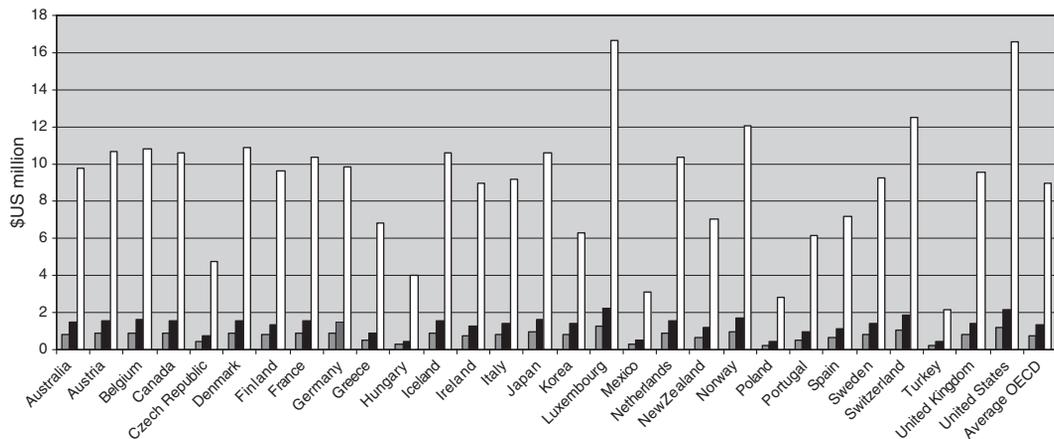


Figure 5. The net cost of averting fatality criteria for OECD member countries. The left columns would be defendable by purely economic considerations, the middle columns represent the societal value (derived from the societal indicators), the right columns represent the limit where no regulation should be implemented as individuals would use the resources better on life saving. The OECD average numbers are \$0.76 m, \$2.65 m and \$8.93 m. The factor differences are 3.50 and 3.33.

Table 3. Published GCAFs in use as evaluation criteria.

Organization	Subject	GCAF	Source
US Federal Highway Admin.	Road transport	\$2.5 m (£1.6 m)	FHWA (1994)
UK Department of Transport	Road transport	£1.0 m (1998, up-rated with GDP/capita)	DETR (1998)
UK Health & Safety Executive	Industrial safety	As above or higher	HSE (1999)
Railtrack (UK rail infrastructure controller)	Overground railways	As above to £2.65 m	Railtrack (1998)
London Underground Ltd	Underground railways	£2 m	Rose (1994)
EU	Road transport	€1 m (\$1 m)	Evans (1998)
Norway	All hazards	NOK10 m (\$1.4 m)	Norway (1996)

(1990) derives a value of \$7.5 m. These calculations were in 1980 dollars, and converts to \$12.71 m 1999 dollars by assuming a 3% annual inflation rate. Keeney's results were based on a regression model for annual mortality data in the US. The basic idea of Keeney's model is therefore similar to that of the global regression model suggested Skjong and Ronold (2002). With a purchasing power of \$36,200 (CIA, 2001) the formula in Eq. (6) gives \$16.6 m. It

appears that the indications from the different types of data and models give similar results. All models should be taken as indicative. More detailed studies would be required to arrive at criteria for use in any specific country.

In Figure 5, the results for all OECD member countries are presented. For illustration the acceptance criteria from the human capital approach, indicated as  $ge/2$  is plotted together with the results from the LQI (a willingness-to-pay approach) and the limiting NCAF (Voluntary). In this way a recommended criterion is proposed together with a lower and upper limit.

## 2.6 Some criteria used by regulatory bodies

Table 3 gives values of GCAF used by some authorities. It is seen that the criteria are similar to those derived by the LQI approach.

## 3 DISCUSSION

It is seen that the techniques used to derive risk acceptance criteria are resulting in similar results. Within the OECD countries, excluding a few new members, a cost of averting a statistical fatality is at about \$1.5–3.0 m. In a risk assessment, where the question is about implementing or not implementing a safety measure the uncertainty in the criteria is not very important. A risk analysis will in most cases end up with risk control options with cost effectiveness above or below the criteria. Some knowledge of the criteria will therefore be sufficient input to accepting or rejecting a specific proposed risk control option.

Table 4. GCAF/NCAF in US\$ m for increases of the reliability index  $\beta$  (mid ship bending moment capacity).

$\beta$	Flat bar	L-Profile
2.5→3.09	0.402/−2.80	0.133/−3.07
3.09→3.50	1.76/−1.74	2.55/−0.645
3.50→3.72	4.44/1.24	10.3/7.13

In SRA most design variables are continuous, and the exact number used will have direct influence on the resulting structural design. However, the few studies that have been performed, see Skjong and Bitner-Gregersen (2002), see Table 4, does not indicate any dramatic effect and in practice the uncertainty in the calculations may be larger than in the acceptance criteria.

The advantage with using the marginal safety return as criteria relates more to the consistency between normal risk assessment practice and structural reliability analysis as the same criteria may be used in both cases.

Furthermore, the structural reliability analysis is based on Bayesian probabilities. Probabilities are thus properties of our knowledge of the structure and the loads it is subjected to. To use acceptance criteria that are based on a frequency interpretation of probabilities is therefore discomfoting. It is actually more satisfactory to use the NCAF criterion, because only information relating to relative changes in the probabilities as a function of design parameters is used in the decision process.

The paper suggests that the human capital approach is used to define a lower limit, the life quality index is representing a recommended value and the cost effectiveness of voluntary measures represent an upper limit for cost of averting fatalities. The three criteria could be referred to as "life for \$", "\$ for life" and "life for life"; respectively.

#### ACKNOWLEDGEMENT

The work reported in this paper has been carried out under the DNV strategic research programmes. The opinions expressed are those of the author and should not be construed to represent the views of DNV.

#### REFERENCES

- CIA (2001) US Central Intelligence Agency "The World Fact Book, 2001".  
 DETR (1998) "1998 Valuation of the Benefits of Prevention of Road Accidents and Casualties", Highways Economics Note No1: 1998, Department of the Environment,

Transport and the Regions. [www.roads.detr.gov.uk/road-safety/hen198/index.htm](http://www.roads.detr.gov.uk/road-safety/hen198/index.htm).

- Ditlevsen, O (2003) "Decision Modeling and acceptance criteria" Structural Safety 25, 165–191.  
 DNV (1992) Classification Note 30.6 "Structural Reliability Analysis of Marine Structures".  
 Evans (1998) "Automatic train protection and the valuation of statistical life". ESRa Newsletter, January 1998.  
 FHWA (1994) "Motor Vehicle Accident Costs", US Federal Highway Administration, Technical Advisory T7570.2, 1994. [www.fhwa.dot.gov/legisregs/directives/techadvst75702.htm](http://www.fhwa.dot.gov/legisregs/directives/techadvst75702.htm).  
 Hahn, RW, RW Lutter and WK Viscusi (2000) "Do Federal Regulations Reduce Mortality", AEI – Brookings Joint Center for Regulatory Studies.  
 HSE (1999) "Reducing Risks, Protecting People". Discussion document, Health & Safety Executive.  
 Keeney, RL (1990) "Mortality Risks Induced by Economic Expenditures", Risk Analysis, Vol 10, No. 1, 1990. pp 147–159.  
 Keeney, RL (1994) "Mortality risks Induced by the Cost of regulations", Journal of risk and Uncertainty, Vol. 8, 95–110.  
 Keeney, RL (1997) "Estimating Fatality Induced by Economic Costs of Regulations", Journal of Risk and Uncertainty, Vol. 14, 5–23.  
 Lave, L and EP Seskin (1970) "Air pollution and human health", Science, 109, 723–732, August 1970.  
 Lind, NC (1996) "Safety Principles and Safety Culture", Proceedings, 3rd International Summit on Safety at Sea, Conference organized by Norwegian Petroleum Society, Oslo, Norway.  
 Lutter, R and JF Morrall III (1994) "Health-Health Analysis: A new way to Evaluate Health and Safety regulations", Journal of risk and Uncertainty, Vol. 8, pp 43–66.  
 Lutter, R, JF Morrall III and WK Viscusi (1999) "The Costper-Life-Saved Cutoff for Safety-Enhancing Regulations", Economic Inquiry 37 (4): 599–608.  
 Norway (1996) Stortingsproposisjon No 1 1996–97 (In Norwegian).  
 NPD (1994), "Regulations Relating to Load bearing Structures in the Petroleum activities", Norwegian Petroleum Directorate.  
 Pritchett, L and L Summers (1996) "Wealthier is Healthier", Journal of Human resources 31 (4): 840–68.  
 Railtrack (1998) "Railway Group Safety Plan 1998–99", Safety & Standards Directorate, Railtrack, London.  
 Ramberg, JAL and L Sjøberg (1997) "The Cost-Effectiveness of Lifesaving Interventions in Sweden", Risk Analysis, Vol 17. No 4, 1977.  
 Rice, D (1966) "Estimating the cost of illness", US Department of Health and Welfare, Public Health Service, Home Economic series, No.6 (May, 1966).  
 Rose, J (1994) "Risk Assessment – To Quantify or Not to Quantify? Is that the Question?" Conference on Practically Implementing Safety Case Regulations in the Transport Industry, IBC, London, March 1994.  
 Skjong, R, E Bitner-Gregersen, E Cramer, A Croker, Ø Hagen, G Korneliussen, S Lacasse, I Lotsberg, F Nadim and KO Ronold (1996) "Guidelines for Offshore Structural Reliability Analysis – General".  
 Skjong, R and ML Eknes (2000) "Decision Parameters including Risk Acceptance Criteria". Available as IMO MSC 72/16 submitted by Norway. <http://research/dnv.com/skj>.

- Skjong, R and ML Eknes (2001) "*Economic activity and societal risk acceptance*", ESREL 2001, 16th–20th September, 2001, Turin, Italy.
- Skjong, R and ML Eknes (2002) "*Societal Risk and societal benefits*", Risk Decision and Policy (2002), vol 7, pp 1–11, Published by Cambridge University Press 2002.
- Skjong, R and KO Ronold (1998) "Societal Indicators and Risk Acceptance", Offshore Mechanics and Arctic Engineering Conference, OMAE 1998.
- Skjong, R and K Ronold (2002) "So much for Safety", OMAE-2002-28451, Oslo, June 2002.
- Skjong, R and E Bitner-Gregersen "*Cost Effectiveness of Hull Girder Safety*" OMAE 2002-28494.
- Tengs, T et al. (1995) "*Five hundred life-saving interventions and their cost effectiveness*", Risk Analysis, Vol. 15, 369–391.
- UNDP (1990) United Nations Development Programme, "*Human Development Report*", Oxford University Press, 1990.

## Risk assessment of passenger vessels

H. Soma, S. Haugen & B. Øygarden

*Safetec Nordic AS, Norway*

**ABSTRACT:** Some severe capsizes and fire accidents have taken place with passenger vessels in the latest years. The objective in this paper is to describe the issues that must be addressed in a Quantitative Risk Assessment (QRA) for passenger vessels and some of the required development tools. Further, IMO has launched the concept of Formal Safety Assessment (FSA), and the usefulness and possible shortcomings of FSA as compared to a QRA are evaluated. The conclusion is that a QRA is a powerful tool in enhancing passenger ship safety, while a FSA has a limited potential, mainly because it is not applied on a concrete ship.

### 1 INTRODUCTION

Some severe capsizes and fire accidents have taken place with passenger vessels in the latest years as referred in Table 1.

The accidents have demonstrated a clear need for improvements, and highlighted deficiencies inherent in the safety regime in force.

The regulatory regime for passenger vessels is based upon international co-operation in IMO. The regulation requirements are prescriptive and very detailed. The development is based on re-use of proven solutions and technologies and has been influenced by ad-hoc solutions after accidents.

In several industries Quantitative Risk Assessment (QRA) has proven a powerful tool in enhancing safety. It may be mentioned that in the late 60s, IMO issued Res. A265 (the equivalent) for passenger vessels, based upon a probabilistic method. Collision

damages were statistically predicted based on accidents that had occurred. At that time IMO was a forerunner in the field of risk analysis. However, A265 was an alternative to the prescriptive regulations in force, and the ship owners stuck to the legislative regime they were familiar with. Hence Res. A265 was never really implemented in practical ship design, and the scene of risk assessment was dominated by the nuclear and process industries.

### 2 OBJECTIVE

The objective of this paper is to describe how a QRA for passenger vessels can be performed and the tools required for making it. Further, IMO has launched the concept of Formal Safety Assessment (FSA), and the usefulness and possible shortcomings of FSA as compared to a QRA is evaluated.

Table 1. Accidents with passenger vessels.

Ship	Date	Accident	Fatalities
Herald of Free Enterprise	March 1987	Rapid capsizes, high list	193
Scandinavian Star	April 1990	Fire, toxic smoke	158
Moby Prince	April 1991	Fire	140
Estonia	Sept. 1994	Rapid cap-size, high list	852
Express Samina	1999	Grounding and capsizes	83

### 3 QRA AND FSA METHODOLOGIES

In a QRA a specific passenger vessel, which operates in a specific environment, is analyzed.

In a FSA as proposed by IMO, the risk assessment is used as a tool for development of rules and regulations for a generic ship in a representative environment, based on cost-benefit analyses. The "generic ship" is defined in order to represent a selected ship group with common properties, e.g. ro-ro ferries. The FSA is quantitative, and might as well have been classified as "a QRA for a generic ship operating in a representative environment". Hence, the principal

difference between a QRA and a FSA is that a QRA is performed for a specific ship in its real environment, while a FSA is performed on a generic ship in a representative environment. Except for this difference, the basic methodology is similar for a QRA and a FSA. However, it may only be meaningful to define a generic ship at a relatively coarse level of detail. Otherwise there will be severe differences between the “generic ship” and most ships it is intended to represent. This difference in specification level as compared to a “real ship” in a QRA introduces methodological differences as well.

The main steps in a QRA and FSA are:

- Hazard identification
- Cause and frequency analysis
- Consequence analyses
- Risk calculation and evaluation
- Evaluation of preventive and mitigating measures

In the following, the execution of the above steps in a QRA is explained. Most of these steps will be similar, or even identical in a FSA, but there will be some important differences. At the end of each section, the differences as compared to a FSA are therefore explained and commented.

#### 4 HAZARD IDENTIFICATION

In the offshore industry, the Hazard Identification (HAZID) method has proven a powerful tool in identifying hazards. In a meeting where specialists on different topics participate, a set of predefined control words are systematically applied on each area of the installation being analyzed, in order to identify hazards. When a hazard is identified, it will be subject to further analyses as part of the QRA process.

It is evident from the accident statistics for passenger vessels that flooding events and fires represent the main high level hazards.

Flooding events include collisions, groundings, flooding through openings not properly closed or through damages caused by structural failure. In the HAZID, these hazards may be evaluated in some detail. For each relevant ship area, potential causes for flooding will be identified, together with the potential for progressive flooding. It may e.g. be questioned what the effects of possible rupture of pipes in a collision may be.

With respect to fire, the amount of flammable material, ignition temperatures, possible ignition sources, ventilation conditions that may worsen the fire, etc., will be evaluated in relevant areas.

Hazard identification will be performed both in a QRA and FSA. However, the “generic” ship in the FSA will only be defined at a relatively coarse level. At a more detailed level, there will also be major differences

between the individual ships belonging to the “generic” group. HAZID has proved a very successful activity in offshore projects, provided the object being analyzed is concrete and sufficiently defined. It may easily be foreseen that a HAZID performed on a “generic” vessel will suffer from several deficiencies.

#### 5 CAUSE ANALYSES

The cause analysis focuses upon the possible causes for e.g. flooding and fire. In some cases it may be possible to prevent accidents by implementing measures on the specific vessel. The bow port on Estonia, could for example have been prevented from falling off and cause flooding of the deck. However, only to a limited extent it is possible to prevent collisions by implementing measures on a specific vessel. In these cases focus have to be put on mitigation in order to control risks.

Based on the HAZID and Cause analyses, accident scenarios should be established. These scenarios must be sufficiently defined to facilitate a consistent assessment of the potential consequences. The probability of initial fire events may be based upon accident statistics.

With respect to collisions and similar accidents, frequencies may also be established based on generic accident data. However, theoretical models have also been developed. In larger parts of the North Sea, ship lanes have been mapped and the sizes and types of vessels operating at each lane have been recorded. These data are used to predict the collision frequencies for offshore installations.

The models used for prediction of ship to ship collisions may also account for the ship course and size distributions in the area. Ship owners may, however, hesitate in designing a ship for a particular area, and for this reason they may tend to assume “worst case” traffic data to have the flexibility to traffic other areas with a ship.

It is reasonable to assume that the likelihood of fire events to take place is independent of the weather conditions and time of the day. Hence, the conditional probability of a ship evacuation in severe weather due to fire may be assumed to correspond to the probability of severe weather to occur.

Collision events, however, are most likely to take place in weather conditions with reduced visibility, e.g. in “calm” weather with dense fog during night. Some flooding events are, however, strongly correlated to bad weather (ref Estonia). It is important that the correlations between accident frequencies and weather conditions are established and documented in order to make consistent analyses within the QRA.

The above described approach will be similar for a QRA and FSA. However, it will not be meaningful to address detailed issues in a FSA.

## 6 CONSEQUENCE ANALYSES

### 6.1 Flooding

In the specific regulations, it is a requirement that a ship shall survive certain damage conditions. According to “the Equivalent”, which in general is stringent as compared to the SOLAS requirements, a ship with less than 600 POB shall survive any damage between bulkheads. A ship with at least 1200 POB shall survive damage to any bulkhead.

In a QRA, it will be focused upon the potential losses of lives. Hence, it is a key issue whether a ship keeps afloat for sufficient time for evacuation to take place. If a ship sinks due to progressive flooding during hours like Titanic, most people will survive in normal cases (with enough lifeboats). On the other hand, a rapid capsizing during an intermediate stage of flooding will cause heavy loss of lives (ref Estonia and Herold of Free Enterprise).

IMO has presented a comprehensive data basis for “the Equivalent”. Based on recorded collision damages on ships, probability distributions with respect to length and penetration of damages were established, together with a theoretical framework for assigning conditional probabilities to different damages.

In Table 2, it is shown that the “Equivalent” is a powerful tool for assessing damage probabilities for a ship being rammed by another vessel. In the examples it is assumed that a ship is subdivided into 10, respectively 5 watertight compartments by evenly spaced transverse bulkheads.

The first line in Table 2 is applicable for a ship, which is subdivided into 10 compartments with equal length. Based on formulas in “the Equivalent” the probability of damage between two specific adjacent bulkheads has been assessed at 0.038. The total probability of (the 10 cases with) damages between bulkheads sums up to 0.38, as shown in the table. Therefore, given a collision, the probability that the damage will be more severe and include damage to one or more bulkheads is  $1.0 - 0.38 = 0.62$ . Hence, if the ship is designed to survive damages between bulkheads only, the probability for a more severe

damage will be 0.62. The last line in the table shows that if the distance between bulkheads is doubled, it becomes, as expected, more likely that damage may occur in between bulkheads. Note that “the Equivalent” includes an adjustment to account for the fact that damages are more likely to occur in the forward part of the ship. It is not accounted for this adjustment in the above presentation.

Table 2 also gives an indication that collision damages are relatively likely to exceed the requirements in the regulations in force. For this reason it is even more important to address the possibility people have to survive flooding accidents in which the ship sinks.

As an alternative or supplement to “the Equivalent”, collision scenarios may be established and the sizes of damages may be predicted by use of Finite Element Programs, which account for large deformations.

The time development of the flooding process is mainly a function of the size of the “hole” and the submergence of it. The amount of flooding water depends upon the size of the compartment being flooded, as well as on possible progressive flooding through openings that may become submerged during the process.

Due to the free surface effect, a small amount of water may cause a ship to capsize at an early flooding stage. In a QRA, the potential of this failure must be given much attention. For Estonia, a relatively small amount of water that could shift from side to side on the bulkhead deck caused the ship to lose its stability and to capsize. In ship collision events, there may be potential for free surface effects at two or more decks, possibly causing the ship to capsize at an early flooding stage. These effects must be carefully evaluated.

The “Equivalent” provides a comprehensive and useful tool for assigning conditional probabilities to flooding cases.

The time development of the flooding process and corresponding ship draught and inclination can be calculated with reasonable accuracy based on basic hydrodynamic equations.

The “Equivalent” is an example of a successful FSA activity relating to damage stability. A risk assessment was performed as basis for development of specific regulations. The “Equivalent” can of course form the basis for QRAs as well. Detailed evaluations, e.g. relating to extent of flooding, may not be feasible within a FSA.

Table 2. Damage probabilities.

Ship design, no. of compartments	Damage case	Probability of damage case
10	Damage between bulkheads	0.38
10	Damage to one bulkhead or in between bulkheads	0.84
5	Damage between bulkheads	0.64

### 6.2 Fire

Fires are most likely to start in machinery rooms or in passenger sections. The main risk is that a fire may spread so fast that people may be trapped. Several safety barriers are built into passenger vessels to prevent this from happening:

- Use of material with high ignition temperature.

- Sectionalizing by use of Passive Fire Protection (PFP).
- Closing of fire doors and ventilation shut down to extinguish fire and prevent smoke spread.
- Fire alarms to notify people.
- Fire extinguishing systems. Sprinkler requirement on new ships.

The safety barriers will prevent most fires from developing into disasters. However, unforeseen events together with failure or operational errors with safety systems may cause severe fires to develop. The Scandinavian Star disaster is an example of this. Arson in combination with unforeseen operational errors and technical faults resulted in an extreme fire with 158 fatalities. The main reason for the disaster was extremely unfavorable ventilation conditions in some corridors because a door between the passenger section and car deck was left open. The fire spread like a “fire ball” in some corridors and through a few fire doors that failed to close, and in some places the propagation speed was so fast that fire victims had difficulties in running away.

What may be assumed is that there exist a large number of very unlikely combinations of events and failures that may develop into fire disasters. It may not be feasible to address all of them in a realistic way, and most of them may be so peculiar that most people would say they never could happen. As a hypothetical example it may be claimed that if somebody had presented a fire scenario similar to what happened on Scandinavian Star as basis for safety evaluations prior to the accident, he might not have been taken serious. Hence, it is very important that creativity is exercised in the HAZID when fire risks are addressed, in order to identify critical scenarios.

Reliability calculations of safety systems are standard practice in offshore QRAs, and failures are probabilistically accounted for. Further, vulnerability analyses that focus on the possibility that safety systems may be damaged by the accident are performed. Such calculations should also be part of a passenger ship QRA. As it may not be meaningful to define representative safety systems in detail, these calculations may not be feasible within a FSA.

As soon as a concrete scenario is defined, a suitable fire development model together with a CFD code may be used to simulate the fire development and smoke spread. There exist several CFD codes, and some of them also include a fire model. As part of the Scandinavian Star investigation, such simulations were performed, and they showed good agreement with observations from the accident. The important results of the simulations are the time development of the fire and smoke spread, together with smoke concentration and visibility.

The described approach involves so many design details, that a FSA may not be feasible.

### 6.3 Mustering

Mustering is defined as the process whereby passengers move towards their muster areas, which normally is near the lifeboats. Mustering is initiated with alarm and PA messages, when the captain has decided that evacuation must be performed. There are several examples that delayed decision taking has contributed to loss of lives. Suitable measures for decision support, helping the captain to get an overview of the situation, are therefore important.

The external conditions that may complicate mustering are possible static heel of the ship, motion of it in waves and smoke impact in case of fires. All these effects have contributed to heavy loss of lives in the recent accidents with passenger vessels.

In flooding accidents, it is important to account for escapeway impairment due to possible list. List makes walking and climbing stairs difficult, and reduces the capacity of escapeways. It may become difficult to open heavy doors in case of list. Loose items may slide towards the low side and further restrict escape. If the ship in addition should be moving due to wave impact in bad weather, evacuation may be even more difficult. Passengers inside the ship will be afraid to get trapped inside a sinking and capsizing ship, and they will try to get up and out as fast as possible. Possible muster area inside the ship may not be used.

The impact of list and ship motion on the evacuation performance was investigated in the MEP Design project. To study passenger motion in corridors and stairs, TNO performed empirical studies by use of mockups of passenger cabin sections and a motion simulator (Bles, 2000). Volunteers who constituted a representative sample of the population participated, and they had also to find their way with guidance from different signposting concepts. A full scale mustering test was performed with the Danish passenger ship “Kronprins Fredrik” with about 600 passengers aboard.

The mustering simulation program EVAC was developed as part of the MEP Design project. Individuals, each with his distinct properties, constitute the basic entity. As the program performs Monte Carlo simulations, several variables are assigned values based on weighted drawings from probability distributions. At least 15–20 replications of a simulation are required to produce statistically significant results.

In fire scenarios, escape ways may be impaired by dense smoke. In the Scandinavian Star disaster, a part of the passenger section became filled with dense smoke. The visibility in the smoke was down to 0.3 m. Some exit doors were located a short distance from

the end of the corridors, and several evacuees lost their lives just inside the door because they did not find the door handle where they expected. Others were trapped in a blind end. Most of the passengers who lost their lives were in their cabins, which they did not leave to enter the smoke filled corridors. The cabins were kept free from smoke for a long time, but when the ventilation system was shut off as it should according to the procedures, smoke penetrated into the cabins, and intoxicated all the passengers who remained in their cabins. Passengers in other areas of the ship mustered without severe problems.

There exist a lot of empirical data on human behavior in fires. These data have been collected in questionnaires and interviews with fire victims. There are for example established probabilities that evacuees may turn back in smoke as a function of the visibility. Such behavior was important at the Scandinavian Star disaster, where several passengers remained in their cabins. Further, intoxication by smoke, usually by CO, represents the main hazard in fires. There exist sufficient data to calculate time until incapacitation of resting or walking persons, as well as how long time they may stay alive. In a validation project of evacuation programs, the two programs being tested (ASERI – German and Evacsim – Norwegian/French) were both able to represent the Scandinavian Star fire in a reasonably correct manner.

It is shown in this section that there exist a lot of empirical data with respect to Mustering in case of fire or list with passenger ships. In addition, computer programs are available.

The mustering simulation requires a detailed topological description of the escapeway system, and is not feasible for a “generic” ship within a FSA.

#### 6.4 Evacuation

Evacuation from the ship is usually performed by means of enclosed lifeboats. However, ships operating close to shore are allowed to substitute lifeboats with inflatable life rafts. In UK, a study of lifeboat performance in real situations was performed, and it was shown that the historical success rate was low. Later on, lifeboat launch simulation programs as well as model tests of lifeboat evacuation have clearly confirmed lifeboats to be unsafe evacuation means unless the weather is good. The failure modes with lifeboat evacuation are:

- Difficulties in starting launching on a possibly inclined ship.
- Collision with ship side during descent, caused by lifeboat pendulum motion and ship motion in waves.
- Release of lifeboat while it still is in the air.
- Release failure of lifeboat fallwires.

- Collision with ship side due to wave impact after lifeboat has become seaborne.
- Damages caused by obstructions on the ship side.

It is particularly collisions with the shipside that is of much concern. The passengers in the boat may be seriously injured due to the impact, and the lifeboat may be damaged and subsequently flooded when seaborne.

The LBL lifeboat launch simulation program was originally developed for simulating launches from offshore installations, where there normally is considerable clearance between the installation structure and lifeboat during descent. Despite this, in launches on the windward side in severe weather, high waves and wind may sweep the boat a long distance back and cause a collision with the installation. The program performs Monte Carlo simulations, and the time for commencement of the launch operation is the random parameter. A stochastic wave and wind model is applied. In the MEP Design project, LBL was amended to simulate launches from a rolling ship. In the same project, systematic model tests were carried out with launches of lifeboats from a ship model in a model basin.

The model tests as well as the LBL simulations showed that launch of lifeboats from a passenger vessel broadside the oncoming sea was unsafe in 2–3 m wave conditions.

The above evidence clearly demonstrates that evacuation from passenger vessels is an unreliable operation. This is also a strong indication that IMO should focus more on the operational reliability of lifeboat evacuation and less on the time development.

It is shown above that empirical data from model tests as well as computer programs are available for assessment of the launch failure probability of lifeboats.

In the present situation with very standardized evacuation means, there may not be much differences between a QRA and FSA. However, there is a need for improvements of evacuation systems. In a FSA approach, the authorities will take the responsibility for the specific regulations and their possible shortcomings. In a QRA approach, the full responsibility will be put on the ship owners and the design team. Improvements and innovation will be more likely in this case.

#### 6.5 Rescue

Following an accident where a passenger ship sinks, there will be people in distress in lifeboats, rafts and possibly in the sea. For people in lifeboats, the rescue operation itself may represent the main hazard. The disaster with the offshore installation Ocean Ranger is an example of this. A lifeboat collided with the vessel trying to rescue it in stormy and cold weather, and

nobody survived the accident. To avoid such accidents, rescue of people in lifeboats in bad weather will normally be postponed until the weather improves.

People having entered the sea are in the worst situation. They normally have donned their life vests. If the weather is bad, they may get their head submerged below wave crests for sufficient time to drown. If the sea temperature is low, the survival time may only be a few minutes, and they may perish from hypothermia.

Rescue will be carried out by ships in the area and by helicopters. In most cases, it will be possible for SAR helicopters to reach the site of the accident. The helicopter needs some mobilization time, and it takes some time to fly to the area. They then have to detect people in the sea, and to rescue them by use of the rescue hoist. The capacity of the helicopter may be about 20 persons, and they have to bring the rescued people to a safe place before they can return to the scene of the accident. Altogether, it may take long time to rescue a large number of people in distress at sea by helicopters.

Ships in the area will usually try to pick up people in the sea by launching their MOB boats. They need some time to detect each person in the sea, and also to get him into the boat, which may be very difficult in bad weather. The boat may only have capacity to take a few rescued persons on board before they must be brought back to the mother vessel.

The simulation program Offshore Sea Rescue was developed several years ago, to simulate a rescue operation of people in distress at sea. The program was based upon a macroscopic model. As part of the development, a Delphi session was arranged with participation from helicopter pilots and MOB boat personnel, who were questioned about time requirements to detect and rescue people in distress at sea under varying weather conditions.

The program contains default data on survival times as function of sea temperature and clothing.

The user of the program has to specify number of people in distress at sea, the rescue resources available and their arrival and shuttle times, as well as the environmental conditions. The program simulates the time development of the rescue operation. Picked up people may be alive or dead, depending on how long time they have been in the sea. As there are a few probabilistic variables, the program performs Monte Carlo simulations, but few replications are required.

It will not be meaningful to perform rescue simulations for people in distress at sea in a "representative environment" as defined in a FSA.

## 7 RISK ACCEPTANCE CRITERIA

Risk acceptance criteria usually address two types of concerns. One concern relates to the maximum

acceptable risk that it is ethically acceptable to expose a group of people to. The corresponding requirement must be explicitly stated, e.g. by a maximum allowable average number of fatalities per year.

The other concern is that if it is possible to reduce the risk in a cost efficient way that should be done. This refers to the so-called "As Low As Reasonably Practicable" (ALARP Principle). In order to perform cost-benefit analyses, the limiting acceptable cost in order to avert a fatality may be defined. The soundest and most feasible proposal (Skjong, 1998) may roughly be said to originate from the following logic: Quality of life in a society should be optimized. If a minor amount of resources are spent on health and safety, the inhabitants may live a short life in luxury. If, however, a large amount of resources are spent on health and safety, there will not be much left for consumption, and the inhabitants will live a long life in poverty. Obviously there exist an optimum quality of life in between these extremities, and the maximum amount of money to be used to avert a fatality can be assessed as function of the BNP in the society. It follows that it will be justified to use less money to avert a fatality in poor countries than in rich ones. In rich European countries, it was shown that something like 4 million Euro should be used to avert a fatality in order to optimize quality of life.

The above approach is feasible both within a QRA and FSA.

## 8 EVALUATIONS

In the following, the potential of QRA to serve as a tool for enhancing passenger ship safety is considered, and some of the main differences between a QRA and a FSA are evaluated. In this respect, focus is placed on the following three issues:

- Safety involvement and resources
- Level of detail in the analyses
- Assumptions of average or representative values

### 8.1 Feasibility of passenger ship QRA

In the paper it has been shown that there exists plentiful tools for addressing passenger ship safety in a realistic manner in a QRA. A lot of relevant experience is already available in the offshore sector. What may be lacking, however, is that operational errors are included with the same realism. In the offshore industry there has been performed a lot of work to achieve this, and inclusion of human error analyses is rather a question about acceptable uncertainties in the estimates than on available methods.

Prediction of human error is usually performed at a microscopic level, addressing detailed design and

applied operational procedures. The FSA may not be feasible for this purpose.

### 8.2 Safety involvement and resources

During the design of a passenger ship, the designers and representatives from the ship owner spend most of their safety related efforts on securing that specific regulation requirements are complied with. If they instead had focused on prevention and mitigation of concrete accidents, and combined this effort with their detailed knowledge of the ship being designed, this would have given a very high contribution to the efforts towards safer ships. This is what has happened in the offshore sector, where engineering teams are strongly involved with QRA issues.

Similar concerns played an important role when the investigation committee for the disaster at the UK offshore installation Piper Alpha recommended to transfer the safety responsibility from the DOT, who had implemented a safety regime for offshore installations similar to that for ships, to the HSE who was familiar with QRAs and goal setting requirements.

Development of good specific regulations on a high level is a very difficult or even impossible task. The regulation makers have to address a more or less inhomogeneous group of ship and expected future development as well. In addition, the development tends to be biased because representatives from different countries try to promote concerns relating to the competitiveness of their national fleet. Goal setting requirements on a high level in combination with a QRA related legislative regime is the obvious response to these difficulties.

### 8.3 Level of detail

A QRA addresses safety issues at a relatively high level. However, the methodology also includes features to capture detailed safety problems as explained in the following.

Reliability and vulnerability analyses of safety critical systems address properties of these systems at a detailed level. The results of these analyses are usually input to Event Trees in a QRA. Hence, the reliability and vulnerability standard of these systems are reflected in the outcome of a QRA.

The Hazop has the potential to identify detailed safety problems in the area being analyzed. Once identified, the problems may be resolved or alternatively accounted for in the QRA.

Hence, the QRA do possess properties to address detailed issues. In addition, it is usual to perform QRAs on the assumption that detailed safety regulations and standards are adhered to. A FSA, however, almost completely lacks the capability to account for

detailed properties, as it addresses an average ship in a representative environment.

### 8.4 Assumptions of average or representative values

The FSA addresses an average ship in a representative environment. In relation to risk assessment, this is an obvious oversimplification. Accidents are often related to unusual properties and extreme conditions. Taking Titanic and Estonia as examples, many people lost their lives because the seawater temperature was very low. If these accidents had been analyzed beforehand based on an assumption of representative environmental conditions (as in the FSA), the outcome of these analyses would have shown far less dramatic consequences than what occurred in reality. Hence, assumptions of average or representative conditions in a FSA may in some cases introduce severe errors.

## 9 CONCLUSIONS

The conclusion is that a legislative regime based on QRAs may be a powerful measure in enhancing passenger vessel safety. There exist a set of comprehensive and realistic tools for addressing relevant safety issues in QRAs.

The FSA proposed by IMO has limited potential because it is not concrete in addressing a particular vessel. Hence, a FSA may not be considered as an alternative to a QRA, but rather a supplementary aid to improve prescriptive regulations.

## REFERENCES

- Bles, W. & Boer, CL. 2000. *Design Features: Effect of ship listing on mustering speed. MEP Design report, WP2b.*
- Canter, D. 1980. *Fire and Human Behaviour.* John Wiley & Sons, Ltd.
- Haugen, S. 1998. *An overview over ship-platform collision risk modelling*, in Ed. C Guedes Soares, A.A. Balkema, 1998. *Risk and Reliability in Marine Technology.*
- Haugen, S. 1997. *Ship-Platform Collision Risk Analysis*, ESREL, Lisboa 1997.
- Haugen, S. 1993. *Effect of Platforms in Shipping Lanes*, COLLIDE seminar, Aberdeen, June 1993.
- IMO, 1974. *Resolutions and Other Decision (Resolutions 259-314).* Assembly, Eight Session 1973.
- Marin Accident Report, 1982. *Capsizing and Sinking of the U.S. Mobile Offshore Drilling Unit OCEAN RANGER, off the East Cost of Canada 166 Nautic Miles East of St. John's, New Foundland.*
- Paulsen, T. 1995. *Evaluation of Simulation Models of Evacuation from Complex Spaces.* SINTEF report no. STF75 A95020.
- Solem, R. 1987. *Modelling and Simulation of an Offshore Evacuation and Rescue Operation.* IMACS-International

- Symposium on AI, Expert Systems and Languages in Modelling and Simulations. Barcelona, Spain.
- Soma, H. 2001. *Computer Simulation of Passenger Ship Evacuation*. ESREL 2001 in Torin.
- Soma, H. 1998. *How to Account for Working Environmental Conditions in QRAs*. OMAE 1998 in Lisbon.
- Soma, H. 1996. *Validation of Egress Simulation Programs*. OMAE 1996 in Florence.
- Soma, H. 1995. *Computer Simulation for Optimisation of Offshore Platform Evacuation*. OMAE 1995 in København.
- Skjong, R. 1998. *Societal Indicators and Risk Acceptance*. OMAE 98.
- Technica, 1983. *Risk Assessment of Emergency Evacuation from Offshore Installations*.
- The Scandinavian Star Investigation Board, 1991. *The Scandinavian Star Disaster*. NOU 1991.
- Tsychkova, E. *Influence of Waves and Ship Motions on Safe Evacuation of Passenger Ships*. Licentiate Thesis, Royal Institute of Technology, Stockholm.
- Vinnem, J. & Haugen S. 1987. "Risk .....
- Vinnem & Haugen, 1987. "Risk Assessment of Buoyancy Loss (RABL) – Introduction to Analytical Approach", International Conference on Mobile Offshore Structures, London, Sept. 1987.
- Wang, J. 2001. *The current status and further aspects in formal ship safety assessment*. Safety Science 38 (2001).

## Measuring the safety standard of organizations

T. Soma

*Norwegian University of Science and Technology, Department of Marine Technology, Trondheim, Norway*

**ABSTRACT:** This paper describes a new general method for measuring the safety standard of an organization. It is assumed that a high safety standard is a result of systematic management and control. The principal idea is therefore to focus on the systematic pattern of safety performance variables in the measurement calculations, which is in sharp contrast to common measuring techniques. The paper focuses on description of the principal idea and some examples for calculations. The most important finding is the methods' efficiency in measuring the safety culture maturity of seven shipping companies. The method uses a database of nearly 3000 responses on the Ship Management Attitude Questionnaire (SMAQ) held by Risø National Laboratories. The analysis shows that the maturity of the safety culture can describe about 50% of the variation in an accident performance indicator and more than 60% of the variation of a Port State Control performance indicator.

### 1 INTRODUCTION

The term substandard and blue chip organizations have become frequently used labels of companies being respectively very poor and extremely good in safety issues. It has also become common practice to conceptually distinguish between an organizations' experienced safety performance and its safety standard, which focus on its resistance against accidents. This shift in focus is caused by a need for more efficient prevention of losses. The safety standard of an organization is commonly measured through rating schemes or similar methods. This paper describes a new general method for measuring the safety standard of an organization. It is assumed that a high safety standard is a result of systematic management and control. The principal idea is therefore to focus on the systematic pattern of safety performance variables in the measurement calculations. Focus on pattern is in sharp contrast to common measuring techniques like ranking scheme, regression analysis and factor scores, which all treat individual variables independent of each other. Even artificial neural networks, which is commonly used in pattern recognition, does not efficiently capture the dependency between pairs of variables (Soma & Kristiansen, 2001). However, most conceptual models used in safety management, accident investigation and human error and reliability analysis agree upon that there is a dependency between some distal core safety factors and the performance variables commonly

used in measuring techniques e.g. incidents, audit and inspection findings.

Several authors have realized that we have serious measuring problems within safety management, safety research and safety analysis. The uncertainties involved in measuring safety performance. There has been a shift towards more proactive methods attempting to measure safety standard of an organization. Incident happens too rare within an organization to be a basis for common statistical inference. It is also realized that the statistics drawn from investigation reports are unreliable due to subjective interpretations and questionable scope (Pedrali et al., 2002) (Wagenaar et al., 1997) (Reason, 1987). Hence the importance of near miss reporting has been emphasized. The reporting frequency of near-misses is however too unreliable to form a basis for evaluation of performance (Scaaf et al., 1991). Expert judgment is assumed to have a large measuring potential, but has also been staggered due to lacking reliability (Skjong & Wentworth). We have diagnosed a number of accidents as being a result of poor safety culture. Therefore the importance of a mature safety culture is stressed. No technique has however yet been able to measure the maturity of an organizations' safety culture (Cox & Flin, 1998) (Sorensen, 2002). We know that the majority of the accidents are caused by operator errors (Wagenaar & Groeneweg, 1987). Quantitative analyses of human factors have probably stronger influence on safety through their ensuing discussions and disputes (Fragola, 2000) (Hollnagel, 2000) than

their quantitative results. Within maritime transport rating techniques has become popular for targeting and screening purposes. This reaction on accidents like Erika is unlikely to have any effect over longer periods as they only emphasize on the present general characteristics of substandard managers and not their essential safety management problems. We also know that the techniques fail to pinpoint catastrophe vessels such as Estonia and Exxon Valdez.

Despite of the problems, the situation is not too pessimistic. The public focus on safety has forced more safety information to be generated, collected and made public available. Today safety inspection findings, accident history and ship characteristics are available on the Internet even for individual ships. When we still are unsatisfied with the applied quantitative safety measurements it might seem reasonable to take two steps back and critically consider the applied measuring techniques. This study has explored the potential of using an alternative measuring principle. The alternative approach seems to be valid and extremely advantageous in measuring safety culture maturity.

## 2 PRINCIPAL IDEA

Commonly used quantitative approaches apply a linear ( $Y = w_i \cdot x_i$ ) model for evaluation of the safety characteristic. These models treat the variables ( $x_i$ ) independent. In a rating scheme like International Marine Safety Rating System (DNV, 1995) the weights ( $w_i$ ) may be estimated through approaches like statistical inference or expert judgment. By regression analysis the weights ( $w$ ) are typically optimized on the basis of minimal least squared sum of the residuals. In factor analysis the scores on each factor is a weighted sum of responded values within each principal factor. Also neural networks apply independent calculations of the input ( $x_i$ ).

The lack of consistency related to the independent evaluation of variables may be described through an example. The German magazine ADAC Motorwelt (ADAC, 1998–2001) performs an annual safety assessment of ro-ro passenger ferries sailing in European waters. This assessment is carried out through a six-item rating scheme. Typical items are the quality of Safety Management ( $X_1$ ), the quality of the Emergency Equipment ( $X_2$ ) and the quality of the Fire Protection system ( $X_3$ ). Imagine two ships A and B with the following scores. Ship A is judged to have an extremely poor quality of safety management, but has extremely good quality of the emergency equipment. Ship B on the contrary, is judged to have extremely good safety management, but defective emergency equipment. Both ships have a satisfying fire protection. What is then the likely safety standard of these

two ships? Lay people might consider the three items to have equal importance ( $w_1 = w_2 = w_3$ ), whereas more experienced safety analysts may consider safety management to have higher importance ( $w_1 > w_2, w_1 > w_3$ ). Both evaluations however, miss the crucial fact that neither of the ships demonstrates control of safety management. Because the efficiency of the Emergency Equipment is highly dependent of the quality of the Safety Management is might seem unreasonable to assess these factors independently. Despite ship B is judged to have extremely good Safety Management the contradicting scores for Emergency Equipment is not reflected in the obtained for safety management.

Another example can be drawn from the world fleet accident statistics. A scatter diagram of the world fleets loss ratio due to collisions versus wreckings is showed in Figure 1 (Lloyd's Register of Shipping, 1970 to 1993). Letting each year from 1939 to 1996 (excluding 2. World War figures) be one point in a scatter diagram, the relation between the two loss categories can be computed. The diagram shows that there were no linear relationships between these events prior to 1971. In the 1970s, after about 20 years of existence, the International Maritime Organization (IMO) started to demonstrate some regulative power. Among other achievement it developed a set of traffic regulations for prevention of collisions named COLREG. It is evident that the accident rates decreased after implementation. However, most importantly, the dependency between these two incidents raised from zero to very high (0.90). Navigation has traditionally been very focused on keeping control of the ships' position relative to land. The new regulations may have reduced this bias in focus, causing the same mechanisms to influence on these two aspects of navigational control.

This example indicates that there are two ways of measuring improvements in risk control. The

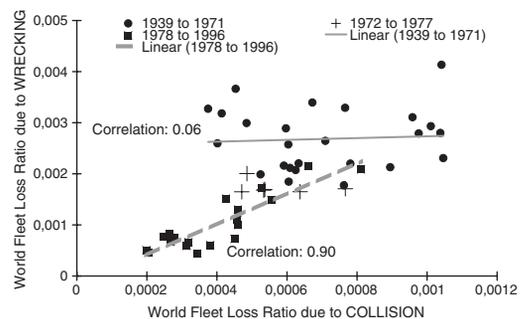


Figure 1. Scatter diagram of the world fleet loss ratio due to Collision and Wrecking (Grounding, Stranding and Contact) before, during and after COLREG 72 implementation.

common technique uses independent absolute values, while the dependency between the values may provide additional knowledge, namely that they are controlled by a joint core factor. The objective of this study is therefore to develop and validate a method taking advantage of the dependencies between safety variables. In order to develop a measuring technique that also evaluates the dependency between the variables a deeper understanding of organizational safety is necessary.

### 3 CONCEPTUAL BASIS

Reason (1997) presents a framework for understanding organizational accidents. His models have one important similarity with the large majority of models used within safety management, accident investigation and human error and reliability analysis. This common characteristic is the dependency between the incident chain of events, and a more basic element of the organizational system. A survey of more than 30 conceptual models (Soma, to be published a) shows that the root casual factors in these models are either Organizational Factors or Culture, External or Social Environment, Lack of Control, Upper Management, Working Conditions, Statements of Goals and Objectives etc. The variation in the definition of these Core Safety Factors (CSF) may be related to the specific purpose of the various models. However, the consensus of the idea that there is one, or at least a few, CSFs that influence or determines the safety performance of the lower level of the organization is interesting in itself. If this understanding of organizational safety is correct, these CFSs should influence the lower level of the organization and even the unsafe acts (Figure 2).

Despite the dependency of the CFSs seems to be accepted by most professional domains involved in safety management, research and analysis it is not reflected in the commonly applied measuring techniques. According to the graph outlined in Figure 2 the

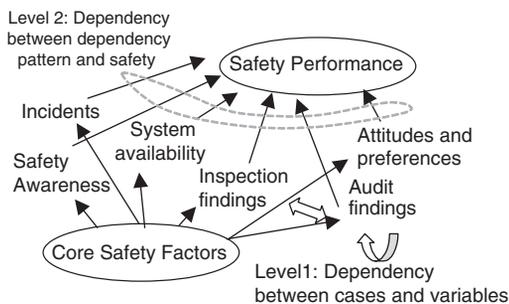


Figure 2. Conceptual model for safety influence.

organizations' CSFs influence the safety variables used in measuring techniques. In principle an organization having a high safety standard should have strong dependencies between the CSFs and the variables.

Strong dependencies are therefore an indication of control. On the contrary, if the organization is substandard the CSFs are weak. Therefore is the safety level of substandard shipping organizations more dependent of other governing ship characteristics like its age, type or size and external factors like classification society or flag of registration. Figure 3 illustrates the necessary knowledge for reasoning with patterns. The patterns represent the dependency between the considered variables. For each pattern we need some logical explanation to interpret the patterns' topography.

### 4 MEASUREMENT AND LOGICS

When developing a measurement tool for safety standard it is extremely important to have some basic understanding of measurement theory. This chapter describes general measuring principles used in item analysis and neural networks. The two last sections describe how the new methods' relationship to this theory.

#### 4.1 Theory of measurement

Successful questionnaires or rating schemes can be developed through selection of suitable items, variables and scales. For inspections the formal requirements are the basis for selection of items, variables and questions while the scales are typically dichotomous (compliance or not). In an analysis each questionnaire response, inspection result or audit finding is considered as a case (Table 1).

In order to optimize the set of selected items, variables and values it is common to carry out an item and discrimination analysis (Anastasi & Urbina, 1997). In this way the most suitable items can be selected and

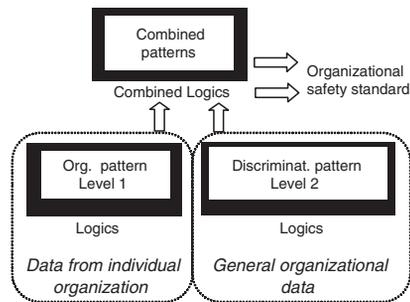


Figure 3. Outline of method.

Table 1. Examples of cases, variables and values.

Cases	Measurement variable	Scale	Core Safety Factor
Different time series	Safety inspections	Compliance or not	Compliance to requirements
Different respondents	Questionnaire items/variables	Degree of agreement	Safety culture
Different time series	Audit findings	Practice according to plans	Safety practice/plans
Different years	System availability	Operates or not	Maintenance management
	Incidents	Happens or not	Safety management

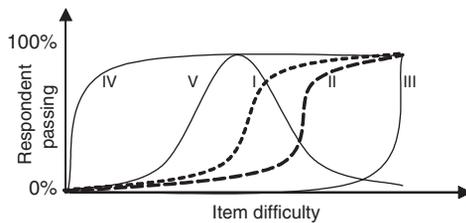


Figure 4. Examples of item discrimination functions.

their scales can be optimized for the measuring purpose. Artificial neural networks also use this, although this process is automatically learned through network training. Both in item analysis and in neural network sigmoid functions (I and II in Figure 4) are considered to be powerful for this purpose. These continuous functions effectively divide the low from the high (passing) values. The most effective way to measure the performance through a test is to select items that only 50% of the respondents pass. However, if we want to disguise the very few best or the very few worst from the group other functions may be effective. The convex and concave exponential functions (III and IV) are for instance used to distinguish the few worst and the few very best respectively. After collection of data a measurement tool has to be validated to confirm it measures what it is supposed to do. Also the reliability has to be considered in order to assess the how accurate the tool is.

There are several ways to quantify indicators of the safety standard of an organization. The number of deficiencies of a safety inspection, the number of non-conformities identified through a safety audit or the number of fulfilled items of a check-list are some examples. In contrast to incidents these indicators are a result of a more or less formalized test with a specific

and often restricted purpose. Therefore, the obtained correlation coefficients from such data also include the reliability and the different scope of these approaches. The correlation coefficients should therefore be interpreted with care.

Two indicators are used to validate the results of this study (Soma, in review). One indicator is based on severe accidents collected in a Lloyds Register database. The other is based on Port State Control findings collected in Paris MOU's database and the Equasis database. The PSC regime is a measure to counteract the relaxed attitude towards fulfillment of international regulations of some flag states. Both indicators provides the likelihood of a ships' safety standard to be among the 25% highest quality, the 50% average standard or the 25% most substandard vessels of the world fleet. These figures are combined into a single safety performance measure  $P_d$ .  $P_d$  has values from  $-100$  to  $100$  where  $100$  reflects a probability of one for being among the 25% highest standard vessels and vice versa.

#### 4.2 Linear dependencies

In theory dependencies can take many forms. Linear dependencies are considered most feasible when describing the dependency between variables and the computation is straightforward. The measuring method outlined in this paper uses a two-stage dependency calculation. The first stage is to calculate the organization's pattern of dependencies between variables. This is the first level in Figure 2. This pattern of dependency has certain linear characteristics to variables of similar scope and similar influence from the CSFs. The next stage is to assess the safety effects of this dependency pattern. Therefore the similarity between the organizations' dependency pattern and a pre-established norm pattern is calculated. This norm pattern reflects how efficient CSFs should influence on safety variables. This similarity is also expressed through a linear model. The dependency to safety performance may however be non-linear.

The correlation coefficient expresses the degree of linear correspondence, or relationship between the values of two variables. Because the correlation coefficient varies from  $-1$  to  $1$ , it can be used to compare the strength of the linear relationship between the variables. Two variables with a correlation of either  $-1.0$  or  $+1.0$  are highly correlated because knowledge of one variable provides precise knowledge of the other. Independent variables have a correlation of zero. There are several ways to calculate the correlation. The two most common types are the Pearson's correlation,  $\rho_p$ , for variables having values on an interval or ratio scale and Spearman's correlation,  $\rho_s$ , for ordinal value. The correlation coefficients are

Table 2. Example of dependencies between variables.

	Incidents			Inspections			Safety audit	
	Oil Pollution	Property loss freq.	Process availab.	Vetting	PSC	In house	External	Internal
LTIF	-0.30	0.22	0.30	-0.04	-0.01	-0.69	0.88	0.94
Oil pollution incident		0.01	-0.37	0.48	0.01	-0.07	-0.75	-0.78
Property loss frequ.			0.04	0.55	0.21	-0.38	0.17	0.31
Process availability				-0.68	-0.64	-0.26	-0.02	0.11
Vetting					0.75	0.61	-0.12	0.22
PSC						0.30	-0.01	0.04
External audit								0.97

defined as:

$$\rho_p = \frac{\sigma_{xy}}{\sigma_x \cdot \sigma_y} \tag{1}$$

$$\rho_s = 1 - \frac{6 \cdot \sum d^2}{n \cdot (n^2 - 1)} \tag{2}$$

where:

- $\sigma_{xy}$  = Covariance of the variables x and y
- $\sigma_{x,y}$  = Standard deviation of the variables x and y respectively
- n = Number of data points
- d = Difference between the most discriminating ranking of the variables when each have a sum of  $n(n + 1)/2$

An example of the estimated linear dependencies between safety variables for a large tanker company is outlined in Table 2. The cases are taken from different ship management departments and years. The accident history and port state control findings for this specific company indicates that its fleet is among the worlds 25% highest safety standard.

Table 2 is an example of the dependency pattern developed through the first stage of the measuring technique (level 1 in Figure 2). The table shows that the incidents related to operational aspects (LTI and oil pollution) are dependent of the number of audit non-conformities. The incidents related to more technical aspects (Process availability) are more dependent of the number of inspection findings. The norm pattern, which could be used to assess if this organization is a good safety performer or not, is however not yet developed (Level 2 in Figure 2). The similarity or correlation between a norm pattern would provide estimates of the companies' absolute safety standard. This second stage is later carried out for incident patterns and safety culture survey results. More detailed assessments of the individual dependencies are however considered first. The objective is now to start the next

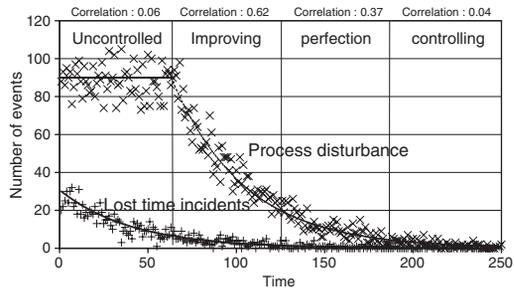


Figure 5. Principles of incident correlations.

$\sigma_p$  LOGICS

- Low at least one uncontrolled OR at least one controlled
- Moderate one under perfection AND one under improvement
- High both under improvement

dependency level. In such an analysis knowledge of how the dependencies are for high standard and sub-standard organizations has to be developed.

### 4.3 Incident correlations

Within the ship management as for aviation and train transport, offshore and land based industry there is today regulative requirements for continuous safety improvement activities. A stochastic process governs the occurrence of incidents. It is for instance common to describe the occurrence of accidents through a Poisson process. A Poisson process can be described as a counting process where the occurrence accidents is dependent of an accident rate,  $\lambda$ , and a time window. Within an organization there are several stochastic processes that may be of relevance for the safety. A graph demonstrating the relationships between two incident processes, namely Lost Time Incidents and Process disturbance incidents is shown in Figure 5.

The first 63 weeks the safety management is only involved in reducing the lost time incidents. Consequently, the process disturbances are independent

of the CSFs and also independent of the LTI rate. However, because the organization has no control over process incidents it is not having a satisfactory safety management. After 63 weeks, however, the safety management's scope is increased and a risk control measure is implemented to also handle the process disturbances. From this stage both risks are under improvement. This results in higher correlation between the time series. After a period the process disturbance rate has been reduced considerable and they experience weeks with no events of either kind. The correlation is now reduced again because the time window is too small relative to the event rate ( $\lambda \cdot t < 3$ ). Hence both the uncontrolled and controlled states have low correlation.

A relatively new discriminating function used in neural network analysis is the bell-shaped function (V in Figure 2). When applying a bell-shaped function only the average pass the item. On a single item this may seem ridiculous because it do not distinguish the best from the worst. However, in combination with other items, it is possible to distinguish between the three groups instead of two. Experience in neural networks show that this is more effective because fewer neurons (items) are required. From figure 5 it can be seen that the correlation between incidents have a similar nature. Both the most substandard and the highest standard level have in fact correlation coefficient of zero.

#### 4.4 Analysis of CSF influence

The dependency between the CSFs and the safety level illustrated in Figure 2 could be assessed through another approach. As already described a substandard organization is assumed to have weak CSFs. Therefore the safety performance are dependent of other factors, like the age of the ship. In order to assess this hypothesis a sample of 1700 ships selected randomly from the fleet having class society within the International Association of Classification Societies (IACS) covering more than 90% of the world tonnage. These ships were assessed according to their PSC findings.

Table 3 shows that there is a significant reduction in correlation for the most quality operators. Especially the correlations between the PSC indicator and age and ship size are significantly lower for the 25% best. Also the correlation between the indicator and the selected flag and Protection and Indemnity Insurer is lower for the most quality vessels. This means that factors like the ships age, flag and size may be suitable indicators for identification of the most substandard, but that these factors have little potential for identification of the best ships. More precisely, the commonly used age factor is statistical significant because it is relevant for 75% of the fleet (average and substandard). To assess whether the

Table 3. Correlation between ship characteristics and PSC performance (Soma, to be published b).

PSC Performance	25% best	50% average	25% worst
Gross Tonnage	-0.01	0.20	0.16
Ship type	0.02	0.01	-0.04
Age of ship	0.03	-0.21	-0.17
Flag	-0.04	0.05	0.09
Classification Society	-0.05	0.04	0.06
P&I	0.00	0.05	0.06
External membership	-0.06	0.06	0.07
Sum of absolute values	0.21	0.62	0.64

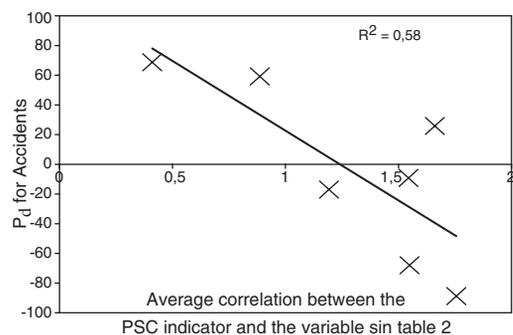


Figure 6. Relationship between the sum of absolute correlation values and the PSC indicator.

correlations described in table 6 also can be an indicator for individual companies seven organizations are selected for assessment. The sum of the absolute correlation values for the companies and their PSC indicator score are presented in Figure 6. The scatter plot indicates that the dependency between the ship characteristics and the PSC indicator may be a suitable indicator for estimating the companies CSF quality.

## 5 INCIDENT CORRELATIONS REASONING

The incident statistics for the fleets of twelve different flags of registration is presented to describe the measuring principle.

The numbers is the average correlation between the time series from 1970 to 1996 for the flags ratio of losses due to collision, foundering, wrecking and fire. A high correlation indicates that both flags are under improvement (Figure 5). A low correlation is as shown earlier an indication of at least one is uncontrolled or both controlled. In order to perform a complete evaluation the flags have to be discriminated. For this purpose the correlation between the accepted safety resolutions adopted by the IMO is used. High

values indicate that the pair of flags has accepted a similar pattern of resolutions.

The complete ranking of the flags is then the correlation between the patterns of the two matrices (Table 6). This value is a measure of the flags' safety performance. Negative values indicate that the flags having similar regulative pattern has low incident correlations and those with moderate or high incident correlations have dissimilar regulative patterns. According to the logical tables this indicates a flag within a Perfecting or Controlling phase (Figure 5). Similar argumentation can be used to identify those having positive values as being under Improvement. The estimated performance measurements are in correspondence with other performance measures. The correlation with the Flag State Conformity Index (FLASCI) Score (Alderton, 2001) is 0.82 and the correlation with the flags total loss ratio for 1998–2001 is 0.61.

Table 4. Incident dependencies.

	Cy	Gr	Ja	Li	No	No	Pa	SK	UK	US	De	Sp
Cyprus	0.8	0.5	0.3	0.4	0.2	0.4	0.3	0.4	0.5	0.3	0.3	0.3
Greece	0.5	0.8	0.3	0.2	0.3	0.4	0.4	0.6	0.4	0.2	0.5	0.5
Japan	0.3	0.3	0.8	0.5	0.4	0.5	0.4	0.4	0.5	0.5	0.5	0.5
Liberia	0.4	0.5	0.5	0.8	0.3	0.3	0.4	0.4	0.4	0.3	0.7	0.7
Netherlands	0.2	0.3	0.3	0.3	0.8	0.5	0.3	0.3	0.3	0.5	0.7	0.7
Norway	0.4	0.2	0.4	0.3	0.3	0.8	0.2	0.2	0.4	0.5	0.6	0.2
Panama	0.4	0.4	0.3	0.3	0.3	0.2	0.8	0.4	0.4	0.8	0.4	0.4
South Korea	0.3	0.4	0.4	0.3	0.3	0.3	0.3	0.8	0.3	0.5	0.3	0.4
United Kingdom	0.4	0.3	0.4	0.3	0.3	0.4	0.4	0.3	0.8	0.4	0.2	0.2
United States	0.3	0.3	0.4	0.3	0.3	0.3	0.4	0.3	0.4	0.8	0.6	0.4
Denmark	0.3	0.2	0.3	0.3	0.3	0.3	0.3	0.3	0.4	0.3	0.8	0.4
Spain	0.3	0.5	0.5	0.7	0.4	0.2	0.4	0.4	0.3	0.4	0.4	0.8
Average	0.4	0.4	0.3	0.4	0.6	0.4	0.4	0.4	0.5	0.4	0.4	0.4

$\alpha_p$  LOGICS

Low	Dissimilar regulative pattern
Moderate	Some similarities in regulative pattern
High	Similar regulative patterns

Table 5. Regulative dependencies.

	Cy	Gr	Ja	Li	No	No	Pa	SK	UK	US	De	Sp
Cyprus	0.5	0.5	0.3	0.5	0.5	0.3	0.5	0.3	0.4	0.4	0.3	0.3
Greece	0.5	0.8	0.3	0.4	0.4	0.6	0.6	0.2	0.5	0.4	0.3	0.3
Japan	0.3	0.3	0.8	0.5	0.4	0.5	0.4	0.2	0.3	0.2	0.3	0.3
Liberia	0.5	0.3	0.4	0.8	0.3	0.2	0.3	0.2	0.3	0.1	0.1	0.2
Netherlands	0.3	0.4	0.3	0.3	0.2	0.6	0.2	0.3	0.1	0.4	0.4	0.4
Norway	0.5	0.4	0.4	0.3	0.2	0.4	0.4	0.0	0.4	0.4	0.4	0.4
Panama	0.5	0.5	0.3	0.4	0.5	0.4	0.8	0.3	0.3	0.4	0.4	0.4
South Korea	0.3	0.3	0.3	0.3	0.2	0.4	0.3	0.8	0.5	0.5	0.2	0.4
United Kingdom	0.3	0.2	0.2	0.3	0.3	0.3	0.3	0.3	0.1	0.5	0.1	0.1
United States	0.4	0.5	0.2	0.3	0.1	0.4	0.4	0.5	0.1	0.3	0.3	0.3
Denmark	0.4	0.4	0.3	0.2	0.1	0.4	0.4	0.2	0.3	0.3	0.8	0.1
Spain	0.3	0.3	0.3	0.3	0.2	0.4	0.4	0.3	0.1	0.3	0.1	0.1
Average	0.5	0.4	0.4	0.4	0.3	0.4	0.4	0.4	0.2	0.3	0.3	0.3

$\alpha_p$  LOGICS (table 5)

Negative	Low $\alpha_p$ - High $\alpha_i$ , AND Low $\alpha_p$ - High $\alpha_i$
Positive	High $\alpha_p$ - High $\alpha_i$ , AND Low $\alpha_p$ - Low $\alpha_i$

Table 6. Correlation between dependency patterns.

Cyprus	Greece	Japan	Liberia	Netherl.	Norway	Panama	S. Korea	UK	US	Denmark	Spain
0,67	-0,04	0,27	0,29	-0,45	-0,29	0,21	0,19	-0,15	-0,56	-0,21	0,33

## 6 SAFETY CULTURE PATTERNS

There is a range of definitions of safety culture (Cox & Flin, 1998) (Sorensen, 2002). Their common characteristic is the involvement of a system or pattern of believes, values, symbols, attitudes, etc. that influence the way the members of the culture act and work with safety. The common attempt to measure safety culture is to perform a questionnaire survey. The responses are analyzed in a factor analysis to group correlated items into groups called factors, dimensions or principal components. If the analysis includes several groups, ships, departments or companies the score on each factor describes the cultural variation between these groups. Several authors (Zohar, 1980) (Itoh & Andersen, 1999) have attempted to quantify the relationship to the companies safety level but only with marginal success managed to quantify such factors (Cox & Flin, 1998) (Sorensen, 2002). The trend in fighting this problem seems to be towards combining factors and conceptual models (Cooper, 2002) (Alistair, Cox, Amparo & Tomas, 1998). All these attempts seem to ignore the fact that safety culture only includes the common patterns of safety attitudes in contrast to individual safety attitudes independent of the others. In the majority of the approaches the scores of each factor are added together as a weighted sum. Hence, in principle, adding more individuals who give positive responses to the questionnaire items improves the score independent of the cultural influence. When using a questionnaire survey to measure safety culture we assume that the cultural pattern can be reflected into the way the respondents answer it.

$\alpha_p$	LOGICS
Low	Non-common perception of at least one variable OR independent variables
Moderate	OR neutral responses to at least one variable
High	Dependent variables AND portions of common perceptions
	Common perception of the variables AND dependent variables
	Strongly Disagree
	Slightly Disagree
	Neutral
	Slightly Agree
	Strongly Agree

### 6.1 Safety training is important

At the most basic level the pattern can be represented by the correlation between the variables in the questionnaire as a level 1 in Figure 2. There is established some experience that makes us able to interpret the obtained correlation coefficients. Zohar (1980) has proved that high safety level imply that the respondents answer higher level of agreement on safety related questions compared to organizations having lower safety level. In a measuring context this is advantageous because values far from the average increase the value of the correlations coefficient. It should be remembered that it is common to design both positive and negative questions. The item describe above is therefore followed up by a negatively stated question e.g. *Training is not very important*. Therefore, according to Zohar's findings organizations having high safety standard should obtain higher correlations between dependent variables.

A recent study on safety attitudes of four shipping companies having the same national culture has found that the organizations having lower safety performance not only give responses of lower absolute values but answer in a more neutral manner (Soma, to be published c). Hence, in principle when asked if safety training is important the respondents of a sub-standard organization may not only answer lower agreement but has also a tendency to be more neutral. A high portion of natural responses causes the correlation coefficient to be low because the difference between the individual scores and the average value is small.

The correlation matrix alone does however not represent a measurement value because there is not any norm to measure it against (Level 2 Figure 2). Therefore a norm is developed based on inter-organizational correlation of the correlation matrix. This norm represents to which degree the pattern of attitudes towards safety issues correlates with other organizations. Some might disagree with this norm because they believe that there are several patterns describing a mature safety culture. That might be theoretically true, but experience show that the patterns drawn from the questionnaire surveys of blueprint organizations are similar for all domains. Safety commitment is for instance measured to be a significant factor within aviation, railway, nuclear-process- and offshore industry, medical institutions, and also within the maritime domain. Similarly are factors like communication, training etc. general factors. It would be methodological impossible to identify these in several companies, nor domains, if the correlation matrices of the various companies or domains were different.

To quantify the suitability of the technique the dependency between 39 SMAQ variables were expressed by their correlation matrix. The obtained scores are expressed by the average correlation

between the matrices as shown on the abscissa of Figures 7 and 8. The critical 95% confidence level of the correlation coefficient is 0.316. The ordinal values of Figures 7 and 8 are the accident and PSC indicator respectively. As indicated in Figure 7, the safety culture indicator can explain 53% of the variance in the accident statistic indicator. The Pearson correlation between the two measures is 0.73. Figure 8 shows that the dependency between the PSC indicator and the safety culture indicator is even higher. The inter-organizational safety culture score can explain 65% of the variance in the PSC indicator. The Pearson correlation is significantly 0.81. The sensitivity of national cultures is also calculated. The standard deviation of the score due to national variation was estimated to be 0.04 and insignificant variations with a 95% level confidence.

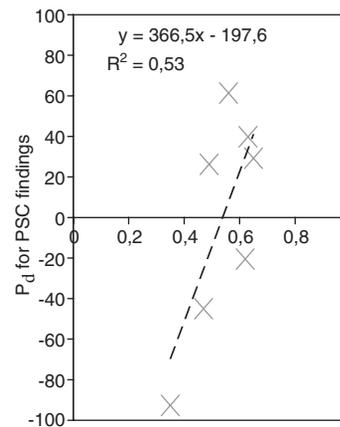


Figure 7. Estimated linear dependency between accident statistics indicator and safety culture indicator.

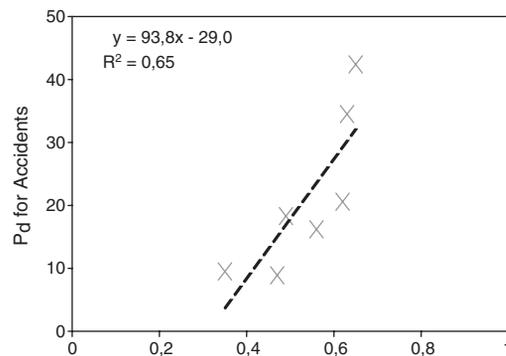


Figure 8. Estimated linear dependency between PSC indicator and safety culture indicator.

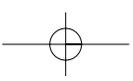
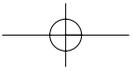
## 7 CONCLUSIONS

This study has presented and validated a new general safety measuring principle. In contrast to existing techniques, which treat the variables independently, the new approach focuses on the pattern of dependencies between variables. In addition to valid quantifications, it is stressed that the method is more in line with the conceptual understanding of organizational safety as well as definitions of safety culture.

It is believed that this method can be used as an alternative to existing safety standard measuring techniques. The technique requires several organizations to be measured on an identical scheme. In theory this scheme may contain any safety related variables. It is, however, especially fit for measuring safety culture maturity and aspects of safety management within organizations.

## REFERENCES

- ADAC, 1998–2001, *ADAC Motorwelt*, no. 6 (each year), B2706E, München
- Alderton, 2001, T., Winchester, N., *Flag state conformance: a comparative global analysis*, Globalisierung und seefahrt conference, University of Bremen, June
- Alistair, C., Cox, S., Amparo, O., Tomas, J.M., 1998, Modelling safety climate in the prediction of levels of safety activity, *Work and stress*, vol. 12, no. 3
- Anastasi, A., Urbina, S., 1997, *Psychological Testing*, Prentice Hall, New Jersey
- Cooper, D., 2002, Safety Culture; A model for understanding & quantifying a difficult concept, *Professional safety*, June, 2002
- Cox, S., Flin, R., 1998, Safety culture: philosopher's stone or man of straw? *Work and stress*, vol. 12, no. 3
- DNV, 1995, *International Marine Safety Rating System Working copy*, International loss control institute, Atlanta, 1995
- Itoh, K., Andersen, H., 1999, *Motivation and Morale of Night Train Drivers Correlated with Accident Rates*, CAES' 99: International Conference on Computer – Aided Ergonomics and Safety, Barcelona, Spain
- Fragola, J., 2000, *Focus, Strengths, and Weaknesses of HRA, Risk Management and human reliability in Social Context*, 18th ESReDA seminar, Sweden
- Hollnagel, E., 2000, *On understanding risks: Is human reliability a red herring?* Risk Management and human reliability in Social Context, 18th ESReDA seminar, Sweden
- Lloyd's Register of Shipping, 1970–1993, *Casualty Return*, annual summary, London
- Pedrali, M., Andersen, B.H., Trucco, P., 2002, *Are Maritime Accident Causation Taxonomies Reliable? An experimental study of the Human Factors classification of the IMO, MAIB and CASMET Systems*, RINA conference
- Reason, J., 1987, *Too little and too late: a Commentary on accident and incident reporting system*, Department on Psychology, University of Manchester, UK
- Reason, J., 1997, *Managing the Risk of Organisational Accidents*, Ashgate, Hampshire, England
- Scaaf, I.W., Lucas, D.A., Hale, A.R. (eds), 1991, *Near miss Reporting as a Safety Tool*, Butterworth-Heinemann, Oxford
- Skjong, R., Wentworth, B., *Expert judgment and risk perception*,
- Soma, T., Kristiansen, S., 2002, Safety assessment of ship operators – a neural network approach, Maritime Transport Conference, Barcelona
- Soma, in review, Ship safety standard classification based on accident history and port state control findings, *Engineering reliability and safety science*, Elsevier Science
- Soma, to be published a, working title: *Modelling the safety performance of maritime operations- aggregation of symbolic knowledge*
- Soma, to be published b, working title: *Safety assessment through artificial neural networks integrated with symbolic knowledge*
- Soma, to be published c, working title: *The relationship between safety cultural factors and the safety standard of maritime operators*
- Sorensen, J.N., 2002, *Safety culture: a survey of the state of the art*, article in press for Reliability Engineering and system safety, Elsevier Science Ltd., 2002
- Wagenaar, W., Groeneweg, J., 1987, Accident at sea: Multiple Causes and Impossible Consequences, *Int. Journal Man-Machine Studies*, 1987
- Wagenaar, W., Schrier, J., 1997, Accident analysis – The goal and How to get there, *Safety Science*, No. 1/2
- Zohar, D., 1980, Safety Climate in Industrial Organisations: Theoretical and Applied Implications, *Journal of Applied Psychology*, Vol. 65, No.1, pp 96–102



## Application of a Bayesian approach to sequential life testing with an underlying Weibull model

D.I. De Souza Jr.

*Industrial Eng. Lab., North Fluminense State University, Campos, RJ, Brazil*

*Fluminense Federal University, Civil Engineering Dept., Graduate Program, Niterói, RJ, Brazil*

**ABSTRACT:** An example is used to illustrate a new Bayesian approach to sequential life testing proposed in a previous work by De Souza (2002). The underlying sampling distribution was the Weibull model. The intended Bayesian sequential life testing approach uses a posterior probability statement that is continually updated as new test data become available. Since the underlying sampling distribution was the two-parameter Weibull model, in order to find a final expression for the posterior distribution, some numerical procedure had to be applied. For formulating the prior information on the scale parameter  $\theta$  of the Weibull sampling model, we have used the Type II Extreme Value distribution, and for formulating the prior information on the shape parameter  $\beta$  of the Weibull model, we have applied a Beta distribution, defined between two probabilistic limits (L, U). In a following article, we should present a truncation mechanism to the Bayesian sequential approach proposed in this paper.

### 1 INTRODUCTION

Life testing situations in which the product under analysis is a well-known one have been treated before by De Souza (1999, 2000, 2001a, 2001b). The Bayesian approach to sequential testing uses a posterior probability statement, which is continually updated as new data or information become available. In this work, an example is used to illustrate a new Bayesian approach to sequential life testing proposed in a previous work by De Souza (2002). The underlying sampling distribution was the Weibull model and the product under analysis had been recently modified in such a way that one of its main characteristics had experienced significant changes in its tensile strength value. The source of modification was in the product's chemical composition. The amount of Vanadium used in the product's chemical composition (0.08%) was replaced by Niobium (0.12%). Both components (Vanadium and Niobium) are used to increase a product's tensile strength resistance. In this work, we used the Type II Extreme Value distribution and the Beta distribution defined between two unknown limits for the prior information about the scale and shape parameters, respectively, of a Weibull model. Some numerical integration procedures (a combination of Simpson's 1/3 rule with Simpson's 3/8 rule in this work) had to be used for finding the posterior distribution. We provided rules for making one of the three possible decisions as

each observation becomes available; that is: accept the null hypothesis  $H_0$ , reject the null hypothesis  $H_0$  or obtain additional information by making another observation. In a following article, we should present a truncation mechanism to the Bayesian sequential approach proposed in this paper.

The Weibull density function is given by

$$f(t) = \frac{\beta}{\theta} \left(\frac{t}{\theta}\right)^{\beta-1} \exp\left[-\left(\frac{t}{\theta}\right)^\beta\right]; \quad t \geq 0 \quad (1)$$

### 2 PRIOR DISTRIBUTIONS

Most of the difficulties in performing a Bayesian life testing analysis concern the identification, selection and justification of the prior distribution. Such relevant questions as: "What sort of prior should I use?"; "What sources of data are available for selecting a prior model?"; or yet "How should I quantify the subjective information?"; must be addressed. If multiple sources of relevant data are available for use in the analysis, there is even a more fundamental issue that must be settled. It must be decided which data are to be used in fitting the prior distribution and which data are to be used in the likelihood function. This is not always an easy task. Traditionally, the softer and more

subjective data sources have been allocated to the prior, whereas the harder and more objective sample test data have been used in the likelihood. The following example is from Martz & Waller (1982). "Suppose we are interested in Bayesian inferences about the frequency of core meltdown in commercial United States nuclear power reactors. Risk assessments have produced estimates of this event, which are available to us. There are usually somewhat subjective estimates based on analysis. In addition, there are historical operating data from the population of commercial power reactors, both within and outside the United States. There are also various historical data sources on noncommercial, such as military, power reactors. Which of these data sources should be used to fit a prior distribution is not clear cut and judgment must be exercised. It may even be decided to use certain subjective data sources in the likelihood portion of Bayes' theorem, as there is nothing inherent in Bayes' theorem that prohibits this usage".

Soland (1969) used a Gamma and a finite discrete prior distribution for the scale and shape parameters, respectively. A finite discrete prior distribution can assume only a finite number of values in a certain interval. Tsokos & Canavos (1972) developed *fully* ordinary as well as *empirical* bayes estimators of the scale parameter and the reliability function with respect to the usual life testing procedures. The shape parameter was assumed to be known. Papadopoulos & Tsokos (1975), developed Bayesian point estimates of the scale and shape parameters and reliability function of the Weibull failure model. They also developed Bayes confidence bound for the scale parameter under the assumption that the shape parameter was known. Furthermore, they obtained lower Bayes confidence bounds for the reliability function of the same model. For the prior information for the scale parameter two situations were considered: a) an inverted gamma prior pdf; b) a uniform prior pdf. They also investigated the case when wrong prior values are assumed for the scale parameter. Kamat (1977) developed a Monte Carlo simulation method for Bayesian estimation of reliability of systems with statistically independent two-state components. The time-to-failure distribution for each component was assumed to be Weibull with different parameter's values for each one of the components. The shape parameter was assumed to be known, and the prior distribution for the scale parameter was the gamma model with known parameters. We could say that the Bayes approach to reliability evaluation for the Weibull distribution is relatively easy when the shape parameter is known. But when both shape and scale parameters are unknown, we have a more difficult problem. Erto & Rapone (1984) assumed respectively the Uniform and the Inverse Weibull distributions as prior information for the shape and scale parameters of a Weibull sampling population. According to Martz & Waller (1982), the

Uniform distribution represents a state of total ignorance that is not characteristic of most life testing situations. However, when the Uniform model is used as a prior distribution, the resultant posterior distributions are usually tractable, and this fact helped to promote the Bayesian approach. Lamberson & De Souza (1987), used the Inverse Weibull and a Beta distribution defined between two unknown limits for the prior information about the scale and shape parameters, respectively, of a Weibull model. De Souza & Lamberson (1995) used, respectively, the Inverse Weibull and a Negative-Log Gamma distribution defined between two unknown limits for the prior information about the scale and shape parameters. De Souza (1997) used the Type II Extreme Value distribution and the Beta distribution defined between two unknown limits for the prior information about the scale and shape parameters, respectively, of a Weibull model. We will use these distributions here as the prior information for the Weibull  $\theta$  and  $\beta$  parameters.

### 3 PRIOR DISTRIBUTION FOR THE SCALE PARAMETER

The Type II Extreme Value distribution was used here for formulating the prior information on the scale parameter  $\theta$  of the Weibull sampling model. This Type II Extreme Value distribution has its density function (pdf) given by

$$f(\theta) = \frac{b}{a} \left(\frac{a}{\theta}\right)^{b+1} \exp\left[-\left(\frac{a}{\theta}\right)^b\right]; \quad \theta \geq 0 \quad (2)$$

This *pdf* has an expected value and variance given respectively by

$$E(\theta) = a\Gamma\left(1 - \frac{1}{b}\right) \quad (3)$$

$$V(\theta) = a^2 \left[ \Gamma\left(1 - \frac{2}{b}\right) - \Gamma^2\left(1 - \frac{1}{b}\right) \right] \quad (4)$$

The coefficient of variation for the scale parameter of the prior distribution for  $\theta$  depends only on the shape parameter  $b$  and is given by

$$\frac{\sigma_{\theta}}{E(\theta)} = \frac{\left[ \Gamma\left(1 - \frac{2}{b}\right) - \Gamma^2\left(1 - \frac{1}{b}\right) \right]^{1/2}}{\Gamma\left(1 - \frac{1}{b}\right)} \quad (5)$$

The coefficient of variation represents the percentage of error in the estimation of  $\theta$ . The pre-selected value (0.10) for the coefficient of variation, although considered reasonable, is arbitrary and could be changed for different situations. Then

$$\frac{\sigma_\theta}{E(\theta)} = \frac{\left[ \Gamma\left(1 - \frac{2}{b}\right) - \Gamma^2\left(1 - \frac{1}{b}\right) \right]^{1/2}}{\Gamma\left(1 - \frac{1}{b}\right)} = 0.10,$$

given  $b = 12$ . As an initial estimate of  $\theta$ , the scale parameter of the Weibull sampling distribution, we will use an average  $\theta_0$  value obtained from the failure times observed during life testing of the sample under analysis. We will apply the methodology presented in Appendix (1) to calculate this initial estimate  $\theta_0$ . Then, using equation (3) with the  $E(\theta)$  replaced by  $\theta_0$ , we get

$$a = \frac{\theta_0}{\Gamma\left(1 - \frac{1}{b}\right)} \tag{6}$$

We have determined the values of the shape parameter  $b$  and scale parameter  $a$  of the Type II Extreme Value distribution. We shall now discuss the prior distribution for the shape parameter  $\beta$ .

#### 4 PRIOR DISTRIBUTION FOR THE SHAPE PARAMETER $\beta$

The Beta model, defined between two probabilistic limits ( $L, U$ ), proposed by Lamberson & De Souza (1987), was used for formulating the prior information on the shape parameter  $\beta$  of the sampling Weibull distribution. The Beta *pdf* is given by

$$f(\beta) = \frac{(c+d+1)!}{c!d!} \frac{1}{(U-L)^{c+d+1}} (\beta-L)^c (U-\beta)^d \tag{7}$$

$\beta_L < \beta < \beta_U$

As an initial estimate of  $\beta$ , the shape parameter of the Weibull sampling distribution, we will use an average  $\beta_0$  value obtained from the failure times observed during life testing of the sample under analysis. The methodology to calculate an initial estimate for  $\beta$  is given in Appendix (1). The mode of  $f(\beta)$  given by equation (7) can be obtained by taking the derivative of  $f(\beta)$  with respect to  $\beta$  and setting the resulting expression to zero. We propose that  $\beta_0$  be taken as the mode

of the prior. Then, we have

$$\text{Mode} = \beta_0 = \frac{cU + dL}{c + d} \tag{8}$$

The coefficient of variation is given by

$$\frac{\sigma_\beta}{E(\beta)} = 0.10 = \frac{(U-L)(c+1)^{1/2}(d+1)^{1/2}}{(c+d+3)^{1/2}[U(c+1)+L(d+1)]} \tag{9}$$

Here,  $c$  is given by

$$c = \frac{d(\beta_0 - L)}{U - \beta_0} \tag{10}$$

Again, the pre-selected value (0.10) for the coefficient of variation, although considered reasonable, is arbitrary and could be changed for different situations. We now have the necessary quantities for the posterior distribution.

#### 5 THE POSTERIOR DISTRIBUTION

According to De Souza (2002), letting  $t$  be the time to failure, and assuming that  $\beta$  and  $\theta$  are independently distributed variables, the joint density function  $f(\theta, \beta | t)$  was given by

$$f(\theta, \beta | t) = \frac{e^{-(a/\theta)^b} \exp\left[-\sum t_i^\beta / \theta^\beta\right] \left(\prod t_i\right)^{\beta-1} [B]}{\theta^{b+1} \theta^{n\beta}} \tag{11}$$

$$\int_{\beta_L}^{\beta_U} \beta^n \left(\prod t_i\right)^{\beta-1} (\beta-L)^c (U-\beta)^d [A] d\beta$$

$$\beta_L < \beta < \beta_U; \quad 0 \leq \theta \leq \infty$$

$$[A] = \int_0^\theta \frac{e^{-(a/\theta)^b} \exp\left[-\sum t_i^\beta / \theta^\beta\right]}{\theta^{b+1} \theta^{n\beta}} d\theta$$

$$[B] = \beta^n (\beta-L)^c (U-\beta)^d$$

The integral given by [A] is very similar to the one solved in De Souza & Lamberson (1995), and is equal to

$$L = \frac{1}{b a^{n\beta+b}} \Gamma\left(\frac{n\beta}{b} + 1\right) \tag{12}$$

Appendix (2) shows the solution of this integral. Then, if we substitute equation (12) into equation (11) we obtain

$$f(\theta, \beta \setminus t) = \frac{e^{-(a/\theta)^b} \exp\left[-\sum t_i^\beta / \theta^\beta\right] [B] (\prod t_i)^{\beta-1}}{\theta^{b+1} \theta^{n\beta}} \int_{\beta} \frac{1}{b a^{n\beta+b}} \beta^n (\prod t_i)^{\beta-1} (\beta-L)^c (U-\beta)^d \Gamma\left(\frac{n\beta}{b} + 1\right) d\beta \tag{13}$$

[B] was given before. Now, solving the integral in equation (13) by numerical methods, we will obtain a value of, let's say, M. Then, according to De Souza (2002), our expression for  $f(\theta, \beta \setminus t)$  becomes

$$f(\theta, \beta \setminus t) = \frac{e^{-(a/\theta)^b} \exp[-C] \beta^n (\prod t_i)^{\beta-1} (\beta-L)^c (U-\beta)^d}{M \theta^{b+1} \theta^{n\beta}} \tag{14}$$

Here,  $C = \sum t_i^\beta / \theta^\beta$ .

### 6 SEQUENTIAL TEST

According to Kapur & Lamberson (1977), the hypothesis testing situations will be given by

A. For  $\theta$ :  $H_0: \theta \leq \theta_0$ ;  $H_1: \theta > \theta_0$

The test criterion was based on the posterior probability  $P(\theta > \theta_0)$ . The probability of accepting  $H_0$  will be set at  $(1 - \alpha)$  if  $P(\theta > \theta_0) \leq \gamma$ . If  $P(\theta > \theta_0) \geq (1 - \alpha)$ , we will reject  $H_0$ . In this case, the probability of accepting  $H_0$  will be set at a low level  $\gamma$ . If it now happens that  $\gamma < P(\theta > \theta_0) < 1 - \alpha$ , we continue sampling.

B. For  $\beta$ :  $H_0: \beta \leq \beta_0$ ;  $H_1: \beta > \beta_0$

Again, the test criterion was based on the posterior probability  $P(\beta > \beta_0)$ . The probability of accepting  $H_0$  will be set at  $(1 - \alpha)$  if  $P(\beta > \beta_0) \leq \gamma$ . If  $P(\beta > \beta_0) \geq (1 - \alpha)$ , we will reject  $H_0$ . In this case, the probability of accepting  $H_0$  will also be set at a low level  $\gamma$ . If now  $\gamma < P(\beta > \beta_0) < 1 - \alpha$ , we continue sampling. Therefore, if the probabilities  $P(\theta > \theta_0)$  or  $P(\beta > \beta_0)$  become large, then we would suspect that  $H_1$  was the true hypothesis. When the decisions about these quantities  $\theta_0, \theta_1, \beta_0, \beta_1, \alpha$  and  $\gamma$  are made, the sequential test is totally defined.

The development of a sequential test uses the sequential probability ratio given by the following relationship (De Souza 1999) and (Kapur & Lamberson 1977).

$$SPR = L_{1,1,n} / L_{0,0,n} \tag{15}$$

Applying equation (15) to our present problem, we have

$$SPR = \left(\frac{\beta_1}{\beta_0}\right)^n \prod_{i=1}^n \left(\frac{t_i^{\beta_1-1}}{t_i^{\beta_0-1}}\right) \times \exp\left[-\frac{\sum t_i^{\beta_1}}{\theta_1^{\beta_1}} + \frac{\sum t_i^{\beta_0}}{\theta_0^{\beta_0}}\right] \frac{\theta_0^{n\beta_0}}{\theta_1^{n\beta_1}} \times \prod_{i=1}^n \left\{ \left(\frac{\beta_1-L}{\beta_0-L}\right)^c \left(\frac{U-\beta_1}{U-\beta_0}\right)^d \exp\left[-\left(\frac{a}{\theta_1}\right)^b + \left(\frac{a}{\theta_0}\right)^b\right] \left(\frac{\theta_0}{\theta_1}\right)^{b+1} \right\} \tag{16}$$

$$SPR = \left(\frac{\beta_1}{\beta_0}\right)^n \prod_{i=1}^n \left(\frac{t_i^{\beta_1-1}}{t_i^{\beta_0-1}}\right) \exp\left[-\frac{\sum t_i^{\beta_1}}{\theta_1^{\beta_1}} + \frac{\sum t_i^{\beta_0}}{\theta_0^{\beta_0}}\right] \times \frac{\theta_0^{n\beta_0}}{\theta_1^{n\beta_1}} \left(\frac{\beta_1-L}{\beta_0-L}\right)^{nc} \left(\frac{U-\beta_1}{U-\beta_0}\right)^{nd} \left(\frac{\theta_0}{\theta_1}\right)^{n(b+1)} \times \exp\left[-\left(\frac{a}{\theta_1}\right)^b + \left(\frac{a}{\theta_0}\right)^b\right]^n$$

So, the continue region becomes  $A < SPR < B$ , where  $A = \gamma / (1 - \alpha)$  and  $B = (1 - \gamma) / \alpha$ . We will accept the null hypothesis  $H_0$  if  $SPR \geq B$  and we will reject  $H_0$  if  $SPR \leq A$ . Now, if  $A < SPR < B$ , we will take one more observation. Then, we will have

$$\frac{\gamma}{(1-\alpha)} < SPR < \frac{(1-\gamma)}{\alpha}$$

By taking the natural logarithm of each term in the above inequality and rearranging, we get

$$[Z] - \ln\left(\frac{1-\gamma}{\alpha}\right) < X < [Z] + \ln\left(\frac{1-\alpha}{\gamma}\right) \tag{16}$$

$$[Z] = A + B - C + D + E + F + G$$

$$A = n \left[ \ln(\beta_1) - \ln(\beta_0) \right]; \quad B = n\beta_0 \left[ \ln(\theta_0) \right]$$

$$C = n\beta_1 \left[ \ln(\theta_1) \right]; \quad D = nc \left[ \ln(\beta_1 - L) - \ln(\beta_0 - L) \right]$$

$$E = nd \left[ \ln(U - \beta_1) - \ln(U - \beta_0) \right]; F = n \left[ \left( \frac{a}{\theta_0} \right)^b - \left( \frac{a}{\theta_1} \right)^b \right]$$

$$G = n(b+1) \left[ \ln(\theta_0) - \ln(\theta_1) \right]$$

$$X = (\beta_0 - \beta_1) \sum_{i=1}^n \ln(t_i) + \sum_{i=1}^n \left( \frac{t_i^{\beta_1}}{\theta_1^{\beta_1}} - \frac{t_i^{\beta_0}}{\theta_0^{\beta_0}} \right) \tag{17}$$

7 EXAMPLE

A new low alloy – high strength steel product will be life tested. Since this is not a well-known product, some preliminarily life testing was performed in order to determine possible estimated values for the shape and scale parameters of its sampling distribution. It will be assumed here that a Weibull model could represent its sampling distribution. In this preliminary approach, a set of 20 items was life tested, with the testing being truncated at the moment of occurrence of the eighth failure. Table (1) below shows the failure time data (tensile strength units – tsu) from the preliminary life testing. The failure times are arranged in order to facilitate the use of the estimation model described in Appendix (1).

We want to determine initial estimates of  $\beta$  and  $\theta$ , the parameters of the Weibull underlying distribution. Using equations (A1), A(2) and (A3) derived in Appendix (1), we obtained 28 possible failure time combinations, resulting in 28 estimators of  $\beta$ . The average  $\beta$  value obtained from these 28 estimators was 2.7427845 and after some sensitivity analysis we arrive at the  $\beta$  estimator of 2.5127671.

Tables (C1) included in Appendix (3) shows the results of this computation. We will use this estimated  $\beta$  value (2.5127671) to calculate an estimator of the scale parameter  $\theta$ . Using equation (A1) and the 8 failure times listed in Table 1, we obtain the final  $\theta$  estimator of 88.72238 tsu.

A sequential life testing was then performed with this new steel product. We elect the null hypothesis parameters to be  $\theta_0 = 88.72238$  tsu;  $\beta_0 = 2.512767$ ; with  $\alpha = 0.05$  and  $\gamma = 0.10$  and choose some possible values for the alternative parameters  $\theta_1$  and  $\beta_1$ .

Table 1. Failure Time Data (tsu) for the Life Testing Situation.

27.2	34.7	44.3	49.6
55.8	58.2	60.4	69.6

So, we choose  $\theta_1 = 95$  hours and  $\beta_1 = 1.75$ . We also choose  $L = \beta_0 - 1 = 1.512767$  and  $U = \beta_0 + 1 = 3.512767$ . With  $b = 12$ , and using equations (6), (8) and (10), we obtain  $a = 84.0540$ ;  $c = d = 6.439209$ . Then, using equations (16) and (17), we have:

$$A = -0.3617687 \times n; \quad B = 11.271047 \times n$$

$$C = 7.9692846 \times n; \quad D = -9.2641705 \times n$$

$$E = 3.6502893 \times n; \quad F = 0.2926067 \times n$$

$$G = -0.8887414 \times n$$

$$3.270022 \times n - 2.890372 < X < 3.270022 \times n + 2.251292$$

$$X = 0.762767 \times \sum_{i=1}^n \ln(t_i) + \sum_{i=1}^n \left( \frac{t_i^{1.75}}{(95.0)^{1.75}} - \frac{t_i^{2.512767}}{(88.72238)^{2.512767}} \right)$$

The procedure is then defined by the following rules:

1. If  $X \geq n \times 3.270022 + 2.2512918$  we reject  $H_0$ .
2. If  $X \leq n \times 3.270022 - 2.8903718$ , we accept  $H_0$ .
3. If  $n \times 3.270022 - 2.8903718 < X < n \times 3.270022 + 2.2512918$ , we will take one more observation.

Table 2 and Figure 1 show the results of this test.

According to De Souza (2000), this sequential life testing procedure has been shown to be sensitive to “wrong” choices for the null shape and scale parameter values. In the fourth case presented in the example from that paper, even after the observation of 20 failure times, it was not possible to make the decision of accepting or rejecting the null hypothesis. The solution encountered for that situation was the development of a truncation mechanism for the life testing procedure. So, we carried out several life testing simulations with different alternative parameter values to find out if our calculated null parameter values could

Table 2. Sequential test results for the Weibull model. ( $\beta_1 = 1.75$ ;  $\theta_1 = 95$  tsu;  $\beta_0 = 2.512767$ ;  $\theta_0 = 88.72238$  tsu).

Unit number	Failure time (tsu)	Lower limit	Upper limit	Value of X
1	57.92	0.379650	5.521314	3.174310
2	86.62	3.649672	8.791336	6.486675
3	67.91	6.919694	12.06136	9.749080
4	56.00	10.18972	15.33138	12.90139
5	99.89	13.45974	18.60140	16.15800
6	32.30	16.72976	21.87142	18.88111
7	43.84	19.99978	25.14145	21.85307
8	68.79	23.26980	28.41147	25.12116
9	25.80	26.53983	31.68149	27.65772
10	31.96	29.80985	34.95151	30.37205
11	73.27	33.07987	38.22153	33.66398
12	91.86	36.49892	41.49157	36.96351
13	29.12	39.61991	44.76158	39.60056

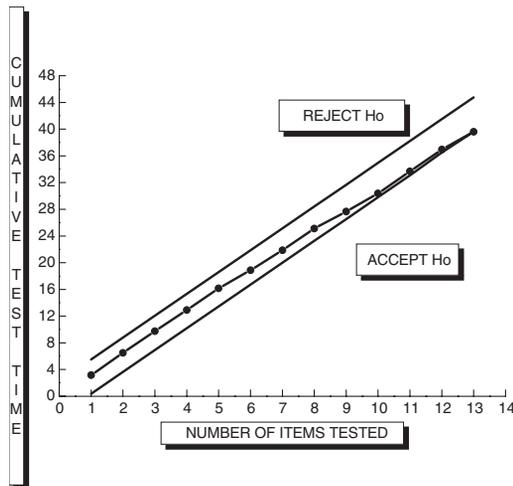


Figure 1. Sequential probability ratio results for the Weibull model.

lead to a situation in which such a mechanism would be needed. Figure 1 above shows the “worst case scenario”, in which 13 units had to be life-tested to allow the decision of accepting the null hypothesis.

## 8 CONCLUSION

The intended Bayesian sequential life testing approach uses a posterior probability statement that is continually updated as new test data become available. Since the underlying sampling distribution was the two-parameter Weibull model, in order to find a final expression for the posterior distribution, some numerical procedure had to be applied. In a following article, we should present a truncation mechanism to the Bayesian sequential approach proposed in this paper.

The Bayesian sequential life testing approach developed in this work provides rules for working with the null hypothesis  $H_0$  in situations where the underlying sampling distribution is the Weibull model. After each observation one of three possible decisions is made:

- Accept the null hypothesis  $H_0$ .
- Reject the null hypothesis  $H_0$ .
- Take one more observation.

The practical estimation procedure presented in Appendix (I) was able to produce reasonable estimates for the shape and scale parameters of the underlying Weibull sampling distribution. In fact, it was necessary to test only 13 units of the product

under analysis to reach the decision to accept the null hypothesis  $H_0$  ( $\theta_0 = 88.72238$  tsu;  $\beta_0 = 2.512767$ ).

Again, we would like to state that we are aware of the fact that the use of Bayesian statistics in sequential life testing is not yet a well-defined process, and that it requires a certain level of knowledge about quantification of the parameters of the prior distributions, as well as of the underlying Weibull sampling distribution. Nevertheless, those willing to use this model will find it to be a reasonably defined alternative for use in the decision procedure in industrial applications.

## REFERENCES

- De Souza, Daniel I. 2002. The Bayesian Approach to Sequential Testing with an Underlying Weibull Model. *European Conference on System Dependability and Safety, ESREL 2002 Conference*, Lyon, France, 18–21 March 2002; 2: 617–621,  $\lambda\mu$ 13 (eds).(6).
- De Souza, Daniel I. 2001a. Truncation Mechanism in a Sequential Life Testing Approach with an Underlying Two-Parameter Inverse Weibull Model, *COMADEM 2001 Conference*, Andrew G. Starr and Raj B.K. Rao (eds), Manchester, U.K., 4–6 September 2001, 809–816, Elsevier Science.
- De Souza, Daniel I. 2001b. Sequential Life Testing with a Truncation Mechanism for an Underlying Weibull Model. *Towards a Safer World, ESREL 2001 Conference*, Zio, Demichela & Piccinini (eds), Torino, Italy, 16–20 September 2001; 3: 1539–1546, Politecnico Di Torino.
- De Souza, Daniel I. 2000. Further Thoughts on a Sequential Life Testing Approach Using a Weibull Model. *Foresight and Precaution, ESREL 2000 Conference*, Cottam, Harvey, Pape & Tait (eds), Edinburgh; Scotland; 14–17 May 2000; 2: 1641–1647, Rotterdam: Balkema.
- De Souza, Daniel I. & Lamberson, Leonard R. 1995. Bayesian Weibull Reliability Estimation. *IIE Transactions*, Vol. 27, Number 3, 1995, 311–320, USA.
- De Souza, Daniel I. 1997. Bayesian Weibull 2-Parameters Estimation. *1 International Congress of Safety Engineering, Accessibility and Risk Management, SEGRAC 97*, Universidade Federal do Rio de Janeiro (eds), 13–17 October 1997, 5–16, Rio de Janeiro, Brazil.
- Erto, P. & Rapone, M. 1984. Non-Informative and Practical Bayesian Confidence Bounds for Reliable Life in the Weibull Model. *Reliability Engineering* 7, 181–191. USA.
- Kamat, S.J. 1977. Bayesian Estimation of System Reliability for Weibull Distribution Using Monte Carlo Simulation. *The Theory and Applications of Reliability*. 123–131.
- Kapur, Kailash & Lamberson, Leonard R. 1977. Reliability in Engineering Design. *John Wiley & Sons, Inc.*, 1977, USA.
- Lamberson, Leonard R. & De Souza, Daniel I. 1987. Bayesian Weibull Estimation. *1987 – ASQC Quality Congress Transactions*, April 14–17, Minneapolis, 1987, pp. 497–506, USA.
- Martz, H.F. & Waller, R., (1982). Bayesian Reliability Analysis. *John Wiley & Sons, Inc.*, USA.
- Papadopoulos, A.S. & Tsokos, C.P. 1975. Bayesian Confidence Bounds for the Weibull Failure Model. *IEEE Transactions on Reliability*. Vol. R-32, N1, April, 21–26.

Soland, R.M. 1969. Bayesian Analysis of the Weibull Process with Unknown Scale and Shape Parameters. *IEEE Transactions on Reliability*. 18(4), 181-184.  
 Tsokos, C.P. & Canavos, G.C. 1972. Bayes Concepts for the estimation of Reliability in the Weibull Life Testing Model. *Int. Stat. Rev.* Vol. 40, N2, 153-160.

APPENDIX 1

Initial Estimators for the Parameters  $\beta$  and  $\theta$  of a Weibull Sampling Distribution.

From equation (1), we have

$$t_R = \theta \left[ \ln \left( \frac{1}{R(t)} \right) \right]^{1/\beta}$$

Solving the above equation in terms of  $\theta$  and  $\beta$  we will get

$$\theta = \frac{t_R}{\left[ \ln \left( \frac{1}{R(t)} \right) \right]^{1/\beta}} \tag{A1}$$

$$\beta = \frac{\ln \left( \ln \left( \frac{1}{R(t)} \right) \right)}{\ln(t_R) - \ln(\theta)} \tag{A2}$$

Thus, given the failure times  $t_{r1}, t_{r2}, \dots, t_{rn}$  from a random sample of  $n$  items ( $i \leq n - 1$ ), in order to calculate the surviving percentage of the population at the moment of occurrence of failure number  $r_i$ , we should obtain the following

$$R(t_{ri}) = 1 - \frac{r_i}{n} \tag{A3}$$

Here,  $r_i/n$  indicates the failing percentage of the population until time  $t_{ri}$ . Then,  $R(t_{ri}) = 1 - r_i/n$  indicates the surviving percentage of the population until time  $t_{ri}$ . So, to estimate values for the two parameters  $\beta$  and  $\theta$  of a Weibull sampling distribution, we need only calculate two failing percentages of the population being tested, and apply (A1) or (A2). As an example, if we have a sample size of 9 items,  $n = 9$ , with truncation of the test at the moment of occurrence of the sixth failure, and we decide to use failures number 1 and 4, the reliability function values  $R(t_{ri})$  for failures 1 and 4 will be given by

$$R(t_{r1}) = 1 - \frac{r_1}{n} = 1 - \frac{1}{9} = 0.888;$$

$$R(t_{r4}) = 1 - \frac{r_4}{n} = 1 - \frac{4}{9} = 0.555.$$

Using equation (A1), we will have

$$\begin{cases} \theta = \frac{t_{r1}}{\left[ \ln \left( \frac{1}{0.888} \right) \right]^{1/\beta}} \\ \theta = \frac{t_{r4}}{\left[ \ln \left( \frac{1}{0.555} \right) \right]^{1/\beta}} \end{cases}$$

Using the failure time values  $t_{r1}$  and  $t_{r4}$ , and solving the above system of two equations, we will get estimated values for  $\beta$  and  $\theta$ . We could combine any two of the failure times and obtain estimators for the two parameters. For example, a sample with six failures will allow a total of  $6 \times 5/2 = 15$  possible combinations of failure times, each one of the combinations allowing an estimator for  $\beta$  and an estimator for  $\theta$ . Now, if we remove all possible "outliers" or "freak" values, we could then utilize the average of the values  $\beta$  and  $\theta$  as preliminary estimators of these two parameters. After that, we should perform a sensibility analysis with each one of the failure time combination results, discarding the ones which have values that are very different from the average values. Here,  $t_{ri}$  will be used to represent the failure time  $r_i$ .

This proposed practical approach allows determination of initial estimates for the shape parameter  $\beta$  and for the scale parameter  $\theta$  of a Weibull sampling distribution, and for an initial failure time  $t_R$ .

APPENDIX 2

Solving the integral

$$\int_{\theta} \frac{e^{-(a/\theta)^b} \exp \left[ -\sum t_i^\beta / \theta^\beta \right]}{\theta^{b+1} \theta^{n\beta}} d\theta$$

Let  $(X) = \int_{\theta} \frac{e^{-(a/\theta)^b} \exp \left[ -\sum t_i^\beta / \theta^\beta \right]}{\theta^{b+1} \theta^{n\beta}} d\theta \tag{B1}$   
 $\infty > \theta > 0$

Let also  $C = \sum t_i^\beta$ ;  $U = \left( \frac{a}{\theta} \right)^b$   
 $du = \left| \frac{-ba^b}{\theta^{b+1}} \right| d\theta$  where  $\theta = \frac{a}{U^{1/b}}$

So, when  $U \rightarrow 0, \theta \rightarrow \infty$ ; when  $U \rightarrow \infty; \theta \rightarrow 0$ . Then, we will have

$$(X) = -\frac{1}{ba^{n\beta+b}} \int_0^\infty e^{-CU^{\beta/b}/a^\beta} e^{-U} U^{n\beta/b} du$$

As we remember,  $\int_0^\infty S dr = [RS]_0^\infty - \int_0^\infty R ds$ . Then, using integration by parts, with  $S = e^{-CU^{\beta/b}/a^\beta}$ ;  $dr = e^{-U} U^{n\beta/b} du$ ; and with  $W = \frac{1}{ba^{n\beta+b}}$ , we will have

$$(X) = -W \left\{ [(A)(B)]_0^\infty - \int_0^\infty (-)(A) \frac{C}{a^\beta} \frac{\beta}{b} U^{\beta/b-1} (B) du \right\} \tag{B2}$$

Here,  $(A) = \int e^{-U} U^{n\beta/b} du$  and

$(B) = e^{-CU^{\beta/b}/a^\beta}$ . Letting now  $E = n\beta/b$ , we will have  $(A) = \int U^E e^{-U} du$ . Using integration by parts sequentially, we get

$$(A) = -e^{-U} \times [U^E + EU^{E-1} + E(E-1)U^{E-2} + \dots + E(E-E+1)U^{E-E+1}]$$

More precisely;

$$(A) = -e^{-U} \left( E! \sum_{k=0}^E \frac{U^{E-k}}{(E-k)!} \right) \tag{B3}$$

If we insert the value of (A), given by equation (B3), into equation (B2), we get

$$(X) = -\frac{1}{ba^{n\beta+b}} \times \left[ E! e^{-U} \sum_{k=0}^E \frac{U^{E-k}}{(E-k)!} e^{-CU^{\beta/b}/a^\beta} \right]_0^\infty - \frac{1}{ba^{n\beta+b}} \times E! \int_0^\infty (-) e^{-U} \sum_{k=0}^E \frac{U^{E-k}}{(E-k)!} \frac{C}{a^\beta} \frac{\beta}{b} U^{\beta/b-1} e^{-CU^{\beta/b}/a^\beta} du$$

Now, consider the term

$$\left[ E! e^{-U} \sum_{k=0}^E \frac{U^{E-k}}{(E-k)!} e^{-CU^{\beta/b}/a^\beta} \right]_0^\infty$$

As  $U \rightarrow \infty$ ,  $e^{-U} = 1/e^U \rightarrow 0$  faster than  $U^{E-k}$  increases, and so the term tends to 0. As  $U \rightarrow 0$ ,  $U^{E-k} \rightarrow 0$  and so the term tends to zero again. Then, (X) becomes

$$(X) = -\frac{1}{ba^{n\beta+b}} \times E! \int_0^\infty (-) e^{-U} \sum_{k=0}^E \frac{U^{E-k}}{(E-k)!} \frac{C}{a^\beta} \frac{\beta}{b} U^{\beta/b-1} e^{-CU^{\beta/b}/a^\beta} du$$

As we know, the following two series are equal:

$$\sum_{k=0}^E \frac{U^{E-k}}{(E-k)!} \text{ and } \sum_{i=0}^E \frac{U^i}{i!}$$

Then, the expression for (X) becomes

$$(X) = -\frac{1}{ba^{n\beta+b}} \times E! \int_0^\infty (-) e^{-U} \sum_{i=0}^E \frac{U^i}{i!} \frac{C}{a^\beta} \frac{\beta}{b} U^{\beta/b-1} e^{-CU^{\beta/b}/a^\beta} du$$

As we recall,  $U = (a/\theta)^b$ . From equation (3), we have  $E(\theta) = \theta = a\Gamma(1 - (1/b))$ .

When  $b > 1$ , the minimum value that  $\Gamma(1 - (1/b))$  could have occurs when the term  $1/b$  goes to zero. So,  $\Gamma(1 - (1/b)) \approx 1$ . Then, in any practical application, since  $\theta = a\Gamma(1 - (1/b))$ , we can see that  $\theta > a$ . Therefore,  $U = (a/\theta)^b < 1$ .

The value  $E = n\beta/b$  in any life testing situation could vary, say, from 2 to a maximum of 7. For practical purposes, when the value of E is not an integer, it will be approximated to the next largest one. Now, even if the value of E is small, for example 3, and since  $U < 1$ , we can see that

$$\sum_{i=0}^E \frac{U^i}{i!} \approx e^U \tag{B4}$$

Then, if we use this practical approximation in (X), we obtain

$$(X) = -\frac{1}{ba^{n\beta+b}} \times E! \int_0^\infty (-) e^{-U} e^U \frac{C}{a^\beta} \frac{\beta}{b} U^{\beta/b-1} e^{-CU^{\beta/b}/a^\beta} du$$

$$(X) = -\frac{1}{ba^{n\beta+b}} E! \int_0^\infty (-) \frac{C}{a^\beta} \frac{\beta}{b} U^{\beta/b-1} e^{-CU^{\beta/b}/a^\beta} du,$$

where the integral

$$\int_0^{\infty} (-) \frac{C}{a^\beta} U^{\beta-1} e^{-CU^{\beta/b}/a^\beta} du \text{ is of the form}$$

$$\int_0^{\infty} (-) x' e^{-x} dx = [e^{-x}]_0^{\infty}. \text{ Then}$$

$$(X) = -\frac{1}{ba^{n\beta+b}} E! \left[ e^{-CX^{\beta/b}/a^\beta} \right]_0^{\infty}$$

$$(X) = -\frac{1}{ba^{n\beta+b}} E! [0-1] = \frac{1}{ba^{n\beta+b}} E!$$

With  $E = n\beta/b$ , we have  $(X) = (1/(ba^{n\beta+b}))(n\beta/b)!$ .  
The integral finally becomes

$$(X) = \frac{1}{ba^{n\beta+b}} \Gamma\left(\frac{n\beta}{b} + 1\right) \quad (B5)$$

APPENDIX 3

Table C1 – Estimator results for  $\beta$  (first analysis)  
Sample Size = 20; Number of failures = 8.

27.2	34.7	44.3	49.6
55.8	58.2	60.4	69.6
Beta (1, 2) 2.9558964	Beta (1, 3) 2.3643108		
Beta (1, 4) 2.4472690	Beta (1, 5) 2.3996651		
Beta (1, 6) 2.5494221	Beta (1, 7) 2.6674838		
Beta (1, 8) 2.44463564	Beta (2, 3) 1.7744746		
Beta (2, 4) 2.1005596	Beta (2, 5) 2.1145173		
Beta (2, 6) 2.3580143	Beta (2, 7) 2.5407629		
Beta (2, 8) 2.2680803	Beta (3, 4) 2.8053410		
Beta (3, 5) 2.4743857	Beta (3, 6) 2.8802800		
Beta (3, 7) 3.1445028	Beta (3, 8) 2.5349375		
Beta (4, 5) 2.1568527	Beta (4, 6) 2.9332434		
Beta (4, 7) 3.3390597	Beta (4, 8) 2.4447379		
<b>(E)Beta (5, 6) 5.1047568</b>	<b>Beta (5, 7) 5.0968520 (E)</b>		
Beta (5, 8) 2.5981742	<b>Beta (6, 7) 5.0878804 (E)</b>		
Beta (6, 8) 2.0080782	Beta (7, 8) 1.2020698 (E)		

First sum = 76.79797; First  $\beta$  estimator = 2.7427845  
Number of Combinations = 28; (E) = Combination to be eliminated from computation.

Beta  $\pm$  50% Beta = 2.7427845  $\pm$  1.3713923 = (1.3713923; 4.1141768).

Number of combinations to be excluded from computation = 4.

Final number of combinations used to calculated  $\beta = 24$ ; Final sum = 60.306411.

Final  $\beta$  estimator = 2.5127671.

Table C2 – Estimator results for  $\theta$  (first analysis)  
Sample Size = 20; Number of failures = 8.

27.2	34.7	44.3	49.6
55.8	58.2	60.4	69.6

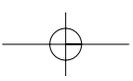
$\beta$  estimator used to calculate  $u$  5 2.5127671

THETA(1) 88.69988	THETA(2) 84.97126
THETA(3) 91.29320	THETA(4) 90.09984
THETA(5) 91.61559	THETA(6) 87.72109
THETA(7) 84.44817	THETA(8) 90.93002

First sum = 709.779052

Final  $\theta$  estimator = 88.72238

Number of combinations = 8.



## Establishing steel rail reliability by combining fatigue tests, factorial experiments and data transformations

D.J. Stewardson

*Industrial Statistics Research Unit, University of Newcastle, UK*

M.F. Ramalhoto

*Mathematics Department, Instituto Superior Tecnico, Portugal*

L.F.M. da Silva

*Instituto de Engenharia Mecanica e Gestao Industrial, Universidade do Porto, Portugal*

L. Drewett

*Corus Group UK*

**ABSTRACT:** This paper demonstrates a combination of the use of Factorial Experiments, Material Test Failure Analysis, Data Transformations and Plots of Residual Errors from “moving” Regression curves to determine the nature of Fatigue Crack Growth Rate in steel rails. Fatigue cracks in rails are a particular problem in Europe and a major threat to passenger safety. The project was intended to harmonise results under the current EC standard for determining crack growth rates, and hence the reliability, of a particular grade of steel railway line. Previous studies had shown considerable scatter between both the testing laboratories and the rail manufacturers. The consortium used fractional factorial designs to establish the effect of various nuisance variables that were thought to be responsible for much of the scatter. Two stages, screening and secondary, involving six laboratories produced results that were subjected to novel graph based analytic techniques that led to major recommendations to the European Standards Bodies. The results also pointed to a new way to determine changes in growth rate generally when a mechanical test is applied to steel. It was well known that there are three stages of growth rate in steel rails, but finding the change points from stage to stage had always been a problem. First and third stage growth can be either faster or slower than second stage rates but are highly unpredictable both in appearance, duration and magnitude. This leads to difficulty in describing failure rates and hence the quality of the rails. The paper shows how the application of a combination of statistical techniques with accelerated testing lead to a new robust method of determining the change points and better estimates of the second stage growth rates. This in turn leads to effective ways of monitoring the output from steel production and the calibration of test equipment. The findings can be used to estimate the relative lifetime of steel rails under normal operating conditions.

### 1 INTRODUCTION

The work described here was conducted by a consortium of Partners funded by the European Commission under the Standards Measurements and Testing programme of the European 4th Framework programme. The purpose of this work was to determine the effects of stress ratio and relative humidity on the fatigue crack growth rates measured in grade 260 rail steel. The objective relates to the need to verify the procedures and specifications in a draft European Rail Standard,

and to measure the scatter in fatigue crack growth rates measured in six laboratories under conditions specified in the draft. Approximately 75% of the rails currently produced for use in Europe are 260 grade. The setting of acceptance limits for qualifying tests on rails requires that the scatter between results due to the test procedure is sufficiently small so that the test can identify acceptable rails and reject unacceptable ones. A previous exercise carried out to determine acceptance limits found that there were considerable differences in results between laboratories, which resulted in

apparently acceptable rails failing the proposed specification. The cause of these differences needs to be identified so that a verified test procedure and acceptance limits can be written into the standard.

The rails from four manufacturers were machined to produce ten single edge-notched bend specimens from each rail, as described in the draft standard. The research was split into two parts, Part 1 determined the effects of rail source, laboratory, stress ratio at values of 0.2 and 0.5, and relative humidity at levels of <10%, 35% and 60%. Stress ratio refers to the ratio of the maximum and minimum loads, that are applied in cycles, to a sample. A ratio of 0.5 means that the maximum load is double the minimum. Part 2 tests were carried out under a fixed stress ratio of 0.5, with cyclic test frequency in the range 10–120 Hz added as a factor in the experimental design. Temperature and relative humidity were recorded but not controlled in this stage. Test frame and crack monitoring details were also recorded, but not explicitly studied.

## 2 TEST PROCEDURE

Rails were supplied by four European rail manufacturers and ten specimens were machined from each of the four. All of the specimens were machined by the same facility using standardised conditions. The experimental design for the Part 1 tests was set up as shown below. Humidity was investigated at three levels, Stress Ratio at two only. There were only 5 samples available from each manufacturer due to budgetary constraints. Because there are 4 manufacturers this design is based on a half fraction of an L32 (see for example Grove and Davis 1992) plus some centre point combinations. These centre point combinations represent a one-quarter fraction of the 16 possible centre combinations.

In fact the factorial part of the plan can be designated under the notation  $4^m 2^{n-p}$  as discussed in Ankeman (1999). In that case this is a  $4^1 2^{3-1}$  resolution IV Design. That means that no main effect estimate or any two-factor interaction estimates are confounded and thus inestimable. The design was intended to be able to accommodate one or two further factors if required, without changing the structure of the design. This was because the partners in the work, the labs, were competitors and it was not clear from the outset that every potential factor could be included, yet the design had to be agreed in advance and was embedded within the contract! In the event, the new factors could not be controlled in practice. If it were not for our wanting to accommodate two potential factors, the design would have been slightly different, and thus a resolution V design, but no great loss of efficiency occurred. A fuller discussion of the different designs is given in Stewardson (2000).

Table 1. First stage experimental array.

Design Factor Settings				
Test	Rail Maker	Lab	% Humidity	Stress Ratio
Factorial Points				
A1	1	B	~60%	0.5
A2	1	A	<=10%	0.5
A3	1	A	~60%	0.2
A4	1	B	<=10%	0.2
A6	2	A	~60%	0.5
A7	2	B	<=10%	0.5
A8	2	B	~60%	0.2
A9	2	A	<=10%	0.2
A11	3	A	~60%	0.5
A12	3	B	<=10%	0.5
A13	3	B	~60%	0.2
A14	3	A	<=10%	0.2
A16	4	B	~60%	0.5
A17	4	A	<=10%	0.5
A18	4	A	~60%	0.2
A19	4	B	<=10%	0.2
Centre Points				
A5	1	A	~35%	0.5
A10	2	A	~35%	0.2
A15	3	B	~35%	0.5
A20	4	B	~35%	0.2

In the stage 1 experimental design in Table 1, the extra centre points are there to establish if the humidity levels had a non-linear effect on results. The centre points considered separately are themselves a heavily saturated design, an L4 or  $2^2$  of Stress ratio and Laboratories but with humidity fixed at 35% and with each of the 4 runs allocated to a different manufacturer. Analysis of the factorial part was completed separately from these additional points.

The Labs reported their calculated values of crack growth rate,  $da/dN$ , and the stress intensity factor range,  $\Delta K$ , for each test performed. The growth rate  $da/dN$  is simply the ratio of the measured change in crack length divided by the number of cycles that this was recorded over. The calculation of  $\Delta K$  is based upon the stress ratio and the size of the sample as well as a number of correction factors that depend upon the relationship between the size of sample and the crack length achieved at each point. The associated formulae are somewhat complex and are beyond the scope of this paper.

Each laboratory reported the values of crack length against the number of cycles and the loads applied (see Figure 1 for a plot of  $da/dN$  vs  $\Delta K$  from a typical test result).

The plot of  $da/dN$  vs  $\Delta K$  has a roughly straight curve if plotted on a log-log scale (see Figure 2 for a graph of  $\log(da/dN)$  vs  $\log(\Delta K)$  for the data of

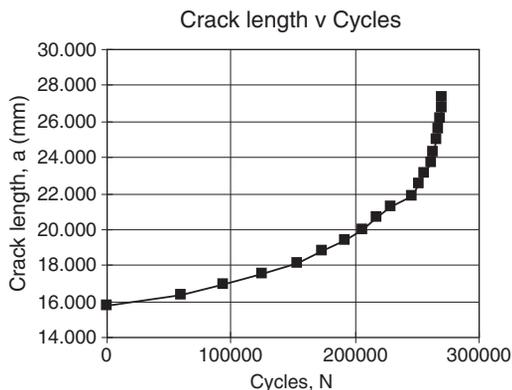


Figure 1. Typical plot of  $da/dN$  vs  $\Delta K$ .

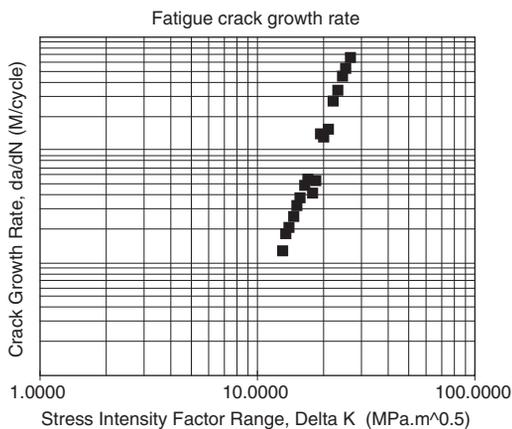


Figure 2. Plot of Figure 1 data on a Log-Log scale:  $\log(da/dN)$  vs  $\log(\Delta K)$ .

Figure 1). Some problems were experienced in two cases, fracture of the specimen occurred during pre-cracking. When this happened a sub-size test piece was machined from one of the broken halves of the original test piece and re-tested.

Following the first stage findings (see below), the second stage tests involved five more specimens, tested in each of four more laboratories under a stress ratio of 0.5, with temperature in the range +15 to +25°C, and cyclic test frequency in the range 10–120 Hz. The laboratory air environment was recorded but not controlled. These were all the factors still thought to be potentially important by that stage. In the second stage each laboratory tested at least one specimen from each of the four rail manufacturers included in the study.

The unbalanced nature of the design, derived from the budget limitations inherent in the project is

discussed in Stewardson (2000) but in the event no other factor was found to be significant, although Humidity does brook further investigation.

Four different methods of monitoring crack growth were used: direct current potential drop, compliance of the test piece, fractomat gauges, and optical microscope. The first three techniques give a continuous output for determining the crack length, but the optical method, in this case, required interruptions to the test overnight. Details of interruptions were recorded as required in BS 6835: 1988. A complete description of this from an engineering standpoint is given in Da Silva (2003).

### 3 DATA ANALYSIS

The data were analysed in terms of the  $\log(da/dN)$  vs  $\log(\Delta K)$  relationship. This is approximately a straight line when the crack growth rate is stable (as in the middle part of Figure 2) and can be assessed, or broken down, into the slope, the intercept and the residual error. Residual error is a measure of the “scatter” or uncertainty around this straight line that is fitted to the data, added to any lack of fit between the data and the straight line. This lack of fit is an indication of the veracity of using a straight line at all. It is possible, at least partially, to separate these two components of error or uncertainty (see for example Davies and Goldsmith 1972). The data from each test could be separated into “sections” that represent different rates of change (or slopes). These may or may not indicate two or more of the three known stages in crack growth. There was strong evidence that these growth stages did appear in the data and could be separated by use of the analysis of the scatter apparent within each section of data. For example, the third, most unstable, growth stage the growth rate may either accelerate or slow down. Acceleration may be due to cleavage bursts and slowing may be due to blunting of cracks after cleavage bursts, and if data associated with these problems is included then this will tend to cause an underestimate or overestimate of the true slope related to the underlying growth rate.

Thus the importance of using data sections in the analysis is that it is possible to get a greater, or lesser growth rate than the more stable second stage growth rate in either of stages one or two. If all the data from a test is used to estimate the quality of the rails then results could be unreliable. Second stage growth tends to represent the “true” status of the rail quality. Table 2 shows the various responses discussed here including two versions for calculating  $da/dN$ . Version denoted (1) is the current standard BS 6835 1988. Version (2) a possible improvement.

There are a number of ways to successfully split the data into sections. One way is to calculate a moving

Table 2. Responses.

Response	Description
Slope(1)	The slope of the log-log plot using the method in clause 10 of BS 6835: 1988
Slope(2)	The slope of the log-log plot when using a point to point calculation of da/dN & ΔK
S(1)	The mean error of the log-log plot using the method in clause 10 of BS 6835: 1988
S(2)	The mean error of the log-log plot when using a point to point calc' of da/dN & ΔK
Int(1)	The intercept of the log-log plot using the method in clause 10 of BS 6835: 1988
Int(2)	The intercept of the log-log plot when using a point to point calc' of da/dN & ΔK
Note*	(1) $(da/dN)_i = (a_i + 1 - a_i - 1)/(N_i + 1 - N_i - 1)$ (2) $(da/dN)_i = (a_i - a_i - 1)/(N_i - N_i - 1)$

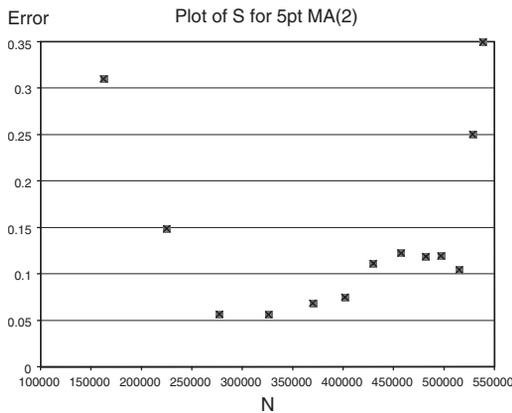


Figure 3. Plot of error for 5 point regression lines of test A2 data.

regression line, with 5 data points used in each, right through the data and plot the results. The plots could be of either the slope, or perhaps more usefully, the residual or mean error.

An example is shown to illustrate the effect. The plot in Figure 3 shows the mean error associated with the regression lines of,  $\log(da/dN)$  vs  $\log(\Delta K)$  each based on 5 points only, calculated through the data for the test A2. The (2) denotes that da and dN had been calculated without first smoothing the data as done in BS 6835 (see Table 2).

The first two and the last two points on the plot show greater levels of error. This indicates increased lack of fit, or scatter, at the beginning and end.

The second plot (Figure 4) shows the slope coefficients for the same data. It is now clear that the early increased error (in Figure 3) was probably scatter due to an "outlier" or unusual result because the slope estimate

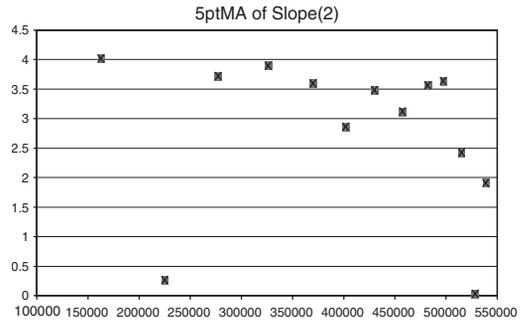


Figure 4. Plot of slope for 5 point regression lines of test A2 data.

(Figure 4) is seen to drop for only one point on the plot. The later increase in error was, however, due to a change (a fall) in the measured crack growth rate, possible due to an arrest after cleavage bursts. This change shows up on the slope plot (Figure 4) as a fall in the final 3 points. It is clear that there are at least 2 stages represented in the data.

In the plot of S (Figure 3), the increased error at the end of the data is due to an increase in the "lack of fit". The more "stable" period in the middle of the plot demonstrates the minimum lack of fit, plus background (or pure) error, however much that is.

Not all the plots were as clear cut as the example given and it is possible to use more sophisticated methods to determine where a cut should be made, if any. These methods could involve the use of formal statistical formulae, or even simple, but effective probability plots, such as Half-Normal plots.

### 3.1 Analysis of initial results without splitting data into sections

In the Part 1 tests the analyses of effects on slope had been carried out both with and without splitting the data into the different stages of crack growth. When the data was not split the analysis of the 2 level fraction showed found no significant factors, Table 3.

### 3.2 Analysis of initial design second stage growth section data only

Under the more stable data section, Stress ratio and the rail manufacturers were seen to be weakly significant factors as in Table 4.

### 3.3 Analysis of second experiment stable growth rate section data only

Following the initial experiments the Part 2 tests were carried out using a fixed stress ratio of 0.5, chosen as

Table 3. Anova table for effects on slope estimates using full data from Part 1.

Factor	df	F	P
Rail manufacturer	3	1.64	0.26
Laboratory	1	1.53	0.25
Humidity	1	0.42	0.54
Stress ratio	1	0.17	0.69
Humidity* stress ratio	1	0.10	0.77
Error	8		
Total	15		

Table 4. Anova table for effects on slope estimates in stable stage growth data from initial results.

Factor	df	F	P
Rail manufacturer	3	3.51	<b>0.06</b>
Stress ratio	1	4.90	<b>0.05</b>
Relative humidity	1	0.00	0.95
Humidity* stress ratio	1	1.12	0.32
Error	9		
Total	15		

Table 5. Part 2 results from second stage growth data, derived by method (1) in Table 3.

Factor	df	F	P
Number of cycles	1	0.25	0.62
Rail manufacturer	3	1.50	0.25
Laboratory	5	0.34	0.88
Start – stable data	1	0.68	0.42
Humidity	1	1.72	0.21
Error	17		
Total	28		

a suitable value with which to fix the European standard. It was also possible to include a number of the other measurements as potential factors, such as the starting point or number of total cycles, and these were included in the analysis, Table 5.

### 3.4 Within-lab scatter

The following Table 6 shows the general difference in random uncertainty between the laboratories using the analysis of variance for the mean error  $S$  using method (2).

These tables show that the manufacturers had little effect on the uncertainty and that different laboratories had more variable results than others. Labs A and B had the highest level of variability, then labs D and F while Labs C and E had the lowest levels. It was

Table 6. ANOVA of scatter within Labs.

Factor	df	F	P
Number of cycles	1	0.25	0.63
Rail manufacturer	3	2.46	0.10
Laboratory	5	4.84	0.01
Humidity	1	1.44	0.25
Error	18		
Total	28		

seen that laboratories C and E both used fractomat gauges for monitoring the crack growth and that this appears to be a better technique.

### 3.5 Some project findings

- Stress ratio has a significant effect on the slope and intercept. Higher stress ratios produce lower crack growth rates. This should be taken into account in the standard by fixing the set ratio.
- There was no significant difference between the crack growth rate in samples from different manufacturers: this applied to both the slope and the intercept based on the stable crack growth region of the log (da/dN) (log  $\Delta K$ ) plot.
- All Labs produced similar growth rate estimates provided stable stage data was used.
- There was no effect on the results with regard to different cyclic test frequencies.
- Humidity had no direct significant effect on the results.
- The results from some laboratories displayed more variance around the log–log relationship between da/dN and  $\Delta K$  than others did. This is due to the different equipment used
- The mean slope for all of the tests using stress ratio of 0.5 was close to 4.

## 4 CONCLUSIONS

The best way to analyse data from these types of test is to break the data down into sections, and use only the stable data in the analysis. A suitable way is to find the sections of data that show the least scatter around the log–log curve of the stress and crack growth. This can be achieved by using moving Linear Regression lines. It is also possible to derive quality monitoring of the test data using charts of the Regression parameters; slope, error and intercept. The method has been recommended to the Commission and monitoring formulae have been provided. Examples of typical formulae can be found in Hines and Montgomery (1990).

#### ACKNOWLEDGEMENT

The work described was carried out under project number SMT4 – CT98 – 2240 – part-funded under the SMT part of the “Growth” programme of the 4th Framework of the European Commission. The writing of this paper was also supported under the European Commission’s 5th Framework “Growth” Programme via the Thematic Network “Pro-ENBIS” contract reference: G6RT-CT-2001-05059.

#### REFERENCES

- Ankenman BE (1999) Design of Experiments with Two-and Four Level Factors *Journal of Quality Technology* v 31 363–375.
- British Standard BS 6835: 1988 “*Determination of the rate of fatigue crack growth in metallic materials*”.
- Da Silva L, De Oliveira FMF, De Castro PMST & Stewardson DJ (2003) Fatigue Crack Growth of Rails for Railways *Journal of IMECHE Series 6* in print.
- Davies OL & Goldsmith PL eds. (1972) *Statistical Methods in Research and Production* 4th ed. Oliver & Boyd, Edinburgh.
- Grove DM & Davis TP (1992) *Engineering, Quality & Experimental Design* Longman, London.
- Hines WH & Montgomery DC (1990) *Probability and Statistics in Engineering and Management Science* Wiley, New York.
- Stewardson DJ, Drewett L, da Silva, Budano LS, Joller A, Mertens J & Baudry G (2000) Using Designed Experiments and the analysis of Statistical Error to Determine Change Points in Fatigue Crack Growth Rate *Proceedings of Industrial Statistics in Action Conference September 2000 Newcastle upon Tyne UK* Vol 2, p. 59–69.

## Improved methods of power systems availability indices determination

M. Stojkov

*HEP group, Distribution, Area Slavonski Brod, Croatia*

S. Nikolovski

*Faculty of Electrical Engineering, University of Osijek, Croatia*

I. Mravak

*HEP group, Distribution, Zagreb, Croatia*

**ABSTRACT:** This paper presents a role of reliability aspect in the power system supply quality. Increasing importance of availability indices in quality improvement evaluation in power delivering and some cost savings at the same time is given here. The evaluation method has been developed to solve a real technical and management problem – define optimal power system switching state. The evaluation method is based on Markov state space model of power lines as system components, enumerating all possible power system states and composed of an independent power system components failures time-series data, their coincidence of the first, second and the third order for the branches (lines and transformers), storing in a relational system database. Some input variables and detailed reliability results calculated for all buses in the distribution power system of area Slavonski Brod are a part of this paper too.

### 1 INTRODUCTION

#### 1.1 *Power quality*

Anyone with a technical background can define power delivering as a dynamic process depending on customer demands during any time period. So, power quality consists of the several main variables describing some kind of a dynamic process according to EN 50160. One of these variables describing power system reliability is maximum allowed failures number per year and the second one is maximum allowed duration of voltage interruption per year for each end-user. To determine the above mentioned systems parameters, the power system (nodes and branches) has to be permanently monitored day by day during the whole year. The object of this approach are only components failures, which cause the power interruption to the end-users.

According to the EN 50160 voltage drop period starts when voltage drops down to a level less than 1% of the nominal voltage level. There are two possible voltage absence periods: planned maintenance (consumers are informed a days in advance) and accident failures. The last one can be divided further in long term (permanent failure) and short voltage interruptions (transient failure, duration is less than

3 minutes). The latter failures are expected to last about several hundreds, but duration of 70% of them should be less than 1 s. Long term non voltage periods should not be more than 10–50 per year.

The power system is given with its branches (power lines and transformers) and buses (nodes) describing actual topology order. The nodes are the points with load feed (generators and load input from a higher voltage network), load output points from the distribution network to the customer, branching points or points of the power line type changeability (like overhead line – buried line, isolation technology type, radius and conductor material).

#### 1.2 *Reliability aspect*

The power system is composed of a great number of mechanical and electrical components, which can be removed when a failure occurs or even in a maintenance process (periodic maintenance or when any component parameter deviate outside of the regulated range). There are also some organizations imperfections and human faults as possible failure causes.

The power system is an open dynamic technical system with a number of strong connections with its

environment. The environment is structured in two parts: technical with material parameters and physics essentials in one side and probability variables (demands, weather conditions) at the other side. However, at any time, the system is in one and only one possible state that is completely described by a set of variables.

The power delivering is object process we monitored within the system and its states. If the next system state can be predicted for sure on the base of physical process low, it is deterministic system. If we only know probability distribution of a next system state, it is stochastic system. The power system is exactly a stochastic technical system. Some uncertainties in the power demand, external temperature, other weather conditions, pollution and other factors become into consideration here.

## 2 RELATIONAL POWER SYSTEM DATA BASE

### 2.1 Introduction

All time-series events about systems and components states and their changes have been continually recorded in the power system management documents obligated by the law. It was very hard and slow to retrieve data from these documents based on only one component state in a particular moment in the past. All recorded data were extremely unconnected, hard readable and unsorted. So, the relational power system database is designed to solve above mentioned problems and to provide greater accuracy in the power system availability. Now, all the information about power system and its components faults are recorded in the place where it could be simultaneously available to several

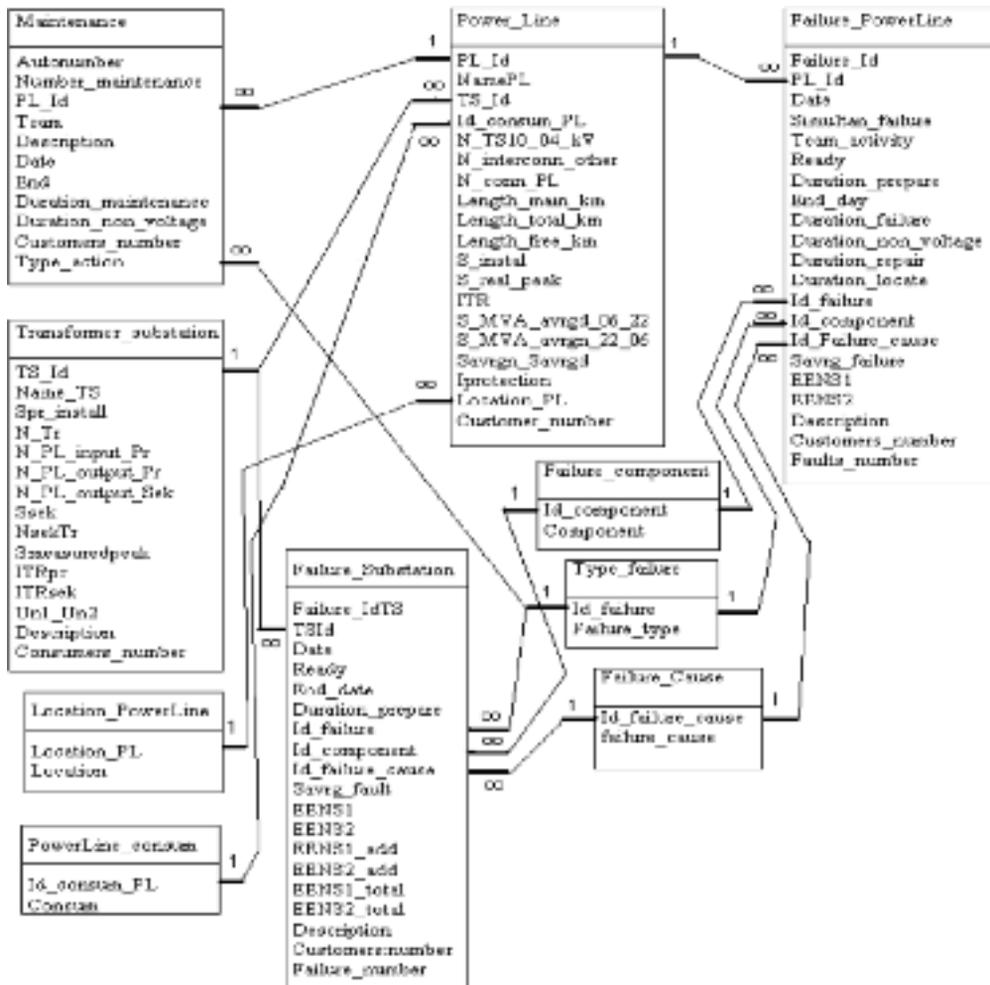


Figure 1. Relationships scheme in the database kikaE2.mdb.

users. The other advantage is in a recording immediately after faults occur, which give us fresh and accurate data. The traditional approach on a faults registration till now was to collect and store these data after some time, some of the important facts used to be neglected, based on a subjective men opinion or memory.

## 2.2 Main parts

The relational database KikaE2.mdb (Microsoft Access) with its main parts – tables and relationships is illustrated in Figure 1. The most of the data in database is structured, interconnected, fast accessed, non redundant and sorted, describing events (faults, maintenance), system states (switching states, failure type, failure cause) and objects (components, power lines and transformer substations).

The relation between two tables depends on the connection key determination, with its connection properties and rules. By means of data base queries, it is very easy to filter out desired information. For example, it is easy to filter only one power line faults a user wants from all power system lines faults, and to take into account only faults in desirable time period between two dates by users choice. It is possible to do further filtration by selecting only faults with the same cause, faults of the same components, faults with duration more then 5 or 20 minutes and so on.

Here, two expected energy not supplied (EENS) evaluations are calculated, traditional (EENS1) based on transformers installed power and new real (EENS2) based on real measured power of the previous day in the same non voltage period of the fault day.

## 3 POWER SYSTEM TOPOLOGY

### 3.1 Substations and power lines

The analyzed power systems area Slavonski Brod cover 1983 square kilometers and population of 186,000, about 40,000 consumers and 33.13 MW peak power that is between 1.6% and 2% of Croatian National Electricity Board. The distribution power system is presented in Figure 2.

There are following transformer substations in distribution network in observed area (Table 1): Podvinje 110/35 kV (80 MW) – basic systems feed point and Bjelis 110/35/10 kV (40 MW) – secondary systems feed point and eight transformer substations 35/10 kV, 66.7 km overhead power lines 35 kV and 10.6 km buried power lines 35 kV (see Tables 1–2, and Figure 2). Here, branches are marked by two incident buses.

### 3.2 The power load flow model

The real yearly load diagram (electric power against days during the year, see oscillating line, Figure 3) for

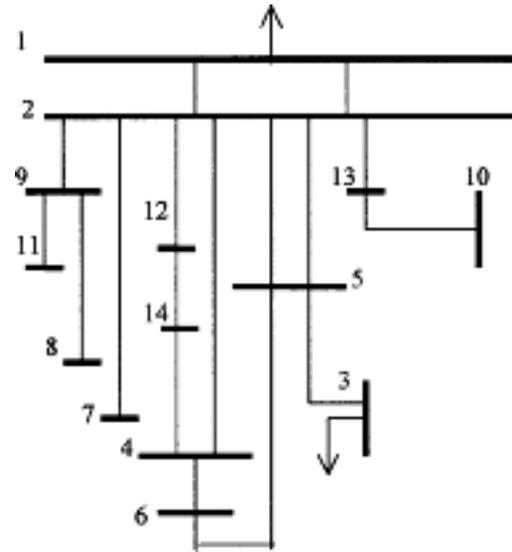


Figure 2. Power system's scheme.

Table 1. Distribution network nodes.

Node/Bus number	Bus name (location)	Transformers installed (MVA)
1	Podvinje110	80.00
2	Podvinje35	80.00
3	Bjelis35	40.00
4	Slavonski Brod1	32.00
5	Slavonski Brod2	16.00
6	Slavonski Brod3	16.00
7	Brodsko Brdo	8.00
8	Oriovac	6.50
9	Brodski Stupnik	0.00
10	Donji Andrijevci	12.00
11	Bebrina	6.50
12	INA-gas	0.00
13	Topolje	0.00
14	Zrinski Frankopan	0.00

the power system is approximated by the stepwise linear lines presenting load duration (Figure 4). The decreasing line (Figure 3) presents the electric power for all days (D) during the year but sorted by their values from the largest to the lowest value.

Each level is marked by the system peak load level (absolute and relative to peak load of the first level) and its occurrence probability (Table 3). The power systems load duration diagram is specified by 5 levels, where the first level is 100% (33.13 MW). It means, for example that 0.55% of the time (48.18 hours/year) load is  $P_M$  (33.13 MW).

Table 2. Distribution network branches.

Branch number	Start node	End node	Power line/transformer type
1	1	2	Transformer 110/35 kV 40 MVA
2	1	2	Transformer 110/35 kV 40 MVA
3	2	4	NA2XS (F) 2Y 3 × (1 × 240) mm <sup>2</sup>
4	2	12	Overhead line Copper 3 × 70 mm <sup>2</sup>
5	2	5	Overhead line Al-steel 3 × 150 mm <sup>2</sup>
6	2	5	Overhead line Al-steel 3 × 120 mm <sup>2</sup>
7	5	6	NKBA – 3 × 150 mm <sup>2</sup>
8	4	6	NKBA – 3 × 150 mm <sup>2</sup>
9	3	5	Overhead line Al-steel 3 × 120 mm <sup>2</sup>
10	13	10	Overhead line Al-steel 3 × 120 mm <sup>2</sup>
11	2	9	Overhead line Al-steel 3 × 120 mm <sup>2</sup>
12	9	11	Overhead line Al-steel 3 × 120 mm <sup>2</sup>
13	2	7	Overhead line Al-steel 3 × 120 mm <sup>2</sup>
14	12	14	NA2XS(F)2Y 3 × (1 × 240) mm <sup>2</sup>
15	14	4	NKBA – 3 × 240 mm <sup>2</sup>
16	2	13	Overhead line Al-steel 3 × 95 mm <sup>2</sup>
17	9	8	Overhead line Al-steel 3 × 120 mm <sup>2</sup>

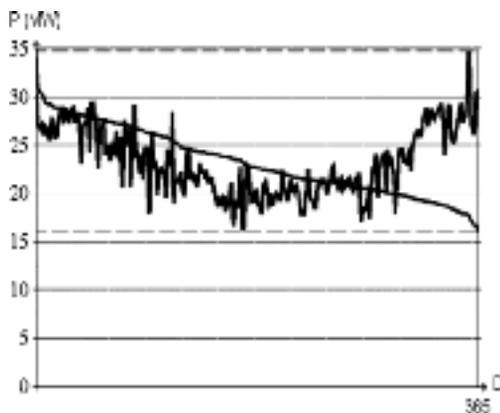


Figure 3. Electric power load diagram during the year (oscillating) and same decreasing characteristic in Area Slavonski Brod, 1999.

The most important step in load approximation process is to preserve the area under load curve in load time dependency graph (save equity of distributed electric energy to consumers). Any quantity evaluation for a part of the year (season, month), which is based on load estimation, has to be start from a beginning by raw load data. In that case this approximation is not good enough to cover usual accuracy.

#### 4 RELIABILITY EVALUATION

Although it is not so easy and grateful to make a model of a power system with distributed components in different weather and load conditions, there are several

Table 3. Stepwise linear lines load duration, Area Slavonski Brod, 1999.

Level	P (MW)	Days per year (D)	P/Ppeak	T (%)
1	33.13	2	1.00	0.55
2	28.26	45	0.85	12.33
3	24.39	155	0.74	42.46
4	20.32	154	0.61	42.19
5	16.89	9	0.51	2.47

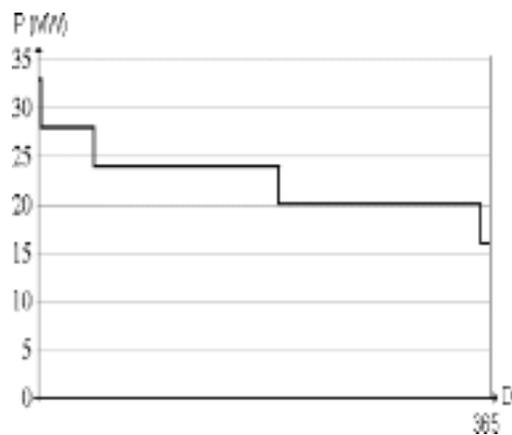


Figure 4. The stepwise linear lines load characteristic in Area Slavonski Brod, 1999.

modeling methods used to accomplish that task. Here, reliability evaluation is based on the analytical method of state space enumeration (using Markov's state space model). This evaluation composes independent failures of the power system components, their coincidence of the first, second and the third order for the branches.

##### 4.1 Reliability output indices

The power system reliability indices we use for quantification adequacy aspect are:

4.1.1 *The number and type of supply interruption*  
 Number of contingencies causing split network – Splt  
 Number of contingencies causing bus isolation – Isol

4.1.2 *The load curtailment reliability indices*  
 Probability of load curtailment (Prob × 10<sup>-3</sup>)  
 Frequency of load curtailment (Freq occ./year)  
 Duration of load curtailment (Dur hours/year)

4.1.3 *The Bulk Power Energy Curtailment Index (BPECI, BP MWh/MW, year)*

This parameter shows quantity amount of unsupplied energy (MWh) per 1 MW installed load power yearly.

It is usually expressed in the system minutes – SM (by multiplying BPECI by 60). It has two interpretations: a) actual system malfunction index SM is presented on an equivalent fault state of power system under the peak load for so many system minutes and b) SM is duration of outage time per each consumer at the system peak load.

#### 4.1.4 The Expected Energy Not Supplied (EENS, ENS)

This parameter is usually shown in MWh/year, but here is in kWh/year. The program does not calculate this parameter directly, and then we calculate it out from BPECI, multiplying with the peak system load ( $P_M = 33.13$  MW).

## 4.2 Output results

Now, we can compare the reliability indices n-1, n-2 and n-3 of the branches failure coincidence level for the observed system. Only the power systems switching states of the same order of the coincidence level during the monitored time period can be compared. It is obvious that reliability evaluation based on the second order for branches (one or two possible failures) include all events of n-1 order of level contingency and all events with two component failures in the power system. Although it is possible to function in closed ring topology (except four transformer substations), the power system can function in the radial topology. Table 4 presents possible radial networks appearance with its marks and branches with open connections between two buses.

It is obvious that there are important differences in output reliability indices between different switching states of the distribution network. Reliability indices listed in chapter 4.1 are evaluated and given in Tables 5–7 depending on contingency order for different power system switching states mark according to Table 4. If the systems switching state C (the best case) is compared with that marked B (the worst switching state by the reliability aspect), it is found out even 53.94% less curtailment load probability, around

Table 4. Distribution network switching states, (radial).

Switching states mark	Open branch 1	Open branch 2	Open branch 2
A	2–4	4–6	2–5 II
B	2–4	5–6	2–5 II
C	12–4	4–6	2–5 II
D	12–4	5–6	2–5 II
E	12–4	5–6	2–5 I
F	2–4	5–6	2–5 I
G	2–4	4–6	2–5 I
H	12–4	4–6	2–5 I

45.55% less expected unsupplied electric energy per year, around 52.4% less load curtailment frequency and 46.6% less load curtailment duration for case A. And furthermore, switching states can be sorted by their reliability indices of n-1 order as following: C, D, A, E, H, G, F and B.

This evaluation is composed of the independent failures of the power system components, their coincidence of the second order for branches. Switching state sorting order is exactly the same as for the reliability evaluation of the first order with significant differences between indices of different switching states of the power system.

In the third order for branches reliability evaluation of the monitored power system, there are not important differences in the output reliability indices between different switching states of the distribution network. For example, if the systems switching state marked C

Table 5. Reliability indices of n-1 order, Distribution power network, area Slavonski Brod (radial topology).

State	A	B	C	D	E	F	G	H
Splt	3	5	1	2	2	5	4	3
Isol	7	6	8	7	8	6	7	7
Prob	4.19	7.56	4.03	4.09	7.35	7.56	7.50	7.40
Freq	24.7	50.0	23.8	24.7	48.1	50.0	49.0	49.0
Dur	36.7	66.2	35.3	35.8	64.4	66.2	65.7	64.9
BP	3.51	6.51	3.29	3.38	6.06	6.51	6.27	6.15
ENS	20.8	34.5	18.8	19.0	30.7	34.5	32.8	30.9

Table 6. Reliability indices of n-2 order, Distribution power network, area Slavonski Brod (radial topology).

State	A	B	C	D	E	F	G	H
Splt	37	47	23	38	29	48	41	42
Isol	59	52	66	52	64	52	58	50
Prob	4.22	7.60	4.07	4.12	7.39	7.60	7.55	7.45
Freq	25.1	50.4	24.2	25.1	48.6	50.5	49.5	49.5
Dur	37.0	66.6	35.6	36.1	64.8	66.6	66.1	65.2
BP	3.55	6.56	3.33	3.42	6.11	6.56	6.32	6.19
ENS	21.0	34.7	18.9	19.1	30.9	34.7	32.9	31.1

Table 7. Reliability indices of n-3 order, Distribution power network, area Slavonski Brod (radial topology).

State	A	B	C	D	E	F	G	H
Splt	209	236	155	248	167	237	220	258
Isol	237	216	273	184	273	216	237	184
Prob	7.55	7.60	7.39	7.45	7.39	7.60	7.55	7.45
Freq	49.5	50.4	48.6	49.5	48.6	50.5	49.5	49.5
Dur	66.1	66.6	64.8	65.2	64.8	66.6	66.1	65.2
BP	6.32	6.56	6.11	6.19	6.11	6.56	6.32	6.19
ENS	32.9	34.7	30.9	31.1	30.9	34.7	32.9	31.1

(the best case) is compared with that marked F (the worst switching state by the reliability aspect), it is found out only 2.74% less curtailment load probability, around 11% less expected unsupplied electric energy per year, around 3.76% less load curtailment frequency and 2.73% less load curtailment duration for case A. The third contingency order evaluation has only theoretical meaning due to low probability value for state with more then two fault components in the same time.

Switching states can be sorted by their reliability indices of n-3 order as following: C, E, H, D, A, G, B and finally F. This switching states ranking is different then rankings for n-1 and n-2 branches order reliability evaluation and it could be used when one branch is on planned revision for long time period.

Besides reliability indices for complete power system it is possible to obtain some kinds of result indices for each bus; for example Tables 8, 9, 10 and

Table 8. Expected bus indices of n-1 order, Distribution power network, area Slavonski Brod (radial topology, marked E).

Bus k	Probk	Freqk	ENSk	Durk
10	3.551	25.84	133.77	31.11
11	3.478	18.21	48.14	30.47
8	2.678	15.19	86.32	23.46
6	0.089	1.26	4.09	0.78
7	0.081	0.75	2.40	0.71
4	0.029	0.24	1.80	0.25

Table 9. Maximum energy curtailed bus indices of n-1 order, Distribution power network, area Slavonski Brod (radial topology, marked E).

Bus k	Probk	Freqk	ENSk
4	0.029	0.24	7.46
8	2.492	12.95	6.20
10	0.200	1.26	5.97
6	0.089	1.26	3.25
7	0.081	0.75	3.22
11	2.492	12.95	2.66

Table 10. Maximum duration curtailed bus indices of n-1 order, Distribution power network, area Slavonski Brod (radial topology, marked E).

Bus k	Probk	Freqk	Durk
8	2.492	12.95	1.69
11	2.492	12.95	1.69
10	0.200	1.26	1.39
4	0.029	0.24	1.04
7	0.081	0.75	0.95
6	0.089	1.26	0.62

11 presents bus indices for the switching state of the power system marked E, n-1 contingency order.

All presented output reliability indices are results of the evaluation for the power system as it is today according to the relational database for power lines faults for period from 1. January 1998. to 30. April 2000. There are power faults data for period from June 1992 to June 1997 obtained from the Plant Logs of each transformer substation. Power system in that period was constituted of 16 branches (one less then today) because one-third of overhead line between buses 2 and 12 is latter changed by buried power line NA2XS (F) 2Y 3 × (1 × 240)mm<sup>2</sup>, making a new bus (14). Above mentioned reconstruction reduced impact of weather conditions and war damages. The output reliability indices for the radial topology marked G (disconnected branches 2-4, 4-6 and 2-5 I) of the former power system for coincidence of the first, second and third order are presented in Table 12.

Although the number of contingencies causing split network (Splt) and bus isolation (Isol) in the former power system is less then indices in today power system (because of existing one extra bus today), all others reliability indices are lower than indices in today power system.

All in all, we have done quantity analysis of the reliability in the power system for radial network. Now it

Table 11. Average bus indices of n-1 order, Distribution power network, area Slavonski Brod (radial topology, marked E).

Bus k	ENSk	Durk
4	7.475	1.04
8	5.683	1.54
10	5.178	1.20
6	3.255	0.62
7	3.215	0.95
11	2.644	1.67

Table 12. Reliability indices of n-1, n-2 and n-3 order, Distribution power network, former constitution of area Slavonski Brod (radial topology, marked G).

Coincidence order	n-1	n-2	n-3
Splt	3	34	179
Isol	7	51	189
Prob	7.816	7.869	7.869
Freq	52.08	52.63	52.63
Dur	68.47	68.93	68.93
BP	6.709	6.767	6.767
ENS	34.83	35.01	35.01

is very easy to select a system topology and to sort it by their reliability indices.

## 5 CONCLUSION

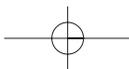
One of the main reliability evaluations of power system targets is system and its components analysis and approaching the power system by reliability aspect. It means that power system engineer have to be informed in advance about the further possible steps in the selection topology of a power system with as much as possible savings. No one can expect from a technical manager to do the evaluation when the fault(s) occur, reliability evaluation study have to be already done, defining and directing sequence of switching devices manipulation in any circumstances. Maybe the most logical way to meet these requirements is to create manipulation tables based on results of the reliability evaluation, reestablish the rules and constitutions to control a system function. It is useful to skip power system buses with good reliability parameters, find out branches which are endangered (planned for reconstruction them or for adding parallel branch), reduce faults number and duration, diminish prearranged supply interruptions number and duration (scheduled revisions on the power system or its parts), improve repair

efficiency on faults occurrence including storage of spare components with short age, in four words – better power supply quality.

The basic quality indices of the power supply are acceptable level of voltage and frequency variations as well as interruptions (number, duration) in the power supply. All of these criteria are essential for our business customers, and especially for the industry, trades, hospitality, restaurants, farming, agriculture, education, government etc. So, important financial decisions in the power system managing are made on the basis of the reliability evaluation.

## REFERENCES

- Billinton R. & R.N. Allan 1983. Reliability Evaluation of Engineering Systems. Boston, London, Melbourne: Pitman Advanced Publishing Program Inc.
- Power System Research Group, University of Saskatchewan 1995. COMREL Users Manual. San Diego: Power Math Associates Inc.
- Billinton R. & R.N. Allan 1984. Reliability Evaluation of Power System. Boston, London, Melbourne: Pitman Advanced Publishing Program Inc.
- Wang L. & J. Endreny 1993. Reliability techniques in large electric power systems. Toronto: Academic Press.



## The safety of risk or the risk of safety?

S.I. Suddle

*Delft University of Technology & Corsmit Consulting Engineers Rijswijk, The Netherlands*

P.H. Waarts

*TNO, The Netherlands*

**ABSTRACT:** Safety is nowadays one of the main items on the agenda during the planning, realisation and management of most large-scale projects, particularly in infrastructure and building projects in intensively used areas such as multiple use of land projects. It is vital that safety aspects are properly assessed at an early possible stage of the project. In this paper relations between safety and risk are suggested. In order to quantify the safety in objective terms, risk (analysis) is used as an important tool. However, definitions of risk vary from global and informal to objective variants and consists both psychological and mathematical elements. When a risk analysis is performed, one has to consider these definitions. In this paper, both psychological and mathematical risk definitions are mentioned and their interrelation is described. An essential element in risk assessment is risk evaluation. When a risk analysis is performed, it is also important to realise that decision making about risks is very complex and that not only technical aspects but also economical, environmental, comfort related, political, psychological and societal acceptance play an important role. Finally, a recommendation has been made for narrowing the gap between deterministic and probabilistic approach by use of Bayesian Networks. It appears that these networks are also useful in order to integrate psychological and mathematical definitions of risk.

### 1 INTRODUCTION

From a psychological, social and risk point of view, safety is a wide notion. According to [Vrouwenvelder et al., 2001], safety is the state of being adequately protected against hurt or injury, freedom from serious danger or hazard. In the philosophy of safety, safety is usually classified into *social safety* and *physical safety* [Durmisevic, 2002; Suddle, 2002<sup>A</sup>; Voordt & Wegen, 1990]. Social safety implicates the behaviour among persons. Crime incentive factors, spatial factors, institutional factors and social factors of an area are characteristics of social safety. In contrast, physical safety contains both the probability of a person being killed or injured by *natural hazards*, like bad weather, an earthquake, floods and the probability by *man-made hazards* like traffic, calamities by transport of dangerous materials, calamities by nuclear reactors etc. In some cases, like fire, it is difficult to classify which kind of safety it is. A subdivision within physical safety is made by *internal safety* and *external safety* [Vrijling et al., 1998]. The following subdivision, here ranked according to increasing benefit to the persons at risk is frequently found.

Safety		
<i>Social Safety</i>	<i>Physical Safety</i>	
	<i>Natural &amp; Man-made hazards</i>	
Crime incentive factors Spatial factors Institutional factors Social factors	Internal Users Passengers Personnel	External Third parties

Figure 1. Subdivision of safety.

### 2 SAFETY AND RISK

#### 2.1 Introduction

Generally, safety consists both of subjectivity and objectivity elements. A person who experiences that he is safe from a psychological point of view, does not automatically implies he is safe from a mathematical point of view and vice versa. The relation between subjectivity and objectivity components of safety can be presented with aspects of irrational behaviour [Bouma, 1982].

	Subjective Safe	Subjective Unsafe
Objective Safe	Healthy un-concern	Paranoia
Objective Unsafe	Naivety	Healthy anxiety

Figure 2. Aspects of irrational behaviours.

Subjective safety is related to psychological aspects (see also [Stoessel, 2001]), while objective safety is based on mathematical grounds. Note that sometimes the objective safety is also based on subjective estimates. To define and to quantify the objective elements of safety, it is vital to link safety with *risk*. In essence, it can be assumed that safety, either internal or external, is complementary with the level of risk [Suddle, 2002<sup>A</sup>] (see fig. 3). This means to reach a low-risk level, one has to make investments for safety measures, while one may expect both human and financial risks, such as casualties and loss of human live in accordance with a minimum level of safety (high-risk level). If the level of acceptability and tolerability of risk would be embedded correctly, the optimum level of safety would have laid on the minimum of the sum of investments and expecting risks.

The survey of Vlek [Vlek, 1990] yielded 20 definitions of risk, which vary from global informal definitions to objective variants. The 11 formal definitions of risk or riskiness, which can be distinguished from those 20, are presented in table 1.

This collection of risk definitions may be considered by viewing risk as the characterization of: (a) a single possibility of accident, loss or disease (defs 1–4), (b) a collection of accident possibilities (defs 5–7), and (c) an *activity* having accident (and other) possibilities (defs 8–11) [Vlek, 1996]. Table 1 does hardly consist informal definitions of risk, which are related to social and psychological aspects. Still, the community demands that engineers and designers take both social and psychological aspects into account when doing and evaluating risk analysis.

## 2.2 Psychological definitions of risk

One of the first conceptual analyses of risk is carried out by Vlek [Vlek, 1990]. This analysis is based on decision-making and empirical-psychological work on the nature and the dimensions of risks and hazards. Examples of psychological (informal) definitions

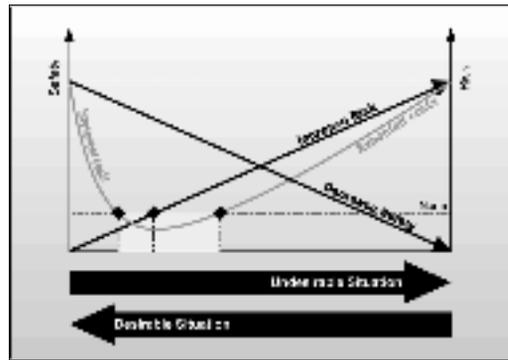


Figure 3. Model safety vs risk [Suddle, 2002<sup>A</sup>].

Table 1. Formal definitions of risk or riskiness (adapted from [Vlek, 1990]).

1. Probability of undesired consequence.
2. Seriousness of (maximum) possible undesired consequence.
3. Multi-attribute weighted sum of components of possible undesired consequence.
4. Probability x seriousness of undesired consequence ("expected loss").
5. Probability-weighted sum of all possible undesired consequences ("average expected loss").
6. Fitted function through graph of points relating probability to extent of undesired consequences.
7. Semivariance of possible undesired consequences about their average.
8. Variance of all possible undesired consequences about mean consequences.
9. Weighted sum of expected value and variance of all possible consequences.
10. Weighted combination of various parameters of the probability distribution of all possible consequences (encompasses 8 en 9).
11. Weight of possible undesired consequences ("loss") relative to comparable possible desired consequences ("gain").

from [Vlek, 1990; Schaalsma et al., 1990] are "lack of perceived controllability", "set of possible negative consequences" and "fear of loss". From [Vlek, 1990], it can be concluded that one has to consider the way people interpret risk in risk management, also called *risk perception*. The interpretation is different for a single person and a group of persons [Gezondheidsraad, 1995; 1996]. The perception of risk differs by factors in relation with [Vlek, 1990]:

- The origin of the hazard
- The social context
- The personal remarks

Table 2. Basic dimensions underlying perceived riskiness (adapted from [Vlek, 1996]).

1. Potential degree of harm or fatality.
2. Physical extent of damage (area effected).
3. Social extent of damage (number of people involved).
4. Time distribution of damage (immediate and/or delayed effects).
5. Probability of undesired consequence.
6. Controllability (by self or trusted expert) of undesired consequences.
7. Experience with, familiarity, imaginability of consequences.
8. Voluntariness of exposure (freedom of choice).
9. Clarity, importance of expected benefits.
10. Social distribution of risks and benefits.
11. Harmful intentionality.

It may be assumed that these aspects are related to the risk perception and aspects of subjective safety, as presented in figure 2. According to [Vlek, 1996] dimensions of underlying perceived riskiness, which are related to risk perception, must be taken into account in risk management, as presented in table 2.

Note that these dimensions of underlying perceived riskiness consists mainly variants of both subjectivity and objectivity (as presented in figure 1). In [Vlek, 1996] different scale-levels of risk and risk management are suggested, which amplify the aspects of subjectivity. These psychological definitions, however, are basic ingredients for the assessment of risk. Besides, these add value to the perception of risk and play a vital role in risk acceptance and decision-making. Additionally, in [Vlek, 1990], it is recommended to take additional measures for the comfort of safety, especially for persons who feel themselves as unsafe, while objectively it is safe. Moreover, it is recommended in the survey [Vlek, 1990] not only to comply with the risk acceptance criteria, but also to apply the safest option regarding measures in accordance with the budget of the project. Therefore in some conditions one may deliberate the costs and the benefits of that project.

Thus, according to [Vlek, 1990; 1996] it may be concluded that (safety) measures are desired, and must be explored in the risk management process to increase the subjective level of safety. However, these argumentation are psychological and do not provide the answer to the question "how much safe or unsafe is an activity or what is the effect of a safety measure in accordance with safety and financial aspects". In order to answer such question in objective terms and to determine safety, there is a need for a quantifiable (mathematical) approach and not an informal psychological. Besides, a mathematical approach enables to compare

risk of different activities and use the risk analysis as a basis for rational decision-making. It is therefore useful to quantify the aspects of subjectivity of table 2 and to integrate in decision-making.

### 2.3 Mathematical definitions of risk

The common definition of risk (associated with a hazard) is a combination of the probability that hazard will occur and the (usually negative) consequences of that hazard [Vrouwenvelder et al., 2001; Vrijling et al., 1998]. In essence, it comes down to the following expression, which is the same definition as definition 4 of table 1:

$$R = P_f \cdot C_f \quad (1)$$

where:

$R$  = Risk [fatalities or money year<sup>-1</sup>];

$P_f$  = Probability of failure [year<sup>-1</sup>];

$C_f$  = Consequence of the unwanted event [fatalities or money].

This definition mostly is used in risk analysis. Consequences ( $C_f$ ) to be taken into account include:

- Injury, or loss of life, due to structural collapse
- Reconstruction costs
- Loss of economic activity
- Environmental losses

Mostly, there is a (reverse) relation between the probability that a hazard will occur and the consequences of that hazard. More complicating still is the gradual unfolding of a host of differing definitions of risk [Coombs, 1972; Libby & Fishburn, 1977; Vlek & Stallen, 1980]. According to [Kaplan & Garrick, 1981], risk consists of three components:

- Scenario
- Probability of scenario
- Consequence of scenario

Following [Kaplan & Garrick, 1981] risk cannot be properly expressed in terms of a single number or even a single curve. In their view the best formal definition of risk is a probability distribution of possible (future) frequencies of harmful consequences, which themselves may be multidimensional in nature.

### 2.4 Comparison of psychological and mathematical definitions

The description of risk given by [Kaplan & Garrick, 1981] hardly differs from the mathematical one of [Vrijling & Vrouwenvelder, 1997], because both probability and consequence of scenario are included. According to [Kaplan & Garrick, 1981] one has to consider all hazards in account, which can be accomplished by summing up all possible hazards (scenarios) with

their consequences for an activity. Therefore as an obvious extension, multiple scenarios (indexed  $i$ ) may be taken into account. This can be presented in the following formula:

$$R = \sum_{i=1} P_{f_i} \cdot C_{f_i} \quad (2)$$

According to [Vrouwenvelder et al., 2001] probability is, generally speaking, the likelihood or degree of certainty of a particular event occurring during a specified period of time. Assuming that a system may be found in mutually exclusive situations  $H_i$ , and the failure  $F$  of the system (e.g. of the structure or its element) given a particular situation  $H_i$  occurs with the conditional probability  $P(F | H_i)$ , then the total probability of failure  $P_f$  is given by the law of total probability as:

$$P_f = \sum_{i=1} P(H_i)P(F | H_i) \quad (3)$$

Substitution of formula (3) in (2) gives:

$$R = \sum_{i=1} P(H_i)P(F | H_i)P(C | H_i \cap F) \quad (4)$$

where:

$P(C | H_i \cap F)$  = the probability of a consequence given that  $H_i$  and  $F$  occur.

Formulas (1), (2) and (4) are presented as mathematical variants. However, these are also mentioned in the psychological dimensions of risk (see table 1). The three components of formula (4) correspond with the definitions of risk as mentioned in tables 1 and 2. Therefore, from an objective safety assessment point of view one may assume that even psychological definitions from [Vlek, 1990] are integrated into mathematical definitions of [Kaplan & Garrick, 1981] combined with [Vrijling & Vrouwenvelder, 1997]. The psychological part of the mathematical definition emphasises particular the consequence of a scenario. From a mathematical point of view, all possible consequences are taken into account in risk analysis (see formulas (2) and (4)). Besides, the subjective aspects with accordance with psychology, which are mostly related to the acceptability of risk, are also integrated in acceptability and tolerability of risk in terms of vulnerability and the direct benefit of a person. From a mathematical point of view, the acceptability and tolerability of societal risk provides a tool in which it is common to accept less the probability of an event consisting big numbers of fatalities. This concept of risk aversion is also included in these risk acceptance criteria (e.g. societal and individual risk (see paper Suddle, S.I., *A Logarithmic approach for Individual risk: The safety-index*, this proceedings).

In some cases, especially scenarios with great consequences, *weighing factors* for all risk dimensions are used in order to make them comparable to each other and to relate them to the measures that must be taken for possible risk reduction [Coombs, 1972; Libby & Fishburn, 1977; Vlek & Stallen, 1980; Vlek, 1990; Vrouwenvelder et al., 2001]. It is, therefore, recommendable to compare and to integrate these definitions in one-dimensional weighted risk ( $R_w$ ) in terms of money as following:

$$R_w = \sum_{j=1} \alpha_j \sum_{i=1} P_{f_{ij}} \cdot C_{f_{ij}} \quad (5)$$

$$R_w = \sum_{j=1} \alpha_j \sum_{i=1} R_{ij} \quad (6)$$

where:

$R_w$  = weighted risk [ $\text{year}^{-1}$ ];

$\alpha_j$  = (monetary) value per considered loss [].

It has to be noted that weighted risk ( $R_w$ ) may consist of cost unities, which can be financial, but it is not necessary (see [Seiler, 2000]). Formulas (5) and (6) can be specified into particular risk components:

$$R_w = \alpha_1 \sum_{i=1} R_{human,i} + \alpha_2 \sum_{j=1} R_{economic,j} + \alpha_3 \sum_{k=1} R_{environment,k} + \alpha_4 \sum_{l=1} R_{quality,l} + \dots \quad (7)$$

where:

$\alpha_1$  = (monetary) value per casualty or injury [-];

$\alpha_2$  = (monetary) value per environmental risk [-];

$\alpha_3$  = (monetary) value per economical risk [-] (mostly  $\alpha_3 = 1$ );

$\alpha_4$  = (monetary) value per quality risk [-], and so on.

According to [Lind, 1996] safety criteria are not absolute. Cost-utility is only a part of the economic, social, cultural and political assessments that are required for responsible decision-making. Note that some  $\alpha_j$  may also be negative (e.g. time). Besides, the  $\alpha_j$  is in particular correlated with the consequences ( $C_j$ ), in which the correlation is not necessary to be linear. (The first component (human risk) of formulas (7) can be subdivided into:

$$\alpha_1 \sum_{i=1} R_{human,i} = \sum_{k=1} \alpha_{1k} \sum_{n=1} R_{human,nk} \quad (8)$$

where:

$\alpha_{1k}$  = monetary value per considered basic dimensions of underlying perceived riskiness as presented in table 2 [money].

So,  $\alpha_{1k} \in \{\alpha_1, \alpha_2, \dots, \alpha_{11}\}$  of table 2. These monetary values  $\alpha_1, \alpha_2, \dots, \alpha_{11}$  are functions of subjective aspects of table 2 and can be determined by multi criteria analysis. If one adds monetary value to these different aspects, one can integrate all kind of subjective aspects into risk analysis, such as value for area effected ( $\alpha_2$ ), value for number of people involved ( $\alpha_3$ ), value for time ( $\alpha_4$ ), value for voluntariness ( $\alpha_3, \alpha_8, \alpha_{11}$ ), etc. According to [Seiler, 2000], the monetary value per casualty or costs per live saved of a person depends on the voluntariness of an activity (see table 3).

If these subjective aspects are quantified in weighted risk (analysis), and thus in one (monetary) dimension, safety measures can be balanced and optimised in respect of decision-making as following:

$$\text{Minimize: } C_{tot} = C_0(y) + \sum_{j=1} \frac{R_{wj}}{(1+r)^j} \quad (9)$$

where:

- $C_{tot}$  = total costs;
- $C_0(y)$  = the investment in a safety measure;
- $y$  = decision parameter;
- $j$  = the number of the year;
- $r$  = real rate of interest;

Hence, one may assume that for rational decision-making it is desired to objectify the safety in terms of probability and the consequences of all events. Therefore, both mathematical and psychological approaches of risk can and should be quantified by the mathematical variant. It may also be recommended that, for safety studies and risk analysis, risk can commonly be estimated by the mathematical expectation of the consequences of an undesired event that often leads to *the sum of the product probability x consequences combined with the monetary value per considered loss*, is an interesting approach (formula (8) and (9)).

### 2.5 Risk evaluation

When a risk analysis is performed, it is also important to realize that decision making about risks is very complex and that not only technical aspects but also political, psychological and societal processes (all) play an important role [Suddle, 2002<sup>A</sup>; Jonkman et al., 2002]. If a risk analysis is carried out for only the qualitative part, the psychological and political aspects play a major role in risk acceptance and decision-making. Contrarily, when risk analysis is carried out till the quantitative part, limits for risk acceptance and economical criteria are considered for decision-making. Additionally, regarding safety management and control, one has to take measures regarding safety for persons who feel themselves as unsafe, while

Table 3. Costs per live saved of a person depends on the voluntariness of an activity.

Voluntariness of an activity	Individual risk [year <sup>-1</sup> ]	Costs per life saved €
1. Voluntary risk	10 <sup>-3</sup>	1.500.000
2. High degree of self-determination, direct individual benefit (car driving)	10 <sup>-4</sup>	6.000.000
3. Low degree of self-determination, individual benefit (working conditions)	5 · 10 <sup>-5</sup>	15.000.000
4. Involuntary, imposed risk exposition, no direct benefit (local resistance of dangerous installation)	10 <sup>-5</sup>	20.000.000

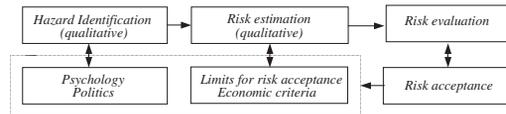


Figure 4. Risk analysis and risk acceptance [Suddle, 2002].

objective it is safe. This is exactly [Vlek, 1990] argued for the comfort of safety for all kind of people.

## 3 APPROACHES FOR RISK ASSESSMENT

### 3.1 Deterministic and probabilistic approach

During the 1950s and 1960s two approaches emerged for analysing safety aspects of potentially hazardous systems, including a *deterministic* approach and a *probabilistic* approach [Weaver, 1980]. The most significant difference between the two approaches is the way probability is dealt with [Vrijling and Stoop, 1999]. *Deterministic* safety analysis is focused on the causal processes of accident scenarios equals 1.

Whereas *probabilistic* risk analysis takes into account the possibility and the likelihood of uncertainty that accident scenarios might occur. As a result, in deterministic analysis the focus is on developing insights into accident scenarios and consequences, whereas in probabilistic risk analysis main efforts are made on the behalf of the quantification of probabilities [Hale, 2000; Rosmuller, 2001]. Thus, one may assume there is an existing gap between the *probabilistic* and *deterministic* methods in risk analysis. If a risk analysis is performed with present models such as fault trees and event trees, this gap will not be narrowed

because of large dimensions and big complexity of such models. Nevertheless, the following paragraphs is an introduction to the theory, which shows that the existing gap can be narrowed by use of Bayesian Networks in risk analysis (see [Suddle, 2001<sup>A</sup>]).

### 3.2 Use of Bayesian Networks

A Bayesian Network is a graphical tool that represents the relations between a set of variables and a set of directed edges between variables [Hansen, 1999; Jensen, 1996; 2001], which can be divided into events and consequences. The major advantage of Bayesian Networks is that these networks can replace and compact both traditional fault trees and event trees in one model [Bobbio et al., 2001]. Thus, these networks provide an effective tool, particularly for enormous risk analysis. According to [Friis-Hansen, 2000] the potential of Bayesian Networks are an intuitive modelling tool, partly based on artificial intelligence that adds transparency and consistency to the models. Normally, the relation between fault trees and event trees are represented in the Bowtie model, which will expand exponentially in case of the relations between the events will increases [Ale, 2002; Oh, 2001]. This can now be replaced into a single compatible Bayesian Network, which grows linear (figure 5).

A Bayesian Network consists of a set of nodes and a set of directed arrows. Each node represents a probability distribution, which may in principle be continuous or discrete. Arcs indicate conditional probabilistic dependence so that the probability of a dependant variable being in a particular state is given for each combination of the states of the receding variables. The dependence structure is thus represented by a set of conditional probability distributions. A variable, which is dependent on other variables, is often referred to as a *child node*.

Likewise, directly preceding variables are called *parents*. Nodes, which have no parents, are called *root nodes* and nodes without children are *leaf nodes*. Bayesian Networks are sometimes referred to as directed acyclic graphs (DAGs), indicating that loops (or cycles) are not allowed. A Bayesian Network is a representation of the joint probability distribution of the entire variable domain  $U = \{X_1, X_2, \dots, X_n\}$ . This is seen by applying the chain rule to factorisation of the joint distribution into a chain of conditional probability distributions [Friis-Hansen, 2000]:

$$P(U) = P(X_1, X_2, \dots, X_n) \quad (10)$$

$$= P(X_1 | X_2, \dots, X_n) P(X_2 | X_3, \dots, X_n) \cdots P(X_n) \quad (11)$$

$$= \prod_i P(X_i | pa(X_i)) \quad (12)$$

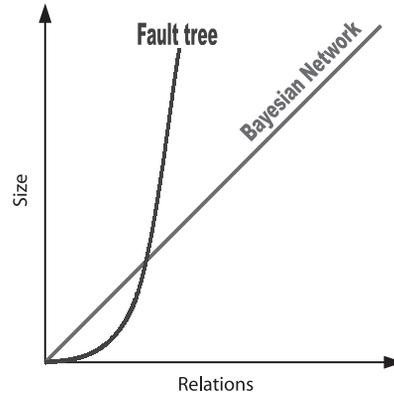


Figure 5. The size of a Bayesian Network is smaller than the traditional fault trees. Hence, a Bayesian Network is much compacter.

where  $P(X_1, \dots, X_n)$  is the joint distribution of  $X_1$  to  $X_n$  and  $P(X_1 | X_2, \dots, X_n)$  is the conditional distribution of  $X_1$  given  $X_2, \dots, X_n$ . The notation  $pa(X_i)$  means the set of parent variables of the variable  $X_i$ . From the updated joint table the marginal distributions of each individual variable may be found by summation over all other variables. This is desired for calculating risk for all scenarios. This is known as sum-marginalisation:

$$P(X_i) = \sum_{U \setminus \{X_i\}} P(U) = \sum_{U \setminus \{X_i\}} \prod_i P(X_i | pa(X_i)) \quad (13)$$

So, if the undesired events ( $H_i$ ), failure modes ( $F$ ), consequences ( $C$ ), safety measures ( $M$ ) and risk ( $R$ ) are elements of the entire variable domain  $U = \{X_1, X_2, \dots, X_n\}$ , than every risk analysis with Bayesian Networks is possible.

$$H_i, F, M, C, S, R \in \{X_1, X_2, \dots, X_n\} \quad (14)$$

These safety measures may include the rescue availability or functional design, which are characteristic for deterministic risk analysis. These measures may also consist structural measures, which are characteristic for probabilistic risk analysis. Besides, integration of these measures is a vital issue from the psychological point of view, as mentioned in section 2.3. This concept provides the methodology for quantifying the effectiveness of safety measures regarding risk, which is desired from a mathematical point of view. A standard Bayesian Network corresponding with a standard risk analysis for basic events may be expressed as:

Considering the previous, it may be assumed that the Bayesian Networks are not only an effective tool for narrowing the gap between the probabilistic and

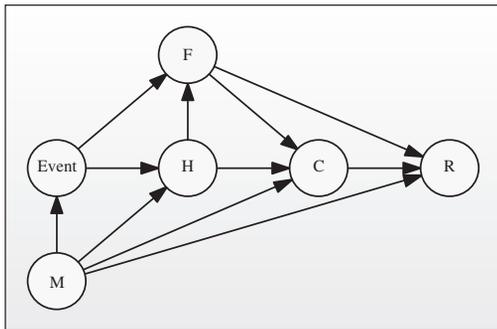


Figure 6. A standard Bayesian Network for risk analysis.

deterministic risk analysis, but Bayesian Networks are useful for combining psychological and mathematical approaches towards risk (analysis). For a case study of such an approach, see paper; Suddle, S.I., *Safety assessment of third parties during construction in Multiple Use of Space using Bayesian Networks*, this proceedings.

#### 4 CONCLUSIONS

Considering the title of this paper “the safety of risk or the risk of safety?”, it is recommendable to observe both components in safety assessment studies. Regarding the safety of risk it is common to objectify the safety in terms of risk with mathematical approaches (the sum of probability  $\times$  consequences) instead of psychological one. In this regard the risk (of the safety) can be computed. In contrast, the safety of the risk characterises the opposite approach. For the safety of the risk it is recommended to take psychological definitions in consideration in risk management process. Therefore one has to combine all risk elements with the monetary value per considered loss.

Hence, one can accomplish all risks in one (monetary) dimension including psychological aspects. In this paper an approach for the integration of both mathematical and psychological definitions is proposed. Such integration can be accomplished with the use of Bayesian Networks. Moreover, these networks provide transparency and consistency to the risk analysis and are useful to both probabilistic and deterministic risk analysis and to combine both mathematical and psychological definitions of risk in a risk management process.

#### LITERATURE

Bobbio, A., L. Portinale, M. Minichino & E. Ciancamerla, *Improving the analysis of dependable systems by mapping fault trees into Bayesian networks*, Reliability

Engineering and System Safety, Volume 71, March 2001, pp. 249–260.

Bouma, H., *Als het leven je lief is*, Max Gelder Stichting, 1982.

Combs, C.H., *A review of Mathematical Psychology of Risk and Risk taking*, University of Michigan: Michigan Mathematical Psychology Program Report MMPP 72-6.

Durmisevic, S., *Perception aspects in underground spaces using intelligent knowledge modeling*, Delft DUP Science 2002. 159 pp.

Friis-Hansen, A., *Bayesian Networks in a Decision Support Tool in Martine Applications*, Department of Naval Architecture and Offshore Engineering, Technical University of Denmark, KGS. Lingby, December 2000, 183 pp.

Gezondheidsraad: Commissie Risicomaten en risicobeoordeling, *Niet alle risico's zijn gelijk*, Den Haag: Gezondheidsraad, 1995; publicatie nr 1995/06, pp. 122.

Gezondheidsraad: Commissie Risicomaten en risicobeoordeling, *Risico, meer dan een getal*, Den Haag: Gezondheidsraad, 1996; publicatie 1996/03, pp. 130.

Hale, A.R., *Collegedictaat WM0801TU: Inleiding algemene veiligheidskunde*, TU-Delft, 2000.

Hansen, P.H., *Introduction to risk analysis; Structural and Stochastic Load Modeling*, Lyngby, Department of Structural Engineering and Materials, Technical University of Denmark, August 9–20, 1999.

Jensen, Finn V., *An introduction to Bayesian networks*, London UCL Press 1996, 178 pp.

Jensen, Finn V., *Bayesian networks and decision graphs*, New York Springer 2001. 268 pp.

Jonkman, S.N., P. van Gelder, H. Vrijling, *An overview of quantitative risk measures and their application for calculation of flood risk*, ESREL 2002, Volume 1, pp. 311–318.

Kaplan, S. & B.J. Garrick, *On the quantitative definition of risk*, Risk Analysis, Volume 1, pp. 11–27.

Libby, R., P.C. Fishburn, *Behavioural models of risk taking in business decisions: a survey and evaluation*, Journal of Accounting Research, Autumn, pp. 272–292.

Lind, N.C., *Target reliability levels from social indicators*, Structural safety, 1994.

Oh, J.I.H., *Co-operation between regulator and industry with respect to inspections*, Ministerie van Sociale Zaken en Werkgelegenheid, mei 2001.

Rosmuller, N. *Safety of transport Corridors*, dissertation, TU-Delft, Trail Thesis Series, May 2001, pp. 336.

Schaalma, H.P., C.A.J. Vlek & P.F. Lourens, *Veiligheid vervoer te water; perceptie, beoordeling en acceptatie van risico's van het vervoer over de Nederlandse binnenwateren*, Haren Rijksuniversiteit Groningen, Verkeerskundig Studiecentrum 1990, 158 pp.

Seiler, H., *Risiko-basiertes Recht – Elemente einer einheitlichen Politik zur regulierung technischer Risiken. Abschlussbericht des Gesamtprojekts FNP Risk Based Regulation – ein taugliches Konzept dur das Sicherheitsrecht*, Berne Staempfi, 2000.

Stoessel, F., Can we learn to accept risks, Conference report, “Safety, Risk and reliability – Trends in engineering”, Malta, 2001.

Suddle, S.I., *Veiligheid van bouwen bij Meervoudig Ruimtegebruik*, afstuderrapport, TU-Delft, April 2001, 298 pp.

- Suddle, S.I., *Beoordeling veiligheid bij Meervoudig Ruimtegebruik*, Cement, Volume 54, no. 1/2002, Februari 2002, pp. 73–78.
- Vlek, C.A.J., *Beslissen over risico-acceptatie; een psychologisch-besliskundige beschouwing over risicodefinities, risicovergelijking en beslissingsregels voor het beoordelen van de aanvaardbaarheid van riskante activiteiten*, Rijksuniversiteit Groningen, 's-Gravenhage: Gezondheidsraad, 1990, 236 pp.
- Vlek, Ch. & P.J. Stallen, *Rational and personal aspects of risks*, Acta Psychologica, Volume 45, pp. 273–300.
- Vrijling, J.K. en J. Stoop, *Naar één beslismodel voor de veiligheid*, Watertovenaars, Vol. 17, pp. 202–213, Rijkswaterstaat, 1998.
- Vrijling, J.K., W. van Hengel, R.J. Houben, *Acceptable risk as a basis for design*, Reliability Engineering and System Safety, Volume 59, 1998, pp. 141–150.
- Vrijling, J.K., A.C.W.M. Vrouwenvelder e.a., *Kansen in de civiele techniek, Deel 1: Probabilistisch ontwerpen in de theorie*, CUR-rapport 190, CUR, Gouda, maart 1997.
- Vrouwenvelder, A.C.W.M., *Risk Assessment and Risk Communication in Civil Engineering*, CIB Report, Publication 59, Februari 2001.
- Voordt, D.J.M. van der & H.B.R. van Wegen, *Sociaal veilig ontwerpen; checklist ten behoeve van het ontwikkelen en toetsen van (plannen voor) de gebouwde omgeving*, TU-Delft: Publikatieburo Bouwkunde, 1990, 128 pp.
- Weaver, W.W., *Deterministic criteria versus probabilistic analysis: Examining the single failure and separation criteria*, Nuclear Safety, Volume 47, No. 2, 1980, pp. 234–243.

## Safety assessment of third parties during construction in multiple use of space using Bayesian Networks

S.I. Suddle

*Delft University of Technology & Corsmit Consulting Engineers Rijswijk, The Netherlands*

**ABSTRACT:** Lack of space leads to the design and construction of projects which make intensive and optimal use of the limited space. Buildings above roads, railways and buildings themselves are examples of intensive use of space projects. The construction processes of those buildings are in general extremely complicated. Safety is one of the critical issues. A research has recently been completed [Suddle, 2001] about the safety for people present in the neighbourhood of these projects (such as users of infrastructure where above buildings are being built). This paper will purpose a methodology for the assessment of safety for such people using Bayesian Networks.

### 1 INTRODUCTION

In spite of many obstructions regarding construction safety, there have been already a number of different projects realised in The Netherlands. Examples of such projects are buildings situated on top of the motorway "Utrechtse Baan" in The Hague. An important lesson from these projects is learned; activities during construction phase of such projects form a hazard for people present on infrastructure beneath – called *third parties* – such as drivers and passengers [Meijer & Visscher, 2001; Suddle, 2001<sup>A</sup>]. However, on the basis of law there are no explicit norms for the safety of third parties during construction, especially not for such projects [Suddle, 2001<sup>B</sup>]. Besides, methodology of safety assessment of third parties in such conditions is up until now not developed. Case studies of projects built over the motorway Utrechtse Baan showed that specifying requirements regarding safety at an early possible stage during the design phase decreases risks for third parties during construction. It is essential to have clarity among those who are responsible for taking safety measures. Moreover, it is necessary to have an adequate and effective organisation at the construction site. This can restrict potential danger during construction [Meijer & Visscher, 2001; Suddle, 2001<sup>A</sup>].

Before realising such projects, one has to consider, which aspects mainly influence the safety of third parties during construction and how the safety of third parties can be assessed during construction of

such projects. Moreover, the use of infrastructure must be maintained during construction of the building above. Therefore the knowledge about safety system in construction phase of such projects and effectiveness of safety measures in accordance with human and financial risks is essential. It has to be noted that the measures have to be financial attractive and must comply with the level of risk acceptance criteria, to be divided into criteria on an individual and on a social basis [Vrouwenvelder et al., 2001; Vrijling & Vrouwenvelder, 1997].

### 2 CLASSIFICATION OF SAFETY ASPECTS DURING CONSTRUCTION PHASE

To determine the safety and thus the risks for third parties in multiple use of land projects, a classification has been made for aspects, which influence the safety of third parties during construction. This classification consists of four main aspects (see figure 1). A full scope of these aspects is presented in [Suddle, 2001<sup>A</sup>].

#### 2.1 Regulations

In order to carry out a flexible process, regulations basically provide an effective tool for all actors and their relations during any stage of any project. In essence, regulations, like guidelines for contractors, that control the safety during construction. However, in case of multiple use of space projects, these regulations

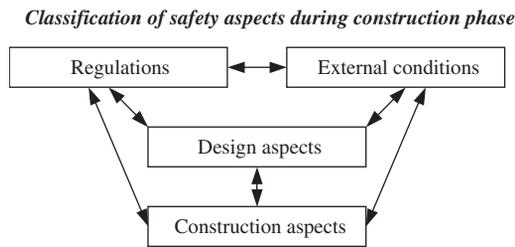


Figure 1. Classification of safety aspects of third parties during construction phase [Suddle, 2001<sup>A</sup>].

are hardly effective and thus not explicit. Other types of regulations are meant for structural calculations, materials, quality sets, organisation at the site etc. Both national and international standards are a part of this main aspect.

### 2.2 External conditions

External conditions are a main parameter for the safety of third parties. The location of the building, which depends on the (traffic) condition beneath, forms a fundamental aspect of external conditions. These parameters determine both the intensity and the speed of traffic. Furthermore, it is important to realise that safety (of third parties) during construction depends on whether the building is being constructed (e.g. above roads or above railway tracks) or the height level of the infrastructure. Typically, the surroundings impose these conditions. The position of cables in the underground can be also considered in this main part. Therefore, some of these parameters can hardly be influenced. However, one may prevent risk for third parties by logistic measures e.g. close off the road and reroute the traffic during construction.

### 2.3 Design aspects

Other parameters, which influence safety of third parties, are related to design aspects. These aspects depend on e.g. dimensions of the building, architectural design, structural elements, functional design of the building and technological aspects. These parameters, which are characteristics of the considered project can be influenced and controlled in the project design phase.

### 2.4 Construction aspects

Finally, characteristic aspects related to construction work can be mentioned as a main part for safety of third parties. Aspects fixed in the design phase hardly can be changes during construction. Hence, mistakes made in the design phase will always come to light in the construction phase. The construction (phase) is

characterised by many parties involved. Therefore, the organisation between these parties is crucial as well. In this phase, regulations, boundaries and preventive measures regarding safety of third parties during construction, is relevant.

## 3 RISK ANALYSIS

### 3.1 Qualitative risk analysis

Considering the safety aspects during construction phase, the relation between these aspects of construction in multiple use of land and their risk has been analysed. Accordingly, risk analyses have been made for several cases. First, a qualitative risk analysis for the safety of third parties has been performed by FMEA-techniques (Failure Mode and Effect Analysis). This technique represents a complete view of hazards and consequences. In this study this technique is applied for the construction of a building over a motorway (a full scope of the FMEA is presented in [Suddle, 2001<sup>A</sup>]). Normally a FMEA consists effects of failure like cost increase, time loss, loss of quality, environmental damage and loss of human life. Considering the aim of this study, risk regarding cost increase and loss of human life are taken into account. A part of the FMEA is presented in table 1 (adapted from [Suddle, 2001<sup>A</sup>]).

It appeared from the FMEA [Suddle, 2001<sup>A</sup>] that safety of third parties during construction largely depends on *falling elements*. The falling objects may consist of bolts, screws, part of concrete (structures), parts of a scaffold, building parts, hammers, beams, or even construction workers.

### 3.2 Quantitative risk analysis

Hence, these falling elements may cause casualties among people present at the infrastructure and in some cases economical risks as well as. This observation is analysed in more detail by a quantitative risk analysis using Bayesian Networks for a case [Suddle, 2001<sup>A</sup>]. This case consists of a building of 10 stories that is built above a 2 × 2 lane motorway. The span and the linear direction of the building are respectively 20 meters and 50 meters. Two risks, loss of human life and economic loss, are considered in these networks. (see figure 2)

In this regard, possible quantifiable parameters should be transformed into conditional probabilities, which are determined from both the classification aspects for safety of third parties during construction (section 2) and the FMEA (table 1). These quantifiable aspects are the following:

- the position where the element falls (inside or outside the building);

Table 1. An example of the FMEA for safety of third parties during construction (adapted from [Suddle, 2001<sup>A</sup>]).

Failure mode	Failure mechanism	Effect of failure
<i>Activity: Ground activities</i>		
<i>Activity: Fabricate elements</i>		
<i>Activity: Fabricate elements</i>		
<i>Activity: Concrete work</i>		
Logistic problems	Planning fault	Time loss
Collapse of concrete element	Design fault	Costs, time loss, casualties
Fixing concrete elements	Element falls	Costs, time loss, loss of quality, casualties
Huge deformations of elements	Element collapses and falls	Costs, time loss, loss of quality, casualties
No right composition of concrete	Production fault	Costs, time loss, loss of quality
<i>Activity: Installing temporary structures/scaffolds</i>		
Fixing temporary structures	Construction fault	Costs, time loss, casualties
	Collapse of temporary structures	
	Construction falls	
	Construction element falls	
<i>Activity: Remove temporary structures</i>		

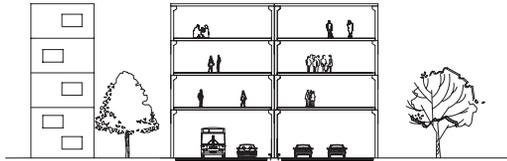


Figure 2. Case 2 × 2 lane motorway.

- the situation below the building;
- (design) errors;
- the weight of the falling element;
- the actions of elements in relation with the installation of elements;
- the collapse of the main structure of the building caused by falling elements;
- the probability of elements falling;
- the height from which the element is falling;
- fatalities and economic risk.

These aspects are taken into account in Bayesian Networks. Each aspect is represented as a node or is integrated in these networks (see figure 3). Each node is divided into categories corresponding with events of that node. The relations between the nodes are connected with arcs, which specify the probable influence between these nodes.

These probabilities are determined by historical data, expert opinion or by engineering judgement.

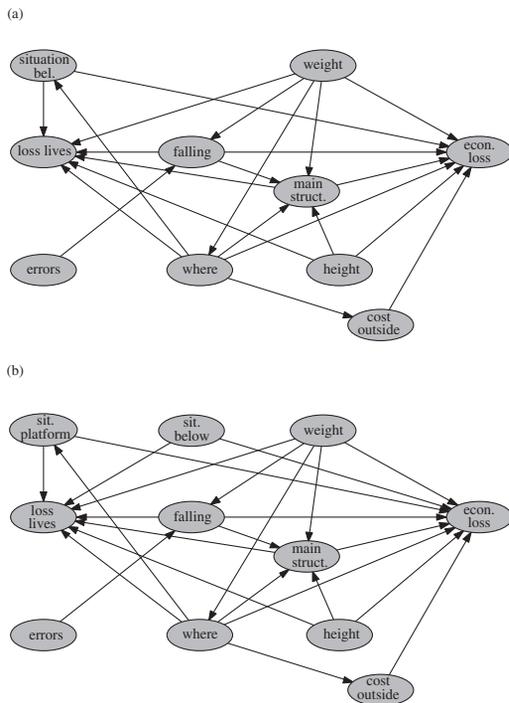


Figure 3. Bayesian Network for building above roads (a) and above railway tracks (b).

In some cases, especially cases, where historical data cannot be found in literature and for that reason expert opinion or engineering judgement is used. Same order magnitude following from occurrence frequencies of hazardous events combined with different probabilities are used to determine the failure probability.

### 3.3 Quantification of probabilities and relations of aspects

- the position where the element falls (inside or outside the building);
 

The position where the element falls depends on the considered surface. The ratio of the building surface and the surface of risk zones outside the building  $A_{building}/A_{outside1,2}$  determines the  $P(\text{element falls outside or inside the building} | \text{element falls})$ . In this analysis, the value of risk zones outside the building ( $A_{outside1,2}$ ) is estimated on 2 meters out of the façade of the building (see figure 4).
- the situation below the building;
 

In order to compute the probability of a person of the third party is being hit by a falling element, it is relevant to know the situation below the building. The situation below the building corresponds with the  $P(\text{element falls on a car or the road} | \text{element falls outside})$  and  $P(\text{element falls on cars} | \text{element falls inside} | \text{building collapses})$  can be determined respectively by the ratio of total cars in the risk zones  $A_{cars}/A_{outside2}$  and total cars beneath the building  $A_{cars}/A_{building}$ .
- (design) errors;
 

An assumption has been made for fatal (design) errors. The  $P(\text{design errors}) = 10^{-4}$ , which correspond with category "remote".
- the weight of the falling element;
 

To investigate the effect of falling element, five different weight-classes (of falling elements), which are used in the building, are formulated: (see table 2)
- the actions with elements in relation with the installation of elements;
 

It is not only the weight class that determines the risk of third parties, but the actions per element particularly are the main cause whether the element falls or not. Therefore, the distribution of total elements in the building is determined regarding the case-study (see figure 5). Subsequently, this distribution is transformed into the distribution of the actions of elements (see figure 5). This means that the output probabilities should be multiplied with the total actions per project per year.
- the collapse of the main structure of the building caused by falling elements;
 

A collapse of the building can only occur if the element falls inside the building during construction. In this respect, the  $P(\text{collapse of the building} | \text{weight$

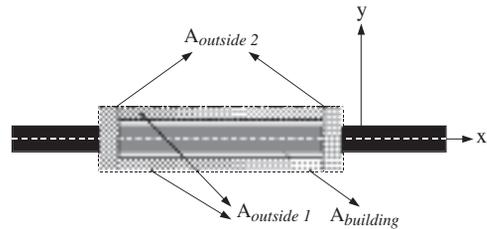


Figure 4. The building surface and the surface of risk zones outside the building.

Table 2. Examples of different weight classes.

Weight-class	Example of elements
<5 kg	Very light material, bolts, screws, concrete remains, etc.
5–100 kg	Light material, interior material, light dividing walls, construction workers, etc.
100–1000 kg	Structural elements for the façade construction, etc.
1000–10000 kg	Structural elements, beams, hollow core beams, etc.
>10000 kg	Heavy structural elements, main structure of the building, etc.

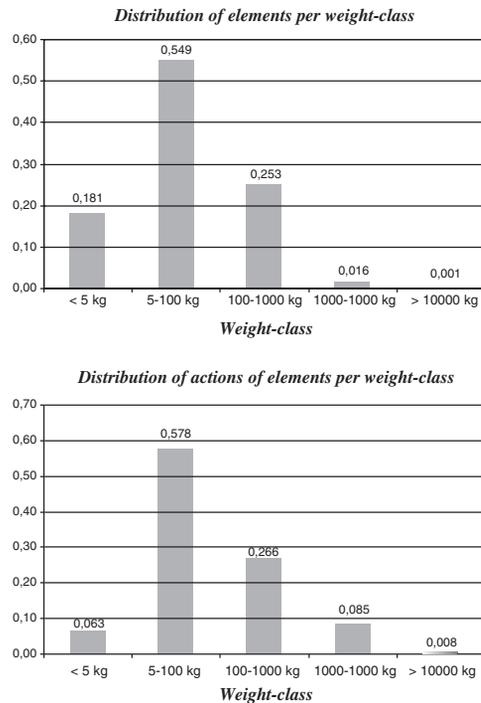


Figure 5. Distribution of elements and distribution of actions per element.

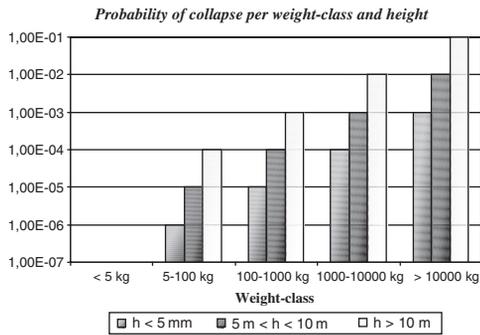


Figure 6. Probability of collapse of the building if element falls inside the building.

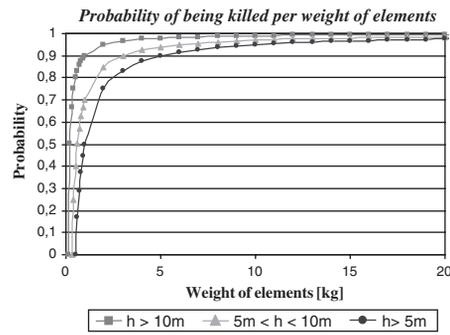


Figure 8. The probability of being killed due to an falling element.

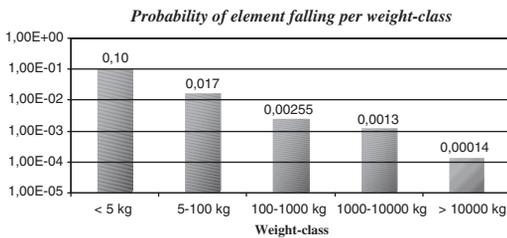


Figure 7. The average probability of element falling [project<sup>-1</sup>].

Table 3. Examples of different weight classes.

Cost-class	Example of costs
No costs	In case of no elements falls
<€ 10,000	Very light damage to vehicles, etc.
€ 10,000–€ 100,000	Light damage to infrastructure and total loss of (expensive) vehicles, etc.
€ 100,000–€ 1,000,000	Damage to infrastructure, etc.
>€ 1,000,000	Heavy damage in case of close off the road and reroute the traffic for a long period, etc.

class | element falls inside building | element falls) is determined by a combination of engineering judgement and laws of mass and impulse.

A logic assumption has been made that the heavier the element and the higher from it falls, the higher the probability that the building collapses due to the falling of an element inside the building (see figure 6).

- the probability of elements falling;
 

Because of no data could be found about the probability of elements falling per weight class, an extensive expert opinion has been performed (see Appendix A). The experts varied from scientist specialised in construction technology in multiple use of space projects and construction workers. It seemed that their opinion regarding the probability of failure corresponded with each other. The average probability of elements falling per weight class per project is given in figure 7.
- the height from which the element is falling;
 

The height from which the element is falling is integrated in the Bayesian Network as a variable in the risk analysis. This variable corresponds with the ratio of the height of the building. Three

different height levels are proportionally considered;  $h < 5$  m;  $5 \text{ m} < h < 10$  m and  $h > 10$  m.

- fatalities and economic risk;
 

The probabilities of the node fatalities and economic risk are determined by engineering judgement (for a full overview see [Suddle, 2001<sup>A</sup>]). The node fatalities is divided into injury and loss of live. It has to be noted that  $P(\text{person being killed} | \text{an element falls on a person})$  is almost 1, if an element is even less than 5 kg falling (see figure 8).

A large economic damage mainly depends on the case of closing the infrastructure for a long period of few weeks, due to e.g. collapse of the building above. In this regard five different cost-classes (of economic risk) were considered and particularly the effect is determined if elements fall in the risk-zones (see table 3 and Figure 9):

A full overview of conditional probabilities of fatalities and economic risk is presented in [Suddle, 2001<sup>A</sup>].

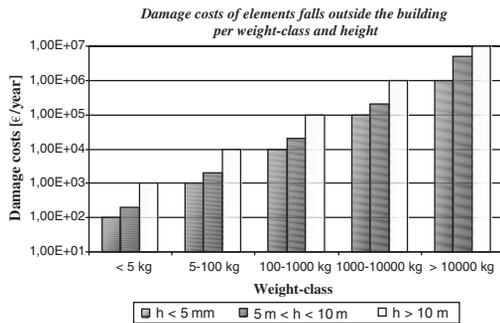


Figure 9. Damage costs of elements falls in the risk-zones of the building.

### 3.4 Quantification of probabilities above railways and existing buildings

To determine the risks for third parties in the construction phase by building over railways and existing buildings, such networks are composed for cases both cases. In the Bayesian Network building above railway track an extra node is added, which represents the situation at platform (see figure 3). It has to be noted that the financial damage given an element falls in railways is much bigger than by roads, because there is no option for rerouting the train traffic [Suddle, 2001<sup>A</sup>]. Finally, the risks for third parties are also determined by making these networks for building over an existing building, in which the situation beneath the building is less dynamic.

## 4 RESULTS OF THE RISK ANALYSIS

### 4.1 Individual Risk

Basically, the probabilities those are determined consists probabilities per year per action of a considered element. The individual risk (*IR*) during construction can be determined by multiplying the computed probabilities with the number of actions (see table 4). In this regard the individual risk in both building above road and railway tracks is almost the same order ( $10^{-6}$ ).

This can be presented as individual risk contours at the construction site (figure 10). The expected loss of human life ( $E(N_d)$ ) can be computed by multiplying the individual risk (*IR*) with the number of participants. The results of the risk analyses comes down to the following:

The results show that building over road infrastructure is the unsafe way to build, followed by building over rail infrastructure. Building over existing buildings is with less risk. From financial point of view, building over rail infrastructure is not significantly different from building over road infrastructure.

Table 4. Results of the risk analysis.

Building over	Roadway	Rail track	Building
Expected loss of human life	1,65	1,33	$8,01 \cdot 10^{-4}$ human risks
Expected injuries	5,46	1,72	$8,10 \cdot 10^{-6}$ human risks
Expected costs	€ 945,000	€ 1,035,750	€ 17,700 economical risk

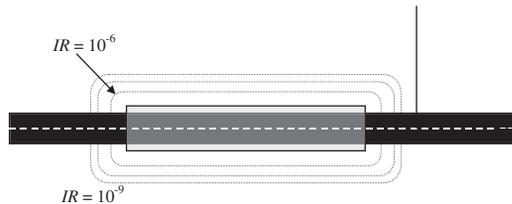


Figure 10. Risk contours during construction phase for building above road.

Again, building over existing buildings is with less risk.

### 4.2 Group Risk

In the same way, group risk is considered for constructing buildings above roads railways and existing buildings. The group risk for building above roads, railway tracks and existing buildings is almost negligible. Note that building over existing buildings is with less group risk.

### 4.3 Check for limits of risk acceptance

Because of a lack of explicit norms of risk acceptance for the safety of third parties during construction, the method of [Vrijling et al., 1996] based on voluntariness is used ( $\beta_i = 0.01$ ) When considering these acceptance limits for risk acceptance, to be divided into criteria on an individual and on a social basis the results for building over rail and road infrastructure are slightly exceeded. Therefore, safety measures are analysed and optimised for building above road infrastructure.

## 5 SENSITIVITY ANALYSIS

In order to formulate safety measures and to determine their effect on risks, a sensitivity analysis is

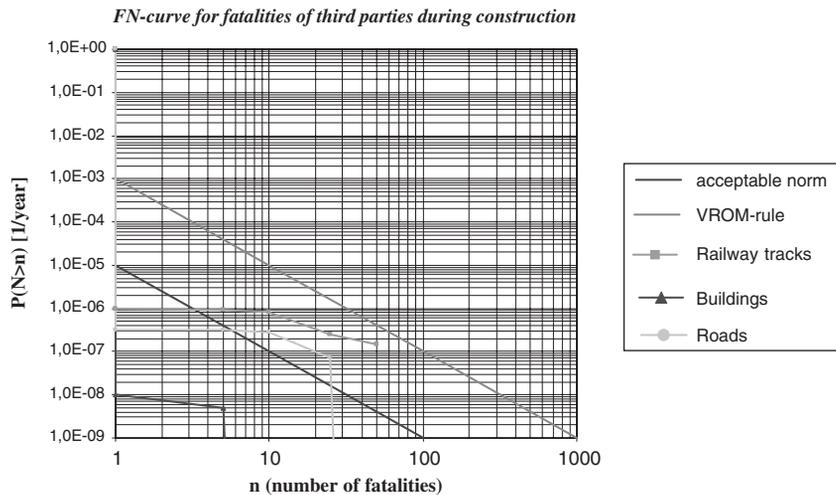


Figure 11. Group risks of building on top of transport routes.

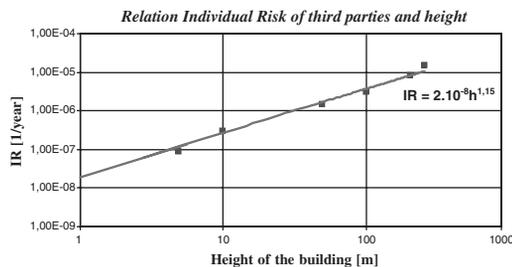


Figure 12. The relation between height of the building the individual risk of third parties.

performed. The sensitivity analysis provides both transparency of relevant scenarios and deviation of results of risk analysis using Bayesian Networks. The dominant aspects are:

- the number of actions per project;
- the position where the element falls;
- situation below the building;
- the weight of the falling element.

Furthermore, the risk zones of the building, the façades that are crossing the road, form an important nexus for the safety of third parties (see also figure 10). Surprisingly, factors that turned out to be hardly of any influence are (design) errors and collapsing of the main structure of the building caused by falling elements. The error in the calculated probabilities is approximate 40%. This is determined by evaluating the conditional probabilities that were

determined by engineering judgement. So, the result of expected loss of human live varies between 1,20 and 2,31. If the height of the building is considered with the individual risk (*IR*) of third parties, the following relation can be presented.

Figure 12 presents the higher the building, the higher the individual risk of third parties. It also means that the higher the building, the more safety measures have to be taken.

## 6 CONCLUSIONS

This paper presented the probabilistic approach for the safety of third parties during the construction phase. The relation between FMEA-techniques and Bayesian Networks is treated. This study showed that the risk zones of the building, the façades that are crossing the road, form an important nexus for the safety of third parties. The safety measures should be integrated into these zones.

## LITERATURE

- Meijer, F. en H.J. Visscher, *Bouwveiligheid en bouw hinder bij meervoudig stedelijk ruimtegebruik*, Onderzoeksinstituut OTB, DUP Satellite, 2001, 113 pp.
- Suddle, S.I., *Veiligheid van bouwen bij Meervoudig Ruimtegebruik*, afstudeerrapport, TU-Delft, april 2001<sup>A</sup>, 298 pp.
- Suddle, S.I., *Veilig bouwen bij Meervoudig Ruimtegebruik*, *Land + Water*, Volume 41, no. 9/2001, september 2001<sup>B</sup>, pp. 24–27.

Suddle, S.I., Safety of construction in intensive use of space, *Proceedings of Congress Risk Analysis*, Volume III, Editor: C.A. Brebbia, Sintra (Portugal), WIT Press, Southampton, June 2002, pp. 305–314.

Vrijling, J.K., W. van Hengel, R.J. Houben, *Acceptable risk as a basis for design*, Reliability Engineering and System Safety, Volume 59, 1998, pp. 141–150.

Vrijling, J.K., A.C.W.M. Vrouwenvelder e.a., *Kansen in de civiele techniek, Deel 1: Probabilistisch ontwerpen in de theorie*, CUR-rapport 190, CUR, Gouda, maart 1997.

Vrouwenvelder, A.C.W.M, e.a., *Risico-analyse bouw fase boortunnel*, CUR/COB Uitvoeringscommissie N510, tussenrapportage, TNO-Bouw, Delft, 25 november 1996.

Vrouwenvelder, A.C.W.M., *Risk Assessment and Risk Communication in Civil Engineering*, CIB Report, Publication 59, februari 2001.

APPENDIX A

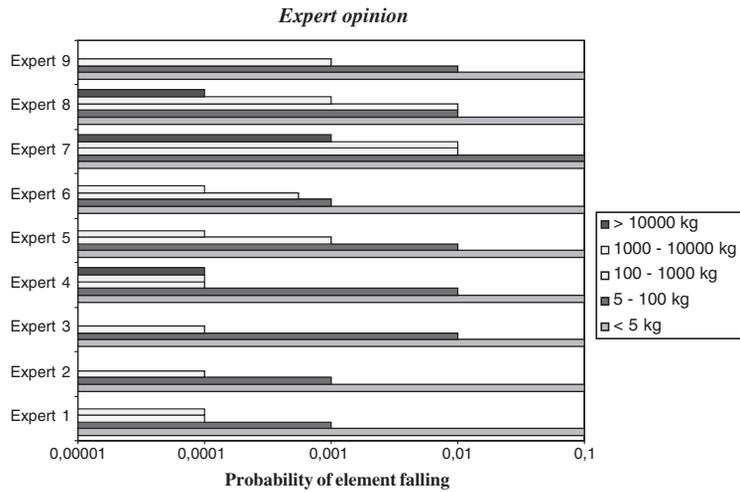


Figure 13. Results of expert opinion for probability of an element falling.



Figure 14. Construction of the Malie Tower in The Hague (The Netherlands).

## A logarithmic approach for individual risk: the safety-index

S.I. Suddle

*Delft University of Technology & Corsmit Consulting Engineers Rijswijk, The Netherlands*

**ABSTRACT:** Risk analyses can be undertaken to examine the required safety measures that are needed to realise complex projects near hazardous installation. When doing this risk analysis, the results have to be checked for risk acceptance criteria. In this paper, the three main criteria for risk acceptance criteria, which can be divided into individual risk, risk on a social basis and the economic criterion, are analysed and their interrelation is described. One of the relations between these criteria is the expected number of casualties. To quantify this expected number of casualties in term of economics, the expected numbers of casualties are taken into account by using monetary value per casualty. This paper discusses the variation of the monetary value per casualty. Furthermore, the acceptable level for societal risk is analysed for different countries. Finally, a new approach for the individual risk criterion on logarithmic scale, namely *the safety-index* is discussed in this paper. This paper describes a full derivation of the safety-index. Besides, on the basis of the safety-index, a dimensionless criterion for individual risk is proposed. The safety-index provides an effective tool for the assessment of individual risk dimensionless regarding the acceptance of risk.

### 1 INTRODUCTION

During the design phase of a complicated project, risk analyses can be undertaken to examine the required safety measures that are needed to realise such projects. When doing this risk analysis, the results have to be checked for risk acceptance criteria. If the results do not comply with these risk acceptance criteria, to be divided into criteria on an *individual* and on a *social* basis, extra measures can be taken to increase the level of safety. However, these risk acceptance criteria are different to each country. In order to take decisions for safety measures it is useful that the main criteria for risk acceptance criteria are analysed and their interrelation with economic considerations is described.

Moreover, the realisation of safety measures is related to investments. In this regard, economic considerations have to be taken into account when risk analysis is performed and measures are going to be taken. These economic considerations consists costs for investments and the economic risk. Considering these measures, the decision maker finds himself in a dilemma: which measure has to be given preference, the one that minimises the economic risk or the one that decreases the loss of human lives. Generally, in such analyses it comes down to the fact that human risks e.g. expected number of casualties are also transformed into monetary terms. This paper will present the variation of the monetary value per casualty.

Another complexity during the design phase of complicated projects is the transparency of the risk acceptance criteria for not-scientists e.g. municipalities. Considering these criteria, it is a difficulty for the decision maker to understand these criteria. The individual risk, which is one of these criteria, is traditionally depicted as contours on a – two-dimensional – map [Ale et al., 1996]. When depicting such risk contours, only the probability of a person is given, who permanently is present at a certain location in the vicinity of a hazardous activity will be killed as a consequence of an accident with that activity. However, these risk contours does not provides the acceptance of risk, which can be divided into the voluntariness and the direct benefit, of that person. Different participants in the exploitation phase require different demands and therefore have a different perception of safety. Therefore, it is recommendable to implement these risk contours including the voluntariness and the direct benefit of these participants.

Accordingly, in this paper, a new (dimensional) approach for the individual risk criterion on logarithmic scale, namely *the safety-index* is proposed [Suddle, 2002<sup>A</sup>]. This logarithmic approach is adapted from medical sciences and insurance policies [Boudier et al., 1985], which can be applied in building engineering and physical planning around hazardous installations and infrastructure with transport of hazardous materials to present safety results dimensionless and including

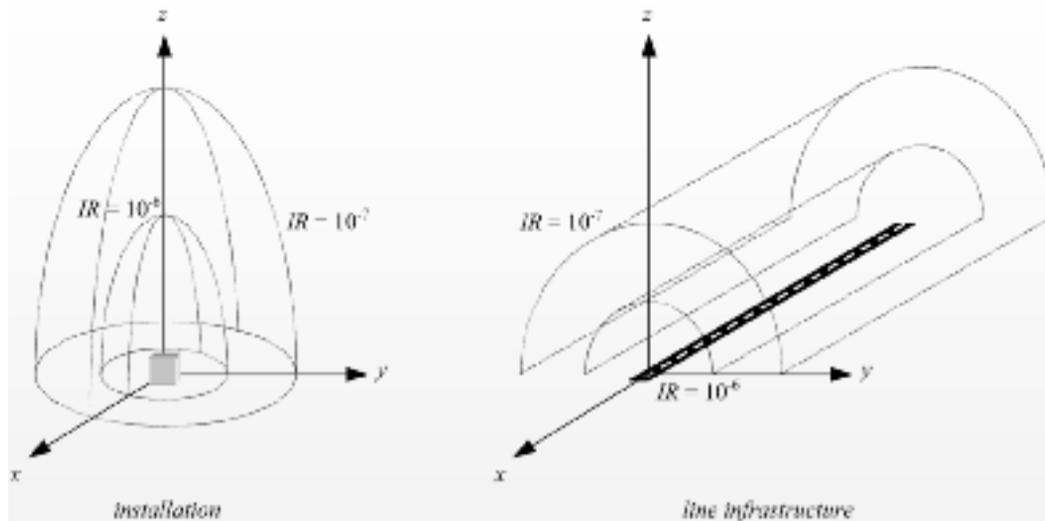


Figure 1. Two and three-dimensional individual risk contours for an installation and line infrastructure [Suddle et al., 2002].

personal acceptable level of risk. The formula of safety-index is applied to a line infrastructure case in which (individual) safety contours are depicted. This concept can be handy for policy makers and thus effective in risk communication.

## 2 RISK ACCEPTANCE AND DECISION-MAKING

Risk analysis is a method that can be used to examine the safety in objective terms. When doing this risk analysis, the results have to be checked for risk acceptance criteria. Criteria for accepting or rejecting the assessed risks include two related entities: the frequency of an undesired event and the consequences (casualties, monetary values, environmental values). In general, one may state that the higher the consequences, the lower the accepted probabilities are. In more detail, the acceptance limits for a given event may originate from three different angles [Vrouwenvelder et al., 2001]:

1. A comparison with other risks related to individual safety;
2. Societal aversion to big disasters, especially when many casualties are involved;
3. Economic considerations.

If the results do not comply with these risk acceptance criteria, measures can be taken to increase the required level of safety. However, these measurements have to be attractive in terms of economics. Moreover, these three aspects should be integrated and/or prioritised.

## 3 A SET OF RULES FOR THE ACCEPTABILITY OF RISKS

### 3.1 Personally acceptable level of risk

An overview of measures to express the individual risk is given by [Bedford & Cooke, 2001]. The smallest component of the social acceptable of risk is the personal cost-benefit assessment by the individual [Vrijling et al., 1998].

Individual risk ( $IR$ ) is defined as the probability that a person who permanently is present at a certain location in the vicinity of an activity will be killed as a consequence of an accident with that activity. Usually,  $IR$  is expressed for a period of a year. It can be pictured both on two and three-dimensional [Suddle et al., 2002] map by connecting point of equal  $IR$  around a facility, the risk contours [Ale, 2002].

From a personally point of view, the probability of failure (a fatal accident) should meet the following requirement [Vrijling & Vrouwenvelder, 1997]:

$$P_{fi} \leq \frac{\beta_i \cdot 10^{-4}}{P_{d/fi}} \quad (1)$$

In which:

$P_{fi}$  = probability of failure  $f$  as a result of an event  $i$  [ $\text{year}^{-1}$ ];

$P_{d/fi}$  = probability of being killed if failure  $f$  as a result of an event  $i$ , occurs;

$\beta_i$  = the policy factor that varies with the degree of voluntariness with which an activity  $i$  is undertaken and with the benefit perceived. It ranges from 100, in case of complete freedom of

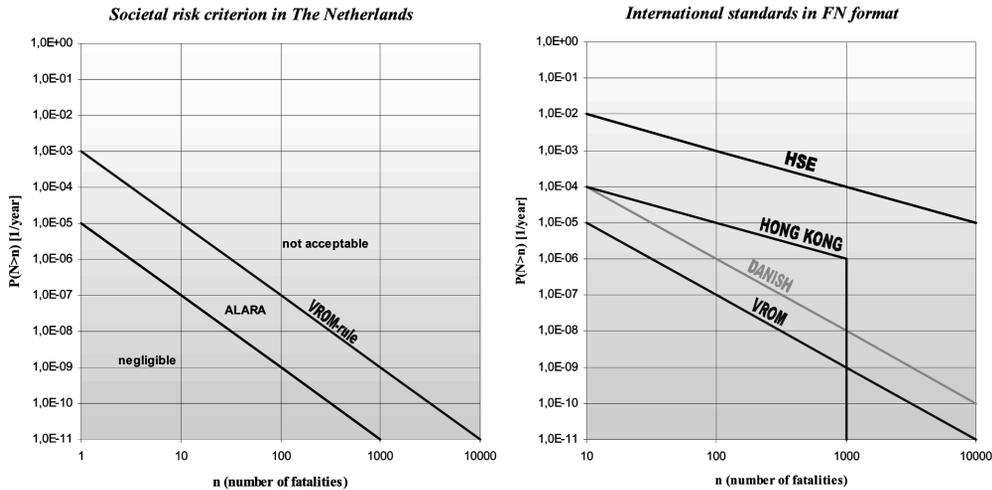


Figure 2. FN curves where  $1 - F_N(n) = P(N > n \text{ in one year})$  is illustrated in The Netherlands (left) and some international FN standards (right).

Table 1. Personal risks in Western countries, deduced from the statistics of causes of death and the number of death and the number of participants per activity [Vrijling et al., 1998].

Statistics of causes of death	Acceptance of risk		Policy factor
	high	yes	
Mountaineering	↑	↑	$\beta_i = 100$
illness	↑	↑	$\beta_i = 10$
motoring	↑	↑	$\beta_i = 1$
flying	↓	↓	$\beta_i = 0,1$
factory	↓	↓	$\beta_i = 0,01$
	low	no	

choice like mountaineering, to 0,01 in the case of an imposed risk without any perceived direct benefit;  
 $10^{-4}$  = statistical probability of dying per year of young people [ $\text{year}^{-1}$ ].

### 3.2 Socially acceptable level of risk

Societal risk (SR) is defined as the probability that in an accident more than a certain number of people are killed. Societal risk usually is represented as a graph in which the probability or frequency  $F$  is given as a function of  $N$ , the number killed. This graph is called the FN curve. A mathematical expression in the case of a straight FN curve (on log-log-scale) can be presented as a combination of [Vrijling et al., 1998] and [Vrouwenvelder et al., 2001]:

$$1 - F_N(n) \leq \frac{C_i}{n^\gamma} \text{ for all } n \geq 1 \tag{2}$$

$$1 - F_N(n) = P(N > n) \tag{3}$$

where

$$C_i = \left[ \frac{\beta_i \cdot 100}{k \cdot \sqrt{N_A}} \right]^2 \tag{4}$$

In which:

- $C_i$  = the (imaginary) acceptable probability for  $n = 1$ ;
- $1 - F_N(n)$  = frequency of more than  $n$  fatalities [ $\text{year}^{-1}$ ];
- $N$  = the number of people being killed in one year in one accident;
- $n$  = number of fatalities in one year in one accident;
- $N_A$  = the independent locations;
- $\gamma$  = the slope of the FN curve, also called the risk aversion factor [Vrijling & Gelder, 1997]; the value of  $\gamma$  ranges from 1 to 2;
- $k$  = the risk aversion factor; the value of  $k$  mostly is 3.

A standard with a steepness of  $\gamma = 1$  is called risk neutral. If the steepness  $\gamma = 2$ , the standard is called risk averse. In this case larger accidents are weighted more heavily and accepted with a relatively lower probability. Some international FN standards are given in figure 2 (right) [Jonkman et al., 2002]. In contrast to other countries, the societal risk criterion in The Netherlands is much stringent. Hence, it is not remarkable that the result some safety studies does not comply with the Dutch criteria (VROM-rule), while for instance in other countries, they do comply.

In general, the *FN* curve indicates the border between “acceptable” and “unacceptable” in a diagram with probability on one axis and the number of casualties on the other. It is quite customary to have two *FN* curves as indicated in figure 2 (left):

- One curve representing an upper limit above which activities or situations are not acceptable;
- Another curve representing a lower limit below which no further risk reductions are necessary.

In figure 2 the societal risk criterion in The Netherlands, also called the VROM-rule, is illustrated. In the area in between risk reducing measures should be considered and judged on an economical basis. Between these levels, it is required to reduce risks to levels as “as low as reasonable achievable” (ALARA) that is, until the costs of further measures would be grossly disproportionate to the benefit gained.

### 3.3 Economic criteria

According to [Vrouwenvelder et al., 2001], the third acceptance creation can be schematised as a mathematical-economic decision problem by expressing both investments and all consequences of the disaster in terms of money (assuming a given period of time).

Besides, it may be suggested that a measure with less human risk is more expensive than a one with gigantic risk. To balance these measures an economic creation is required. It means that the most economical solution from all alternatives that are allowable from the human safety point of view. Mathematically it comes down to [Vrouwenvelder et al., 2001]:

Minimise:

$$C_{tot} = C_0(y) + \sum_{j=1}^{P_{Fj}} \frac{P_{Fj} \cdot \{C_j + \alpha \cdot E(N_d | F)\}}{\beta_i \cdot 10^{(1+r)^j}}$$

Conditional upon:  $P_{fi} \leq \frac{\beta_i \cdot 10^{-4}}{P_{d|fi}}$  or (5)

$$S = \log \frac{\beta_i \cdot 10^{-4}}{P_{fi} \cdot P_{d|fi}} \geq 0 \text{ (see section 4)}$$

$$1 - F_N(n) \leq \frac{C_i}{n^r}$$

In which:

- $C_{tot}$  = total costs;
- $C_0(y)$  = the investment in a safety measure;
- $j$  = the number of the year;
- $r$  = real rate of interest;
- $C_j$  = damage cost in year  $j$ ;
- $y$  = decision parameter;
- $\alpha$  = monetary value per casualty;
- $E(N_d | F)$  = expected number of casualties given a failure;  $E(N_d) = P_{fi} \cdot P_{d|fi} \cdot N_{pi}$ ;  $E(N_d | F) = P_{d|fi} \cdot N_{pi}$ ;

Table 2. Investments in Risk Reduction, per nominal lives saved [University of East Anglia in 1998].

Theoretical Evaluations	Value for $\alpha$ [€ per person]
Human capital calculations	300,000
Willingness to pay (hypothetical)	1,600,000
Road Safety (UK, 1987)	500,000
Cost of medical procedures for comparison (real)	2,000–300,000

$N_{pi}$  = number of participants in activity  $i$ ;  
 $P_{Fj}(y)$  = the failure in year  $j$ .

One should realise that  $P_{Fj}(y)$  denotes the failure exactly in year  $j$ , that is not in any year before or later. The term  $C_j$  includes all costs after failure (also called the material losses): it includes direct damage, cost of repair, but also future failure costs of the repaired structure (if any).

### 3.4 Monetary value per casualty

Most decision makers prefer to treat the economic and human safety criteria completely separated. In that case, the value of  $\alpha = 0$ ; this is the creation fully compatible to the approach of a purely economic decision problem. Still, there are some decision makers who compare the advantage of safety measures in comparison with economic investments. Having this in mind, it might be better to assess some amount of money to the event for death or injury. For this purpose the amount for material damage is increased with the monetary value per casualty multiplied by the expected number of death (as presented in formula 5). The monetary value per casualty depends on factors such as Willingness To Pay (WTP), Willingness To Accept compensation (WTA), voluntariness, and responsibility [Jones-Lee & Loomes, 1995]. According to the Environmental Protection Agency the value of a citizen in the US is approximately €5,600,000. = . It may be concluded from [1], that these values result in a wide range. According to [Vrouwenvelder et al., 2001] a reasonable value seems €1,000,000. = . Another method to determine this value is the so called Life Quality Index (LQI) (see [Lind, 1994]). The values per casualty can be summarised in table 2.

## 4 THE SAFETY-INDEX

### 4.1 Introduction

According to [Boudier et al., 1985], most decision makers prefer to present the risk results on a dimensionless scale. Therefore [Boudier et al., 1985] used a logarithm scale for presenting the individual risk dimensionless. This logarithmic scale is used in medical sciences and

insurance policies [Boudier et al., 1985]. In this scale, *the unikhohort*, is defined as the negative logarithm of individual risk for a period of 1 year:

$$U = -\log P_{fi} \cdot P_{d,fi} \tag{6}$$

In which:  
 $U =$  unikhohort.

Note that this formula does not contain a correction factor for risk acceptance. In order to integrate the factor for risk acceptance we can analyse the individual risk. Considering the acceptable level for individual risk, one may remark that improvements in the level of risk do make sense, when risk increases with a factor ten [Suddle, 2002]. Similarly, a decrease of risk with a factor ten is a remarkable worsening. The factor ten suggests a logarithmic scale with base 10. Obviously, societal risk is displayed on a (double) logarithm scale. Individual risk, as early mentioned in this paper, can be determined by risk analysis and subsequently checked for the risk acceptance criteria. Writing formula (1) in another configuration gives:

$$IR = P_{fi} \cdot P_{d,fi} \leq \beta_i \cdot 10^{-4} \tag{7}$$

In which:  
 $IR =$  the individual risk (as mentioned before).  
 Formula (7) can be written as:

$$\frac{P_{fi} \cdot P_{d,fi}}{\beta_i \cdot 10^{-4}} \leq 1 \tag{8}$$

Though the check in formula (8) is dimensionless, yet, it presents the ratio of individual risk and the risk acceptance criterion, which is hardly interesting. This check is rather attractive if this is done on a base of a (negative) logarithmic scale. By considering the usual definition of risk, a possible standard or a scale for safety in terms of individual risk can be given by:

$$S = -\log \frac{P_{fi} \cdot P_{d,fi}}{\beta_i \cdot 10^{-4}} \tag{9}$$

In which:  
 $S =$  the safety-index (Dutch: Veiligheidsmaat (see [Suddle, 2002])) [-];

This introduces a new definition for the individual risk; *the safety-index*. In this formula (9), the referential level for acceptable safety is the level that (just) complies with the acceptability of individual risk. Eliminating the minus before the logarithm gives the following:

$$S = \log \frac{\beta_i \cdot 10^{-4}}{P_{fi} \cdot P_{d,fi}} \tag{10}$$

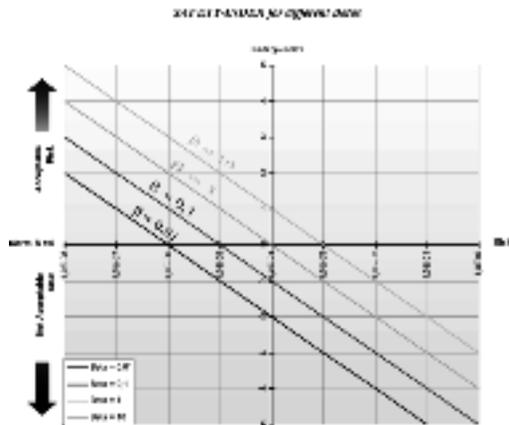


Figure 3. Safety-index versus individual risk by different  $\beta_i$ s.

The result of the safety-index  $S$  is a particular number. In fact, a distinction can be made for the three following situations:

1.  $S < 0$  The computed safety/risk does not comply with the level of risk acceptance. The more the risk exceeds the norm ( $\beta_i \cdot 10^{-4}$ ), the smaller is the safety-index, and the unsafe is the activity. (A decrease of the safety-index with one means that the risk increases with one level);
2.  $S = 0$  The computed safety/risk complies with the level of risk acceptance;
3.  $S > 0$  The computed safety/risk complies largely with the level of risk acceptance. (An increase of the safety-index with one means that the risk decreases with one level).

It can be assumed that one strives for situation 2 and 3, thus  $S \geq 0$ . Combined with formula 10, this results in the norm for safety in terms of individual risk:

$$S = \log \frac{\beta_i \cdot 10^{-4}}{P_{fi} \cdot P_{d,fi}} \geq 0 \tag{11}$$

For decision maker it is attractive to present safety results of in terms of individual risk, formula (11) can be used rather than formula (1). Note that different safety-index cannot be summed up. If one likes to present risk results on a dimensionless scale, one has to sum up different individual risks and than to take the logarithm of it.

The result of the safety-index depends on the individual risk and the  $\beta_i$ . Table 3 and the diagram represent the relation between the safety-index and individual risk for different  $\beta_i$ s. This model enables safety in terms of individual risk can be quantified and can be checked directly for the limits of risk acceptance for

Table 3. Safety-index versus individual risk for different  $\beta_i$ s.

Individual Risk $IR = P_{fi} \cdot P_{d/fi}$	Safety-index			
	$\beta_i = 0,01$	$\beta_i = 0,1$	$\beta_i = 1$	$\beta_i = 10$
$10^{-2}$	-4	-3	-2	-1
$10^{-3}$	-3	-2	-1	0
$10^{-4}$	-2	-1	0	1
$10^{-5}$	-1	0	1	2
$10^{-6}$	0	1	2	3
$10^{-7}$	1	2	3	4
$10^{-8}$	2	3	4	5
$10^{-9}$	3	4	5	6

individual risk. This instrument provides an effective tool for determining the effects of the safety(-index) on safety-measures if the design limit is based upon the individual risk.

Furthermore, the next limit is applicable:

$$\lim_{IR \rightarrow 0} (S) = \infty \tag{12}$$

With other words: if there is no risk, the safety (-index) will approach infinite.

#### 4.2 Unikohort and the safety-index

If the unikohort is compared to the safety-index, there is no correction factor for acceptance of risk taken into account. In order to deduce the safety-index from the unikohort, the risk acceptance factor must be integrated into the unikohort. The correction factor for acceptance of risk can be given by:

$$A = -\log \beta_i \cdot 10^{-4} \tag{13}$$

In which:

$A$  = correction factor for acceptance of risk.

In order to compute an index for individual safety including the acceptability, one can deduce the correction factor for acceptance of risk:

$$S = U - A \tag{14}$$

$$S = -\log P_{fi} \cdot P_{d/fi} - (-\log \beta_i \cdot 10^{-4}) \tag{15}$$

$$S = \log \beta_i \cdot 10^{-4} - \log P_{fi} \cdot P_{d/fi} \tag{16}$$

$$S = \log \frac{\beta_i \cdot 10^{-4}}{P_{fi} \cdot P_{d/fi}} \tag{17}$$

This formula is exact the same as formula (10).

Table 4. Different approach for local residents near infrastructure and car drivers at the infrastructure.

Local residents near infrastructure	Car drivers at the infrastructure
$P_{fi} = 10^{-5}$ [year <sup>-1</sup> ]; $P_{d/fi} = 0.99$ [-]; $\beta_i = 0.01$ (involuntary activity)	$P_{fi} = 10^{-5}$ [year <sup>-1</sup> ]; $P_{d/fi} = 1$ [-]; $\beta_i = 1$ (voluntary activity)
$IR = 9.9 \cdot 10^{-6} \cong 10^{-5}$ [year <sup>-1</sup> ]	$IR = 10^{-5}$ [year <sup>-1</sup> ]

#### 4.3 Example

Formulas (10) and (11) provide an effective tool, particularly for decision makers, which can be presented in the following example in which the individual risk and the safety-index is computed and compared for local residents near infrastructure and car drivers at the infrastructure. Suppose the following situation in which an accident occurs on the infrastructure with a probability of  $10^{-5}$  [year<sup>-1</sup>]:

The safety-index  $S$  for this example can be computed with formula (10), which is for local residents near infrastructure:

$$S = \log \frac{0,01 \cdot 10^{-4}}{10^{-5} \cdot 0.99} = \log \frac{10^{-6}}{9.9 \cdot 10^{-6}} = \log 0.11 \cong -1 \tag{10a}$$

The safety-index  $S$  for car drivers at the infrastructure is:

$$S = \log \frac{1 \cdot 10^{-4}}{10^{-5} \cdot 1} = \log \frac{10^{-4}}{10^{-5}} = \log 10 = 1 \tag{10b}$$

The result of the safety-index  $S$  is a particular number, which is respectively  $-1$  and  $1$  for local residents near infrastructure and car drivers at the infrastructure. Though the individual risk  $IR$  for both local residents near infrastructure and car drivers is almost the same ( $10^{-5}$  year<sup>-1</sup>), the safety-index  $S$  has a different

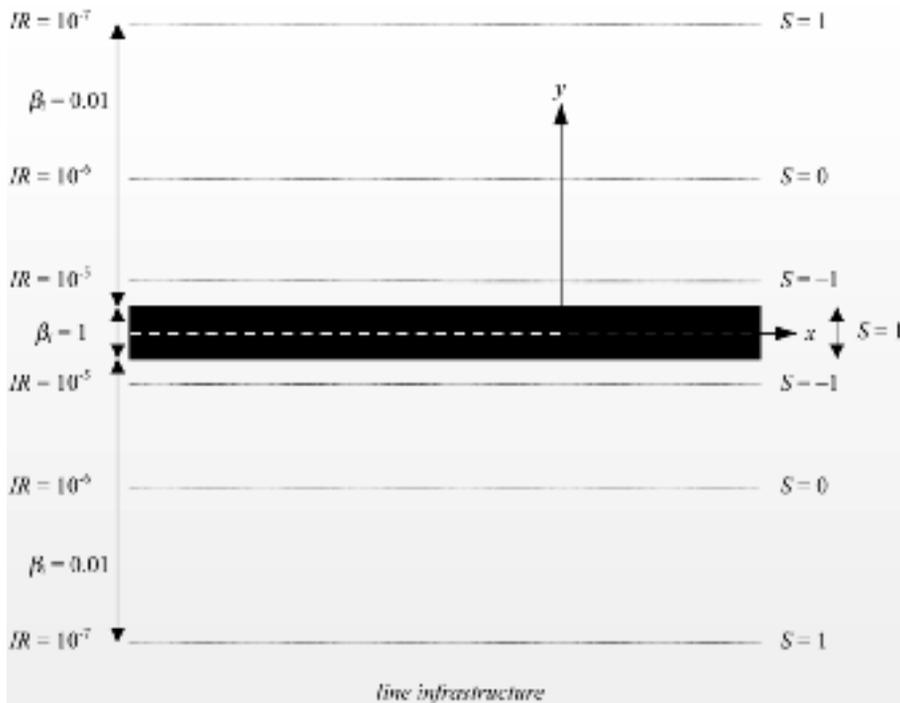


Figure 4. Individual risk contours (left) and safety contours (right).

value for both. This comes down to the fact that the safety (in term of individual risk) for local residents near infrastructure is insufficient, because the limit for acceptance of risk is exceeded. Accordingly, people present in the neighbour of the infrastructure, especially within the  $10^{-5}$  risk contour, will accept less risk than the car drivers.

The phenomena of the safety in terms of individual risk can be illustrated by connecting the points with the same safety-index yields an iso-safety contour, which is related both to the individual risk and the acceptance of risk. Figure 4 visualizes the idea of individual risk contours and the safety contours. In this figure, the policy factor  $\beta_i$  is given, which represents the risk acceptance as mentioned in table 1.

It can be noted that just outside the boundary of the infrastructure the safety-index is below zero ( $S < 0$ ). Furthermore it can be seen that the individual risk decreases results in the increase of the safety(-index).

## 5 CONCLUSIONS

This paper contributes to the transparency of the risk acceptance criteria. As a consequence, the interrelation between three main criteria for risk acceptance criteria, which can be divided into individual risk, risk on a

social basis and the economic criterion, is described. It may be concluded, the new approach for the individual risk criterion on logarithmic scale, namely *the safety-index* is handy for policy makers and therefore effective in risk communication. Thus, this logarithmic approach for the individual risk criterion partly adapted from medical science and insurance policies can be applied in civil engineering to present risk results on a dimensionless scale.

## LITERATURE

- Ale, B.J.M., *Risk assessment practices in The Netherlands*, Safety Science, Volume 40, Issues 1–4, February–June 2002, pp. 105–126.
- Bedford, T., Cooke, R.M., *Probabilistic Risk Analysis: Foundations and methods*; Cambridge University Press, 2001.
- Boudier, H.S., Heilmann, K., Urquhart, J., *Risiko's meten: een antwoord op de angst voor een technologische cultuur*, Baarn, In den Toren 1985, 167 pp.
- Jones-Lee, M.W. & Loomes, G. Scale and Context Effects in the Valuation of Transport Safety, *Journal of Risk and Uncertainty*, 1995, pp. 183–203.
- Jonkman, S.N., van Gelder, P., Vrijling, H. *An overview of quantitative risk measures and their*

- application for calculation of flood risk*, ESREL 2002, Volume 1, pp. 311–318.
- Lind, N.C., Target reliability levels from social indicators, *Structural Safety and Reliability*, Scheuller, Shinozuka and Yao (eds), Balkema, Rotterdam, 1994.
- Suddle, S.I., *Beoordeling veiligheid bij Meervoudig Ruimtegebruik*, Cement, Volume 54, no. 1/2002, februari 2002, pp. 73–78.
- Suddle, S.I., Th. S. de Wilde, B.J.M. Ale, The 3rd dimension of risk contours in multiple use of space, *Proceedings of Congress ESREDA 2002*, Editor: C.A. Brebbia, Delft (The Netherlands), November 2002, pp. ...–....
- Vrijling, J.K., and van Gelder, P.H.A.J.M. 1997, *Societal risk and the concept of risk aversion*, *Advances in Safety and Reliability*, Vol. 1, pp. 45–52.
- Vrijling, J.K., van Hengel, W., Houben, R.J. *Acceptable risk as a basis for design*, *Reliability Engineering and System Safety*, Volume 59, 1998, pp. 141–150.
- Vrijling, J.K., Vrouwenfelder A.C.W.M. e.a., *Kansen in de civiele techniek, Deel 1: Probabilistisch ontwerpen in de theorie*, CUR-rapport 190, CUR, Gouda, maart 1997.
- Vrouwenfelder, A.C.W.M., *Risk Assessment and Risk Communication in Civil Engineering*, CIB Report, Publication 59, februari 2001.
- <http://www.fem.nl/story.asp?artikelid = 588>.

## Reduced vertical separation minimum (RVSM): pre- and post-implementation safety cases

Bernd Tiemeyer

EUROCONTROL/Directorate Safety, Airspace, Airports and Information Services/Safety Management, Brussels, Belgium

**ABSTRACT:** On 24 January 2002, the introduction of a Reduced Vertical Separation Minimum (RVSM) in the EUR RVSM Airspace provided six additional flight levels between 29,000 ft and 41,000 ft inclusive. This has been achieved by reducing the vertical separation minimum between aircraft from 2,000 ft to 1,000 ft. The EUR RVSM Programme – managed by EUROCONTROL on behalf of the participating States – has been implemented simultaneously in the airspace of 41 European and North African countries and was the biggest change in Europe's Airspace for 50 years. This paper outlines the different elements of the Pre- Implementation and Post-Implementation Safety Cases, such as the derivation of the requirements, the regulatory process and how Collision Risk Assessment, Functional Hazard Assessment and National Safety Planning combined together provide a conclusive argument that the concept of RVSM and its implementation are safe before and remain safe after introduction.

### 1 INTRODUCTION

On 24 January 2002, the introduction of a Reduced Vertical Separation Minimum (RVSM) in the EUR RVSM Airspace provided six additional flight levels between 29,000 ft (FL290) and 41,000 ft (FL410) inclusive (Figure 1). This has been achieved by reducing the vertical separation minimum between aircraft from 2,000 ft to 1,000 ft. The RVSM Programme – managed by EUROCONTROL on behalf of the participating States – has been implemented simultaneously in the airspace of 41 European and North African countries and was the biggest change in Europe's Airspace for 50 years (Figure 2).

As required in other regions, EUR RVSM had to demonstrate to the international aviation community that the Target Level of Safety (TLS) set out by ICAO for the vertical collision risk would not be exceeded in the European RVSM Airspace.

However, during the initiation of the EUR RVSM Programme, it was felt, that to demonstrate the achievement of this criterion would be viewed as being necessary but not sufficient for the EUR RVSM airspace. At that stage the decision was taken to develop the EUR RVSM Safety Policy in coordination with the EUROCONTROL Safety Regulation Commission (SRC) in order to establish the basis for the safety

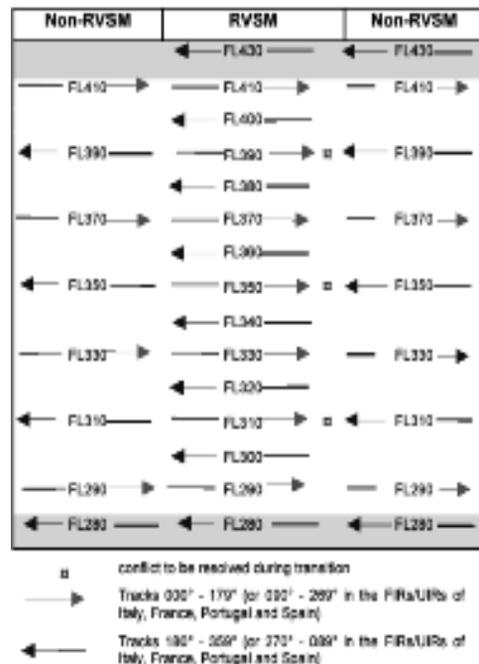


Figure 1. Flight level orientation scheme.

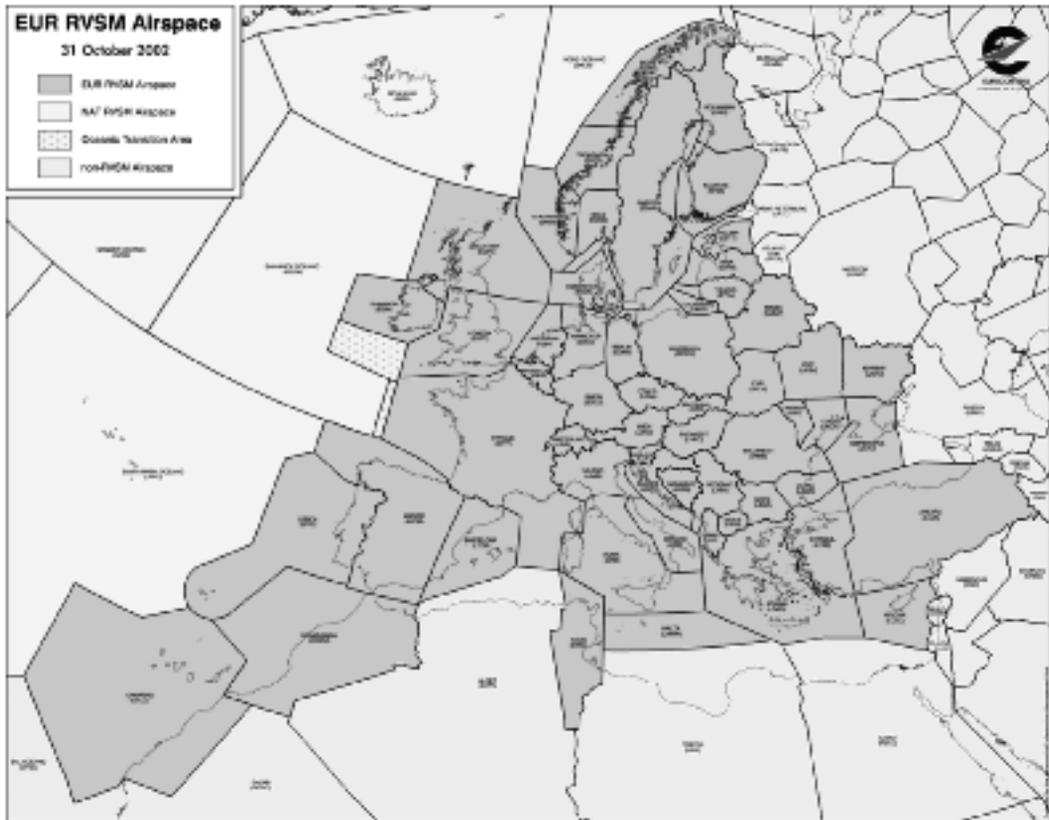


Figure 2. EUR RVSM airspace.

assurance of the RVSM Concept and its safe Implementation in the EUR RVSM Airspace and, in particular, demonstrating compliance with the ATM 2000 + Strategy [3].

To ensure that all safety conditions would be met, EUROCONTROL set up a dedicated safety assurance programme. One key deliverable was the EUR RVSM “Pre-Implementation Safety Case” (PISC) [1], which was finalised in August 2001 and approved by the SRC in September 2001 paving the way for the “Go”-decision of the EURCONTROL Provisional Council (PC) to implement RVSM ontime. This paper explains the different aspects of the Safety Case, such as the Functional Hazard Assessment, the Collision Risk Modelling and the National Safety Planning and how these elements were developed into a conclusive argument providing the evidence that the concept of RVSM and its implementation are safe. Second deliverable of the EUR RVSM Programme is the “Post-Implementation Safety Case” (POSC), which looks into the initial months of RVSM operations and

contains the evidence that RVSM was safely implemented and that RVSM operations are safe and continue to be safe.

## 2 PRE-IMPLEMENTATION SAFETY CASE

The assurance of flight safety is paramount in the EUR RVSM Programme. All elements of the Programme are related to safety management in one way or another. Given the importance of the safety aspects, a separate safety assurance programme undertook activities to ensure that RVSM meets its safety objectives, and that this is demonstrated satisfactorily, covering the following three main aspects:

- The preparedness of the (41) EUR RVSM participating States,
- The preparedness of the aircraft operators, and
- The acceptability of the EUR RVSM Pre-Implementation Safety Case.<sup>7</sup>

In order to address these aspects, Safety Objectives – as described in the next section – were set to be achieved through the Safety Case development.

### 2.1 *Safety objectives*

The Safety Policy for RVSM implementation was established to meet the requirements of ICAO Standards and Recommended Practices and Guidance Material on managing collision risk and to be fully compliant with the EATMP Safety Policy [2] and the ATM 2000+ Strategy [3].

The RVSM Safety Policy is described in [4], where the following statements define the main Safety Objectives for the RVSM Programme:

- i. The RVSM Programme shall conduct a full Functional Hazard Analysis looking at the whole system including air and ground segments and the proposed operational concept.
- ii. The RVSM Programme shall, as its principal safety objective, minimise the programme's contribution to the risk of an aircraft accident. The RVSM Programme recognises the Safety Objectives of the ATM 2000 + Strategy [3], in particular the general objective to improve safety levels by ensuring that the number of ATM induced accidents and serious or risk bearing incidents do not increase and, where possible, decrease. Therefore, the implementation of RVSM shall not adversely affect the risk of en-route mid-air collision.
- iii. In accordance with ICAO Guidance Material [5], the management of vertical collision risk within RVSM airspace shall meet the Target Level of Safety of  $5 \times 10^{-9}$  fatal accidents per flight hour.
- iv. In accordance with ICAO Guidance Material [5], the risk of mid-air collision in the vertical dimension within RVSM airspace, due to technical height keeping performance, shall meet a Target Level of Safety of  $2.5 \times 10^{-9}$  fatal accidents per flight hour.
- v. Guidance shall be given to the States to explain the necessary activities to provide evidence about the safe implementation of RVSM on the national level and subsequently assure the preparedness of the States.

### 2.2 *Safety argument*

The PISC demonstrates that the Safety Objectives have been met, by means of the following principal safety arguments:

- i. That a set of Safety Requirements has been specified for RVSM that fully address all the functionality, performance and reliability requirements necessary to ensure that the safety risks under RVSM will be tolerable and that, where possible,

risk has been reduced to a level as low as reasonably practicable.

- ii. That the RVSM Concept developed by EUROCONTROL for the European region has the potential to fully satisfy the RVSM Safety Requirements.
- iii. That the Implementation of the RVSM Concept by the individual participating States will fully satisfy the RVSM Safety Requirements.
- iv. That the Switch-Over from the current vertical separation minimum of 2000 ft (600 m) to the RVSM value of 1000 ft (300 m) will not adversely affect the safety of the on-going air traffic operations.

The above safety arguments are based on the assumption that the pre-RVSM levels of safety risk experienced in European airspace between FL 290 and 410 are accepted as tolerable.

Each of the above arguments is further developed in the relevant sections of the PISC, together with evidence showing that all the arguments are valid.

Goal Structured Notation (GSN) is used to graphically illustrate the detailed argument structure. The arguments are decomposed to a level at which clear evidence of the validity of the argument can be provided. This decomposition proceeds along two lines: direct arguments and evidence that the higherlevel arguments are true and backing arguments and evidence that the direct evidence is trustworthy.

#### 2.2.1 *Safety requirements determination*

The overall, high-level safety requirements, which describe the function, performance and reliability required of RVSM are determined as follows:

- RVSM1** – Provide safe vertical separation of aircraft by assigning aircraft to different flight levels (as in RVSM 4 below).
- RVSM2** – Provide safe transition to and from non-RVSM (feet and metric systems) flight levels within the defined transition airspace.
- RVSM3** – Prevent non-approved civil aircraft from entering RVSM airspace.
- RVSM4** – Nominal separation of flight levels shall be:
  - a) 1000 ft between RVSM approved aircraft.
  - b) 2000 ft between:
    - i. non RVSM approved State aircraft and any other aircraft operating within the EUR RVSM airspace.
    - ii. all formation flights of State aircraft and any other aircraft operating within the EUR RVSM airspace.
    - iii. non RVSM approved aircraft and any other aircraft operating within the defined RVSM transition airspace.
- RVSM5** – The accuracy of the Aircraft (technical) height keeping performance (i.e. the performance bounded by the requirements of

the MASPS) shall be sufficient to ensure that the risk of mid-air collision in the vertical dimension, in RVSM airspace, shall meet a Target Level of Safety of  $2.5 \times 10^{-9}$  fatal accidents per flight hour.

- RVSM6** – Provide facilities for safe operation under abnormal conditions – eg aircraft on-board emergencies.
- RVSM7** – The probability of any system failure leading to a mid-air collision shall be sufficiently low to ensure that the overall risk of mid-air collision due to the loss of vertical separation, from all causes, is within the TLS of  $5 \times 10^{-9}$  fatal accidents per flight hour.
- RVSM8** – The system shall be sufficiently reliable to ensure that the number of ATM induced accidents and serious or riskbearing incidents, under RVSM, shall not increase from current (pre-RVSM) levels and shall, where possible, decrease.
- RVSM9** – The performance and reliability of the system shall not deteriorate in service.

Although there are no explicit RVSM safety requirements associated with capacity, in order that the benefits of RVSM are realised, the introduction of RVSM shall not prevent the capacity goals of the ATM 2000+ Strategy from being achieved.

In the absence of any established precedent, the general approach employed in the PISC for deriving the RVSM high-level safety requirements was based on the approach used in International Safety Management Standard IEC 61508, Part 1 [6]. This Standard addresses those aspects to be considered when electrical/electronic/programmable electronic systems are used to carry out safety functions.

In order to ensure that all aspects of the behaviour of Vertical Separation have been considered; a set of *behavioural attributes* derived from those specified in UK CAA document CAP 670 – ATS Safety Requirements [7] – was used. The list of attributes is more comprehensive than those implied in IEC 61508 and therefore more likely to yield a complete set of safety requirements. The PISC contains in one of its Annexes a table, which shows how the highlevel safety requirements relate to these attributes.

A comparison of the high-level safety requirements with the relevant RVSM Safety Objectives specified above shows that all key objectives have been captured in the high-level safety requirements.

Therefore, on the basis that the method of achieving Vertical Separation has not changed, that the current ATS is “safe” and that the key safety objectives for RVSM have been fully addressed, the PISC concludes that high-level safety requirements for RVSM are sufficient as specified.

Subsequently, these high-level safety requirements have been decomposed and allocated to the RVSM system comprising the following elements:

- i. Airspace Design;
- ii. Flight Crew Procedures;
- iii. Flight Crew Training;
- iv. Aircraft Equipment;
- v. ATC Procedures;
- vi. ATC Training;
- vii. ATC Equipment;
- viii. System Monitoring.

A further table in the PISC contains the mapping between the RVSM high-level safety requirements and the safety requirements for each system element. It should be noted that it is not possible to allocate high-level Safety Requirements RVSM7 and RVSM8 to specific system elements; therefore, they are retained as system-level safety requirements and argued as such in the PISC.

A detailed Functional Hazard Assessment (FHA) was conducted to provide assurance that all hazards and risks associated with RVSM were identified. The FHA addressed three separate scenarios:

- i. the situation whereby RVSM has been operational for one year, is fully operational and all introductory problems have been resolved;
- ii. the particular situation in States which have to ensure the transition between RVSM and non-RVSM airspace; and
- iii. the Switch-Over on the day of RVSM introduction.

A complete list of hazards identified in the FHA is presented in respective Hazard Logs. The subsequent analysis indicated that of these some hazards are safety significant in the context of the introduction of RVSM – i.e. either the hazard is new or the level of risk is potentially higher than already present in the ATM system.

For each of the safety-significant hazards, a safety integrity requirement is derived, which is allocated to the appropriate elements of the system, together with an indication of what (if any) mitigation is available to reduce the effect, and/or probability of occurrence, of the hazard concerned.

Where mitigation is available, an explicit functional safety requirement was derived for the relevant system element(s), in order to specify clearly the mitigation required. Where mitigation is not available, the safety integrity requirement from the FHA is allocated to the relevant system element(s), in order to limit the risk to a tolerable level.

The PISC concludes at this stage that a sufficient set of high-level safety requirements have been specified for RVSM, and have been completely and correctly allocated to the appropriate elements of the RVSM system. Safety requirements have also been specified and allocated to the system elements, for each

hazard identified in the FHA, sufficient to control and/or mitigate the hazard.

### 2.2.2 *RVSM concept*

This section of the PISC sets out the argument and evidence that the RVSM Concept satisfies the RVSM high-level safety requirements. For each of the system elements the relevant safety requirements are listed and the approach is defined how their achievement is demonstrated. Subsequently, direct and backing evidence is presented or referred to to demonstrate that the argument is true.

This part of the PISC also presents the results of the Collision Risk Assessment (CRA) to demonstrate that the high-level safety requirements, which are directly related to ICAO requirements, are satisfied.

### 2.2.3 *RVSM implementation*

This section of the PISC provides the argument and evidence that the Implementation of the RVSM Concept will satisfy fully the relevant safety requirements.

It is the States' ultimate responsibility to implement RVSM. To this end all participating States have prepared Safety Plans for the implementation of RVSM within their national airspace. These Safety Plans show in how the respective State responsibility is discharged, what activities it is undertaking to assure the safety of the changes it is making in order to implement RVSM, and how risks to aircraft are identified and managed.

EUROCONTROL's role was to provide guidance, co-ordination and support to the participating States and other parties in their preparation for the implementation of RVSM and to demonstrate that the safety requirements identified in the PISC are traceable from Concept through to Implementation.

EUROCONTROL also provided independent verification and validation for the implementation of RVSM by monitoring the overall performance in terms of altitude deviations. In addition, information of aircraft approval status is obtained from States to provide verification of the RVSM approval status within the filed flight plans, and information on the actual number of RVSM approved aircraft, which was a key parameter in the "Go"-decision process.

Again, this section of the PISC provides the argument and evidence to satisfy the RVSM high level safety arguments associated to RVSM Implementation.

A further section of the PISC demonstrates that the Switch-Over from the pre-RVSM separation minimum of 2000 ft to RVSM of 1000 ft will not adversely affect the safety of the on-going air traffic operations.

## 2.3 *PISC conclusions*

Based on the conclusions drawn in its different sections, the PISC concludes, that the application of the ICAO RVSM Concept in the European Region and the Implementation of RVSM by the participating States

can be considered as tolerably safe and satisfies the criteria defined in the EUR RVSM Safety Policy [4].

## 2.4 *SRC review*

The interface with the EUROCONTROL Safety Regulation Commission (SRC) was established early in the development process of the PISC through the EUROCONTROL Safety Regulation Unit (SRU). The SRC set up on their behalf an expert group – the SRC RVSM Group (SRVG) – to review intermediately delivered safety documentation. Guidance was given to the EUR RVSM Programme until the mature PISC [1] was delivered in August 2001. The positive outcome of the regulatory review formed the basis for the SRC's recommendation to the EUROCONTROL Provisional Council (PC) for their "Go"-decision to implement RVSM on time.

## 3 POST-IMPLEMENTATION SAFETY CASE

Reduced Vertical Separation Minimum (RVSM) was introduced into European airspace at 0001 hrs UTC on 24 January 2002, reducing the vertical separation between RVSM-approved aircraft from 2000 ft to 1000 ft for aircraft operating at/between Flight Levels 290 and 410 inclusive.

The Switchover to RVSM was executed extremely smoothly, and since then there have been no major problems (either safety or operational) related to RVSM.

### 3.1 *Safety objectives and argument*

The Post-Implementation Safety Case (POSC) follows on from the Pre-Implementation Safety Case (PISC) to demonstrate that the key safety objectives set out in the EUR RVSM Safety Policy [4] are actually met in operational service, and addresses any matters that were outstanding when the last version of the PISC [1] was issued.

The POSC demonstrates that this aim has been achieved, by means of the following principal safety arguments:

- i. That the vertical collision risk – i.e. the risk of mid-air collision in the vertical dimension – in RVSM airspace meets the ICAO overall Target Level of Safety (TLS) of  $5 \times 10^{-9}$  fatal accidents per flight hour.
- ii. That the vertical collision risk in RVSM airspace due solely to technical height-keeping performance meets the ICAO TLS of  $2.5 \times 10^{-9}$  fatal accidents per flight hour.
- iii. That the implementation of RVSM has not adversely affected the overall risk of en-route mid-air collision.

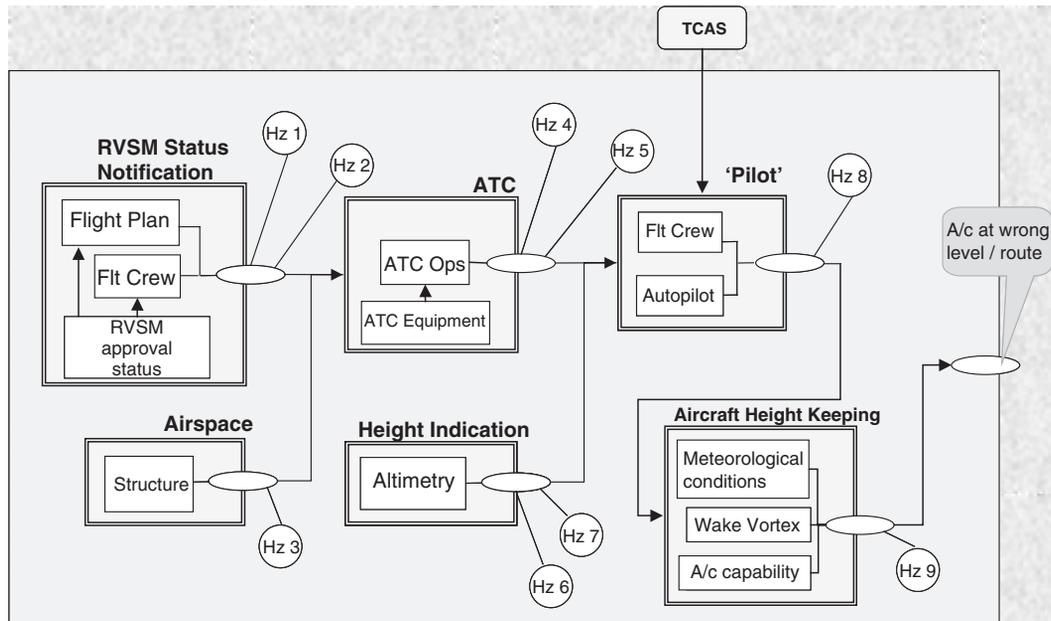


Figure 3. RVSM system and sub-system hazards.

- iv. That all issues that were active when Version 2.0 of the PISC was issued, including validation of the assumptions made therein, have been addressed satisfactorily.

Each of the above arguments is developed in the relevant section of the POSC and evidence is presented that all arguments are valid.

The layout of the POSC follows that of the earlier PISC. In order to address the first two safety objectives a post-implementation Collision Risk Assessment is carried out to demonstrate that the ICAO Target Level of Safety is achieved. The third safety objective is addressed by a re-conduct of the pre-implementation FHA to review the hazards identified earlier, validate their relevance and identify if operational experience indicates the existence of new hazards. This FHA review included also elements of a Preliminary System Safety Assessment (PSSA) [8].

### 3.2 Lessons learnt

A number of lessons were learnt with regard to how to conduct such an FHA with operational experts and how to present the results. Were there 73 hazards identified during the pre-implementation FHA, it became clear that most of them could be considered as causes giving rise to higher-level hazards. Therefore, an RVSM system model was developed (see Figure 3), which

Table 1. RVSM sub-system hazards.

<b>Hz 1</b>	Non-RVSM approved aircraft is indicated as RVSM approved
<b>Hz 2</b>	RVSM approved aircraft cannot indicate loss of RVSM capability to ATC
<b>Hz 3</b>	Airspace structure is wrong
<b>Hz 4</b>	Aircraft is assigned inappropriate level
<b>Hz 5</b>	No clearances/instructions are given to pilot from ATC
<b>Hz 6</b>	Undetectable altimetry system error
<b>Hz 7</b>	Loss of, or detectable error in, altimetry information
<b>Hz 8</b>	“Pilot” deviates from cleared level
<b>Hz 9</b>	Aircraft is unable to maintain cleared level

defined one overall hazard at the system boundary and nine hazards at sub-system level (Table 1).

The terminology regarding “causes”, “hazards” and “consequences” was clarified and lead together with Fault- and Event-Tree Analyses (FTA/ETA) to the “Bow-Tie” model in Figure 4.

The two main objectives of the FHA/PSSA session were:

- i. To identify, and estimate the probability of occurrence of, the possible causes of each RVSM hazard, taking account of the available mitigations to reduce the probability of occurrence;
- ii. To assess the severity of the consequences of each hazard, taking account of available mitigations.

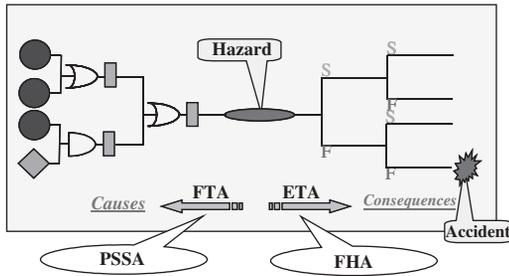


Figure 4. "Bow-Tie" model.

The outcome of this session with operational experts was subsequently analysed to construct "Bow-Ties" for each sub-system hazard. Allowing for the first time to obtain quantitative results describing the aggregate risk from all hazards to be compared to the ICAO TLS.

### 3.3 POSC conclusions

The POSC delivers a conclusive argument and evidence that the key safety objectives set out in the EUR RVSM Safety Policy [4] are met in operational service.

The outcome of the FHA/PSSA showed reasonable consistency with the pre-implementation results and identifies those causes and mitigations, which have the highest bearing on the aggregated risk.

## 4 CONCLUSIONS

The RVSM Pre-Implementation Safety Case was the first of its scale, which had been developed by the EUROCONTROL Agency for one of its Programmes. It established the precedent for a constructive review process with the EUROCONTROL Safety Regulation Commission and provided the basis for the "Go"-decision taken by the EUROCONTROL Provisional Council prior to the implementation of RVSM in 41 participating States.

The RVSM Post-Implementation Safety Case was developed several months subsequent to the successful implementation of RVSM in Europe. It built on numerous lessons learned during the earlier PISC development and concludes that RVSM was safely implemented and that RVSM operations are safe and continue to be safe.

The experience gained during the development of both RVSM Safety Cases together with input from other areas within the EUROCONTROL Agency are now providing the building blocks for a Guidelines Document, which will describe how future Safety Cases should be developed for different EUROCONTROL activities.

## ABBREVIATIONS

A/C	Aircraft
ATC	Air Traffic Control
ATM	Air Traffic Management
ATS	Air Traffic Service
CRA	Collision Risk Assessment
EATMP	European ATM Programme
ETA	Event-Tree Analyses
EUR	European
FHA	Functional Hazard Assessment
FL	Flight Level
FTA	Fault-Tree Analyses
GSN	Goal Structured Notation
Hz	Hazard
ICAO	International Civil Aviation Organisation
MASPS	Minimum Aircraft System Performance Specification
PC	Provisional Council
PISC	Pre-Implementation Safety Case
POSC	Post-Implementation Safety Case
PSSA	Preliminary System Safety Assessment
RVSM	Reduced Vertical Separation Minimum
SRC	Safety Regulation Commission
TCAS	Traffic Alert and Collision Avoidance System
TLS	Target Level of Safety

## ACKNOWLEDGEMENTS

The author would like to outline the important contribution of Derek Fowler during the independent PISC review (with CSE International Ltd.) and during the development of the POSC (with Praxis Critical Systems) and thank him for all the invaluable discussions. Thanks are extended to Diena Seeger on behalf of the team working on the Collision Risk Assessment for their thorough and time-consuming assessment of the data. Finally, the author would like to thank Peter Stastny and Tony Licu of the EUROCONTROL Safety Regulation Unit (SRU) for their continuous support during the review process and their efforts to ensure the timely completion of the review.

The views expressed in this paper are those of the author and do not necessarily represent official EUROCONTROL policy.

## REFERENCES

- [1] EUROCONTROL: EUR RVSM Pre- Implementation Safety Case, RVSM 691, Version 2.0, 14 August 2001.
- [2] EUROCONTROL: EATMP Safety Policy, Edition 1.1, August 1999.
- [3] EUROCONTROL/ECAC: Air Traffic Management Strategy for the Years 2000+ , January 2000.

- [4] EUROCONTROL: EUR RVSM Safety Policy, Edition 1.0, September 2000.
- [5] ICAO Document 9574 (2nd Edition) – Manual on Implementation of a 300M (1000 FT) Vertical Separation Minimum between FL290 and FL410 inclusive.
- [6] Internati Fonal Safety Management Standard IEC 61508 Part 1.
- [7] UK CAA Document 670 – ATS Safety Requirements
- [8] EUROCONTROL: EATMP Air Navigation System Safety Assessment Methodology (Edition 1.0).

#### AUTHOR'S BIOGRAPHY

Dr.-Ing. Bernd Tiemeyer studied aerospace engineering at the Technical University (TU) Braunschweig,

Germany. In 1991 he was appointed as research engineer and project leader in the area of Satellite Navigation at the Institute of Flight Guidance of the TU Braunschweig. In 1994 he joined the EUROCONTROL Experimental Centre where he was appointed Project Manager for the Satellite Navigation GBAS (Ground Based Augmentation Systems) Project and – since mid-2000 – appointed Safety Manager for the Reduced Vertical Separation Minimum (RVSM) Programme. In January 2002 he obtained a Doctorate in engineering from the University FAF Munich. In April 2002 he joined the Safety Management Unit within the Directorate for Safety, Airspace, Airports & Information Services at EUROCONTROL's Headquarters.

## Assessment of the environment vulnerability in the surroundings of an industrial site

J. Tixier, A. Dandrieux & G. Dusserre

*Industrial and natural risks department, LGEI, Ecole des Mines d'Alès, CEDEX, France*

R. Bubbico, L.G. Luccone, B. Silvetti, R. Carta, B. Mazzarotta & S. Di Cave

*Dipartimento di Ingegneria Chimica, Università di Roma "La Sapienza", Italy*

E. Hubert

*Centre SITE, Ecole des Mines de Saint Etienne, France*

N. Rodrigues, O. Salvi & D. Gaston

*INERIS, Parc technologique ALATA, Verneuil en Halatte, France*

**ABSTRACT:** ARAMIS project aims at assessing the risk level of an industrial site. To reach this goal, the environment, as a target, must be studied and taken into account. On the base of a multicriteria decision approach (Saaty method), a structured methodology is proposed. In the first step an identification of generic targets is made in order to assess, in a second step, their vulnerability. The expected results are cartographical representations of the index of vulnerability  $V$  which represents the vulnerability of an area in the surroundings of an industrial site. This methodology must be implemented into a geographical information system (G.I.S) in order to devise an operational tool to evaluate the vulnerability for the competent authorities, the industrialist and the risk experts.

### 1 INTRODUCTION

ARAMIS project aims at developing an integrated risk index based on, among others, the environment vulnerability. Indeed, environment vulnerability is scarcely taken into account in risk assessment, and its integration in ARAMIS project is therefore of great interest. The idea developed is to assess the vulnerability index to identify and characterise the vulnerability of targets located in the surroundings of a Seveso industrial site. To summarise, Figure 1 explains the problematic and ARAMIS project must answer to the following question: Is the area 1, which is composed of human, environmental and material targets, more or less vulnerable than the area 2 also composed of human, environmental and material targets, but in different quantity and of different nature?

To solve this question several steps are necessary, namely, the definition of the study area, the definition of the targets and also the choice of available databases which are essential to characterise the environment.



Figure 1. Problematic of vulnerability definition.

Then, a specific methodology for the assessment of the vulnerability is required.

The methodology used to obtain a semi-quantitative approach of vulnerability is a multicriteria decision method (Saaty's method) based on the experts judgements.

Another critical step is to make a census of the targets in the study area. This step can be supported by the use of GIS (Geographic Information System) databases and tools. The chosen databases are available for all the EC countries and cover information concerning the population, and the characteristics of natural and man made environment. GIS software and tools allow to display the geographical information on maps, and to make operations on the various types of geographical items.

Results of vulnerability and quantification factors are presented in this paper.

## 2 CHARACTERISATION OF THE STUDY AREA

### 2.1 *Size of the study area*

On the base of previous studies (Egidi et al., 1995; ARPAT, 2000) and data concerning the effects distances of major accidents, a study area of 400 km square is retained. This area is expected to cover all the consequences of flammable and explosive events and the greatest part of the consequences of toxic events, but it will not include the impact area of a very large toxic cloud under particular atmospheric conditions. However, in our opinion, the grid size of 20 km  $\times$  20 km will fit our scope, requiring a reasonably limited amount of territorial information. In order to have a more accurate representation of the vulnerability index, it is convenient to cut into meshes the study area. The size of these meshes is of 250 meters in a first approach but it may, in the future, depend on the distance source – targets. In fact, close to the industrial site it may be interesting to have a smaller size of the meshes (for example 50 m  $\times$  50 m) and far from the industrial site to have a bigger size of the meshes (for example 500 m  $\times$  500 m).

All these considerations permit to validate the proposed size of area to answer to the problematic in order to determine the vulnerability of targets in front of major accidents. Now, it is necessary to define the environment.

### 2.2 *Targets typologies*

The aim of this paragraph is to define the environment of an industrial site to determine the risk level of an industrial installation. It is therefore necessary to propose a set of target types to characterise with accuracy the environment, while keeping in mind the importance of the transferability of the method and its flexibility. Indeed, it is necessary to find a proper balance between the number of targets to be taken into account and the limitations due to the multicriteria decision method.

First of all, targets were divided into three categories and each of these categories is then detailed in a list of generic targets:

- Human (H)
  - Staff of the site (H<sub>1</sub>)
  - Local population (H<sub>2</sub>)
  - Population in an establishment receiving public (H<sub>3</sub>)
  - Users of communications ways (H<sub>4</sub>)
- Environmental (E)
  - Agricultural areas (E<sub>1</sub>)
  - Natural areas (E<sub>2</sub>)
  - Specific natural area (E<sub>3</sub>)
  - Wetlands and water bodies (E<sub>4</sub>)
- Material (M)
  - Industrial site (M<sub>1</sub>)
  - Public utilities and infrastructures (M<sub>2</sub>)
  - Private structures (M<sub>3</sub>)
  - Public structures (M<sub>4</sub>)

### 2.3 *Available databases*

Two databases have been retained.

The Corine Land Cover (IFEN, 2002) database provides homogeneous geographical information about land use in each country of Europe. The main information included in this database corresponds to topographical map, vegetation and type of forest map and finally soil and network description.

There are five main types of territory description:

- artificial territory
- land for agricultural use
- forest and natural areas
- humid areas
- water areas

The five previous types are described by forty four classes in order to characterise the natural environment.

The TeleAtlas database is made of local data collection activities in all European countries and in the USA (TeleAtlas, 1996).

The included themes are:

- road and street centre-lines
- address areas
- administrative areas
- postal districts
- land use and cover
- railways
- ferry connections
- points of interest: built-up areas
- settlement centers
- water

These two databases fill most of our objectives to describe the natural environment and man made

targets. Concerning the human targets, specific data provided by each country must be used. The information concerning the population will be obtained with the data provided by the INSEE for France which gives a status of the French population in 1999 by district (INSEE, 1999). In Italy, ISTAT (the National Institute for Statistics) also gives this type of information based on the 1991 (ISTAT, 1992) and, soon, on 2001 census of Italian population by district or census unit.

To use these population data, some rules must be assumed to allocate a number of people to each mesh included in a district, as discussed in the paragraph concerning the quantification of environmental targets. If more precise results are required, information at the cadastral level should be taken into account. This second approach is more time consuming than the first one.

It has to be pointed out that other more specific information concerning some important environmental features, such as parks or protected zones are available from national environmental organisations, such as APAT in Italy, or Natural zone of faunistic and floristic interest in France (ZNIEFF).

Finally, some other information, such as that concerning the industrial site, has to be provided directly from the user, since it is not available to the general public. A specific procedure is proposed to fill these data, which can be used also to add information concerning special targets, such as sites concentrating high number of people, vital infrastructures, monuments, etc.

Figure 2 shows the information available from Corine Land Cover, TeleAtlas, APAT and Istat for an example area in Northern Italy, displayed using the GIS software ArcView (ArcView, 2000) with a  $20\text{ km} \times 20\text{ km}$  grid with  $500\text{ m} \times 500\text{ m}$  meshes ( $50\text{ m} \times 50\text{ m}$  in the proximity of the plant).

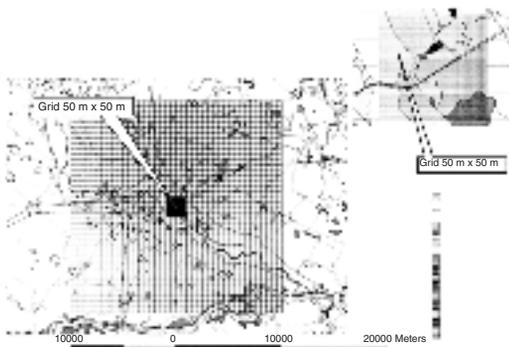


Figure 2. Example of  $20\text{ km} \times 20\text{ km}$  study area.

### 3 THE VULNERABILITY INDEX

#### 3.1 *Generalities on the multicriteria decision method of Saaty (Saaty, 1984)*

In a general way, a decision-taking is a complex process which is not only based on a set of information about a subject. It depends also on feelings which correspond to a more or less vague vision of the reality and on the influence of such or such person of the group of decision. In fact, personal preferences and persuasion can have more importance in the process of decision than a clear and rigorous logic. So logic intervenes in a second time to order words and ideas and to lend weight to the decision taken previously.

A multicriteria hierarchical method brings an organisation of information and appreciation which intervenes in the process of decision-taking.

The purpose of this method is an assessment of priorities. In this goal, the first point is to have a consensus on the objective, then in a second time, to decompose the complex and not structured situation in its main constituents. The types of results can be a classification, an allocation of numerical values of subjective judgments or the aggregation of judgments to determine variable having the biggest priorities. The multicriteria hierarchical method allows to obtain a decision-taking of group in a consensual way due to a better coherence of judgement.

The multicriteria hierarchical method of Saaty (Saaty, 1984) is based on three main steps:

- a construction of hierarchies;
- an assessment of priorities;
- a validation of coherence.

The construction of a hierarchical structure requires the creation or the identification of links between the various levels of this structure.

Each element of a functional hierarchy takes place at a given level of the structure. Its upper level corresponds to the global objective (or dominant element). Some binary comparisons are done between all the elements of a given level according to the element of the upper level, in order to rank the elements among them. The various levels of a hierarchy are, consequently, interconnected.

A complex situation can be analysed by a systematic approach with the help of the hierarchical structure. The priorities have to be assessed. This process is done by a comparison of elements two by two (binary comparison). This one gives the ranking of elements according to their relative importance. Finally, the logical coherence confirms the whole applied process. To do the binary comparisons, it is necessary to use a scale based on classic numerical variables or more qualitative variables contributing to take into account intangible qualities as showed in the Table 1.

Table 1. Scale of binary comparison.

Degree of importance	Definition
1	Equal importance of two elements
3	Weak importance of an element in comparison to the other one
5	Strong importance of an element in comparison to the other one
7	Certified importance of an element in comparison to the other one
9	Absolute importance of an element in comparison to the other one
2, 4, 6, 8	Intermediate values between two appreciation
1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9	Reciprocal values of the previous appreciation



Figure 3. Description of the system.

### 3.2 Application to the determination of the index of vulnerability (Saaty, 1984)

This part consists in the description of the environment (Fig. 3) in order to have a good understanding of the situation. In this aim, three typologies are proposed:

- a typology of targets which is composed of three main classes of targets (human, environmental and material). Each main class of targets is characterised by four types of targets as described in the paragraph 2.3.
- a typology of physical effects. Four types of effects are considered:
  - overpressure;
  - thermal flux;
  - gas toxicity;
  - liquid pollution.
- a typology of impacts. Three impacts due to physical effects are considered to characterise the effects of major accidents on targets:
  - sanitary or integrity impact which qualifies the effect on respectively human or environmental and material structures;
  - economical impact which qualifies an effect in terms of loss of production or of rehabilitation;
  - psychological impact which qualifies an effect in terms of influence on a group of people.

It is then necessary to organise these typologies in order to answer to the vulnerability problematic.

Therefore, the following step consists in the structuring of the information. It is ensued from the following definition of the vulnerability.

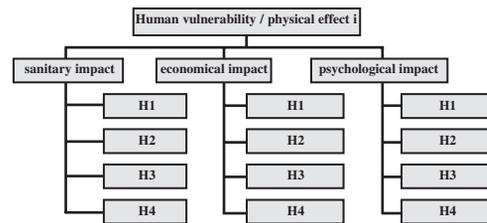


Figure 4. Hierarchical structure for the human vulnerability per physical effect characterisation.

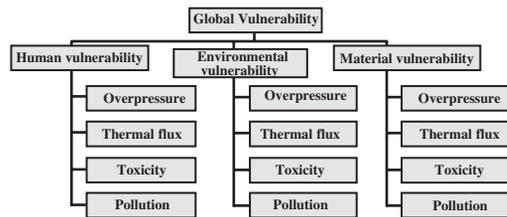


Figure 5. Hierarchical structure of the global vulnerability characterisation.

For a class of targets and a given physical effect, the vulnerability of each type of targets in comparison with the other one is evaluated by the way of binary comparisons in function of characterisation criteria which are the three impacts.

The result is the vulnerability of one class of target for one physical effect. The associated hierarchical structure is presented in Figure 4 for the human vulnerability.

For a class of targets, the importance of each physical effect in comparison with another one is evaluated by the way of binary comparisons: the result is the vulnerability of one class of target (Fig. 5). Finally, the vulnerability of each class of targets is compared to the others, leading to the global vulnerability (Fig. 5).

The same hierarchical structure applies to environmental and material vulnerability.

From this definition and from hierarchical structures too, the matrixes and the functions of the vulnerability index are deduced. The matrixes are translated into a questionnaire which allows to collect the expert judgement for the evaluation of each coefficient of vulnerability of vulnerability functions.

### 3.3 The vulnerability factors and functions (Saaty, 1984)

Thirty eight experts have already been consulted in an individual way. The repartition of experts per country and type are presented in Figures 6 and 7: a great part of them were French or Italian.

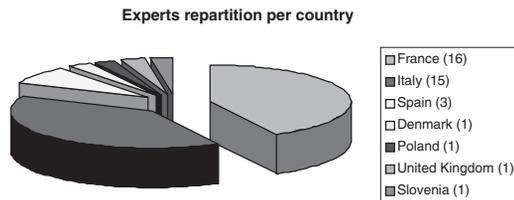


Figure 6. Experts repartition per country.

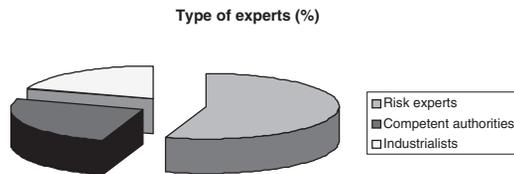


Figure 7. Experts repartition per type.

During all the project, expert judgements will be collected in order to update vulnerability factors.

Concerning the type of experts, about 60% were risks experts (from public or private structures).

A specific treatment must be done to aggregate the appreciation of the above mentioned experts. Each appreciation is aggregated by the mean of geometrical average. So a new questionnaire which is an aggregation of the appreciation of all experts consulted is built. All obtained evaluations are reported into the matrixes and the factors of vulnerability can be assessed. Results are given in the following paragraph.

To assess the vulnerability factors of each function, the eigenvectors of the matrixes must be calculated. The solutions correspond to the factors of vulnerability. The following tables (Table 2 to 5) present the results. The ratios of coherence (RC) must have a value lower than 10% for each matrix to validate the coherence of the ratios and therefore the results. The results obtained for the function of global vulnerability (Table 2) show the great importance (about 75%) of human vulnerability. The vulnerability factor of environmental targets represents 20%, while the material vulnerability represents only 5% of the function.

For human targets (Table 3), the main effect is "gas toxicity" (47%). The effects of "overpressure" and "thermal radiation" have about the same importance (respectively 24% and 23%). On the contrary, the effect of "liquid pollution" has a weak influence on human targets (only 7%).

For human targets and for all the physical effects, the sanitary impact is the dominating impact (about 65%). The psychological impact represents about 25% of the vulnerability factors and the economical impact represents only 10%. For the physical effects of "overpressure" and "thermal radiation", the type of

Table 2. Global vulnerability function.

Function	RC%
$V_{\text{global}} = 0,752 \times V_H + 0,197 \times V_E + 0,051 \times V_M$	0,17

targets  $E_3$  (specific natural area) has the higher vulnerability factor for all impacts. By considering liquid pollution, the type of targets  $E_4$  (wetlands and water bodies) has an important vulnerability. The two other categories  $E_1$  and  $E_2$  (agricultural area and natural area) seem to be less vulnerable to this physical effect than  $E_3$  and  $E_4$ . Concerning material targets (Table 5), the effects of overpressure and thermal radiation represent the main parts of the vulnerability factors (respectively 45% and 41%). For an overpressure effect and a thermal radiation effect, the integrity and the economical impacts are more important than a psychological impact. On the contrary, for a gas toxicity effect and a liquid pollution effect, the economical and the psychological impacts are more important than the integrity impact. For the effects of gas toxicity and liquid pollution, the factors of vulnerability have about the same value for all types of targets except for the type of target  $M_1$ . For a thermal radiation effect, the factor of vulnerability for an economical impact of the type of target  $M_1$  has a dominating value.

All the ratios of coherence (RC) are lower than 10%, so the vulnerability factors based on the thirty eight questionnaires mentioned above are validated.

To complete the functions of vulnerability, quantification factors of each type of targets are implemented. They are defined in the following paragraph.

### 3.4 Quantification factors

The quantification factors are those accounting for the "quantity" of environmental targets in the study area. A quantification factor is defined as a dimensionless variable, assuming values in the range 0–1, where 0 indicates the absence of the target in the area and 1 indicates that the quantity of that target in the area reaches its expected maximum.

Therefore, the quantification factors aims at doing a normalized census of each detailed type of targets ( $H_1-H_4$ ,  $E_1-E_4$  and  $M_1-M_4$ ).

#### 3.4.1 Human targets

The quantification factor  $H_i$  relevant to each of the  $i$ -th types of human targets in the area are determined as:

$$H_i = \frac{N_i}{N_{\text{max}_i}}$$

with  $N_i$  total number of people of the  $i$ -th human target type and  $N_{\text{max}_i}$  maximum number of people of the  $i$ -th human target type, in the area under exam.

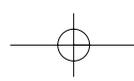


Table 3. Human vulnerability functions.

Functions	RC%		
$V_H = 0,242 \times V_H^{op} + 0,225 \times V_H^{tr} + 0,466 \times V_H^{tox} + 0,067 \times V_H^{poll}$	0,43		
<b>Overpressure</b>	RC%	<b>Thermal radiation</b>	RC%
$V_H^{op} = 0,666 \times V_H^{op_s} + 0,111 \times V_H^{op_E} + 0,222 \times V_H^{op_P}$	0	$V_H^{tr} = 0,648 \times V_H^{tr_s} + 0,122 \times V_H^{tr_E} + 0,230 \times V_H^{tr_P}$	0,3
$V_H^{op_s} = 0,366 \times H_1 + 0,278 \times H_2 + 0,233 \times H_3 + 0,124 \times H_4$	2,5	$V_H^{tr_s} = 0,354 \times H_1 + 0,354 \times H_2 + 0,161 \times H_3 + 0,131 \times H_4$	1
$V_H^{op_E} = 0,404 \times H_1 + 0,340 \times H_2 + 0,139 \times H_3 + 0,117 \times H_4$	1,72	$V_H^{tr_E} = 0,409 \times H_1 + 0,350 \times H_2 + 0,158 \times H_3 + 0,082 \times H_4$	0,86
$V_H^{op_P} = 0,150 \times H_1 + 0,368 \times H_2 + 0,282 \times H_3 + 0,200 \times H_4$	4,57	$V_H^{tr_P} = 0,167 \times H_1 + 0,333 \times H_2 + 0,333 \times H_3 + 0,167 \times H_4$	0
<b>Gas toxicity</b>	RC%	<b>Liquid pollution</b>	RC%
$V_H^{tox} = 0,735 \times V_H^{tox_s} + 0,069 \times V_H^{tox_E} + 0,196 \times V_H^{tox_P}$	0,35	$V_H^{poll} = 0,594 \times V_H^{poll_s} + 0,157 \times V_H^{poll_E} + 0,249 \times V_H^{poll_P}$	4,62
$V_H^{tox_s} = 0,227 \times H_1 + 0,424 \times H_2 + 0,227 \times H_3 + 0,122 \times H_4$	0,57	$V_H^{poll_s} = 0,212 \times H_1 + 0,497 \times H_2 + 0,191 \times H_3 + 0,100 \times H_4$	0,86
$V_H^{tox_E} = 0,351 \times H_1 + 0,351 \times H_2 + 0,189 \times H_3 + 0,109 \times H_4$	0,57	$V_H^{poll_E} = 0,283 \times H_1 + 0,490 \times H_2 + 0,152 \times H_3 + 0,076 \times H_4$	0,57
$V_H^{tox_P} = 0,140 \times H_1 + 0,456 \times H_2 + 0,263 \times H_3 + 0,141 \times H_4$	0,55	$V_H^{poll_P} = 0,138 \times H_1 + 0,479 \times H_2 + 0,256 \times H_3 + 0,128 \times H_4$	0,53

Table 4. Environmental vulnerability functions.

Functions	RC%		
$V_E = 0,071 \times V_E^{op} + 0,148 \times V_E^{tr} + 0,277 \times V_E^{tox} + 0,503 \times V_E^{poll}$	0,4		
<b>Overpressure</b>		<b>Thermal radiation</b>	RC%
$V_E^{op} = 0,333 \times V_E^{op_s} + 0,333 \times V_E^{op_E} + 0,333 \times V_E^{op_P}$	0	$V_E^{tr} = 0,550 \times V_E^{tr_s} + 0,240 \times V_E^{tr_E} + 0,210 \times V_E^{tr_P}$	1,58
$V_E^{op_s} = 0,122 \times E_1 + 0,227 \times E_2 + 0,424 \times E_3 + 0,227 \times E_4$	0,53	$V_E^{tr_s} = 0,195 \times E_1 + 0,231 \times E_2 + 0,426 \times E_3 + 0,148 \times E_4$	2,54
$V_E^{op_E} = 0,289 \times E_1 + 0,246 \times E_2 + 0,289 \times E_3 + 0,175 \times E_4$	3,36	$V_E^{tr_E} = 0,227 \times E_1 + 0,227 \times E_2 + 0,424 \times E_3 + 0,122 \times E_4$	0,57
$V_E^{op_P} = 0,168 \times E_1 + 0,239 \times E_2 + 0,395 \times E_3 + 0,198 \times E_4$	3,36	$V_E^{tr_P} = 0,200 \times E_1 + 0,200 \times E_2 + 0,400 \times E_3 + 0,200 \times E_4$	0
<b>Gas toxicity</b>	RC%	<b>Liquid pollution</b>	RC%
$V_E^{tox} = 0,691 \times V_E^{tox_s} + 0,160 \times V_E^{tox_E} + 0,149 \times V_E^{tox_P}$	0,48	$V_E^{poll} = 0,710 \times V_E^{poll_s} + 0,155 \times V_E^{poll_E} + 0,135 \times V_E^{poll_P}$	1,58
$V_E^{tox_s} = 0,286 \times E_1 + 0,142 \times E_2 + 0,286 \times E_3 + 0,286 \times E_4$	0	$V_E^{poll_s} = 0,227 \times E_1 + 0,122 \times E_2 + 0,227 \times E_3 + 0,424 \times E_4$	0,53
$V_E^{tox_E} = 0,340 \times E_1 + 0,140 \times E_2 + 0,239 \times E_3 + 0,280 \times E_4$	3,36	$V_E^{poll_E} = 0,278 \times E_1 + 0,123 \times E_2 + 0,231 \times E_3 + 0,367 \times E_4$	2,55
$V_E^{tox_P} = 0,205 \times E_1 + 0,169 \times E_2 + 0,338 \times E_3 + 0,288 \times E_4$	3,36	$V_E^{poll_P} = 0,140 \times E_1 + 0,140 \times E_2 + 0,262 \times E_3 + 0,458 \times E_4$	0,53

Table 5. Material vulnerability functions.

Functions	RC%		
$V_M = 0,446 \times V_M^{op} + 0,410 \times V_M^{tr} + 0,069 \times V_M^{tox} + 0,075 \times V_M^{poll}$	0,39		
<b>Overpressure</b>	RC%	<b>Thermal radiation</b>	RC%
$V_M^{op} = 0,571 \times V_M^{op_1} + 0,286 \times V_M^{op_E} + 0,143 \times V_M^{op_P}$	0	$V_M^{tr} = 0,443 \times V_M^{tr_1} + 0,387 \times V_M^{tr_E} + 0,169 \times V_M^{tr_P}$	1,58
$V_M^{op_1} = 0,200 \times M_1 + 0,400 \times M_2 + 0,200 \times M_3 + 0,200 \times M_4$	0	$V_M^{tr_1} = 0,246 \times M_1 + 0,298 \times M_2 + 0,210 \times M_3 + 0,246 \times M_4$	3,36
$V_M^{op_E} = 0,288 \times M_1 + 0,338 \times M_2 + 0,169 \times M_3 + 0,205 \times M_4$	3,36	$V_M^{tr_E} = 0,400 \times M_1 + 0,200 \times M_2 + 0,200 \times M_3 + 0,200 \times M_4$	0
$V_M^{op_P} = 0,143 \times M_1 + 0,286 \times M_2 + 0,286 \times M_3 + 0,286 \times M_4$	0	$V_M^{tr_P} = 0,143 \times M_1 + 0,286 \times M_2 + 0,286 \times M_3 + 0,286 \times M_4$	0
<b>Gas toxicity</b>	RC%	<b>Liquid pollution</b>	RC%
$V_M^{tox} = 0,200 \times V_M^{tox_1} + 0,400 \times V_M^{tox_E} + 0,400 \times V_M^{tox_P}$	0	$V_M^{poll} = 0,260 \times V_M^{poll_1} + 0,413 \times V_M^{poll_E} + 0,327 \times V_M^{poll_P}$	4,62
$V_M^{tox_1} = 0,142 \times M_1 + 0,286 \times M_2 + 0,286 \times M_3 + 0,286 \times M_4$	0	$V_M^{poll_1} = 0,127 \times M_1 + 0,313 \times M_2 + 0,280 \times M_3 + 0,280 \times M_4$	1,2
$V_M^{tox_E} = 0,204 \times M_1 + 0,347 \times M_2 + 0,204 \times M_3 + 0,246 \times M_4$	3,36	$V_M^{poll_E} = 0,204 \times M_1 + 0,347 \times M_2 + 0,204 \times M_3 + 0,246 \times M_4$	3,36
$V_M^{tox_P} = 0,100 \times M_1 + 0,300 \times M_2 + 0,300 \times M_3 + 0,300 \times M_4$	0	$V_M^{poll_P} = 0,127 \times M_1 + 0,280 \times M_2 + 0,313 \times M_3 + 0,280 \times M_4$	1,2

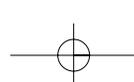
Accordingly, in order to determine the quantification factors for human targets, it is preliminarily necessary to set the maximum value which the number of people belonging to each i-th human category type can reach in the area,  $Nmax_i$ .

It has to be noticed that, should some calculated value of the quantification factor exceed the value of 1, it must in any case be assumed as equal to 1.

The maximum value for the number of people belonging to the staff of the site present at the same

time, based on the number of workers of single, rather large plants, can be assumed as  $Nmax_1 = 2,000$  persons.

The target local population home-body is better described by means of a population density, expressed as number of people/km<sup>2</sup>, which can be calculated based on census data. A maximum reference value of the resident population density,  $PDmax_2$ , can be determined from the individual values of population density of a great number of built-up aggregates. To this



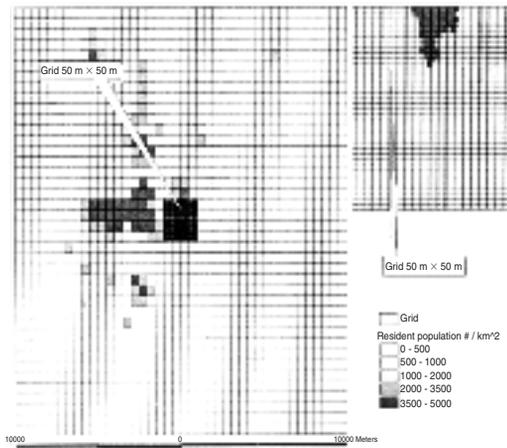


Figure 8. Quantification factor  $H_2$  for resident population.

end, the individual population density values were calculated for about 60,000 Italian built-up aggregates, limiting the analysis to those covering areas larger than the average mesh size (from 0.0625 to 0.25 km<sup>2</sup>).  $PD_{max_2}$  was then taken as the upper 98% limit (i.e. the value that was exceeded only in 2% of the cases), which corresponds to about 15,000 people/km<sup>2</sup>. Due to the rather high population density in the built-up areas in Italy, this value can be assumed to hold all over the EC.

The maximum number of resident population in a study area is therefore:

$$N_{max_2} = PD_{max_2} \cdot A$$

with  $PD_{max_2}$  maximum population density of local population home-body (people/km<sup>2</sup>) and  $A$  extension of the area under exam (km<sup>2</sup>).

The number of resident people can be estimated for each mesh area as follows:

$$N_{2,mesh} = \sum_k (PD_{2,k,mesh} \cdot A_{k,mesh})$$

with  $PD_{2,k,mesh}$  population density of the k-th buildup aggregate falling (totally or partly) in the mesh (people/km<sup>2</sup>) and  $A_{k,mesh}$  extension of the portion of surface covered by the built-up aggregation falling within the boundaries of the mesh (km<sup>2</sup>).

Figure 8, shows the quantification factor  $H_2$  for the local population of the area shown in Figure 2.

The expected maximum value of people in an establishment receiving public may vary considerably depending on its type. It can be assumed that the largest number of people present at the same time in a specific place people may reach, or even exceed, 80,000 persons for some events as sport matches or

rock concerts taking place in stadiums. However, it seems not practical to set the maximum number of people to this extremely high value, since this will mean that, in the absence of this specific type of establishment, the quantification factors will come out very low, due to the much lower number of people who may be present in most of the other types of establishments, such as theaters, schools, restaurants, etc. Accordingly, the maximum number of people in an establishment receiving public was set as  $N_{max_3} = 30,000$  persons.

It should be pointed out that, in most cases, information regarding the number of people in each establishment and, possibly, its location, should be found and added by the user, being not available from databases. However, it is possible to provide the user with some default values based on the type and size of the establishment.

Users of communication ways include people travelling on roads, rails and waterways. Some databases, such as TeleAtlas (TeleAtlas, 1996), give information concerning location and type of the communication ways, but, generally, no data is available concerning the population travelling on them. Therefore, the data should be inserted by the user, based on locally available information concerning traffic data, average number of people travelling on each mean (cars, trains and boats), etc.

The target users of communication ways can be conveniently expressed as number of people per unit length of the communication way (namely road, railway, and waterway).

For example, the number of road users can be estimated as:

$$N_{4,road} = \sum_k (LD_{4,road,k} L_{road,k})$$

with  $LD_{4,road,k}$  linear population density of the k-th portion of road falling within the boundary of the area under exam (people/km) and  $L_{road,k}$  extension in length of the k-th portion of road.

Figure 9 shows, for example, the estimated number of road users for the study area of Figure 2.

Similar expressions can be written for rails and waterways users, as well. The total number of users

$$N_4 = N_{4,road} + N_{4,rail} + N_{4,waterway}$$

of communication ways is obtained as:

The maximum number of users of communication ways,  $N_{max_4}$ , can be calculated as:

$$N_{max_4} = PD_{max_4} \cdot A$$

with  $PD_{max_4}$  maximum population density of this human target, estimated as 1,250 person/km<sup>2</sup>, based on Italian traffic data.

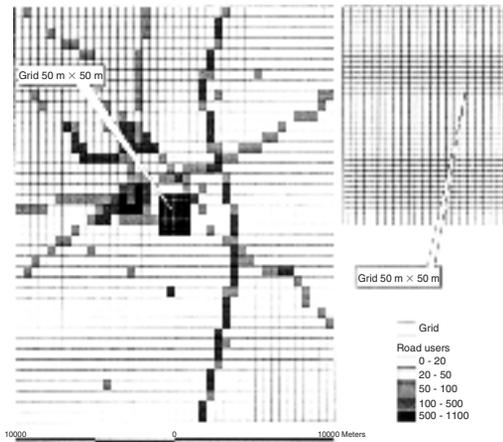


Figure 9. Number of road users N4 in the study area.

### 3.4.2 Environmental targets

All environmental targets can be derived from commercial databases, and GIS tools allow to determine the areas they cover within the study zone.

Accordingly, the quantification factor  $E_i$ , relevant to the  $i$ -th types of environmental targets in the area can be determined as:

$$E_i = \frac{A_i}{A}$$

with  $A_i$  extension of the area covered by the  $i$ -th type of environmental target within the boundaries of the area under exam ( $\text{km}^2$ ) and  $A$  extension of the area under exam ( $\text{km}^2$ ).

Figure 10 shows the quantification factor for agricultural areas,  $E_1$ , for the study area of Figure 2.

### 3.4.3 Material targets

Most material targets can be derived from commercial databases, which, however, may not account for some specific targets, such as the industrial site, or for some outstanding targets, such as vital infrastructures (for material target type 2) or monuments (for material target type 4).

The quantification factor  $M_i$ , relevant to the  $i$ -th types of material targets in the area is:

$$M_i = \frac{A_i}{A}$$

with  $A_i$  extension of the area covered by material target within the boundaries of the area under exam ( $\text{km}^2$ ). However, should some outstanding target (of type 2 and 4 alone) be present, the quantification factor is modified as follows:

$$M_j = \frac{A_j}{A} + \sum_k \frac{I_{j,k}}{\text{Imax}_j}$$

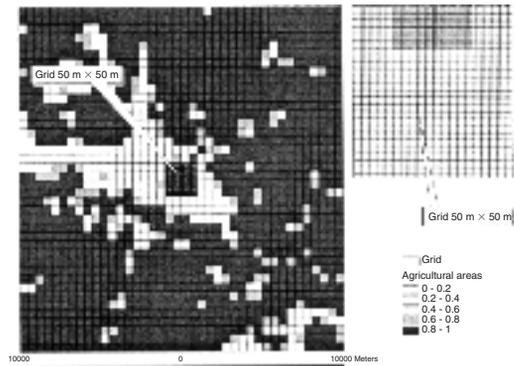


Figure 10. Quantification factor  $E_1$  for agricultural areas.

with  $j$  equal to 2 or 4,  $I_{j,k}$  a factor representing the importance of the  $k$ -th outstanding targets of the  $j$ -th type of specific targets present in the area under exam and  $\text{Imax}_j$  maximum value of the importance of the  $j$ -th outstanding target. In fact, being very difficult to assign a “value” to outstanding targets, it can be obtained based on a relative scale of importance. For example, to a crucial power plant an importance  $I_2 = 0.7$  may be assigned, in a scale from 0 to 1: in that case  $\text{Imax}_2$  will be equal to 1.

However, it has to be remarked that it should always be:  $M_2$  and  $M_4 \leq 1$ : this means that if  $M_2 > 1$  or  $M_4 > 1$ , it should be taken  $M_2 = 1$  or  $M_4 = 1$ .

## 4 TOWARDS AN OPERATIONAL TOOL WITH GEOGRAPHICAL INFORMATION SYSTEM

This paragraph is devoted to do a summary of the presented methodology. It also presents how it can be applied to an area whose vulnerability must be assessed.

### 4.1 Description of the objectives of the GIS tool

The studied area is a square of  $400 \text{ km}^2$  with the industrial site in the middle. In order to assess the vulnerability index, the following steps have to be done:

- divide the studied area into meshes
- assess the vulnerability for each mesh
- identify the targets ( $H_1$ – $H_2$ ,  $E_1$ – $E_4$  and  $M_1$ – $M_4$ ) which are included into the mesh in function of the proposed typologies
- quantify the number of the targets
- calculate the vulnerability index
- map the results

These actions must be repeated for all the meshes of the studied area.

#### 4.2 Expected cartographic results

The vulnerability values obtained in the previous phases can be mapped based on a scale of vulnerability which translates a value of vulnerability index into a class of vulnerability.

Three types of results can be obtained:

- a cartographic representation of the global vulnerability of the studied area
- a cartographic representation of the vulnerability of a class of target (human, environmental or material)
- a cartographic representation of the vulnerability of a physical effect for a class of targets.

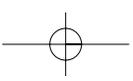
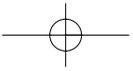
#### 5 CONCLUSION

In conclusion, a structured methodology is proposed to quantify the vulnerability index of an area in the surroundings of an industrial site. This methodology is based on the expert judgements and hierarchical structures to organise the data to answer to the problematic of vulnerability calculation and on the quantification of the different types of environmental targets within the area. This methodology is implemented with a geographical information system to

make available an operational tool for risk managers like the competent authorities, the industrialists and the risks experts. In this way, the end users will have a formalised representation of the situation of the environment in order to manage risks.

#### REFERENCES

- ARPAT, 2000. *Analisi del rischio per l'area di Livorno e strategie di intervento*, Mossa Verre Ed., Firenze.
- Egidi, D., Foraboschi, F., Spadoni, G., Amendola, A. 1995. The ARIPAR project: analysis of the major accident risks connected with industrial and transportation activities in the Ravenna area. *Rel. Eng. and System Safety*. 75–89.
- ESRI, 2000. ArcView, 2000 GIS, 3.2a for Windows.
- ISTAT, 1992. *13° Censimento generale della popolazione e delle abitazioni*, Roma.
- IFEN, 2002. Corine Land Cover cartographical databases, <http://www.ifen.fr>.
- INSEE, 1999. CDROM Populations légales recensement de la population de 1999, <http://www.insee.fr>.
- SAATY T.L. 1984. *Décider face à la complexité: une approche analytique multicritère d'aide à la décision*», collection université – entreprise, entreprise moderne d'édition, Paris.
- TeleAtlas B.V. 1996. Roadnet.



## Increasing of the electric safety in HV systems by means of the ground resistance of the body

R. Tommasini & R. Pertusio

*Department of Electrical Engineering – Polytechnic of Turin, Italy*

**ABSTRACT:** The dangers of personnel in high voltage stations can be very elevated, so the sharp evaluation of the resistance to ground of human body ( $R_{EB}$ ) is very useful to establish and improve the safety levels and the plan interventions. The ground resistance of the body  $R_{EB}$  is the resistance that the current finds when it leaves the human feet for going into the earth; it depends both on the resistivities of the soils and on the thickness of the insulating layer. The aim of this work is to propose new simplified formulas for the calculation of the ground resistance of plate electrodes placed on two-stratus soil, since feet can be assimilated to plates to evaluate the step voltage and the touch voltage, to which the subject can be submitted in the case of a fault in HV systems. The research have been carried out with numerical methods; the results have been compared with semi empirical equations and with experimental tests.

### 1 INTRODUCTION

Purpose of this investigation is the evaluation of the resistance to ground of plate electrodes placed on two-stratus soil. The study of two-stratus soil, in which the superficial layer has a higher resistivity than the lower ground, has a significant practical importance, because one of the usual methods to reduce touch voltage and step voltage (Figs. 1 and 3) just consists in insulating the soil by means of a high resistance layer.

The utilisation of plate electrodes, placed on the soil to simulate the feet, allows to make experimental measures in situ to establish the respect of the safety limits of the electrical system. The figures 2 and 4 show the circuitual plans reported in the CENELEC Standard HD 637 S1 [2] to measure the touch voltage and the step voltage.

Using the Finite Elements Method, with the commercial software Ansys, and the Resistance Grid Method [6], developed and applied by the authors for this specific problem, the influence of the characteristic parameters of the phenomenon has been studied.

The experimental measures on various typologies of soils and materials used in building have been made in the laboratory of Department of Electrical Engineering of Polytechnic of Turin on a scale model, in order to compare with the results of the numerical simulations.

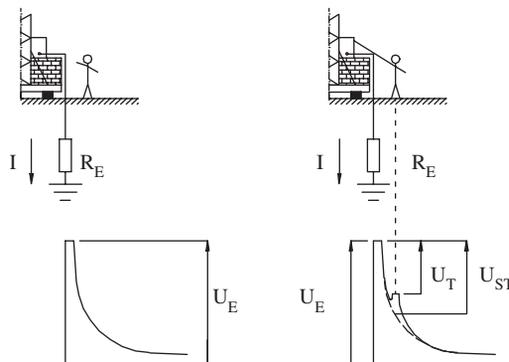


Figure 1. Touch voltage.

### 2 VOLTAGE SAFETY LIMITS

The human body is very sensitive to the electric current; the most dangerous risk is the ventricular fibrillation that can cause death. In the graphic time/current (Fig. 5) the safety limits for the alternating current effects (15 Hz–100 Hz) on the body are proposed.

The effects of current passing through the human body depend both on the flowing time and on the current intensity: the longer the flowing time the lower the admissible current.

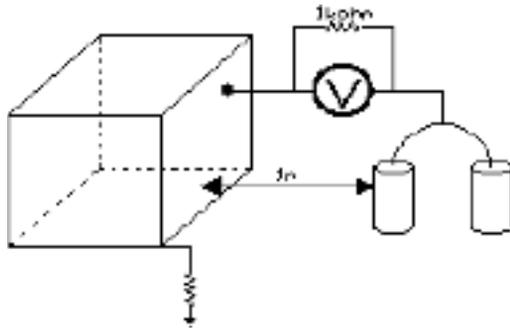


Figure 2. Circuital plan for touch voltage measure.

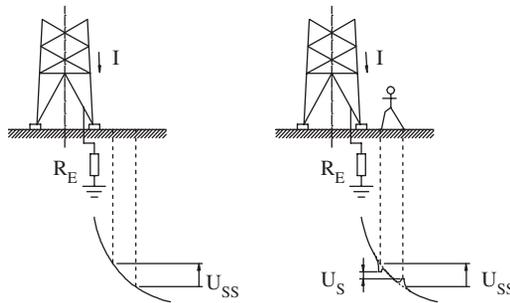


Figure 3. Step voltage.

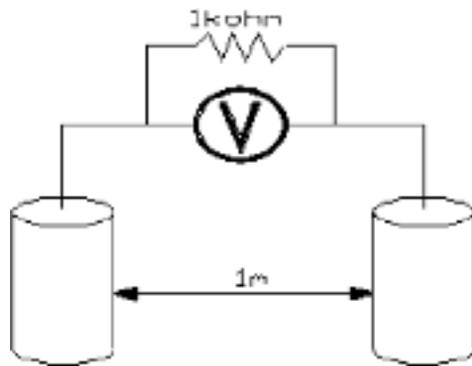


Figure 4. Circuital plan for step voltage measure.

To establish the safety level in the electric plans, the useful parameters are the voltage that the person can be subjected to and the time. In accordance with the Ohm law, the current flowing through the body and the applied voltage are correlated by the body resistance  $R$ , that is not constant but depends on the voltage. Knowing  $R_B(V)$  and  $I(t)$ , it is possible to obtain the graph  $V/t$ , where the voltage that the body can tolerate is function of the time of the fault duration  $t$  (Fig. 6).

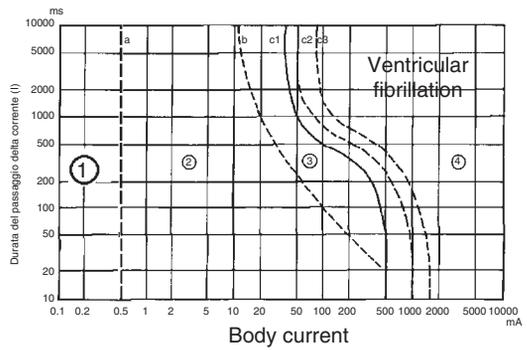


Figure 5. Safety limits  $I/t$  for alternating current 50 Hz.

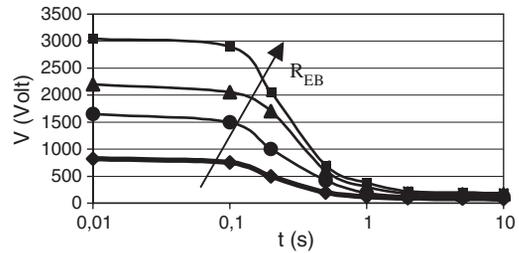


Figure 6. Safety limits  $V/t$  for alternating current 50 Hz, increasing the resistance to ground.

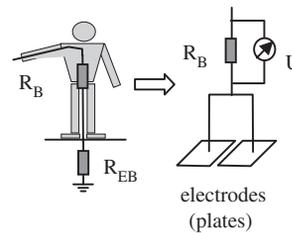


Figure 7. Resistance of the body and resistance to ground.

Usually in HV systems, the fault current intensity  $I_g$  and the disconnecting time of the fault protection  $t$  are defined; besides the resistance of the grounding plan  $R_E$  can be measured, so the voltage which the body can be subjected to is  $V = I_g \cdot R_E$  (Figs. 1 and 3). In several cases, it is very difficult or impossible to respect the safety levels of figure 6. To reach the safety, it is necessary to increase the resistance to ground  $R_{EB}$  that, being in series with the  $R_B(V)$  of the body (Fig. 7), raises the voltage safety level (Fig. 6).

Knowing the duration of fault  $t$ , it is possible to calculate the necessary value of  $R_{EB}$  ( $V = (R_B(V) + R_{EB}) \cdot I(t)_{admissible} \rightarrow R_{EB} = (V - R_B(V) \cdot I_{admissible}) / I(t)_{admissible}$ ). In this work, new formulas to obtain  $R_{EB}$

Table 1. Resistivity of some materials (electrode pressed with a strength of 250 N).

Material	$\rho$ ( $\Omega \cdot \text{m}$ )
Asphalt	100000
Compost (dry)	55–140
Concrete tiles (dry: relative Humidity 0.5%)	12000
Concrete tiles (wet: relative Humidity 3%)	150
Stone – small blocks fixed with sand (dry)	1200–1300
Stone – small blocks fixed with sand (wet)	900

are proposed; the problem is to determine the resistivities of the soils and the thickness of the insulating layer. Since the resistivities of the most common insulating soils have been already investigated [6] (Tab. 1), the relationships allow, chosen a specific insulating layer, to establish the necessary thickness of the superficial one.

### 3 PARAMETRIC STUDY

In order to comprehend the phenomenon, a lot of numerical simulations have been made with FEM method and with the Resistance Grid Method [6], changing the plate side  $L_p$  between 10 and 25 cm and the thickness of the insulating layer  $H$  between 1 and 50 cm, in particular studying the values between 5 e and 20 cm, of higher practical interest.

The value of the ratio  $\rho_1/\rho_2$  changes between 1, case of homogeneous soil, and 1000.

The simulations have allowed to study the influence on resistance to ground of these parameters:

- plate side  $L_p$
- thickness of the insulating layer  $H$  ( $\rho_1$ )
- ratio  $\rho_1/\rho_2$  of the two layers
- ratio  $L_p/H$

To understand how these parameters influence between themselves and how they intervene on the phenomenon, it is important to analyse the spatial form of the electric field around the plate electrode.

A few images of voltage isosurfaces for the cases of higher interest have been reported in the following.

#### 3.1 Parameter $\rho_1/\rho_2$

In the figures 8–10, the ratio  $L_p/H$  is constant, while the parameter  $\rho_1/\rho_2$  changes:

- $\rho_1/\rho_2 = 0.01$  (Fig. 8);
- $\rho_1/\rho_2 = 1$ , homogeneous soil (Fig. 9);
- $\rho_1/\rho_2 = 100$  (Fig. 10).

#### 3.2 Parameter $L_p/H$

Once fixed the value of the ratio  $\rho_1/\rho_2$ , the voltage distribution around the plate electrode depends upon the ratio  $L_p/H$  only.

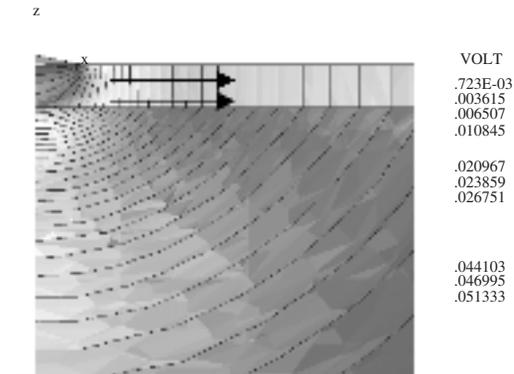


Figure 8. Voltage isosurfaces,  $\rho_1/\rho_2 = 0.01$ .

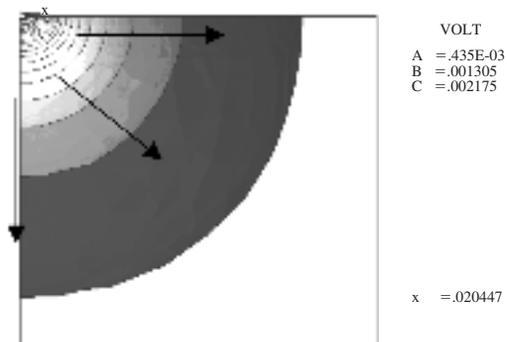


Figure 9. Voltage isosurfaces,  $\rho_1/\rho_2 = 1$ .

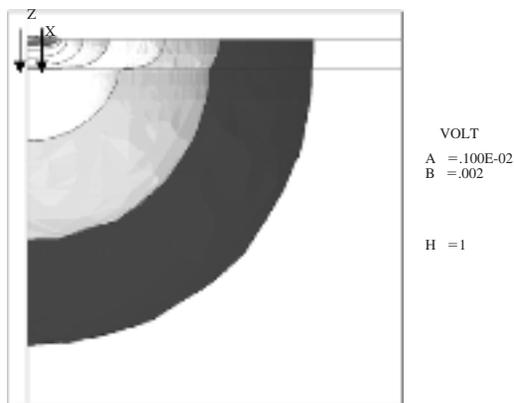


Figure 10. Voltage isosurfaces,  $\rho_1/\rho_2 = 100$ .

For instance, in figures 11 and 12, the images of voltage isosurfaces have been showed for two cases, where the ratio  $\rho_1/\rho_2$  is constant and equal to 1000.

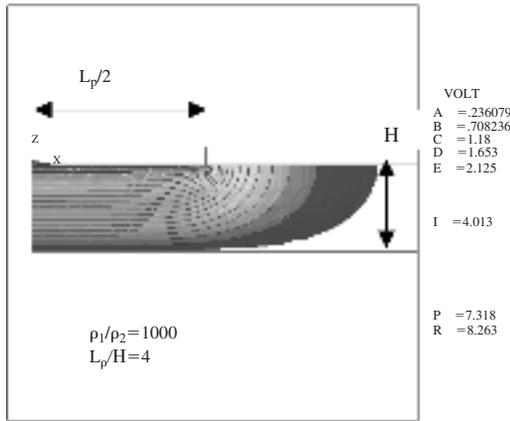


Figure 11. Voltage isosurfaces,  $L_p/H = 4$ .

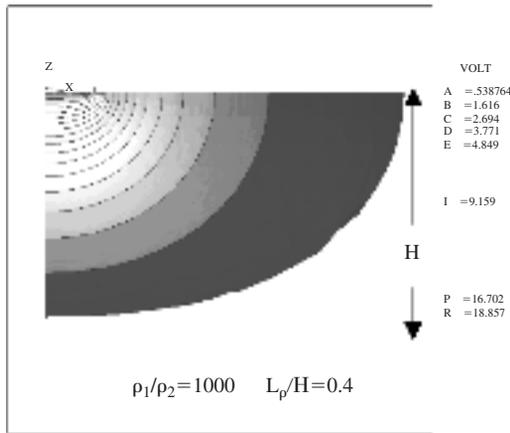


Figure 12. Voltage isosurfaces,  $L_p/H = 0.4$ .

In the first case (Fig. 11), the ratio  $L_p/H$  is high, so that the plate side  $L_p$  is very greater than the thickness  $H$ , consequently the voltage isosurfaces tend to become parallel to the plate, except for the boundary zones, and the current tends to run through the insulating layer vertically.

If the ratio  $L_p/H$  is low, so that the thickness is greater than  $L_p$ , the voltage isosurfaces will tend to become hemispherical, as the case of homogeneous soil (Fig. 9). Now the current shares itself uniformly through all directions (Fig. 12).

#### 4 GENERAL RELATIONSHIP

The proposed equation is based on the trend of two characteristic parameters:  $\rho_1/\rho_2$  and  $L_p/H$ .

The adimensional ratio, named adimensional resistance:

$$R_{\text{adimensional}} = \frac{R \cdot L_p}{\rho_2} = \text{const} \left( \frac{\rho_1}{\rho_2}; \frac{L_p}{H} \right)$$

gives a value only depending on the ratio between the two resistivities  $\rho_1/\rho_2$  and on the ratio between the square electrode  $L_p$  and the thickness of the superficial layer  $H$ , because these parameters establish in a univocal way the voltage conformation and consequently the current flow inside the ground and the corresponding met resistance.

Fixed the two parameters, the value of the adimensional resistance is constant and invariant.

#### 4.1 Homogeneous soil

The case of plate electrode placed on homogeneous soil has been studied to validate the numerical results with analytical treatments. The adimensional resistance has a constant value, approximately 0.44, because the parameters are meaningless or it is possible to consider them fixed ( $\rho_1/\rho_2 = 1, L_p/H = \infty$ ).

The relationship of  $R$  for homogeneous soil is:

$$R = 0.44 \cdot \frac{\rho_{\text{homogeneous}}}{L_{\text{plate}}} \tag{1}$$

The numerical results for the square plate coincide with the analytical data reported in [3] and [4] for the circular plates, because the electrode area, not its specific shape, influences the resistance [12].

#### 4.2 Two-stratus soil

For the two-stratus soil, the adimensional resistance changes between the case of homogeneous soil of resistivity  $\rho_{\text{homogeneous}} = \rho_1$  for  $H \rightarrow \infty (L_p/H = 0)$  and  $\rho_{\text{homogeneous}} = \rho_2$  for  $H \rightarrow 0 (L_p/H = \infty)$ ; for example, for a constant ratio of  $\rho_1/\rho_2$  equal to 1000, the adimensional resistance changes between 440 ( $H \rightarrow \infty$ ) and 0.44 ( $H \rightarrow 0$ ). The trends of  $(R \cdot L_p)/\rho_2$ , increasing the ratio  $\rho_1/\rho_2$  for a fixed ratio  $L_p/H$ , are linear, with an intersection point for the case of homogeneous soil (Fig. 13).  $(R \cdot L_p)/\rho_2$  depends upon two parameters:  $L_p/H$  and  $\rho_1/\rho_2$ .

$(R \cdot L_p)/\rho_2 (L_p/H, \rho_1/\rho_2)$  has to be a function continuous, derivable and increasing for any  $\rho_1/\rho_2$ .

$H = \infty$  represents the case of homogeneous soil with  $\rho_{\text{hom}} = \rho_1$ , so  $(R \cdot L_p)/\rho_2 (0, \rho_1/\rho_2)$  is a straight line of equation  $(R \cdot L_p)/\rho_1 = k \rightarrow (R \cdot L_p)/\rho_2 = k \cdot \rho_1/\rho_2$ , for any  $\rho_1/\rho_2$ .  $H = 0$  is the case of homogeneous soil with  $\rho_{\text{hom}} = \rho_2$ , so  $(R \cdot L_p)/\rho_2 (\infty, \rho_1/\rho_2)$  takes a constant value  $k = 0.44$ .

Consequently it is possible to find an analytical equation for a bundle of straight lines passing through

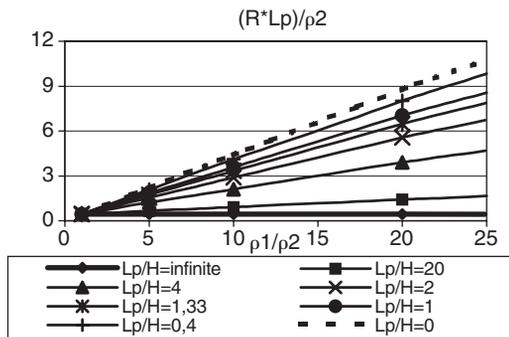


Figure 13. Trend of  $(R \cdot L_p)/\rho_2$  increasing  $\rho_1/\rho_2$ .

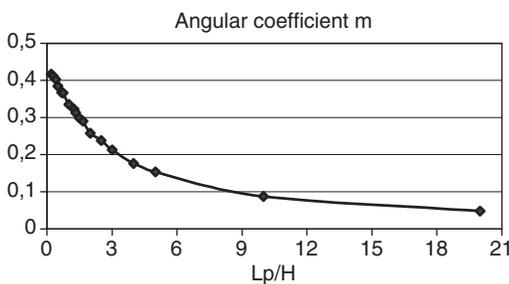


Figure 14. Trend of  $m$  increasing  $L_p/H$ .

the point  $q$ , with the angular coefficient  $m$  function of the ratio  $L_p/H$ .

$$\frac{R \cdot L_p}{\rho_2} = m \cdot \left( \frac{\rho_1}{\rho_2} - 1 \right) + q$$

It is useful to do a translation of the reference system of figure 13, taking the new origin into the point  $(1; 0.44)$ , so it is possible to give the value of  $(R \cdot L_p/\rho_2)$ , got for the homogeneous soil, the term  $q$ . In figure 14, the trend of  $m$ , changing the parameter  $L_p/H$  between 0.2 and 20, is shown;  $m$  varies between 0 and 0.44.

For  $L_p/H < 0.2$ , so that the case where the thickness of the insulating layer  $H$  is at least five times the plate side  $L_p$ , it is possible to refer to the homogeneous case, with a corrective coefficient between the values  $0.9 \div 1$ .

The resistance becomes:

$$R \approx (0.9 \div 1) \cdot \left[ 0.44 \cdot \frac{\rho_1}{L_p} \right] \approx (0.9 \div 1) \cdot \left[ 0.44 \cdot \frac{\rho_{\text{homogeneous}}}{L_p} \right]$$

For  $L_p/H > 20$ , the voltage isosurfaces are parallel to the plate, creating a flux pipe for the current. The study of the current distribution around the plate with

FEM models has shown that, also for superficial layers very resistive, it is necessary that the ratio  $L_p/H$  is very high, so that the boundary perturbations have a little influence and the current is forced to follow the vertical direction, during the travel through the insulating layer.

For  $L_p/H = 20$  and  $\rho_1/\rho_2 = 10$ , the 90% of the current flows into the resistive stratus vertically under the plate. Then the total resistance can be calculated as addition of the resistance given by the insulating layer and the resistance of the II stratus, similar to the case of plate on homogeneous soil.

$$R \approx (0.95 \div 1) \cdot \rho_1 \cdot \frac{H}{S_{\text{plate}}} + 0.44 \cdot \frac{\rho_2}{L_p}$$

For  $0.2 < L_p/H < 20$ , a single accurate equation for the angular coefficient  $m$  does not exist, so two simple relationships are proposed, for  $0.2 < L_p/H < 4$  and  $4 < L_p/H < 20$ .

For  $0.2 < L_p/H < 4$ ,  $m = 0.43 \cdot e^{-0.23 \cdot \frac{L_p}{H}}$ , then

$$R \approx \left( \frac{0.43 \cdot e^{-0.23 \cdot \frac{L_p}{H}}}{L_p} \right) \cdot (\rho_1 - \rho_2) + \left( 0.44 \cdot \frac{\rho_2}{L_p} \right)$$

For  $4 < L_p/H < 20$ ,  $m = 0.56 \cdot \left( \frac{L_p}{H} \right)^{-0.8}$ , then

$$R \approx \left( \frac{0.56 \cdot \left( \frac{L_p}{H} \right)^{-0.8}}{L_p} \right) \cdot (\rho_1 - \rho_2) + \left( 0.44 \cdot \frac{\rho_2}{L_p} \right)$$

### 5 MUTUAL RESISTANCE

The standard HD 637 indicates the value of 400 cm<sup>2</sup> as total feet area. In figure 15, the increase of  $R_{EB}$ , decreasing the distance between the feet, is shown [7]. For  $H = 100$  cm, the 2 electrodes, of area 200 cm<sup>2</sup>, are completely electrical independent. For the two-stratus soil, with  $\rho_1/\rho_2 = 10$ , already at 20 cm, the trend can be considered electrical independent, since the mutual interference is negligible. The higher volt-age gradient around the plate of two-stratus soil than the homogeneous soil causes this very low mutual interference.

### 6 $R_{EB}$ RELATIONSHIP

To evaluate  $R_{EB}$ , a plate of dimension 200 cm<sup>2</sup> simulates one foot; so  $L_p$  is constant and equal to 0.14 m.

In this case, the equations become:

- For  $70 \text{ cm} < H < \infty$ ,  $R_{\text{FOOT}}$  is:

$$R_{\text{FOOT}} \approx (0.9 \div 1) \cdot 3.1 \cdot \rho_1. \tag{2}$$

- For  $3.5 \text{ cm} < H < 70 \text{ cm}$ ,  $m \approx 0.43 \cdot e^{(-0.0325/H)}$  then  $R_{\text{FOOT}}$  is:

$$R_{\text{FOOT}} \approx \left( 3 \cdot e^{\frac{-0.0325}{H}} \right) \cdot (\rho_1 - \rho_2) + 3.1 \cdot \rho_2 \tag{3}$$

- For  $0.7 \text{ cm} < H < 3.5 \text{ cm}$ ,  $m \approx 0.56 \cdot (0.14/H)^{-0.8}$  then  $R_{\text{FOOT}}$  is:

$$R_{\text{FOOT}} \approx (19 \cdot H^{0.8}) \cdot (\rho_1 - \rho_2) + 3.1 \cdot \rho_2 \tag{4}$$

- For  $0 < H < 0.7 \text{ cm}$ , the simplified formula of  $R_{\text{FOOT}}$  is:

$$R_{\text{FOOT}} \approx (0.9 \div 1) \cdot \left( \frac{H}{0.02} \right) \cdot (\rho_1) + 3.1 \cdot \rho_2 \tag{5}$$

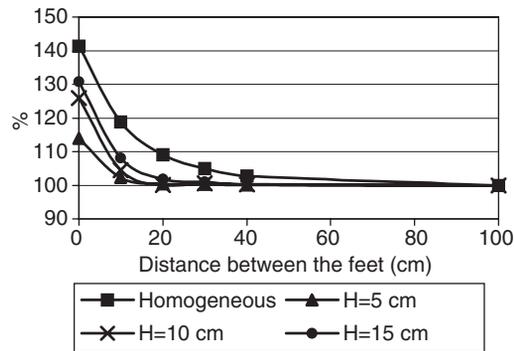


Figure 15. Trend of R, decreasing the distance between feet.

Table 2.

H(m)	r1(Vm)	r2(Vm)	(3)	(4)	(6a)	(6b)	(6c)
0,25	2000	222	2686	*	2771	2639	2701
0,2	2000	222	2611	*	2673	2543	2614
0,15	2000	222	2491,5	*	2521	2399,7	2483
0,1	2000	222	2271	*	2264	2162,6	2263
0,08	15000	222	15110,5	*	14393	14236	15125
0,05	2000	222	1736,4	*	1729	1695,5	1809
0,03	1200	100	*	787	746	778	844
0,02	15000	222	*	6484	5675	6673	7452
0,01	1500	60	*	437	364	451	503

Because the feet are electrical independent between each other, for the touch voltage,  $R_{\text{EB}} = R_{\text{FOOT}}/2$ , being the feet in parallel; instead for the step voltage,  $R_{\text{EB}} = 2 \cdot R_{\text{FOOT}}$ , since the feet are in series.

### 7 COMPARISON WITH Std80 DATA

In Std80-96 and in Std80-2000, there is this formula for calculating  $R_{\text{EB}}$ .

$$R_{\text{FOOT}} = \left[ \frac{\rho_1}{4 \cdot b} \right] \cdot C_s \tag{6}$$

with  $b = 0.08 \text{ m}$ . ( $b =$  radius of circular plate of area  $200 \text{ cm}^2$ ).  $C_s$  is the surface layer derating factor.

In the Standards there are few formulas for  $C_s$ :

$$C_s = \left( \frac{1+k}{1-k} \right) - \left( \frac{4k}{\pi \cdot (1-k)} \right) \cdot \tan^{-1} \left( \frac{2 \cdot H}{b} \right) - 0.21 \cdot k^2 \left[ e^{-7H} - e^{-30H} \right] \tag{6a}$$

with  $k = (\rho_2 - \rho_1) / (\rho_2 + \rho_1)$  between 0 and  $-0.98$  and  $0 \text{ cm} < H < 30 \text{ cm}$ .

$$C_s = 1 - a \cdot \left( 1 - \frac{\rho_2}{\rho_1} \right) / (2H + a) \tag{6b}$$

with  $a = 0.106$ . This equation is more accurate than equation 6a for very thin surface layers between  $0.005 \text{ m}$  and  $0.02 \text{ m}$ .

$$C_s = 1 - a \cdot \left( 1 - \frac{\rho_2}{\rho_1} \right) / (2H + a) \tag{6c}$$

with  $a = 0.09$  and  $5 \text{ cm} < H < 30 \text{ cm}$ .

The equations 6b and 6c are only valid for  $b = 0.08 \text{ m}$ . In table 2, the results of the different equations have been compared, considering  $R_{\text{EB}} = R_{\text{FOOT}}/2$ .

A very good agreement between the formulas has been found.

## 8 EXPERIMENTAL MEASURES

Experimental tests in laboratory have been carried out with a scale model ( $120 \times 120 \times 10$  cm) to measure the resistance of plate placed on homogeneous soil and on two-stratus soil (Fig. 16).

Successively a few experimental results have been reported and compared with the values calculated using the relations previously exposed. In table 3, the experimental data have been compared with the results of relationship 3.

The analytical results show a correspondence with the experimental measures. For the sand, being an incoherent material, the resistivity, depending strongly by the pressure, changes in the zones under the plate and around, modifying the electric field: Grid Models, made considering this variation, have shown an increase of R of 10–20%. For the blocks stone, it is very difficult to realize a perfect and homogeneous contact between the plate and the insulating surface, so the real area of contact is less than the plate area and the R tends to increase.

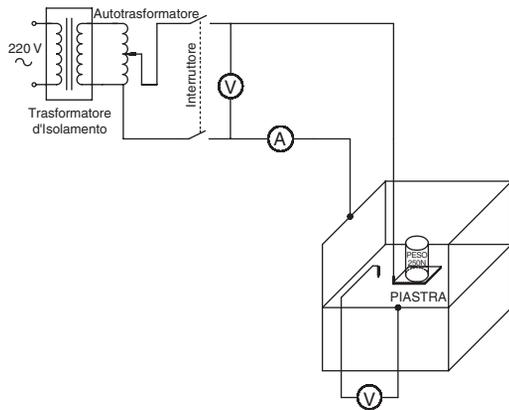


Figure 16. Scale model and circuit apparatus.

Table 3.

Cases	Lp:0.18 m		Experimental data	Data (3)	%	
SAND	H:0.05 m	$\rho_1:150 \Omega\text{m},$	$\rho_2:18.53 \Omega\text{m}$	240 $\Omega$	182.5 $\Omega$	31,51
SAND	H:0.1 m	$\rho_1:150 \Omega\text{m},$	$\rho_2:16.38 \Omega\text{m}$	320 $\Omega$	251 $\Omega$	27,49
SAND	H:0.05 m	$\rho_1:1640.5 \Omega\text{m}$	$\rho_2:57.3 \Omega\text{m}$	2280 $\Omega$	1792.5 $\Omega$	27,20
BLOCKS STONE	H:0.05 m	$\rho_1:1297.24 \Omega\text{m}$	$\rho_2:56.53 \Omega\text{m}$	1850 $\Omega$	1433 $\Omega$	29,10
BLOCKS STONE	H:0.1 m	$\rho_1:1313.1 \Omega\text{m}$	$\rho_2:50.8 \Omega\text{m}$	2660 $\Omega$	2117.5 $\Omega$	25,62
BLOCKS STONE	H:0.1 m	$\rho_1:1218.34 \Omega\text{m}$	$\rho_2:50.8 \Omega\text{m}$	2500 $\Omega$	1968 $\Omega$	27,03
BLOCKS STONE	H:0.1 m	$\rho_1:900 \Omega\text{m}$	$\rho_2:50.8 \Omega\text{m}$	1720 $\Omega$	1465 $\Omega$	17,41

## 9 CONCLUSION

The research has permitted to work out with easier and more general relationships for the evaluation of the resistance to ground of plate electrodes on two-stratus soils. For the two-stratus soil, a study of the electric field around the square electrode has been carried out, so the influence of the parameters  $L_p/H$  and  $\rho_1/\rho_2$  on the current flow inside the ground has been made clear.

For two-stratus soils with the superficial layer more resistive than the lower round, three specific trends have been found, depending by the ratio  $L_p/H$ .

For values of  $L_p/H$  high ( $>20$ ), a simplified model can be studied where all the current flows vertically under the plate electrode through the insulating layer and then spread itself homogeneously in the second layer.

For  $L_p/H$  less than 0.2 the global trend is similar to the case of homogeneous soil, because the superficial stratus influences strongly the phenomenon.

For the intermediate values of  $L_p/H$  ( $0.2 \leq L_p/H \leq 20$ ), two simple relationships have been proposed to value R.

In particular, for the calculation of  $R_{EB}$ , since one foot is modelled as a plate of area  $200 \text{ cm}^2$ ,  $L_p$  is about 0.14 m and  $R_{FOOT}$  is:

- For  $3.5 \text{ cm} < H < 70 \text{ cm}$ :

$$R_{FOOT} \approx \left( 3 \cdot e^{-\frac{0.0325}{H}} \right) \cdot (\rho_1 - \rho_2) + 3.1 \cdot \rho_2 \quad (7)$$

- For  $0.7 \text{ cm} < H < 3.5 \text{ cm}$ :

$$R_{FOOT} \approx (19 \cdot H^{0.8}) \cdot (\rho_1 - \rho_2) + 3.1 \cdot \rho_2 \quad (8)$$

with H in m,  $\rho_1$  and  $\rho_2$  in  $\Omega\text{m}$ .

In equation 1, when  $\rho_1 \gg \rho_2$  ( $\rho_1 > 10\rho_2$ ), it is possible to consider instead of  $(\rho_1 - \rho_2)$  only  $\rho_1$  and to neglect the right term.

For the touch voltage,  $R_{EB} = R_{FOOT}/2$ , being the feet in parallel; instead for the step voltage,  $R_{EB} = 2 \cdot R_{FOOT}$ , since the feet are in series.

These equations have been validated with other relationships and with experimental measures.

## REFERENCES

- [1] IEEE Std 80-2000, IEEE Guide for Safety in AC Substation Grounding.
- [2] CENELEC Standard HD 637 S1, 1998-12.
- [3] H.B. Dwight, *Calculation of resistances to Ground*, "Electrical Engineering", December 1936.
- [4] F. Ollendorf, Erdströme, J. Springer, 1928.
- [5] G.F. Tagg, *Earth Resistances*, George Newnes Limited, London, 1964.
- [6] R. Tommasini and R. Pertusio, *Resistance to ground of human body in non homogeneous soil*, IASTED Power and energy systems, Marina del Rey, 13-15 May 2002, 225-229.
- [7] C.H Lee and A.P. Sakis Meliopoulos, *Comparison of touch and step voltages between IEEE Std 80 and IEC 479-1*, IEE Proc-Gener. Transm. Distrib., 146 (5), 1999, 593-601.
- [8] J.G. Sverak, *Progress in step and touch voltage equations of ANSI/IEE Std8-Historical Perspective*, IEEE Transactions on power delivery, 13 (3), 1998, 762-767.
- [9] B. Thapar, V. Gerez and H. Kejriwal, *Reduction factor for the ground resistance of the foot in substation yards*, IEEE Transactions on power delivery, 9 (1), 1994, 360-368.
- [10] B. Thapar, V. Gerez and P. Emmanuel, *Ground resistance of the foot in substation yards*, IEEE Transactions on power delivery, 8 (1), 1994, 1-6.
- [11] B. Thapar, V. Gerez and V. Singh, *Effective ground resistance of the human feet in high voltage switchyards*, IEEE Transactions on power delivery, 8 (1), 1993, 7-12.
- [12] E.K.N. Yung, R.S.K. Wong and W.W.S. Lee, *Analysis of a rectangular earthing plate*, IEE Proceedings-C, 140 (5), 1993, 381-388.
- [13] B. Thapar, V. Gerez, A. Balakrishnan and A. Blank, *Finite expression and models for footing resistance in substations*, IEEE Transactions on power delivery, 7 (1), 1992, 219-224.

# A Safety Program Framework and its application on a Weapon Control System

Arild Tomter

*Kongsberg Defence & Aerospace AS, Kongsberg, Norway*

**ABSTRACT:** This paper presents a real-life Safety Program Framework, which has been applied on some Weapon Control System projects at Kongsberg Defence & Aerospace. It starts with preparing the plan for the safety effort throughout the project and specifying the safety requirements (including hazard acceptance criteria). It continues with identifying potential hazards based on a checklist of energies present in or controlled by the system. The potential hazards are highlighted and brought to the attention of the design and construction team. Safety is considered an inherent property of the system to be developed, thus emphasizing the important role and responsibility of this team. The system resulting from the design and construction process is then subject to safety verification. Each residual hazard is evaluated with respect to hazard control measures, and resulting combination of hazard probability and severity (the risk assessment code) is assessed and compared with specified hazard acceptance criteria. The safety program concludes with a summary of the safety tasks conducted, including a final statement of the safety of the system.

## 1 INTRODUCTION

Weapon Systems are associated with serious or catastrophic damage potential. In fact, they are designed to cause such serious or catastrophic damage, however on enemy only. Hence, as opposed to systems for civilian use, removing or reducing the capability to cause damage is not a feasible approach for a safety effort. The safety challenge is instead to ensure that the damage capability is tightly controlled by a combination of design solutions, specific protective measures, strict procedures and adequate training of system operators.

Kongsberg Defence & Aerospace AS (KDA) designs Weapon Control Systems for Army, Navy and Air Force within Norway, other NATO countries, and certain other countries, restricted by Norwegian government regulations. As a manufacturer of such systems KDA emphasizes safety as an important part of the business policy. It is vital for KDA to implement adequate measures to prevent any serious accident to happen, as well as to create confidence in the safety of the systems within military agencies as well as the general society.

For each weapon control system project a safety program is tailored to the project characteristics. It follows, however, a general framework, which is based on guidelines in MIL-STD 882 D "Standard Practice for System Safety". This framework specifies a

number of phases, which cover the project phases from the initial project definition until final acceptance and system delivery.

## 2 FRAMEWORK OF THE SAFETY PROGRAM

The framework includes a total of 5 steps, which are described below.

### 2.1 *Plan the safety program, and determine safety requirements*

The safety program is prepared as part of the initial project planning. The safety program will include, in addition to a broad description of the system:

1. A first cut discussion of the damage capabilities and associated potential hazards.
2. A system for categorizing hazards with respect to probability and severity, the combinations of these constitute the risk assessment codes.
3. The safety philosophy employed as well as specific safety requirements. The safety requirements are defined as criteria for acceptance of risk assessment codes.
4. The safety organization, as part of the overall project organization.
5. Safety tasks to be conducted within the project.

The safety plan is documented in a System Safety Program Plan.

## 2.2 Identify and categorize potential hazards

Potential hazards associated with the system will be identified and categorized in the early design phase. In general, accidents and related damage levels are associated with uncontrolled release of some type of energy. Hence, the system is thoroughly evaluated with respect to amount of various types of energy residing in or controlled by the system. A standard checklist of types of energy is employed. (A first cut evaluation of potential hazards is included in the System Safety Program Plan.) Each hazard is closely assessed with respect to its severity and assigned to the appropriate hazard severity category.

The hazard identification and categorization is documented in the *Preliminary Hazard Analysis*. This document constitutes an important part of the design requirements, as the system design should assure that for each hazard, its probability level combined with its severity category (i.e. its risk assessment code) should be within the acceptance criteria specified in the System Safety Program Plan.

For complex systems composed of several significant subsystems (as for Air Defence Systems), the Preliminary Hazard Analysis may be split in one analysis for each subsystem.

## 2.3 Resolve all potential hazards, i.e. eliminate or reduce hazards to within acceptance criteria

Safety of a system is considered to be an inherent system property, and is built into the system as part of the system design process. The main function of a weapon control system is to control the firing of the weapon(s), i.e. to cause damage to the enemy. Hence, reducing the hazard potential by designing for reduced damage capability is no feasible approach. Instead, the design must basically rely on tight control of the firing procedure, i.e. high system reliability (especially for safety-critical functions), combined with presence of adequate safety barriers. The safety barriers shall deny any firing of weapon unless a number of very strictly defined conditions and criteria are true. The final design and construction shall fulfil the safety requirements, i.e. each hazard shall be associated with a risk assessment code residing within the acceptance criteria.

During the design process, specialized safety analyses may be conducted as deemed required. This may e.g. include Failure Mode Effect and Criticality Analysis (to determine top-level effects of component failures); Fault Tree Analysis (to determine all combinations of failures which may cause top-level mishaps); Sneak Circuit Analysis (to determine

presence of hidden design errors); etc. Such specialized safety analyses may be used especially for safety critical functions.

## 2.4 Verify acceptability of residual hazards

Upon completion of the design, each hazard identified in the Preliminary Hazard Analysis is re-evaluated with respect to its probability and severity resulting from the final design solution. Associated risk assessment codes are determined, and compared with the risk acceptance criteria. If a hazard resides outside the risk acceptance criteria, additional effort will be conducted for reducing the hazard probability and/or severity to within the acceptance criteria. The results from this analysis are documented in the *System Hazard Analysis*.

For complex systems composed of major subsystems, this verification task may be undertaken in two steps: each major subsystem is addressed in an associated *Sub-system Hazard Analysis*, leaving the *System Hazard Analysis* to cover system-level hazards only.

Safety tests are conducted in order to verify that all safety barriers implemented are truly effective. If firing is initiated when any one of the necessary predefined conditions and criteria is not true, the tests shall verify that firing is denied by the system. The results from these tests may be documented in a specific *Safety Test Report*, or may be incorporated in the reporting from the overall system test program.

The system operator is a critical element in the total system behaviour. Man is created fallible, and making errors is recognized as a basic human property. Hence, the system operator constitutes a fundamental safety risk, but may also act as an important safety barrier. The hazard potential associated with operator errors is analysed in the *Operator Hazard Analysis*. This analysis focuses on those operator tasks where an operator error has the capability to cause an accident, and therefore is a potential hazard. Each hazard is closely evaluated with respect to its probability and severity (i.e. risk assessment code), which is compared with the basic acceptance criteria. Hazards residing outside the acceptance criteria are subject to additional effort in order to reduce those hazards to within the acceptance criteria.

## 2.5 Summarize and conclude upon the safety of the system

The safety program concludes with the *Safety Assessment Report*. This is not a separate safety analysis, but rather a summary of the various safety tasks undertaken throughout the project. The results and conclusions from the safety effort are presented. The Safety Assessment Report concludes with a safety

statement, stating the evidences derived from the subordinate safety reports as well as the final conclusion regarding the safety of the system.

### 3 EXAMPLE: AN AIR DEFENCE SYSTEM

An Air Defence System consists basically of 3 major subsystems:

1. The Sensor (e.g. radar), which detects and tracks air targets and transmits target data to
2. The Fire Distribution Centre. This receives target data from the sensor, determines whether the target shall be engaged, calculates when and in which direction the missile(s) shall be fired, and transmits fire message to
3. The Missile Launcher (loaded with missile). The launcher receives the fire message from the Fire Distribution Centre, and fires the missile at prescribed time and direction.

The system is complex and consequences of a failure may be catastrophic.

Application of the safety program framework on an Air Defence System is presented below.

#### 3.1 Safety Program Planning (*The System Safety Program Plan*)

The System Safety Program Plan includes among others the following chapters:

- Energy levels involved with the system
- Hazard categorization and acceptance criteria, and
- Safety organization.

##### 3.1.1 Energy levels and associated damage capabilities

When discussing potential hazards it is easy to overlook potential, but not so obvious, hazards. In order to avoid this, a systematic approach based on a checklist of various types of energy is employed. The following energies were identified to be present: *Movement, Electricity, Explosives, Chemical, Heat, Radiation, Vibration and Noise*. Presence of each one of these energies is associated with a potential for uncontrolled release and associated damage. The safety effort focuses on establishing measures to assure adequate control of these energies and prevent any uncontrolled release.

##### 3.1.2 Hazard categorization and acceptance criteria

Hazards are categorized with respect to both their probabilities and severities in accordance with MIL-STD 882 D.

The following hazard probability levels are defined:

Table 1. Hazard probability levels.

A	Frequent	Likely to occur frequently
B	Probable	Will occur several times in the life of an item
C	Occasional	Likely to occur some time in the life of an item
D	Remote	Unlikely, but possible to occur in the life of an item
E	Improbable	So unlikely it can be assumed occurrence may not be experienced

The following hazard severity categories are defined:

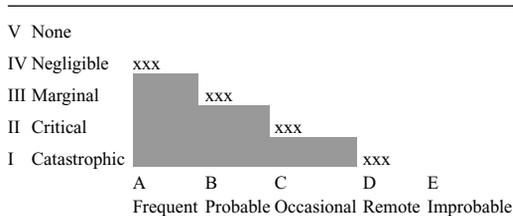
Table 2. Hazard severity categories.

I	Catastrophic	Death, system loss or severe environmental damage
II	Critical	Severe injury, severe occupational illness, major system or environmental damage
III	Marginal	Minor injury, minor occupational illness, minor system or environmental damage
IV	Negligible	Less than minor injury, occupational illness or less than minor system or environmental damage
V	None (not in MIL-STD 882)	Safety effected, but no expected injury, occupational illness or system or environmental damage

The combinations of hazard probability levels and severity categories constitute the risk assessment codes.

The following risk assessment codes acceptance criteria are defined:

Table 3. Risk assessment codes acceptance criteria.



Hazards with risk assessment codes residing within white boxes are determined to be acceptable, while hazards with risk assessment codes residing within shaded boxes are determined to be not

acceptable. Hazards with Risk Assessment Codes within boxes marked with xxx call for additional safety effort, in order to justify moving to a white box. If this does not succeed, the hazard shall be subject to special assessment and decision by the project manager.

### 3.1.3 Safety organization

Safety has to be designed into the system, making the design and construction team the most important actor in the safety creation process. The safety organization is characterized as follows:

1. The overall program responsibility rests with the Air Defence Manager, while the operational responsibility for the individual project, including its safety, is held by the project manager.
2. The project manager is supported by a named Safety Manager.
3. The creation of safety is an important dimension of all project tasks. The design and construction team, acting as the key player in this process, assumes thus the major responsibility for complying with the safety requirements.
4. The explicit safety tasks (e.g. to prepare the System Safety Program Plan and conduct the various safety monitoring, evaluation and analysis tasks) are the responsibility of the Safety Manager.

### 3.2 Hazard identification and categorization (Preliminary Hazard Analysis)

This analysis is based on the "Energy levels and associated damage potentials" discussed in the System Safety Program Plan, and amplifies and concludes the findings to a set of distinct potential hazards. For the Air Defence System an analysis is prepared individually for each of the subsystems (Radar, FDC and Launcher).

Each potential hazard is discussed and evaluated with respect to its potential consequences and associated severity. The evaluations are presented in separate work sheets. An extract of a work sheet for the Fire Distribution Centre subsystem, including 3 potential hazards, is shown below (table 4).

Note that the hazards are not evaluated with respect to their probability levels at this stage. Probability levels are closely related to the associated design solutions, which remains to be developed at this stage of the program. Instead, it is an important design requirement to justify that, for each residual hazard, the combination of probability and severity is within the acceptance criteria.

### 3.3 Hazard resolution

The Preliminary Hazard Analysis is provided to the design and construction team. Their responsibility is to design and implement measures as required for each hazard to be associated with a final combination of hazard severity and probability (risk assessment code) residing within the acceptance limit. This may be undertaken by measures to reduce the severity of the potential effect of the hazard (e.g. to employ non-toxic ACU medium) and/or to reduce the probability of the hazard to a satisfactory level (e.g. to implement rigorous and formal criteria for a firing message to be accepted as valid by the system).

The final safety associated with the system is integrated in the design and construction, and relies entirely on the design and construction team. The safety program is designed in order to support this process and to verify the level of safety as resulting from this process.

Within the Air Defence System it was deemed appropriate to address the firing procedure within the Fire Distribution Centre on a more detailed level, and

Table 4. Extract from the Preliminary Hazard Analysis for the Fire Distribution Centre subsystem.

No.	Component	Hazard	Possible cause	Potential effect	Severity	Remarks/recommendations
1	General	Fire	-Short-circuit -Ember from cigarette	-Burn injury on personnel -Personnel toxicated from smoke -Equipment damaged	I I II	-Mount fire extinguisher -Avoid use of substances which are flammable or generate toxic smoke in fire -Enforce no smoking in FDC
2	Air Conditioning Unit (ACU)	ACU medium penetrates into shelter	ACU medium leaks into air system	-Personnel toxicated by ACU medium	I	-Use non-toxic medium -Prevent leakage of ACU medium by relevant measures
3	Operator console	Valid fire message generated inadvertently	SW or HW malfunction	Missile launched inadvertently	I	-Employ rigorous criteria for fire message procedure and validity -Conduct formal SW and HW reviews

a quantitative Fault Tree Analysis was conducted. The top event was defined as “Inadvertent transmission of Firing Command”. The firing procedure was modelled as a Fault Tree, and calculation of the probability of the top event to occur within the systems life time was calculated, based on failure rates for each basic event. The results provided evidence that the probability was well below the quantitative value, which corresponds with the qualitative requirements specified in the System Safety Program Plan.

### 3.4 *Verification of residual hazard acceptability (The System/Sub-system Hazard Analysis)*

The System Hazard Analysis is a re-evaluation of the potential hazards included in the Preliminary Hazard Analysis, as well as additional hazards, which are identified during the design and construction phase. This analysis addresses the hazard severities resulting from the measures incorporated in the system design, as well as the associated hazard probability levels. These combinations constitute the risk assessment codes, which for each hazard is matched against the hazard acceptance criteria specified in the System Safety Program Plan. The evaluations are presented in separate work sheets, much similar to the Preliminary Hazard Analysis work sheets.

Within the Air Defence System, this analysis was conducted on two levels: one Sub-system Hazard

Analysis for each of the three basic subsystems (Radar, Fire Distribution Centre and Launcher), and a System Hazard Analysis analysing from a birds view the top-level hazards associated with the overall system as a whole.

An extract of the Sub-system Hazard Analysis work sheets for the Fire distribution centre is presented in the table below (table 5). It includes the same three hazards as presented in the Preliminary Hazard Analysis work sheet (table 4).

The combination of hazard probability and severity (risk assessment code) for each hazard is compared with the hazard acceptance criteria specified in the System Safety Program Plan. In the example work sheet above, the risk assessment codes associated with all three hazards turn out to be within the hazard acceptance criteria.

The system-level System Hazard Analysis is prepared correspondingly, including identical work sheet formats, and the resulting risk assessment codes are assessed following the same procedure.

### 3.5 *Safety summary and conclusion (The Safety Assessment Report)*

The Safety Assessment Report comprises a final assessment of the safety of the system. It goes through the various safety tasks conducted as part of the safety

Table 5. Extract from the Sub-system Hazard Analysis.

No.	Component	Hazard	Hazard control measures	Potential effect	Probability	Severity
1	General	Fire	<ul style="list-style-type: none"> <li>–The FDC compartment complies with fire resistance requirements consistent with MIL-STD 9070B, paragraph 5.3.1.</li> <li>–No substance, which is highly flammable or generates toxic gases in a fire, is used.</li> <li>–Smoking is prohibited within the FDC compartment.</li> <li>–Fire extinguisher is mounted inside the FDC compartment.</li> <li>–The FDC compartment interior is designed for easy evacuation in case of fire.</li> </ul>	<ul style="list-style-type: none"> <li>–Burn injury on personnel</li> <li>–Personnel exposed to smoke</li> <li>–Equipment damaged</li> </ul>	D	II
2	Air Conditioning Unit (ACU)	ACU medium penetrates into the FDC compartment	<ul style="list-style-type: none"> <li>–ACU medium circulates inside the ACU only, completely separated from the air system.</li> <li>–Non-toxic ACU medium employed (R134A).</li> </ul>	–Personnel exposed to ACU medium	D	V
3	Operator console	Valid fire message generated inadvertently	A detailed Fault Tree analysis was conducted. Probability determined to be within level E.	–Missile launched inadvertently	E	I

program, evaluates the findings from each task, and assesses their impact on the safety assessment.

The results support a final Safety Statement, which states that the safety of the system complies with the defined safety requirements. This statement concludes the Safety Assessment Report.

#### 4 CONCLUSION

This paper has presented a framework for a safety program, and how it has been employed on an Air Defence System at Kongsberg Defence & Aerospace

AS. We recognize the fact that such systems are associated with inherent catastrophic damage potential. The safety program framework has proved a useful approach in our struggle to be able to justify the statement that the system holds a safety level complying with our defined requirements, and to provide adequate evidence for establishing confidence in this statement.

It is the author's intention that the framework presented may provide some practical and useful real-life ideas of how the safety effort on such systems may be conducted.

## Cognitive analysis in human reliability: the case of a high-risk plant

M. Tucci, A. Bellucci, I. Cappelli & L. Giagnoni

*Dipartimento di Energetica "Sergio Stecco", Sezione Impianti e Tecnologie industriali,  
 Università degli Studi di Firenze, Italia*

**ABSTRACT:** In order to assess the possible risk and consequence of an initial event, the reliability of the production systems is studied through methodologies reassumed into the risk analysis; they take into account the technological process and, in general, the mechanical elements that constitute it. In other hand, they neglect the aspects that depend on the human factor and on its contribution to the reliability of the system. With this meaning, in order to integrate the common techniques of risk analysis, Human Reliability Analysis-HRA aims to assess the human factor. The search on the HRA, with the second-generation methodologies, developed cognitive models and man-machine interface models, which represent the behaviour of the operator and its interaction with the productive process. The present paper proposes an applicative case of HRA, where the cognitive model defined in CREAM is applied. The analysis allows to individualize the more hazardous procedures and the capacity of workers performing them.

### 1 INTRODUCTION

When the operator performance is a fundamental element of the production process, in particular, when a human error can give rise to an accident with severe consequences, it's necessary to consider the human performance for correctly evaluating the system reliability. Especially in high-risk industry, the Human Reliability Analysis-HRA assumes a relevant role, because in this case the accidents often result in serious injuries and fatalities.

The HRA is developed identifying contextual factors (Common Performance Conditions – Hollnagel & Marsden, P. 1996 – and Performance Shaping Factors – Swain & Guttman, H.B. 1983), classifying human error according to different schemes and, fundamentally, representing the human behaviour in the work context by models.

In particular, the second-generation methodology of HRA produced man-machine interface models (Kuo-Wei Su, et al. 2000, Cacciabue 1998) and cognitive models. These models are focused on describing the worker behaviour through cognitive functions, which represent logical-rational actions. In sequential cognitive models (Shen, S-H et al. 1996) the worker behaviour is represented by a closed and rigid step-by-step path going from one cognitive function to another. In cyclical cognitive models (Hollnagel & Marsden 1996) the worker logic is described like a loop through the different functions.

The HRA is relevant in order to find how to reduce the probabilities of human error (which occurs as a worker attempts to carry out a procedure) or procedural violation (which represents intentional act by workers to violate procedures). Especially, through the cognitive model and its cognitive functions, the analysis can point out procedural tasks which can be misunderstood or which need an excessive cognitive capacity.

This paper describes a human reliability analysis applied to a real case, that is, a chemical industry for the plastic materials production. Aim of the analysis is pointing out the lacks of organisational frame and, in particular, identifying the procedures that require a high cognitive ability or, in any way, ability superior to the operator's one.

In the opening of the analysis, through the risk assessment records (Hazard Operability Analysis, Fault Tree Analysis, What if Analysis) and through the Consequence Analysis jointed to each top event, the more dangerous procedures are identified and the cognitive functions needed to complete them are examined.

Among the numerous cognitive models, the authors adopted the cognitive model defined in CREAM (Hollnagel 1998) and they used it to identify:

- the work load required by the procedure;
- the cognitive capacity available in the man.

Concerning the work load, the cognitive model is used strictly as explained in CREAM; in the evaluation of the cognitive capacity the model is revised in

order to integrate worker interviews and attitudinal tests.

In the second part of this paper, the analysis goes into detail and the cognitive profile required by the procedure is compared with the available cognitive profile of worker, not only in its cumulative value, but also in each single task.

## 2 THE ANALYSIS OF THE CHEMICAL PLANT

### 2.1 The chemical plant

The analysed plant produces plastic materials and it is classified as high-risk industry because of the quantity and the type of materials in storage.

The main department produces ftalic anhydride; in fact, that is a raw material for all the other departments. Its properties determine the quality of the final products.

The ftalic anhydride goes into three departments (Fig. 1):

- D1: special plastic with peculiar chemical and physical properties;
- D2: main and derived synthetic resins;
- D3: general plastic materials.

The plant has redundancy of safety systems, but some accidents can happen: in particular overpressures can bring to opening of safety valves, causing leakage of flammable liquid or gas. Following the results of the analysis of similar facilities, the more common accidents generate explosions and fires.

Depending on the plant organization, the emergency condition is managed mainly basing on outside help: in fact, in case of accident the fire brigade is called immediately and it is entrusted with overcoming the situation. On account of that, for internal management of the plant the conduction procedures become important: only if the process is maintained in the correct conditions and if the procedures are rightly carried out, it is possible to avoid an external intervention. Because of that, the authors chose to deeply analyse

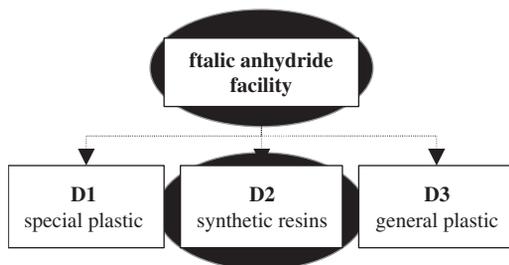


Figure 1. Production facilities of the high-risk plant.

the conduction procedures and to verify the operator capacity to correctly complete them.

### 2.2 The analysis phases

The analysis is modelled according to the real case and it is divided in two main phases: the first one is the preliminary phase, the second one is the operative phase (Fig. 2).

The preliminary phase started from analyzing safety report. Studying it, we got to know the risk analysis applied to the plant and, in particular, the outcomes derived from Fault Tree Analysis, HazOp Analysis and What if Analysis.

According to them, top events were identified together with their frequencies and their consequences; moreover, for each top event, we considered the related procedures, the affected workers, the quantity of persons involved in the area. On account of these records, it was possible to deduce which departments would be more interesting for applying the human reliability analysis, in this case, the ftalic anhydride facility and the D2.

The investigation continued in field and it let us confirm the choice of ftalic anhydride facility and the D2 where to carry out the analysis. In the visits to the plant, the investigation followed two parallel streams: one on the production-level and the other on the men-level. At the production-level, we examined the specific operative manuals (developed just for these departments) and the organisational chart. At the men-level, we met the operators working in these areas and we

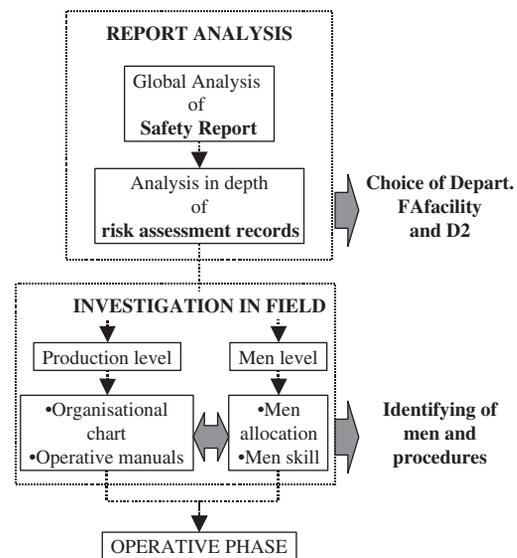


Figure 2. Analysis diagram flow.

identified the actual allocations and the actual skills of the workers. Furthermore, comparing the two levels we associated each procedure to the men that conduct it.

In general the procedures we individuated can be reassumed in:

- preliminary procedures;
- raw materials loading procedures;
- final products unloading procedures.

The men working in the same team are:

- the foreman (which coordinates the operation);
- the control-panel operator (which oversees the operation by means of a control interface);
- one or more operators (which work in the area and help foreman, following the instructions).

After the preliminary phase, we applied the operative phase, conforming to guidelines of CREAM in the use of its cognitive model.

Firstly, the Hierarchical Task Analysis-HTA was performed: HTA rereads and rewrites each procedure according to a time and logical hierarchical frame. In this way, procedures diagrams were built; these show

the temporal-space logic of the procedure which is performed.

In the present case, in the operative manuals the procedures are just organised in a time dependent logic and they involve more men; so the HTA was adapted to their frame and it was built in parallel for all workers that cooperate to the same procedure (Fig. 3).

Afterwards, the Cognitive Task Analysis-CTA was applied to the same procedures: for each task identified in HTA the activities functions, which are necessary to carry it out, were selected. The CTA was the result of the CREAM table that describes the cognitive activities and links them to the main cognitive functions. The main functions are four: observation, interpretation, planning, and execution. Following this table, for each procedure the total occurrence of the cognitive functions was calculated and this was synthesised by the cognitive profile.

In short, through these steps the Required Cognitive Profile-RCP was obtained and it represents the type of work-load that the man has to sustain to complete the procedure.

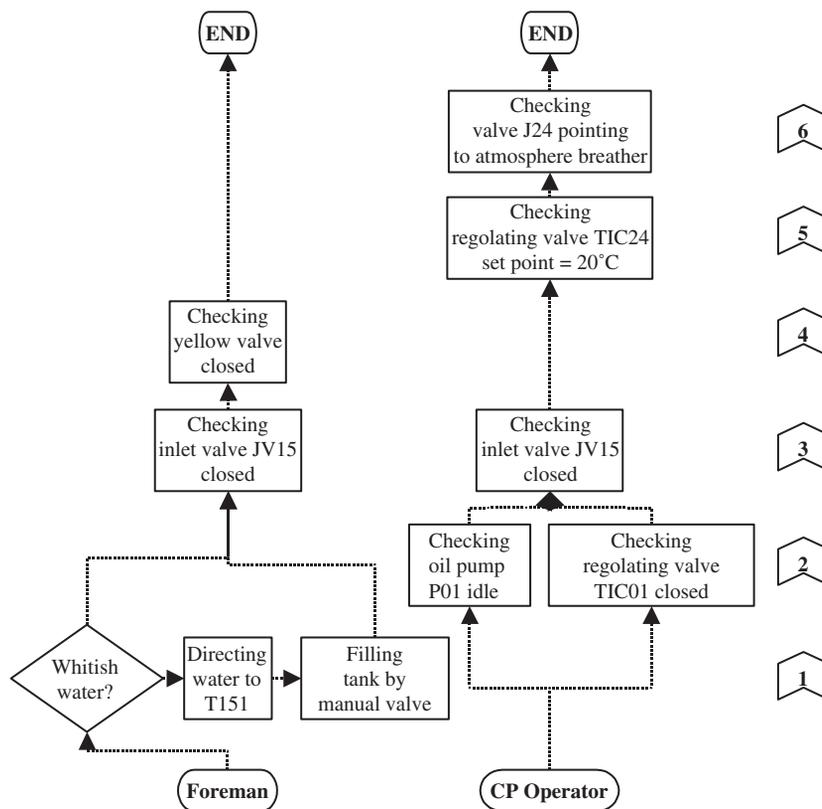


Figure 3. Loading procedure hierarchical task analysis.

As it was possible to meet the workers and to be on familiar terms with them, we were able to propose an attitudinal test in order to evaluate operators' skill and capacities.

The proposed test assumes parameters and links them to the cognitive functions (Table 1). The identified parameters take into account the physical properties of the man, his level of instruction, his knowledge of the plant organisation and structure, his relation with the other team members.

Two types of parameters were defined:

- the cognitive function parameters,
- the personal condition parameters.

All parameters were assumed as independent to each other. The cognitive function parameters are directly linked to each cognitive function, they are two for each cognitive function and they are different from a cognitive function to another. On the contrary, the personal condition parameters are the same for all cognitive functions.

Each parameter can take 4 values, ranging from 0 to 1: if the parameter is 1, it means that the operator is the best possible match for that parameter.

So if:

- $P_I$  and  $P_{II}$  are the first and the second parameter linked to the observation cognitive function;
- $(PC)_i$  is a personal condition parameter, with  $i = 1 \dots 4$ ;

then the cognitive capacity concerning the observation cognitive function results:

$$\frac{\sum_i (PC)_i}{4} \times (P_I + P_{II}) = \text{Observation} \quad (1)$$

It is possible to define as perfect operator a man that has each parameter equal to 1. In this way, as each parameter is linked to one cognitive functions, the Perfect Operator's Cognitive Profile-POpCP is built. In the other hand, from the test compiled by a "real" operator we came to Real Operator's Cognitive Profile-ROpCP. This one is always included in the POpCP.

It is a reasonable hypothesis that the perfect operator would be able to rightly carry out each procedure, that is, the POpCP should completely satisfy the RCP. On account of this hypothesis, for each procedure we found if the real operators was able to complete it or if some of his cognitive functions were inadequate. Actually, in order to be closed to the actual case, the POpCP was decreased of 10% before comparing it to the ROpCP.

Briefly, in the operative phase we obtained the RCP necessary to carry out each procedure and we compared it to the ROpCP, taking into account the hypothesis of POpCP.

Table 1. Cognitive function parameters.

Cognitive functions	I Cogn.Funct. parameter	II Cogn.Funct. parameter
Observation	Defective vision	Time in the plant
Interpretation	School degree	Post qualification
Planning	Training	Time in the same team
Execution	Age	Physical conditions

Table 2. Personal condition parameters.

Personal condition	
1	Time available
2	Extra-working relation
3	Motivation
4	Distance from the plant

In this part, the outputs depend only on the work-load and on the cognitive capacity theoretically available in the operators, without taking into account the workshift and the mix of the productive lines, which the operators are assigned to. Actually, the response of the operator to the RCP can be modified according to the workshift being at the beginning or at the end. Furthermore the response can be modified if the work-load required is constant or changes from low levels to very high ones.

With this meaning, in order to obtain more significant results, the 8-hours-workshift was divided in four stages defined as:

- Stage-A: the first hour of the workshift, in this stage the operator's cognitive capacity isn't completely available, because he has to replace his colleague and verify the system state;
- Stage-B: the second and the third hours of the workshift, in this stage the operator enter in confidence to the system and he is almost completely operative;
- Stage-C: from the fourth to the sixth hours of the workshift, in this stage the operator's cognitive capacity is at its optimum level (the one which results from the attitudinal test);
- Stage-D: the seventh and the latter hours of the workshift, in this stage the operator feels tired and his cognitive capacity greatly decreases.

To each defined stage a different workshift-coefficient was assigned; that modified ROpCP, letting each cognitive function available for a different percent of its optimum level according to the stage. For convenience, this new defined profile was named Cognitive Profile in Workshift-CPW. Afterwards, thanks to Gantt diagram, the tasks of the procedures were allocated along the four stages, in order to compare them to the right CPW.

Then, a Required Cognitive Level-RCL was assigned to each cognitive function required by the tasks; thank to the RCL, we decided not only if a cognitive function is or is not required by the task, but also what attention level is necessary to perform it. The RCL is the result of the application of Table 3 values.

To summarize, for each task we have: the CPW available by the real operator and the RLC necessary to complete the task, furthermore we have still the POpCP of the hypothetical perfect operator.

On the hypothesis that the perfect operator completely satisfies the RLC, we found if CPW is sufficient to performance the RLC of the task. In particular, we can define a critical index as:

$$\frac{CPW}{RLC} = \text{CriticalIndex} \quad (2)$$

where a critical index greater than 1 points out a critical condition.

Through this analysis, we found out the critical tasks, considering critical three types of task:

- end-beginning task: the critical index is greater than 1 due to the allocation of the task in the workshift: if it would be allocated in other stage, it wouldn't be critical;
- high level task: the critical index is greater than 1 due to the high quality of the task request or due to the low cognitive capacity of the real operator;
- gradient task: the critical index isn't significant in this case, but it's important to note the sudden passage from a low RLC task to a high RLC one.

Table 3. Values of required cognitive level.

Level	Cognitive functions			
	Observation	Interpretation	Planning	Execution
0,2	Task requiring very low capacity of observation in elementary operations	Task requiring very low capacity of interpretation in elementary operations	Task requiring very low capacity of planning in elementary operations	Task requiring very low capacity of execution in elementary operations
0,4	Task requiring low capacity of observation in usual operations	Task requiring low capacity of interpretation in usual operations	Task requiring low capacity of planning in usual operations	Task requiring low capacity of execution in usual operations
0,6	Task requiring medium capacity of observation in complex operations	Task requiring medium capacity of interpretation in complex operations	Task requiring medium capacity of planning in complex operations	Task requiring medium capacity of execution in complex operations
0,8	Task requiring high capacity of observation in careful operations	Task requiring high capacity of interpretation in careful operations	Task requiring high capacity of planning in careful operations	Task requiring high capacity of execution in careful operations
1,0	Task requiring very high capacity of observation in critical operations	Task requiring very high capacity of interpretation in critical operations	Task requiring very high capacity of planning in critical operations	Task requiring very high capacity of execution in critical operations

### 3 CONCLUSIONS

The preliminary phase of the analysis allowed to get knowledge of the plant, both on the production-level and on the men-level, and to have deep knowledge of the organisation and management of the facilities.

The operative phase entered into details and tried to more accurately model the operators.

In particular, the critical index knowledge allowed to detect the possible operator cognitive lacks in order:

- to evaluate if the human resources employed at the moment provides for the cognitive request,
- to plan, if necessary, a specific formation programme to fill the operators gaps,
- to recruit the best fitted operator for every skill.

As the direct observation in field confirmed, the foreman RCP varies according to the different procedures: it requires mostly observation and interpretation, in the row materials loading procedures; on the other hand RCP requires mostly planning and execution in the final products unloading procedures. Actually, the foreman is the team coordinator and his versatility is mandatory. This is almost completely satisfied by the foreman ROpCP, that is the 65% of the POpCP in observation, the 74% in interpretation, the 74% in planning and the 80% in execution.

The control-panel operator RCP requires mostly execution and a lot of observation and interpretation. The observation of the actuality confirmed also this result; in fact the control panel operator examines and interprets the display, in order to execute the procedures. The control panel operator ROpCP is the 65% of the POpCP in observation, the 76% in interpretation, the 96% in execution and the 48% in planning.

This could seem to be a problem, if we didn't note that the control-panel operator RCP requires a very low level of planning.

Finally, the operator RCP requires mostly execution; in fact the operator executes the foreman's orders. The operator ROpCP is not very good because that is the 51% of the POpCP in observation, the 62% in interpretation, the 34% in planning and the 59% in execution. These deficiencies can be overcome by a right education and training program provided by the firm. In this meaning, the firm would aim to specialize the operator knowledge on different processes and, in particular, on procedures which resulted more difficult according to the critical index analysis.

An improvement of operator knowledge modifies directly the value of post-qualification and training parameters of the attitudinal test, and it lets immediately the POpCP assume better values.

Getting down to the details of the stages, the outcomes focused on which procedures were more difficult to complete. Concerning foreman and control-panel operator, some end-beginning tasks in observation and interpretation were recognised. This means that the foreman and the control panel operator qualification was generally good enough to complete their work, but they needed a particular attention at end-beginning stage of their workshift.

Concerning the operator, some high-level tasks in planning were recognised as well as some end-beginning tasks in planning. This means a considerable cognitive gap in the operator qualification, however the operator RCP requires Observation Interpretation Planning Execution especially execution, therefore a specific formation to strengthen the operator planning ability may be not necessary.

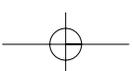
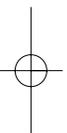
The analysis finally recognized, for every operator, the procedures mix characterized by the highest number of critical tasks. For the foreman and control panel operator, the most unfavourable condition is to start their workshift with the raw materials loading procedures, on the other hand for the operator the heaviest condition is to start with the final products unloading procedures.

The result allowed to identify and to provide the best productive lines assignment mix for the operator, in order to cut down the critical tasks number. Finding such a best mix, the human error probability decreases linked to the critical index.

#### 4 REFERENCES

- Basra, G. & Kirwan, B. (1997) Collection of offshore human error probability data *Reliability Engineering and System Safety* 61(1-2): 77-93.
- Baument, G. et al. (1999) Quantifying human and organization factors in accident management using decision trees: the HORAAM method *Reliability Engineering and System Safety* 70(2): 113-124.
- Cacciabue, P.C. (1998) Modelling and simulation of human behaviour for safety analysis and control of complex systems *Safety Science* 28(2): 97-110.
- Cacciabue, P.C. (2000) Human factors impact on risk analysis of complex system *Journal of Hazardous Materials* 71(1-3): 101-116.
- Centre for Chemical Process Safety (CCPS) (1994) *Guidelines for Preventing Human Error in Process Safety* American Institute of Chemical Engineers, New York.
- Di Giulio, A. et al. (2000) Affidabilità cognitiva dell'operatore umano e sicurezza d'impianto: prospettive di integrazione nei metodi d'analisi *Proceedings Convegno Nazionale ANIMP/OICE/UAMI 12/13October, Trieste*.
- Fussel, J.B. (1976) *Fault Tree Analysis: Concepts and Techniques - Generic Techniques In System Reliability Assessment* NATO, Advanced Study Institute.
- Gertman, D.I. & Blackman, H.S. (1994) *Human Reliability & Safety Analysis Data Handbook* John Wiley & Sons, New York.
- Hollnagel, E. (1998) *Cognitive Reliability and Error Analysis Method CREAM*, Elsevier.
- Iliffe, R.E. et al. (2000) The application of active database to the problems of human error *Journal of Loss Prevention in the process industries* 13(1): 19-26.
- Kuo-Wei Su, et al. (2000) Architecture and framework design for preventing human error in maintenance task *Expert System with Application* 19(3): 219-228.
- Javaux, D.A. (2002) Method for predicting errors when interacting with finite state system. How implicit learning shapes the user's knowledge of system *Reliability Engineering and System Safety* 75(2): 147-165.
- Jung, W.D. et al. (2000) Structured information analysis for human reliability of emergency task in nuclear plants *Reliability Engineering and System Safety* 71(1): 21-32.
- Leung, D. & Romagnoli, J. (2000) Dynamic probabilistic model-based expert system for fault diagnosis, *Computers & Chemical Engineering* 24(11): 2473-2492.
- Marsden, P. & Hollnagel, E. (1996) Human interaction with technology: The accidental user *Acta Psychologica* 91(3): 345-358.
- Mosneron-Dupin, F. et al. (1997) Human-centered modeling in human reliability analysis: some trends based on case studies *Reliability Engineering and System Safety* 58(3): 249-274.
- Parry, G.W. (1995) Suggestion for improved HRA method for use in Probabilistic Safety assessment *Reliability Engineering and System Safety* 49(1): 1-12.
- Paz Barroso, M. & Wilson, J.R. (1999) HEDOMS-Human Error and Disturbance Occurrence in Manufacturing Systems: Toward the Development of an Analytical Framework *Human Factors and Ergonomics in Manufacturing* 9(1): 87-104.
- Ramabrahman, B.V. & Swaminathan, G. (1999) Disaster management plan for chemical process industries. Case study: investigation of release of chlorine to atmosphere *Journal of Loss Prevention in the Process Industries* 13(1): 57-62.
- Reason, J. (1990) *Human Error* Cambridge University Press, Cambridge.
- Rinaldi, R. & Giagnoni, L. (2001) Estimating the influence of the human factors in risk analysis: reliability and safety

- evaluation applied to the organisation management of a petrochemical plant *Proceedings ESREL European Safety and Reliability Conference 16-20 September, Torino*.
- Sasou, K. & Reason, J. (1998) Teams errors: definition and taxonomy *Reliability Engineering and System Safety* 65(1):1-9.
- Sharit, J. (1993) Human reliability modelling *New Trends in System Reliability Evaluation* by K.B. Misra Elsevier, Amsterdam.
- Sharit, J. (1997) Allocation of functions. *Handbook of Human Factors and Ergonomics* 2nd Ed. by G. Salvendy John Wiley & Sons, New York.
- Sharit, J. (1998) Applying Human and System Reliability Analysis to the Design and Analysis of Written Procedures in High-Risk Industries *Human Factors and Ergonomics in Manufacturing* 8(3): 265-281.
- Shen, S-H. et al. (1996) A methodology for collection and analysis of human error data based on a cognitive model: *IDA Nuclear Engineering and Design* 172(1): 157-186.
- Shen, S-H. et al. (1996) The IDA cognitive model for the analysis of nuclear power plant operator response under accident condition. Part I: problem solving and decision making model *Reliability Engineering and System Safety* 55(1): 51-71.
- Starter, O. & Bubb, H. (1999) Assessment of human reliability based on evaluation of plant experience: requirements and implementation *Reliability Engineering and System Safety* 63(1): 199-219.
- Swain, A.D. & Guttman, H.B. (1983) *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications* NUREG/CR-1278 U.S. Nuclear Regulatory Commission, Washington.
- Trucco, P. et al. (2000) Aspetti cognitivi e organizzativi nella sicurezza d'impianto: analisi di un'incidente in una centrale di cogenerazione *Proceedings Convegno Nazionale ANIMP/OICE/UAMI 12/13 Ottobre, Trieste*.



## Draft european standard on safety risk assessment for space missions

R. Tuominen

*VTT Industrial Systems, Tampere, Finland*

C. Preysl

*European Space Agency, Noordwijk, Netherlands*

I. Jenkins<sup>1</sup>, P. Pearson<sup>2</sup>, J. Lenic<sup>3</sup>, G. Canepa<sup>4</sup>, G. Morelli<sup>5</sup> & T. Bedford<sup>6</sup>

<sup>1</sup> *Astrium GmbH, Munich, Germany;* <sup>2</sup> *Astrium Ltd., Portsmouth, England;* <sup>3</sup> *DLR, Bonn, Germany;*

<sup>4</sup> *Alenia Aerospazio, Turin, Italy;* <sup>5</sup> *Galileo Avionica, Florence, Italy;* <sup>6</sup> *University of Strathclyde, Glasgow, Scotland*

**ABSTRACT:** In the framework of European Co-operation for Space Standardisation (ECSS), new international European standards to support safety of space missions have been developed. The ECSS standards for project risk management and system safety specify the foundation of the systematic safety process required on space projects. The analytic part of this process is outlined in further detail in two new complementary standards on hazard analysis and safety risk assessment.

This paper discusses the risk assessment approach in the draft ECSS safety risk assessment standard ECSS-Q-40-03. The paper gives a brief summary of what the proposed standard covers and why the standard is considered important. The paper then describes how the standard is applied: its role in space programmes, how it is made applicable, how it is to be used, etc. Furthermore, the links to other ECSS standards and the disciplines of safety and risk management are explained. While initially written for space systems, the practitioners of safety and risk analysis are invited to consider the use of the described approach for safety risk assessment also for non-space applications.

### 1 INTRODUCTION

As demonstrated by the recent tragic accident of the space shuttle Columbia, space flight is a risky endeavour for which safety is of paramount importance.

Space systems are typically complex and contain, or manage, large amounts of energy. New and not necessarily fully mature technologies are often applied. Failure tolerance and performance margins are limited by severe mass constraints. The threats to safety with space systems originate from the hazardous characteristics of the space system design, its operating environment, and from hazardous effects of system failures of off-nominal situations.

In the framework of European Co-operation for Space Standardisation (ECSS), new international European standards to support safety with respect to space missions have been developed. The ECSS standards for project risk management (ECSS-M-00-03) and system safety (ECSS-Q-40B) specify the foundation of the systematic safety process required on space projects. The analytic part of this process will be outlined in

further detail in two new complementary standards on hazard analysis (ECSS-Q-40-02) and safety risk assessment (ECSS-Q-40-03).

In the context of the ECSS standards for space safety, safety analysis has been defined to comprise *hazard analysis*, *safety risk assessment*, and a variety of supporting analyses, listed in the ECSS-Q-40B, to be applied at the discretion of a particular project. The objective of safety analysis is to identify, assess, propose the means to reduce, control, and accept hazards and the associated safety risks in a systematic, proactive, and complete manner, taking into account the project's technical and programmatic constraints. Safety analysis is implemented through an iterative process. Cycles of the safety analysis process are iterated during the different project phases and evolution of system design and operation.

Safety risk assessment complements hazard analysis – which is defined in the standard ECSS-Q-40-02 and allows the identification of hazard scenarios in the form of sequences of events leading from an initial cause to an unwanted safety consequence – and

comprises the identification, classification and reduction of safety risks in a probabilistic manner. The purpose of safety risk assessment is to determine the magnitude of risks induced by the identified hazards and the associated hazard scenarios, and to identify and rank the risk contributors.

It is emphasised that the standards for safety referred above are applicable to all aspects of space missions, including human spaceflight as well as the unmanned missions. The standards consider, not only the potential harm to people, but also the harm that may be caused to the equipment, property and the environment.

The present paper discusses, in particular, the risk assessment approach specified for the safety risk assessment standard ECSS-Q-40-03. At the time of the writing of this paper, the standard is still being drafted. The paper has been prepared by the members of the ECSS working group that has developed both the hazard analysis standard and the current safety risk assessment standard draft.

## 2 ROLE OF SAFETY RISK ASSESSMENT IN SPACE PROJECTS

Safety risk assessment is the principal probabilistic analysis which assists engineers and managers to include safety aspects in the engineering practices and the decision making process throughout the system life cycle. Ranking of safety risks, according to their criticality for the project success, allows managers and engineers to direct their attention to the essential safety issues, as part of the major objectives of risk management.

The information produced on safety risks is used to:

- assess the level of safety of a system in a probabilistic way;
- increase the level of safety of a system through safety risk reduction;
- drive the definition and implementation of design and operation requirements, specifications, concepts, procedures etc.;
- provide a basis for defining adequate safety requirements, determining the applicability of safety requirements, implementing safety requirements, verifying their implementation and demonstrating compliance or non-compliance;
- support safety related project decisions;
- support safety submissions and reviews through documented evidence;
- support safety certification of a system through documented evidence; and
- provide input to overall project risk management.

The probabilistic approach of safety risk assessment is considered to be most useful and beneficial in relation to large and complex systems, possibly with

some novel technologies involved. The risk values produced by the assessments can be used to support decisions on system design, operations, or upgrades. Regarding complex systems, the safety risk assessment can provide the means needed to point out the *risk drivers* (i.e. main risk contributors), or to *optimise* the system with respect to the defences required for the identified risks. Furthermore, the assessments can show the *safety improvement potential* of design changes or upgrades, and make explicit the *uncertainties* in the state of knowledge regarding possible accident scenarios, showing where the knowledge is weak and where it needs to be improved.

Safety risk assessment and the corresponding new ECSS standard are considered suitable, in particular, to serve the needs of future manned systems (e.g. manned mission to Mars) and complex unmanned systems/missions with significant safety implications. Galileo is an example of a new European unmanned space programme with important implications for services, some of which are clearly safety critical (e.g. air traffic control services).

## 3 SAFETY RISK ASSESSMENT CONCEPT

### 3.1 Hazards and hazard scenarios

The ECSS-Q-40-02 defines a hazard analysis concept in which a clear distinction is made between hazards, intermediate events and consequences. This distinction of hazards and scenarios is considered important to facilitate the identification of all hazards and the associated possibilities for accidents, as well as to support more structured identification and evaluation of hazard reduction and control means. It can also be found important in supporting the hazard analysis interface with the safety risk assessment.

*Hazards* are defined as potential threats to the safety of a system. They are not events, but the prerequisite for the occurrence of *hazard scenarios* with their negative effects on safety in terms of the safety consequences. Hazard scenarios determine the possibilities of accidents, by reflecting the system behaviour in terms of event propagation from initiating events (i.e. causes) to harmful consequences, as shown in Figure 1. Different hazard scenarios can originate from the same hazard, and different hazard scenarios can lead to same safety consequence. The collection of hazard scenarios leading to same safety consequence can be collated into the form of a *consequence tree*.

### 3.2 Safety risk assessment

The safety risk assessment extends on the deterministic hazard analysis by adding a probabilistic dimension (i.e. likelihood and uncertainty) in the identified hazard

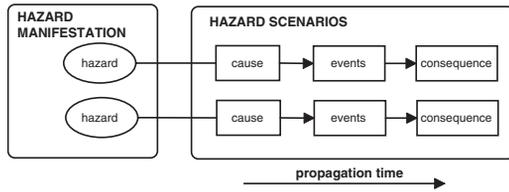


Figure 1. The concept of hazard and hazard scenarios.

scenarios and the associated negative consequences in order to determine the magnitude of risk that they present. Safety risk assessment is based on a probabilistic analysis, in that the ranking of risks and risk contributors is jointly dependent on the severity of the associated consequences and on the likelihood of those consequences occurring. The performance of deterministic hazard analysis, which identifies the hazards, the associated hazard scenarios and their negative consequences on safety, is a prerequisite to performing a safety risk assessment.

The acceptance of safety risks posed by the scenarios is based on a joint ranking of the consequence severity and the likelihood. Hence certain risks may be accepted because their chance of occurrence is considered sufficiently low given the foreseen severity of the consequences.

The nature of safety risk assessment can be twofold. Either the assessment can deal with the risks posed by individual hazard scenarios separately, or it can consider sets of scenarios, collectively in the form of the overall risk posed by them. The safety risk assessment standard ECSS-Q-40-03 draft allows for flexibility in determining and using the most efficient approach depending on the objectives of the assessment, i.e., the intended use of the assessment results in a particular project.

Consideration of the hazard scenarios and the associated risks on the individual basis serves as a tool for risk acceptance and safety verification. The scenarios with high risk can be identified and subjected to risk reduction. The risk acceptance criteria are defined at individual scenario level. In this case, the probabilistic assessment is typically done in a qualitative manner based on subjective data using consequence severity and scenario likelihood categorisations and by applying a risk index scheme and a risk grid (or risk matrix), an example shown in Figure 2. The risk grid transforms the severity – likelihood plane (i.e. risk plane) into a judgementally tractable set of cells and specifies the boundaries for risk tolerance as established in the risk policy. The risk grid is used to communicate the risk assessment results and their evolution.

Overall risk assessment deals with the accumulation of the risks posed by individual hazard scenarios and provides a holistic view that places the scenarios

Risk index	Risk magnitude	Risk Acceptability Criteria for individual risk scenarios
IA, IB, IIA	Maximum risk	Unacceptable risk
IC, IIB	High risk	Unacceptable risk
ID, IIC, IIIA	Medium risk	Unacceptable risk
IID, IIIB, IVA	Low risk	Acceptable risk
Others	Minimum risk	Acceptable risk

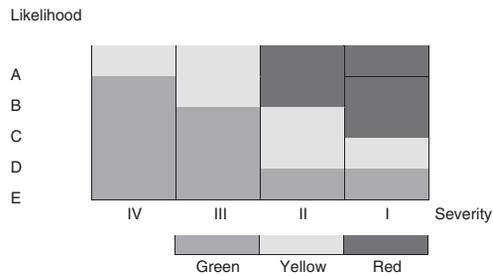


Figure 2. Example of risk index scheme and risk grid.

in perspective and gives the basis for identifying and ranking of risk contributors and optimising safety of the systems. The assessed overall risk can be compared to a probabilistic target (or acceptance criteria) specified for overall risk in the particular system considered.

Probabilistic Risk Assessment (PRA) based on, for example, a comprehensive Event Tree and Fault Tree model, represents one method for performing overall risk assessment. Dependent uncertainty analysis can be used for the propagation of uncertainties in the hazard scenarios (Bedford & Cooke 2001; ESA 2002).

Importance measures such as ‘risk contribution’ provide information on potential safety improvement (i.e. potential reduction of risk) related to a particular scenario event. Design and operation constituents can also be ranked from risk reduction view point by cumulating the contributions of events associated with the particular constituents.

The uncertainties associated with the estimate of the overall risk (posed by the hazard scenarios) call for a precautionary use of the risk acceptance criteria. Conservative assumptions with respect to the risk estimate are preferred to optimistic ones to ensure that a system is not considered to satisfy an agreed risk target (or acceptance criterion) falsely. A representative point value in the upper part of the probability distribution for the overall risk, at a confidence level accepted by the decision-maker, could be used to implement the precautionary principle for risk acceptance decisions, and for risk comparisons.

The estimation of scenario likelihoods can be based on different sources of data, such as:

- previous experience on the particular system (i.e. measured or observed data);
- data from other systems or projects (i.e. extrapolation from generic data, similarity data, or physical models); or
- expert judgement.

Based on these data sources, likelihood estimates of scenario events are generated. As systematic identification and treatment of uncertainties is one of the main objectives of the probabilistic assessments, the likelihood estimates of scenario events are to be presented with the associated (lack of knowledge) uncertainty.

#### 4 SAFETY RISK ASSESSMENT PROCESS

The safety risk assessment process, as defined in ECSS-Q-40-03 draft, comprises the steps and tasks necessary to identify and assess the safety risks, to support safety risk reduction and to establish rational basis for final acceptance of (residual) risks. The basic steps are:

- Step 1: Define assessment requirements;
- Step 2: Identify and assess the safety risks;
- Step 3: Decide and act on the safety risks;
- Step 4: Track, communicate and accept the residual safety risks.

The process of safety risk assessment, including iteration of its tasks, is outlined in Figure 3.

The 4-step safety risk assessment process is further divided into specific tasks and detailed activities needed to achieve the objectives of each specific task. The tasks within each of the steps are summarised in Figure 4.

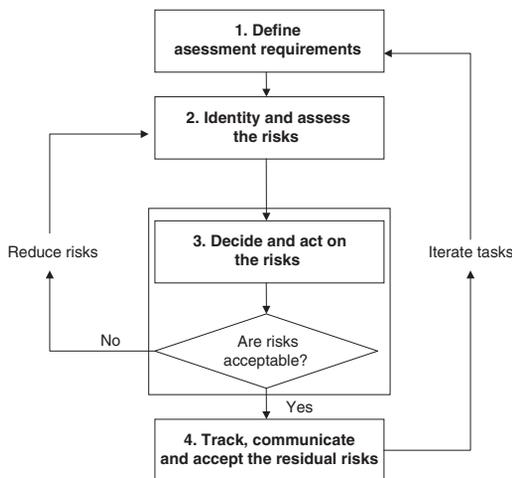


Figure 3. The process of safety risk assessment.

As evident based on Figures 3 and 4, the safety risk assessment process of ECSS-Q-40-03 has been expanded from a mere assessment process to show a process of assessment (i.e. steps 1 to 3) and management (i.e. steps 3 and 4) of safety risks. This has been done simply to align the consideration of safety risks with the general risk management process for technical and programmatic risks in space projects defined in the management standard ECSS-M-00-03.

The safety risk assessment process of the ECSS-Q-40-03 also presumes the performance of hazard analysis, according to ECSS-Q-40-02, as a prerequisite to the performance of safety risk assessment of a system. The possible accident scenarios and their associated severity of consequences are identified and assessed by hazard analysis. For more details on the hazard analysis, see Tuominen et al. (2001).

#### 5 SAFETY RISK ASSESSMENT IMPLEMENTATION

Implementation of safety risk assessment on a project is based on single or multiple i.e. iterative application of the safety risk assessment process. The tasks associated with the individual steps of the safety risk

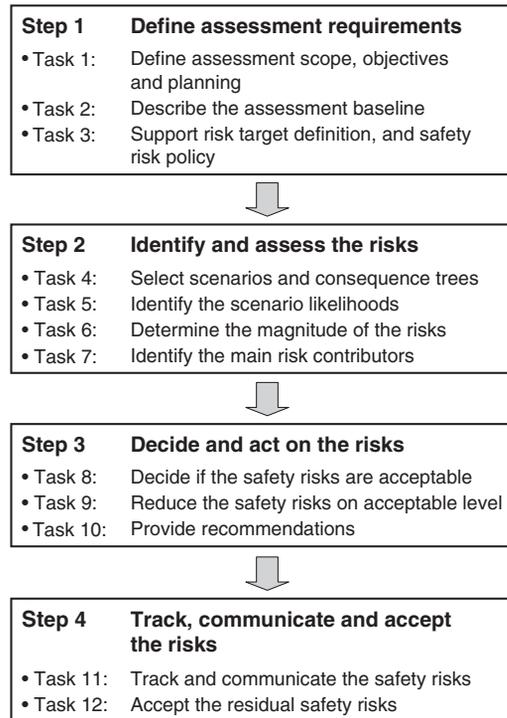


Figure 4. The tasks associated with the 4 steps of the safety risk assessment process.

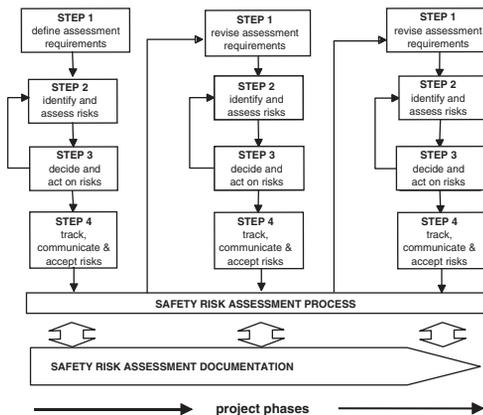


Figure 5. Iterative application of the safety risk assessment process over project lifetime.

assessment process vary according to the scope and objectives specified for safety risk assessment. The scope and objectives of safety risk assessment depend on the type and phase of the project.

According to the specified scope and objectives, the implementation of the safety risk assessment process consists of a number of “safety risk assessment cycles” over the project duration comprising the necessary revisions of the assessment requirements, and the assessment Steps 2–4, as indicated in Figure 4.

The period designated in Figure 5 as “Safety risk assessment process” comprises all the phases of the project concerned. The frequency and the events at which cycles are required in a project (note that only 3 are shown in Figure 5 for illustration purposes) depend on the needs and complexity of the project, and are defined during Step 1 at the beginning of the project.

Safety risk assessment implementation requires commitment in each actor’s organisation, and the establishment of clear lines of responsibility and accountability. Project management has the overall responsibility for the implementation of safety risk assessment, ensuring an integrated and coherent safety risk assessment approach.

The safety risk assessment process needs to be carefully documented to ensure that the scope and objectives of the safety risk assessment are established, understood, implemented and maintained, and that an audit trail can lead to the origin and rationale of all safety related decisions made during the life of the system/project.

## 6 CONCLUSIONS

The presented safety risk assessment approach is process oriented and aimed at providing analyses,

which explicitly state and work towards the goals, objectives and intended use of the analysis results. Analysis results are intended to drive the design and operation through hazard and safety risk reduction, support specific trades between design options, show compliance with safety requirements, risk policy or probabilistic targets, etc.

The presented safety risk assessment approach is an evolution from PRA, which simplifies the conventional PRA approach. PRA’s are often found complex and time consuming and are produced for an existing system rather than driving the system development. The use of the presented safety risk assessment approach allows flexibility regarding the nature of a particular assessment and prioritising the allocation of assessment resources. The approach can make risk results to be available in a shorter time, which makes it easier to deal with short cycle times and the introduction of changes during space system development.

The proposed safety risk assessment standard is not intended to be prescriptive. It only describes a general framework and a process for how to properly perform safety risk assessments. It is not prescribing the detailed methods to be used. The actual implementation of the process can be tailored for particular user needs. The only requirements (“shall’s”) that are expressed in the standard draft are to emphasise the implementation of the systematic assessment process with specific steps and tasks, application of particular analysis principles, and the proper documentation of the assessment and its outputs.

The approach adopted for safety risk assessment is fully in line with and supports the ECSS risk management process for space projects defined in the management standard ECSS-M-00-03. The approach emphasises the importance and application of the coherent risk management process to the discipline of safety.

Whilst, initially written specifically for space systems, the ECSS hazard analysis and safety risk assessment approaches, as described in the ECSS-Q-40-02 and the ECSS-Q-40-03 draft respectively, can also be applied to non-space systems. The practitioners of safety and risk analysis are invited to consider the use of the approaches for non-space applications.

## REMARK

The present paper relates to ECSS-Q-40-03 standard draft as prepared and debated within the corresponding ECSS Working Group. At the time of the writing of this paper, the draft standard had not been submitted to ECSS review, and has not therefore received endorsement in accordance with the ECSS standard process. The views expressed here are those of the authors and

do not necessarily reflect those of the corresponding organisations or ECSS.

#### REFERENCES

ECSS-M-00-03 Space project management – Risk management. (Available via ECSS web site <http://www.ecss.nl/>)  
ECSS-Q-40B Space product assurance – System safety. (Available via ECSS web site <http://www.ecss.nl/>)  
ECSS-Q-40-02 Space product assurance – Hazard analysis. To be published by ECSS.  
ECSS-Q-40-03 Space product assurance – Safety risk assessment. To be published by ECSS.

ESA 2002. ESA “Handbook & Procedure Guide for Risk Management” RIMOX; available at <http://www.estec.esa.nl/qq/RIMOX/Default.htm>

Bedford, T. & Cooke, R. 2001. Probabilistic Risk Analysis: Foundations and Methods. Cambridge: Cambridge University Press. ISBN 0-521-77320-2.

Tuominen, R. et al. 2002. From hazard analysis to safety risk assessment and further: the new European safety standards on hazard analysis and safety risk assessment. In Proceedings of Joint ESA-NASA Space-Flight Safety Conference, Noordwijk (NL), 11–14 June 2002. ESA SP-486. Noordwijk: European Space Agency.

## Extended stochastic petri nets in power systems maintenance models

A.P. Ulmeanu, D.C. Ionescu & A.C. Constantinescu  
University POLITEHNICA of Bucharest, Bucharest, Romania

**ABSTRACT:** The maintenance set of policies for a power system should be done through a coherent policy, complying with the quality service requirements. The cascade failures, common cause failures (environmental condition, use of the same components, etc.), protection-system functions, automatic/manual reconfiguration and the maintenance procedures are the most important dependency concepts considered. The dynamic behavior of the power system is modelled through Extended Stochastic Petri Nets. Their main advantages are considered: modular approach and supporting the integration of several mathematical frameworks (discrete events, stochastic processes, simulations, etc.). On the other hand, the Extended Stochastic Petri Nets have an acquired benefit due to a very rich field for specifying, designing, implementing, verifying and validation. The structural, functional and stochastic dependencies are modelled by rule base, and implemented through two basic types of interfaces: common transitions and marking check. Common transitions describe the occurrence of events that lead to simultaneous marking evolution of the involved modules. The second type of interfaces is the marking check. It is used when the occurrence of an event assigned to a component is conditioned upon the states of other components. A relevant improvement on existing methods is to consider the condition-based maintenance models for power systems, subject to deterioration-failures and to Poisson failures. The Poisson failure process represents all hard faults that might occur instantaneously in any deterioration stage of the components' system. The soft faults grow gradually with the time and lead to a predictable condition, modelled by a multi-state continuous-time deterioration process. After an inspection, based on the degree of deterioration, a minimal/major action is performed, or no action is taken. Generally, the Poisson failures are restored by minimal repairs while the deterioration failures are restored by major repairs. Extended Stochastic Petri Nets are used to represent and analyze the model, which stand for a inspection-based maintenance strategy. Based on maximization of the system performance, an optimal inspection policy within the strategy and optimal inter-inspection time are acquired.

### 1 BASIC OF EXTENDED STOCHASTIC PETRI NETS FOR RELIABILITY MODELLING

#### 1.1 Abbreviations, acronyms, and notations

AM – Age Memory;  
BI – Between Inspections;  
DF – Deterioration Failure;  
DI – Degredation Level I;  
DII – Degredation Level II;  
DIII – Degredation Level III;  
EM – Enabling Memory;  
HF – hard failure mode;  
I – inspection;  
MP – Memory Policy;  
MT – Maintenance Tasks;  
NA – no Action;  
NM – no Memory;  
NH – no Hard Failure Mode;  
NS – no Soft Failure Mode;

m – minimal maintenance;  
M – major maintenance;  
PF – Poisson Failure;  
r – minimal repair;  
R – major repair;  
SF – Soft Failure Mode;  
SyS – System State;  
SPL – System Performance Level;  
d – system degradation level ( $d = 0, 1, 2, \dots, n$ );  
z – system threshold major maintainance level ( $0 < z < n$ );

#### 1.2 Assumptions

By definition (Jensen and Rozenberg 1991), an Extended Stochastic Petri Net (ESPN) is a tuple:

$$ESPN \equiv (P, T, I, O, PDF, M_0) \quad (1)$$

where

- $P$  is a finite set of places
- $T$  is the finite set of timed and immediate transitions.  $T = T_t \cup T_0$
- $I$  is the input function (represented by directed arcs from places to transitions)
- $O$  is the output function (represented by directed arcs from transitions to places)
- $H$  is the inhibition function (circle-headed arcs from places to transitions)
- $PDF$  is the probabilistic distribution functions assigned to the set  $T_t$  of timed transitions
- $M_0$  is the initial marking

In general, the symbol  $M$  is an assignment of a natural number of tokens to each place of the  $PN$ . Also, we are using the following symbols for the pre- and post-sets of the  $ESPN$  nodes (places or transitions):  $t^- = \{p/(p, t) \in I\}$  – the set of the input places for a transition  $t$  connected through directed arcs;  $t^+ = \{p/(t, p) \in O\}$  – the set of the output places for a transition  $t$  connected through directed arcs;  $ti^- = \{p/(p, t) \in H\}$  – the set of the input places for a transition  $t$  connected through inhibitor (circleheaded) arcs.

A transition  $t$  is enabled in a marking  $M$  if all places  $t^-$  are signed, i.e. each type of input place has at least one token. In the case when  $ti^- \neq \emptyset$  the input places  $ti^-$  connected through inhibitor arcs to the transition  $t$  should not be marked in order to ensure that this transition  $t$  is enabled. Any enabled transition can fire (immediately or delayed). When the transition  $t$  is firing, a token is removed from each input place  $t^-$  and another one is added to each output place  $t^+$ . Accordingly, a new marking  $M'$  is reachable. We denote this as  $M\{t\} \rightarrow M'$ . As a rule, a marking  $M_k$  is said to be reachable from the marking  $M_0$  whenever there is a sequence of firings that transforms  $M_0$  in  $M_k$ . A firing or occurrence sequence is denoted by a set of the fired transitions. If for any marking of  $ESPN$ , the number of tokens in any place is finite, and there is at least one enabled transition, then we have a live and bounded  $ESPN$ .

### 1.3 Stochastic semantics of $ESPNs$

The main components of the stochastic semantics of  $ESPNs$  (Marsan and Chiola 1987) are:

- the sequence policy
- the memory policy
- the service policy

The sequence rule first which is the transition to be fired in a given marking. In this paper we follow the race policy (Sim and Endreny 1993), i.e. among the enabled transitions the one which will fire is the one with the smallest residual firing time.

Since the non-exponential distributions are no more memoryless, it is very important to specify how is

going to be managed the residual firing times of the remained enabled timed transitions after the system transition. In principal, there are three cases:

EM	enabling memory: the elapsed time is kept as long as the transition remains enabled;
NM	no memory (resampling): the elapsed time is lost and a new firing delay will be assigned the next time whenever the transition will be enabled;
AM	age memory: the elapsed time is kept whatever the system's evolution. The next time when the transition will be enabled the remaining firing time will be the residual time from the last disabled.

As soon as the stochastic semantics are defined, the distributions of the conditional sojourn times in each  $ESPN$  marking are obtained. Under specific hypothesis, it is possible to define regeneration points of the stochastic process. The asymptotic reliability/performance indices are obtained modelling the process within two regeneration points (Marsan and Chiola 1987).

The service policy defines the Enabling Degree of a transition. Several clients may be served when ED is greater than 1.

## 2 CONSTRUCTION OF AN $ESPN$ – A STUDY CASE

The structural, functional and stochastic dependencies are modelled by a base rule and implemented through two essential types of interfaces: common transitions and marking check (Ulmeanu and Ionescu 1999). Common transitions describe the occurrence of events that lead to simultaneous marking evolution of the involved modules. Consequently, these involved modules share the common transitions. The second type of interfaces is the marking check. It is used when the occurrence of an event ascribed to a component is conditioned upon the states of other components. The basic rules for this kind of interface specify that the marking of the places involved in the check procedure should remain unchanged. Therefore, only bi-directional and inhibitor arcs could be used to implement this kind of interface. Figure 1 presents the  $ESPN$  for a condition-based maintenance model for a system, subject to deterioration-failure and to Poisson-failures (Jensen and Rozenberg 1991; Sim and Endreny 1993). After an inspection, based on the degree of deterioration, a decision is taken: no action / minimal maintenance / major maintenance. Deterioration (soft) failures are restored by major repair, while the Poisson (hard) failures are restored by minimal repair. Table 1 gives the set of decision actions, the associated maintenance tasks, as well as the ageing properties (memory policy).

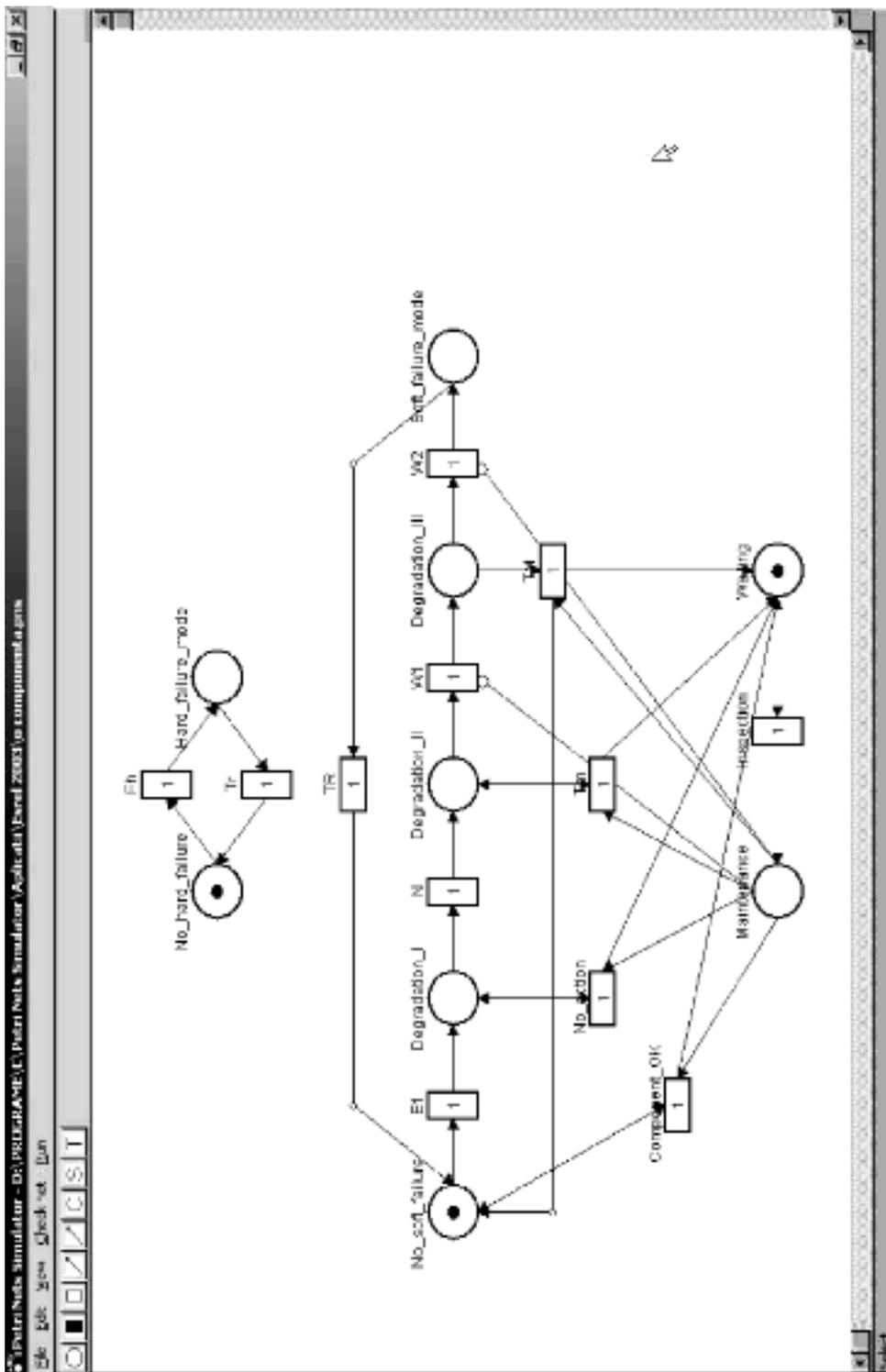


Figure 1.

Table 1. The maintenance policy.

State before MT	MT	State after MT	MP
DF	R	As good as new	NM
PF	r	As bad as old	AM
NS	NA	As good as new	AM
DI	NA	As bad as old	AM
DII	m	As bad as old	EM
DIII	M	As good as new	NM

Table 2.

SyS	Sejourn time	SPL	d
NS	$Exp(\lambda = 10^{-4} h^{-1})$	100 %	0
DI	$N(\mu = 2000 h, \sigma = 100 h)$	75 %	1
DII	$Weib(\alpha = 2000 h, \beta = 2)$	50 %	2
DIII	$Weib(\alpha = 2000 h, \beta = 2.5)$	25 %	3
SF	$Exp(\mu = 0.010417 h^{-1})$	0	–
NH	$Exp(\lambda = 10^{-3} h^{-1})$	100 %	0
HF	$Exp(\mu = 10^{-1} h^{-1})$	0	–
I	Deterministic ( $\delta = 10 h$ )	0	–
BI	Deterministic ( $\Delta = 2200 h$ )	0	–
m	$Exp(\mu = 0.16667 h^{-1})$	0	–
M	$Exp(\mu = 0.013889 h^{-1})$	0	–

## 2.1 ESPN presentation

The initial marking of

- one token in the place labeled *No Soft Failure*
- one token in the place labeled *No Hard Failure*
- one token in the place labeled *Waiting*

denotes that the system is operating, no degradation level ( $d = 0$ ), waiting for the next inspection. Three degradation levels are considered in this study case ( $n = 3$ ), and the threshold major maintenance level is set  $z = 3$ . As soon as the degradation level  $d$  unveiled by a inspection procedure is greater than the threshold  $z$  then a major maintenance action must be performed in order to ensure that the system returns in *NS* state. The sejour probabilistic distribution functions and the system performance standards are shown in the Table 2.

An inspection procedure is scheduled at each  $\Delta = 2200 h$  in order to reveal the degradation state of the system. When the inspection procedure is beginning, the token is removed from the place *Waiting* and another one is set to the place *Maintenance*. After the achievement of the inspection tasks ( $\delta$  is assumed to be the duration of the inspection action), the following three cases are possible:

- whether the unveiled degradation level is corresponding to the state *NS* (i.e. a token is found in the place *NoSoftFailures*), then just after elapsing the

deterministic delay  $\delta$ , the transition *ComponentOK* is firing. Consequently, the tokens are removing from the place *Maintenance* and from place *NoSoftFailures* respectively, and a token is re-appearing in the place *Waiting* and one token in the place *NoSoftFailures* as well. The transition *E1* is re-enabled, the sejour time in the state *NS* is kept, based on the ageing memory property (as shown in Table 1);

- whether the unveiled degradation level is corresponding to the state *DI* (i.e. a token is found in the place *DegradationI*), then the transition *NoAction* is firing just after elapsing the deterministic delay  $\delta$ . As a consequence of the firing, the tokens are removing from the place *Maintenance* and from place *DegradationI* respectively, and one token is reappearing in the place *Waiting* and one token in the place *DegradationI* as well. The transition *N* is re-enabled, the sejour time in the state *DegradationI* is kept, based on the ageing memory property (as shown in Table 1);
- whether the unveiled degradation level is corresponding to the state *DII* (i.e. a token is found in the place *DegradationII*), then the transition *Tm* is firing just after elapsing the random delay that follows the distribution  $Exp(\mu = 0.16667 h^{-1})$ . The tokens are removed from the *Maintenance* and *DegradationII* place respectively, and one token is reappearing in the place *Waiting* and another one in the place *DegradationI*. The transition *W1* is re-enabled while the sejour time in the state *DegradationII* is reset. Following the minimal maintenance action, the system returns to the condition had just after the firing of transition *N* (when pop in the state *DegradationII*). The inhibitor arc connecting the place *Maintenance* and the transition *W1* ensure that during the minimal maintenance action the degradation process is not enabled, i.e. to firing the transition *W1*.
- whether the unveiled degradation level is corresponding to the state *DIII* (i.e. a token is found in the place *DegradationIII*), then the transition *Tm* is firing just after elapsing the random delay that follows the distribution  $Exp(\mu = 0.16667 h^{-1})$ . The tokens are removed from the *Maintenance* and from *DegradationIII* place respectively, and a token is reappearing in the place *Waiting* and another one in the place *DegradationIII* as well. The transition *W2* is not re-enabled, the system returns to the *NS* state, as a result of major maintenance (as shown in Table 1).

Based on the race policy, the transition *W2* might fire before falling the inspection task. In this case, the soft failure mode is occurring. A token is removed from the place *DegradationIII* and a token is put in the place *SoftFailureMode*. After elapsing the random

major repair time that follows the distribution  $Exp(\mu = 0.010417h^{-1})$ , the system returns to the  $NS$  state.

An independent hard failure mode can occur in any deterioration stage and stop the system operation. For example, a fuse burn-out can be replaced in short time, with no effect on the deterioration of the system. The restoration time follows the distribution  $Exp(\mu = 10^{-1}h^{-1})$ .

### 3 PERFORMANCE ANALYSIS

Structural analysis of the ESPN model denotes a net live and bounded. Because of the complexity of the model mainly due to the decision following as inspection, a numerical analysis based on forced Monte Carlo method is purposed. The steps for the numerical solution of ESPN models are :

- generation of the reachability graph (RG) from the ESPN model;
- reduction of the RG, by absorbing the vanishing markings, i.e. without sejour time;
- numerical solution based on Monte Carlo methods.

The expected system throughput is selected as a performance criteria, in the system steady state (long run). Figure 2 shows expected throughput of the system versus the inspection periodicity  $\Delta$  for two figures of the inspection duration  $\delta$ .

### 4 CONCLUSION

We have presented in this paper a study regarding the effectiveness of Extended Stochastic Petri Nets in managing the performability of the maintained systems. The degradation phenomena and the maintenance policies are modelled using ESPN in order to find out an optimal solution, an equilibrium between the loss of performance due to degradation, down times for inspection, repair tasks and the gain due to maintenance actions. Future studies will investigate the best set of maintenance policies indicated for each

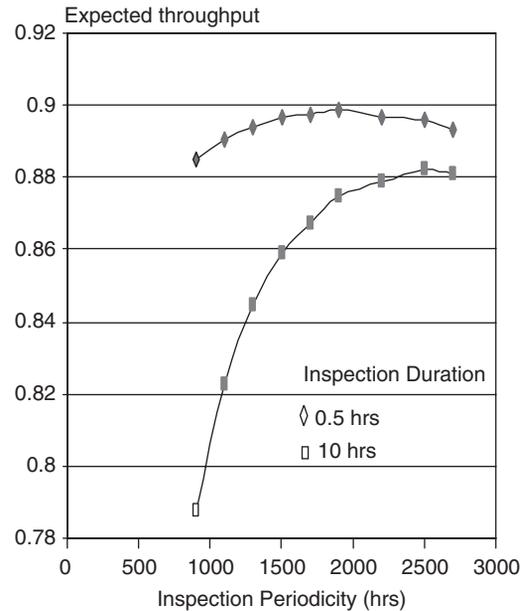
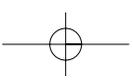
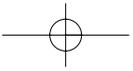


Figure 2. The effect of the inspection duration.

deterioration state of the system, as well as the effect of the maintenance and repair parameters.

### REFERENCES

- Jensen, K. and G. Rozenberg (1991). *High Level Petri Nets*. Springer-Verlag.
- Marsan, M. A. and G. Chiola (1987). *On Petri Nets with Deterministic and Exponentially Distributed Firing Times*, pp. 132–145. Springer-Verlag.
- Sim, S. H. and J. Endreny (1993, March). A Failure-repair Model with Minimal and Major Maintenance. *IEEE Transactions on Reliability* 42(3), 134–140.
- Ulmeanu, A. P. and D. C. Ionescu (1999). *The Computer-Assisted Analysis of the Semi-Markovian Stochastic Petri Net and an Application*, pp. 307–320. Birkhauser Boston.



## An implementation of a life-cycle risk-based design for safety methodology

D. Vassalos & D. Konovessis

*The Ship Stability Research Centre, Department of Naval Architecture and Marine Engineering Universities of Glasgow and Strathclyde Glasgow, United Kingdom*

**ABSTRACT:** Ship safety can be influenced by several factors over time and it is apparent that all such factors should be taken into account, in a balanced and formalised manner during the life-cycle of the vessel, in order to reach an acceptable, viable solution optimally. In this respect, a risk-based methodology addressing design, operation and regulation for ship safety is presented in this paper. Particular attention is paid on the balance of conflicting risks and costs deriving from different hazards, as well as in techniques used for the estimation of risks levels based on first-principles tools. A case study is presented to address the application of the developed methodology, aiming to provide insight in the proposed procedure as well as to demonstrate its potential for wider application.

### 1 INTRODUCTION

For a period of more than ten years a safety culture approach is being promoted through the theme “Design for Safety”, which aims at integrating safety cost-effectively in the ship design process, Vassalos (1999). However, the lack, thus far, of a systematic and all-embracing approach to ship safety, offering a framework that allows for a strategic overview of safety and the derivation of effective solutions, meant that the wealth of information amassed over many years of research and development on stand-alone safety-critical areas remains under-utilised, whilst ship safety continues to be unnecessarily undermined. One of the main elements of the above mentioned R&D work is the assurance of safety within the ship design process, in the continuous search for improving the current state-of-affairs. Through small, albeit bold steps in the direction advocated by “Design for Safety”, it is slowly but steadily being recognised that this approach can greatly contribute to the overall cost-effective improvement of safety in shipping whilst nurturing the evolution of proper practice in the field.

Traditionally ship safety has been dealt with by adherence to rules and regulations, thus treated as a constraint in the design process. With technology and users requirements developing faster than knowledge can be assimilated and best practice produced, this approach to safety assurance is expected to be largely

ineffective. Adopting an integrated approach that links safety performance prediction, risk assessment and design is necessary that treats safety as a life-cycle issue and a design imperative is now becoming prerequisite to attaining optimal solutions. A key target is a formalised risk-based design methodology utilising routinely first principles with safety bestowed as a key objective at the core of ship design and operation. To this end, a top-down approach is advocated, governed by high-level events and their frequencies and consequences, in order to design for safety. The relationships between risk reduction measures and ship performance must be established in the early design phases, as keeping this relationship outside the design process will only result in local optimisation of safety. The effects of risk reducing design features on resistance, seakeeping, loading/unloading, stability, etc. should be determined by utilising relevant tools in the design process. Cost-effectiveness of safety enhancing design features or measures is used as a basis to achieve balance between costs and safety optimally whilst rendering risks as low as reasonably practical whilst accounting for other design priorities and constraints.

Risk-Based Design, as a life-cycle process, should involve all the phases of a vessel, i.e. design, production and operation, as well as facilitate the transfer of knowledge among these phases. The latter is considered to be of paramount importance, since it is evidently the main cause for many deficiencies during operation

and could result in significant improvements for the whole process.

The paper focuses on the description of the approach adopted, focusing in particular in the methods developed for balancing contradicting risks and costs incurred by different hazards, as well as in techniques used for the estimation of risks levels based on first-principles tools.

## 2 ADOPTING A RISK-BASED APPROACH FOR DESIGN, OPERATION AND REGULATION

The structuring of appropriate safety assurance techniques and methodologies into design frameworks, including guidelines for the proper utilisation of tools and procedures provides the basis for the derivation of unified measures of safety, for ship design, as well as for operation and rule development. The elements of the framework, appropriate for different stages of the design process are outlined in this section.

To date ship design practice has focused on balancing technical and economic considerations, with adherence to safety requirements being a design periphery at best, if not a design afterthought. Furthermore, within current ship design practice any safety-related consideration is treated with reference to prescriptive regulations, conformance to which is sought by performing deterministic assessments. In this manner, safety is imposed as a constraint to the design process of a ship, an undertaking that has resulted in the ill-based concept that investment in safety compromises returns. A second observation, closely related, is that this approach is hindering the transfer of knowledge between the design, production and operational phases, thus not allowing the development of competitive designs to be based on a rational basis but rather on the designer's competence.

On this background, the approach presently advocated comprises the following principal characteristics:

- Development of working design frameworks appropriate for various stages of the design process, with particular emphasis paid to the required design input and output for their effective application.
- Utilisation of first-principles tools and techniques for assessment purposes, with the view to adequately take into account prevailing environmental conditions and vessel responses during the design process.
- Transfer of knowledge from the production and operational phases and utilisation within design in the form of input to the working frameworks applicable to the design process.

In so doing, safety is becoming a central life-cycle issue, addressed critically as early as possible within

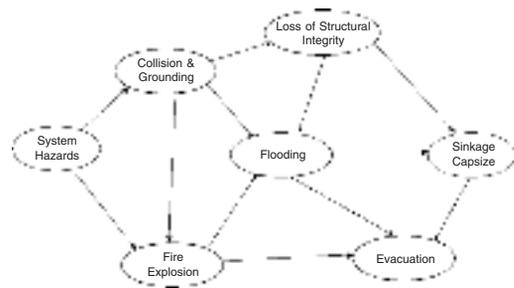


Figure 1. Sequence of scenarios.

design. Appropriate coupling of typical risk assessment techniques with first-principles methods and tools offers the potential for these requirements, not only to provide design input and to be implemented within the design process, but also to assist in the development and assessment of the effectiveness of rules and regulations and in the proposal of appropriate criteria. In this respect, safety assurance is embedded within the ship design process, treated as it should as a core design objective.

The scenarios shown in Figure 1 are meant to provide the “structural links” to be used for the development of the risk-based design framework. Specific elements of the work content include the following:

- In applying first-principles/performance-based approaches, a number of appropriate numerical tools for incidents frequency-of-occurrence prediction and consequence analysis and modelling are deployed. This work is assisted by the updating and completion of the relevant technical data and accident statistics, in order to allow the delivery of comprehensive risk/cost models with reference to potential societal and economic consequences (losses/gains of human life, cargo, property, environment etc.).
- Models addressing the issue of socio-economic implications of shipping (from a organisational/managerial perspective), evaluating individual and societal levels of risk, cost and performance, and finally the way to achieving safety equivalency from a regulatory point of view are required. This information will be integrated into comprehensive risk models (e.g. fault and event trees), which reflect the seriousness of incidents occurring and their potential consequences, with the view to building the reference risk-based design framework.
- The risk-based design framework covers issues such as balance between effects on safety and performance of various risk contributors or choice of appropriate risk control options and the implementation of appropriate design trade-offs in a systematic manner.

### 3 LIFE-CYCLE CONSIDERATIONS

Through the interfacing of top-down (consequence analysis) and bottom-up (frequency prediction) models, assisted where appropriate with comprehensive data and knowledge bases and first-principles tools and techniques pertaining to incident statistics and design and operational measures applicable to risk prevention and mitigation, rational decision support to assist trade-offs between various design and safety indicators is possible. The latter can therefore lead to the development of optimised design solutions.

The various systems of the vessel can be analysed using classical risk analysis techniques, such as Fault Tree Analysis (FTA) and Failure Modes and Effect Analysis (FMEA). An operational procedure that is applied onboard can also be considered as a ship system and analysed using the same techniques. Human effects and interaction can also be modelled within this analysis. Bottom-up models are concerned with the quantification of these systems' representations. When a bottom level cause is considered as initiating, the respective representation is yielding a frequency (likelihood) of the top-level event occurring. Starting from the top event the outcomes (consequences) and their severity are established, utilising the top-down models. The analysis starts with the construction of representations of the chain of events that lead to potential outcomes following an accident. This is being performed in a generic manner, using Event Tree Analysis (ETA). Following this, is the task of establishing the branch probabilities of the event trees. This can be achieved in a number of ways, using: available statistical data, expert judgement or first-principles consequence analysis tools. The overall frequency of the top-level event can be broken down to the expected frequencies of the final outcomes of this event happening. According to the severity of each of the individual outcomes (number of implied fatalities and/or injuries, extent of environmental pollution and implied property loss that includes damage repair, insurance costs, business interruption, etc.), the outcomes can be classified and appropriate actions taken.

Figure 2 shows a breakdown of the generic categories, both technical and operational, of the measures that can be taken to either reduce the frequency of an accident occurring (preventive) or mitigate its consequences. When considering various safetyenhancing measures (also known as risk control options, RCOs) implemented, their costs and benefits can be evaluated and checked using established criteria, for example the Implied Cost to Avert a Fatality (ICAF). Decision support can assist in selecting the best measure available, when taking into account other parameters such as interaction with other functions of the ship.

Risk-Based Design for Safety, as a life-cycle process, should involve all the phases of a vessel,



Figure 2. Generic measures categories.

i.e. design, production and operation, as well as facilitate the exchange of knowledge among these phases. The latter is considered to be of paramount importance, since it is the identified cause for many deficiencies during operation and can result in significant improvements for the whole process.

#### 3.1 Selection of criteria

The criteria to be satisfied should correspond to acceptable levels of risk, as well as to established technical and economic criteria normally applied.

##### 3.1.1 Risk evaluation criteria

There are no established explicit risk evaluation criteria available within the IMO regime to date. There are, however, criteria proposed in a document submitted to IMO for consideration, IMO (2000).

A criterion for risk evaluation is compatible to the presentation form that a risk is expressed. For passenger ships, the following are complementary forms of risk presentation:

- *Individual Risk*, which can be expressed as:
  - A risk of death per year for a specific individual;
  - A Fatal Accident Rate (FAR), which is defined as the number of fatalities per 100 million person-hours at sea.
- *Societal Risk*, which can be expressed as:
  - The Annual Fatality Rate (AFR), which is defined as the long-term average number of deaths per ship year.
  - The F–N curve, which relates the frequency and number of fatalities in accidents.

##### 3.1.2 Design criteria

Typical technical and economic design criteria that could be considered include:

- The requirements for deadweight as expressed by the specified carrying capacity (number of crew and passengers, private cars and trucks).

- The requirement for speed to be fulfilled at minimum required installed power.
- Passenger comfort as expressed by hydrostatic and hydrodynamic properties (GM and accelerations).
- Techno-economic performance as calculated by standard procedures, such as NPV or RFR.

### 3.1.3 Cost-effectiveness assurance

Cost-benefit analysis is a well-known selection technique, which is used when social costs and benefits need to be taken into account to evaluate different alternatives. The assessment is based on the comparison of the benefit gained by the implementation of each alternative, expressed in monetary terms, with the implied cost deriving from implementing the alternative.

## 4 A CASE STUDY

The case study pertains to the application of the developed framework, aiming to provide insight in the proposed procedure. The application focuses on the determination of the number of transverse bulkheads required for effective subdivision of a conventional passenger Ro-Ro vessel, accounting for social and techno-economic benefits, together with considerations of collision preventive measures and evacuability.

### 4.1 Hazards and risk control options considered

An existing North West European passenger Ro-Ro vessel was used as the example ship.<sup>1</sup> Only collision incidents were considered for the application, with the focus on the derivation of an arrangement that reduces the probability of capsizing following large scale flooding. Application of the Fujii model for the prediction of the overall frequency of collision incidents for this vessel, considering her operational route, yields a frequency of  $3.71 \times 10^{-2}$  per ship year. Figure 3 shows the event tree for collision incidents for this case, where all figures are generic except for the overall frequency of collision incidents. In this respect, the frequency for the example ship (assumed to be the struck ship in a collision happening under way that results in a serious casualty involving flooding) was found to be  $1.26 \times 10^{-3}$  per ship year.

As available risk control options, the following design/operational measures have been considered:

- *Collision Avoidance*: Crew collision avoidance training or the presence of a second watch officer on the bridge of the vessel or both.

- *Subdivision*: Varying number of transverse bulkheads.
- *Evacuation*: Two alternative accommodation layouts (Case A and Case B).

### 4.2 Risk and cost-effectiveness analysis

For the various risk control options outlined above, risk and cost-effectiveness calculations have been carried out. The risk analysis for subdivision and evacuability was based on the application of available first-principles tools and techniques, whilst for collision available expert judgement from the literature was used. Available ICAF criteria range between 3 and 8 million Euros, depending on the concerned country and authority, as well as on the transport activity they refer to, IMO (2000). However, it is stated in (DNV Technica 1996) that measures yielding an ICAF value up to 75 million Euros should be carefully evaluated for their benefits, in effect meaning that if there are no more cost-effective alternative measures these should also be considered for possible adoption. Measures having an ICAF value higher than this are normally not considered for implementation.

#### 4.2.1 Subdivision considerations

A damage survivability analysis considering varying number of transverse bulkheads installed below the main vehicle deck was carried out. The probability of survival can be defined as the probability of the significant wave height  $H_s$ , calculated for a given damage condition, *not* exceeding a predetermined significant wave height  $H_{s,90}$  that characterises the area of operation of the vessel (usually calculated excluding the top 10% of the available data, for example, as defined in the Stockholm Agreement for North West Europe). The probability of capsizing, which is the complement of the probability of survival, is calculated using the Static Equivalent Method over a range of predefined conditions and distributions of the relevant design and operational parameters (Monte Carlo simulations), Vassalos & Konovessis (2001).

The results of this analysis were implemented as the corresponding branch probabilities of the event tree (vessel remaining afloat, sinking slowly or capsizing rapidly). In this manner, varying frequency levels for the different outcomes were established corresponding to the number of transverse bulkheads to be considered. The steel weight required for the implementation of each of the arrangements was used as the parameter to trade-off against the available lane metres. This feature was taken into account within a conventional calculation of the Required Freight Rate (RFR). In this respect, trade-offs between safety and cost parameters were taken into account, whilst further trade-offs with performance parameters were not considered. Deriving from relevant literature, DNV Technica (1996), the

<sup>1</sup>Main Particulars: LBP = 156.45 m, B = 27.60 m, D = 8.9 m (main vehicle deck), T = 6.5 m, centre casing on the main vehicle deck.

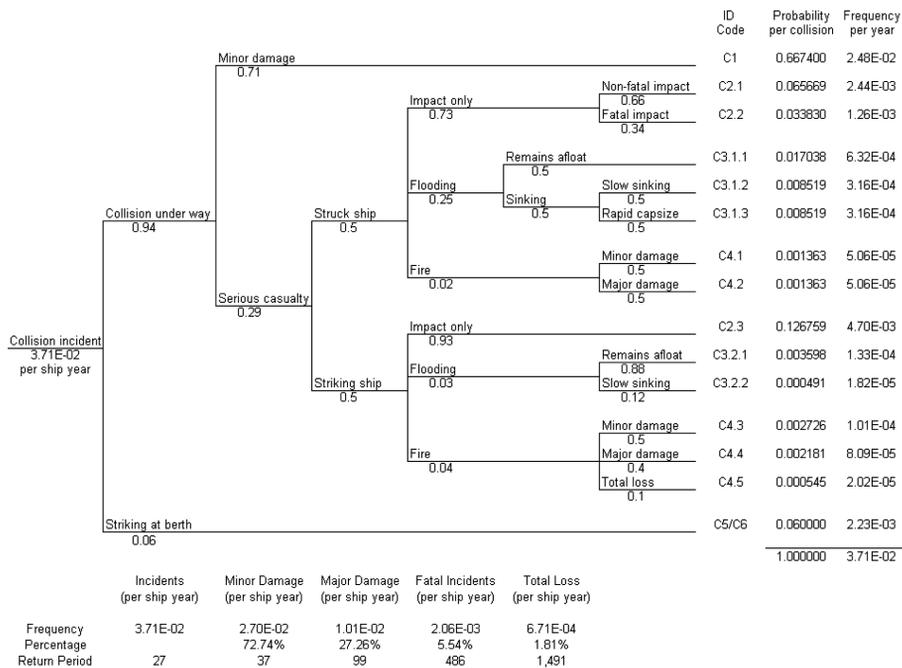


Figure 3. Generic event tree for collision outcomes, DNV technica (1996).

following fatality rates were considered: 2% for the slow sinking case and 72% for the rapid capsizing case. ICAF values were finally calculated, accounting for differential variations of steel and labour costs. These calculations are presented in Table 1 (fatalities reductions and additional costs were calculated with reference to the basis alternative with 8 bulkheads).

The calculations contained in Table 1 indicate that the alternative comprising 14 transverse bulkheads is the most cost-effective over the range of the considered variation, since it achieves the best balance between risk reduction and cost. This conclusion is derived from the fact that the calculated ICAF values demonstrate a local minimum for this alternative arrangement. Of particular interest are also the high ICAF values calculated for the slow sinking case, which are due to the small reduction in fatalities for these cases, raising the point of presence of localised risk evaluation criteria.

When more thorough studies on survivability are contacted, methods that estimate the probability of survival taking time to capsize into account can be used. Work in this area is on-going having already produced useful results on the relation of the critical amount of water on the car deck with the corresponding significant wave height, whilst maintaining a survival time over one hour, Vassalos et al. (1999).

#### 4.2.2 Considerations of collision preventive measures

Measures for prevention of collisions, reducing the frequency of collisions, include a wide range of alternatives that may be implemented. A number of these are contained in various IMO conventions and regulations, such as the Collision Avoidance Regulations or the STCW (watch keeping and navigation). The effect of this kind of measures on the frequency of accidents and the corresponding fatality rates is difficult to quantify, since it is mainly derived from analyses based on expert judgment.

For the purpose of this case study, a 20% reduction on the fatality rates will be considered related to crew training for collision avoidance, and a 10% reduction will be considered for the presence of a second officer at the bridge during navigation. The percentages derive from (SAFER EURORO 1996) and correspond to the reductions on the fatality rates when the above mentioned measures are implemented. The annual present value of collision avoidance training is taken as 46,000 Euros, whilst the cost (salary and overheads) of a second officer is considered to have an annual present value of 108,000 Euros. Table 2 contains the relevant calculations for a subdivision arrangement comprising 14 transverse bulkheads.

These calculations clearly indicate that crew training for collision avoidance is a cost-effective measure,

Table 1. Risk and ICAF calculations for varying number of transverse bulkheads (average number of people on-board 1,500).

	Alternative number of bulkheads	Frequencies of collision outcomes (per ship year)	Fatalities (per ship year)	Fatalities reduction (per ship year)	Additional cost (Euros)	ICAF (million Euros)
Remain afloat	8	$7.65 \times 10^{-4}$				
Slow sinking	8	$4.55 \times 10^{-4}$	0.01365			
Rapid capsizes	8	$4.03 \times 10^{-5}$	0.04352			
Total fatal	8	$4.95 \times 10^{-4}$	0.05717			
Remain afloat	10	$8.30 \times 10^{-4}$				
Slow sinking	10	$3.95 \times 10^{-4}$	0.01185	0.00180	128,206	75.8
Rapid capsizes	10	$3.49 \times 10^{-5}$	0.03769	0.00583	128,206	22.0
Total fatal	10	$4.30 \times 10^{-4}$	0.04954	0.00763	128,206	16.8
Remain afloat	12	$8.68 \times 10^{-4}$				
Slow sinking	12	$3.60 \times 10^{-4}$	0.01080	0.00285	255,458	89.6
Rapid capsizes	12	$3.19 \times 10^{-5}$	0.03445	0.00907	255,458	28.2
Total fatal	12	$3.92 \times 10^{-4}$	0.04525	0.01192	255,458	21.4
Remain afloat	14	$9.29 \times 10^{-4}$				
Slow sinking	14	$3.04 \times 10^{-4}$	0.00912	0.00453	383,971	84.8
Rapid capsizes	14	$2.68 \times 10^{-5}$	0.02894	0.01458	383,971	26.3
Total fatal	14	$3.31 \times 10^{-4}$	0.03806	0.01911	383,971	20.1
Remain afloat	16	$9.66 \times 10^{-4}$				
Slow sinking	16	$2.70 \times 10^{-4}$	0.00810	0.00555	513,046	92.4
Rapid capsizes	16	$2.39 \times 10^{-5}$	0.02581	0.01771	513,046	29.0
Total fatal	16	$2.94 \times 10^{-4}$	0.03391	0.02326	513,046	22.1
Remain afloat	17	$9.75 \times 10^{-4}$				
Slow sinking	17	$2.62 \times 10^{-4}$	0.00786	0.00579	577,798	99.8
Rapid capsizes	17	$2.32 \times 10^{-5}$	0.02506	0.01846	577,798	31.3
Total fatal	17	$2.85 \times 10^{-4}$	0.03292	0.02425	577,798	23.8

Table 2. Risk and ICAF calculations for collision preventive measures (average number of people on-board 1,500).

	Alternative number of bulkheads	Fatalities reduction (subdivision)	Fatalities reduction (training)	Fatalities reduction (officer)	Fatalities reduction (both)
Remain afloat	14				
Slow sinking		0.00453	0.00544	0.00498	0.00588
Rapid capsizes		0.01458	0.01749	0.01604	0.01895
Total fatal		0.01911	0.02293	0.02102	0.02484
Additional cost (Euros)		383,971	430,125	491,663	537,817
	Alternative number of bulkheads	ICAF (subdivision) (million Euros)	ICAF (training) (million Euros)	ICAF (officer) (million Euros)	ICAF (both) (million Euros)
Remain afloat	14				
Slow sinking	14	84.8	79.1	98.7	91.5
Rapid capsizes	14	26.3	24.6	30.7	28.4
Total fatal	14	20.1	18.8	23.3	21.7

since it reduces further the ICAF value for the considered subdivision arrangement, despite the increased cost, whilst the presence of a second officer on the bridge is by no means cost-effective. Implementation of both measures may be recommended, if further reduction of the frequency of collisions is deemed necessary.

#### 4.2.3 Considerations of evacuability

For evacuation of Ro-Ro vessels, the time available to evacuate passengers and crew is likely to be the big unknown (although it may be predicted by computer simulations and controlled through active decision support/active flooding to remain afloat in a stable

Table 3. Risk and ICAF calculations for evacuation alternatives (average number of people on-board 1,500).

Alternatives	Frequencies of collision outcomes (per ship year)	Fatalities (per ship year)	Fatalities reduction (per ship year)	Additional cost (Euros)	ICAF (million Euros)	
Remain afloat	14 BHD	$9.29 \times 10^{-4}$				
Slow sinking	(Generic	$3.04 \times 10^{-4}$	0.00912	0.00453	383,971	84.8
Rapid capsizes	Fatality	$2.68 \times 10^{-5}$	0.02894	0.01458	383,971	26.3
Total fatal	Rates)	$3.31 \times 10^{-4}$	0.03806	0.01911	383,971	20.1
Remain afloat	14 BHD	$9.29 \times 10^{-4}$				
Slow sinking	(Case A	$3.04 \times 10^{-4}$	0.00912	0.00453	383,971	84.8
Rapid capsizes	Fatality	$2.68 \times 10^{-5}$	0.00804	0.03548	383,971	10.8
Total fatal	Rates)	$3.31 \times 10^{-4}$	0.01716	0.04001	383,971	9.6
Remain afloat	14 BHD	$9.29 \times 10^{-4}$				
Slow sinking	(Case B	$3.04 \times 10^{-4}$	0.00912	0.00453	383,971	84.8
Rapid capsizes	Fatality	$2.68 \times 10^{-5}$	0.02412	0.01940	383,971	19.8
Total fatal	Rates)	$3.31 \times 10^{-4}$	0.03324	0.02393	383,971	16.0

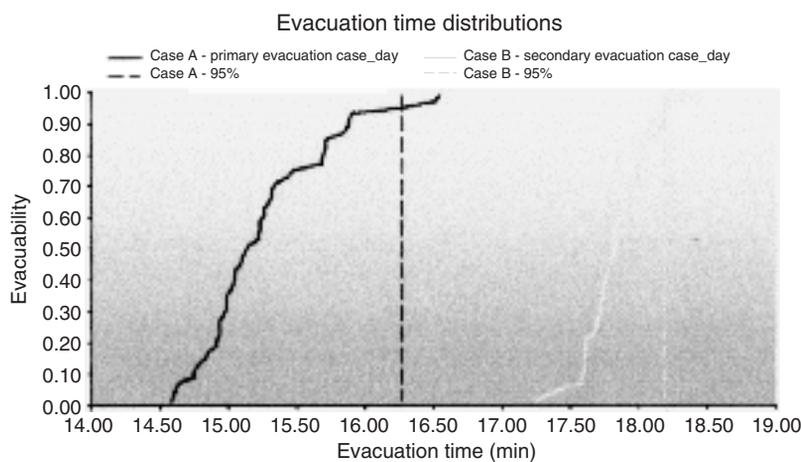


Figure 4. Probability density functions of the total evacuation.

condition). *Herald of Free Enterprise* capsized in a few minutes, *Estonia* in less than 1½ hours, the Greek ferry *Express Samina* went down in about 40 minutes, while *Titanic* took 2 hours 40 minutes to sink. In several accidents where fire has broken out onboard, the vessel involved survived (remaining afloat) for many hours or even days. However, people have been injured or lost their lives, often due to toxic smoke inhalation (e.g. *Scandinavian Star*, *Sun Vista*).

SOLAS II-2/28-1.3, IMO (2002), requires Ro-Ro passenger vessels' (built after July 1st 1999) escape way layout to undergo evacuation analysis. The simulated evacuation time should be less than 60 minutes. The 60 minutes total evacuation time for Ro-Ro passenger ships comprises 30 minutes for mustering and 30 minutes for embarkation and launching of lifesaving appliances (SOLAS III/21-1.4). For this duration, the

assumption is made that the survivability of the vessel due to progressive flooding, which represent the most prevalent cause of Ro-Ro ship losses, is ensured. This time is congruent with the 60 minutes structural fire integrity of any independent main vertical zones (subdivided by A-60 class divisions).

The term *Evacuability* is defined to be the probability of an environment being completely evacuated no later than a given time elapsed after the alarm went off, in a given state of the environment and a given state of initial distribution of people onboard. With this formalism a sound rule may be proposed, e.g., *Evacuability (60 min., entire ship- worst anticipated conditions-, worst passenger distribution) > 0.99*, Vassalos et al. (2002). Figure 4 illustrates the derived probability density functions for the total evacuation times of two alternative arrangements. For an evacuation time of

Table 4. F–N Curve for the case study.

Number of bulkheads	Frequency of N or more fatalities (per year)					
	N = 1	N = 11	N = 68	N = 130	N = 585	N = 1047
8	$3.94 \times 10^{-3}$	$1.11 \times 10^{-3}$	$9.53 \times 10^{-4}$	$5.54 \times 10^{-4}$	$2.36 \times 10^{-4}$	$7.83 \times 10^{-5}$
10	$3.88 \times 10^{-3}$	$1.05 \times 10^{-3}$	$8.87 \times 10^{-4}$	$5.14 \times 10^{-4}$	$2.12 \times 10^{-4}$	$7.07 \times 10^{-5}$
12	$3.84 \times 10^{-3}$	$1.01 \times 10^{-3}$	$8.49 \times 10^{-4}$	$4.89 \times 10^{-4}$	$1.98 \times 10^{-4}$	$6.63 \times 10^{-5}$
14	$3.79 \times 10^{-3}$	$9.48 \times 10^{-4}$	$7.87 \times 10^{-4}$	$4.52 \times 10^{-4}$	$1.75 \times 10^{-4}$	$5.90 \times 10^{-5}$
16	$3.74 \times 10^{-3}$	$9.11 \times 10^{-4}$	$7.50 \times 10^{-4}$	$4.29 \times 10^{-4}$	$1.62 \times 10^{-4}$	$5.48 \times 10^{-5}$
17	$3.73 \times 10^{-3}$	$9.02 \times 10^{-4}$	$7.41 \times 10^{-4}$	$4.24 \times 10^{-4}$	$1.59 \times 10^{-4}$	$5.37 \times 10^{-5}$

18 minutes, evacuability equals to 1.00 for Case A, whilst for Case B evacuability is equal to 0.60. Making the assumption that only half the people survive during this evacuated time (to remedy for the effects of exposure at the sea environment and incidents related to embarkation and lowering of the LSAs), as well as accounting for the fact that there is no significant cost difference between the two cases, fatality rates are assumed equal to 20% for Case A and 60% for Case B.

#### 4.2.4 F–N curve

Table 4 illustrates the benefits gained by considering increased number of transverse bulkheads in the form of selected values of cumulative frequencies of N or more fatalities. The derived figures indicate a similar result with the cost-effectiveness analysis in that the benefit gained when considering more than 14 bulkheads installed is significantly reduced when compared with the benefit gained up to that point, especially for incidents involving large number of fatalities as, for example an incident involving large scale flooding (for N = 585, the benefit of installing 10 bulkheads is 10% over installing 8 bulkheads, for 12 bulkheads becomes 16%, for 14 it is 26%, for 16 bulkheads is 31% and finally for 17 the derived percentage is 33%).

## 5 CONCLUSIONS

A methodology targeting holistic design solutions, by setting global design goals, through the integration of safety-related considerations in the design process has been described. Expected benefits likely to derive from adopting such a procedure include:

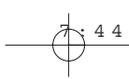
- A methodological framework for the risk-based design, whilst keeping costs at an acceptable level;
- Improved knowledge and related data on the risks associated with an incident at sea involving

collision, grounding, large scale flooding, passenger evacuation, seaworthiness, fire/explosion and ship systems hazards;

- Improved definition of risk evaluation criteria for safety and environmental protection;
- Improved methods/models for probability of occurrence and consequences of risks.

## REFERENCES

- DNV Technica 1996. Safety Assessment of Passenger Ro-Ro Vessels. Joint North West European Research Project Methodology Report and Appendices.
- International Maritime Organisation (IMO) 2000. Formal Safety Assessment: Decision Parameters including Risk Acceptance Criteria. *Maritime Safety Committee*. 72nd Session, Agenda Item 16, MSC72/16, Submitted by Norway, 14 February 2000.
- International Maritime Organisation (IMO) 2002. Interim Guidelines for Evacuation Analyses for New and Existing Passenger Ships. *Maritime Safety Committee*. Circular 1033, 6 June 2002.
- SAFER EURORO 1998. First Year Report of the Risk Assessment Team. *Thematic Network "Design for Safety: An Integrated Approach to Safe European Ro-Ro Ferry Design"*.
- Vassalos, D. 1999. Shaping Ship Safety: The Face of the Future. *Marine Technology* 36(2): 61–73.
- Vassalos, D., Jasionowski, A., Dodworth, K., Allan, T., Matthewson, B. & Paloyannidis, P. 1999. Time-Based Survival Criteria For Ro-Ro Vessels. *Transactions of RINA* 18 pp.
- Vassalos, D. & Konovessis, D. 2001. Damage Survivability of Floating Marine Structures – A Probabilistic Approach. *Proceedings of the Twentieth International Conference on Offshore Mechanics and Arctic Engineering (OMAE 2001)* Paper No. OFT-1285, 3–8 June 2001, Rio de Janeiro, Brazil, 8 pages.
- Vassalos, D., Christiansen, G., Kim, H.S., Bole, M. & Majumder, J. 2002. Evacuability of Passenger Ships at Sea. *SASMEX 2002*. Amsterdam, The Netherlands.



## Availability and failure intensity under imperfect repair virtual age model

J.K. Vaurio

Fortum Power and Heat Oy, Loviisa, Finland & Lappeenranta University of Technology, Lappeenranta, Finland

**ABSTRACT:** This paper develops analytical and numerical techniques to determine two important component characteristics, the failure intensity and the availability, when repairs reduce the virtual age of a unit. Finite repair times are taken into account. An exact Volterra integral equation and an approximate solution are provided for the intensity when component ages during operation and during repairs. A numerical technique is developed and illustrated for the alternative case, i.e. when ageing stops during repairs. The asymptotic behaviour is described in terms of two measures of the age-dependent expected time to the next failure.

### 1 INTRODUCTION

Components are usually assumed to be “as good as new” or “as bad as old” following repair. With perfect repair the times between failures are equally distributed and mutually independent, and the failure-repair process in an alternating renewal process (RP). In the latter minimal repair process the future failure probability of a unit operating at time  $t$  is independent of events before  $t$ , i.e. the same as if the unit never failed before  $t$ . When repair times are negligible, this process is called a non-homogeneous Poisson process (NHPP) because the number of failures in any finite time interval obeys Poisson distribution. Practical analytical and numerical techniques are available to calculate the failure intensity for these processes when repair times are negligible, given that numerical values are available for component reliability parameters. The failure intensity and the availability calculation with finite repair times usually calls for approximations or numerical solutions of integral equations (Vaurio 1997). In reality, the RP assumptions are hardly valid unless the unit is replaced at failure. The existence of truly minimal repairs is also questionable.

A few models have been developed for more general imperfect repairs that make the unit “better than old but worse than new” after repair. Virtual age models are based on the assumption that after repair the unit behaves like a younger unit that never failed. Using this concept Kijima et al. (Kijima et al. 1988) have developed a basic integral equation and an approximate numerical solution method for the failure intensity in the special case of zero repair times when each repair can reduce only the age accrued

after the previous repair. This paper develops other perceptible analytical and numerical techniques to determine two interesting quantities in system reliability and risk analyses, the failure intensity and the availability, both with finite repair times. Taking into account finite repair times is the main contribution. This is done in two ways. An exact Volterra integral equation and an approximate solution are provided for the intensity when component ageing continues during repairs. A numerical technique is developed and illustrated for the alternative case, i.e. when ageing stops during repairs. Asymptotic behaviour of failure intervals are also studied.

#### 1.1 Notation

$A(t)$	Availability, $A(t) = 1 - u(t)$
$F(x)$	$1 - e^{-H(x)}$ , Cumulative distribution of time to first failure, $X_1$
$f(x)$	Probability density of $X_1$ , $f(x) = dF(x)/dx$
$G(t)$	Cumulative distribution of the repair time
$G(t)$	$1 - G(T)$
$H(t)$	Cumulative hazard, integral of $h(t)$ over $(0, t)$
$H(t)$	Hazard rate; $h(t)dt = dH(t)$ is the conditional probability of failure in $(t, t + dt)$ , given that no failure occurred in $(0, t)$
$R(t)$	Reliability, $R(t) = 1 - F(t)$
$u(t)$	Unavailability, $u(t) = 1 - A(t)$
$t_f$	Mean time to first failure, integral of $R(t)$ over $(0, \infty)$
$\tau_r$	Mean repair time (duration)
$\tau$	Fixed repair time
$W(t)$	Expected number of failures in $(0, t)$
$w(t)$	Failure intensity, $w(t) = dW(t)/dt$
$X_n$	Length of the $n$ th lifetime (operational period)

## 2 BASICS OF PERFECT AND MINIMAL REPAIRS

To justify an approach to approximate solutions, some quasi-static or asymptotic results are pointed out for perfect (RP) and minimal repair processes. First, it is well known that the failure intensity of RP in time approaches asymptotically  $w \approx 1/(t_f + \tau_r)$  and the unavailability  $u \approx w\tau_r$ .

Secondly, it is well known that the expected number of failures in time  $t$  for NHPP (minimal repair) with instantaneous repairs is  $W(t) = H(t)$  and the hazard rate  $h(t)$  equals the intensity  $w(t)$ . The unavailability vanishes with instantaneous repairs.

If repair times are finite with minimal repair and the unit continues ageing during repairs, it has been shown (Vaurio 1997, Equation 33) that a good approximation for both small and large  $t$  is

$$w(t) \cong h(t) / [1 + h(t) \int_0^t \bar{G}(t') dt'] \tag{1}$$

approaching  $\rightarrow h(t) / [1 + \tau_r h(t)]$  for large  $t$ , and the availability  $A(t) = w(t)/h(t) \rightarrow 1 / [1 + \tau_r h(t)]$ . These results motivate development of approximation  $w(t) \cong 1/(t_m + \tau_r)$ , where  $t_m$  is the time to the next expected failure, satisfying  $H(t + t_m) - H(t) = 1$ . With imperfect repairs  $t_f$  and/or  $t_m$  will be replaced with a measure of time to the next failure when a unit has a certain virtual age.

### 2.1 Unavailability

It is assumed throughout this paper that repair times (durations) are identically distributed and mutually independent. Then the exact relationship between the unavailability and failure intensity with all models is

$$u(t) = \int_0^t w(t') \bar{G}(t - t') dt', \tag{2}$$

the sum of the probabilities of all failures for which repair is not completed before  $t$ . With a fixed repair time  $\tau$ , the unavailability is exactly  $u(t) = W(t)$  for  $t \leq \tau$  and  $u(t) = W(t) - W(t - \tau)$  for  $t > \tau$ . With a general repair time distribution, when  $w(t)$  changes little within one repair time, Equation 2 yields  $u(t) \cong w(t)\tau_r$  for large  $t$ .

Because Equation 2 is common to all models, we can now concentrate on solving the intensity  $w(t)$ .

## 3 THE VIRTUAL AGE MODEL

### 3.1 Instantaneous repairs

Let  $V_n$  be the virtual age of a unit immediately after the  $n$ th repair. This means that the hazard rate of the

unit at time  $x$  after the repair is  $h(V_n + x)$ . The cumulative distribution of  $X_n$  is

$$F_n(x) = 1 - e^{-H(x+V_{n-1})+H(V_{n-1})} \tag{3}$$

If an instantaneous repair is completed at time  $t$  and the virtual age  $V(t)$  immediately at  $t+$  is known, one can define the distribution of the time to the next failure as a conditional distribution

$$Q[x | V(t)] = 1 - e^{-H[x+V(t)]+H[V(t)]} \tag{4}$$

The mean time to the next failure of a component at age  $V(t)$  is

$$t_f[V(t)] = \int_0^\infty e^{-H[x+V(t)]+H[V(t)]} dx \tag{5}$$

The time to the next expected failure  $t_m[V(t)]$  is the 63th percentile of  $Q(x | V)$  corresponding to the solution of equation

$$H[t_m + V(t)] - H[V(t)] = 1. \tag{6}$$

A rough failure intensity approximation is  $w(t) \cong 1/t_{av}(t)$  where  $t_{av}(t)$  equals  $t_m[V(t)]$  or  $t_f[V(t)]$ . Note that both  $t_f$  and  $t_m$  depend on time  $t$  only through the virtual age  $V(t)$ . It is essential that  $V(t)$  is known, to be able to solve the average lifetime parameters. This is the case with the following virtual age model (Kijima Type I). It is assumed that the  $n$ th repair can remove damages incurred during the  $n$ th lifetime and reduces the additional age  $X_n$  to  $\alpha X_n$ , where  $0 \leq \alpha \leq 1$ . This means that

$$V_n = V_{n-1} + \alpha X_n = \sum_{k=1}^n X_k, V_0 = 0.$$

Thus, when repairs take no time, the age of a unit after repair at time  $t$  is known  $V(t) = \alpha t$ , no matter how many repairs have taken place before. Three theorems in the Appendix indicate close relationships between  $t_m(V)$ ,  $t_f(V)$  and  $h(V)$  in many practical situations. Exploratory numerical studies have been carried out about the validity of  $w(t) \cong h(t)$  and  $w(t) \cong 1/t_{av}(t)$  with a Weibull distribution

$$H(t) = \left[ \frac{t}{\eta} \right]^\beta \tag{7}$$

The initial values at  $V(0) = 0$  are  $t_m(0) = \eta$  and  $t_f(0) = \eta \Gamma[(1 + \beta)/\beta]$ . For  $\beta > 1$ ,  $h(t)$  is increasing and  $t_f(0) < t_m(0)$ . Equation 6 yields

$$t_m(V) = \left[ 1 + \left( \frac{V}{\eta} \right)^\beta \right]^{1/\beta} \eta - V.$$

In case  $\beta = 2$ ,  $t_f(V)$  can be solved numerically from Equation 5. Studies have shown that the approximation  $w(t) \cong 1/t_{av}(t)$  is not quite satisfactory for small  $t$  ( $t < 2\eta$ ) even if  $t_m$  and  $t_r$  are rather close to each other for  $t > 2\eta$ , and both are between the limits  $1/h(V)$  and  $1/h[V + 1/h(V)]$ .

For small enough  $t$  when failures are unlikely, the intensity is  $w(t) \cong h(t)$ . An improved overall approximation is a weighted average of two solutions, one valid for small  $t$  and the other one for large  $t$ , i.e.  $w(t) \cong R(t)h(t) + F(t)/t_{av}(t)$ . This form is valid rather well unless the standard deviation of  $X_1$  is small compared to  $t_{av}(0)$ . In the special case of constant  $h(t) = \lambda$  the approximation is exact  $w(t) = \lambda$  because  $t_r = t_m = 1/\lambda$ . Studies with the Weibull example have shown that  $h(t)$  is close to  $f(t) + F(t)/t_m(t)$  and  $f(t) + F(t)/t_f(t)$ , as it should when  $\alpha = 1$ . The approximations slightly overestimate the intensity for increasing  $h(t)$ , but the accuracy is reasonable over a long period.

Let us now evaluate the integral of the approximation, the expected number of failures

$$W(t) \cong F(t) + \int_0^t \frac{F(t')}{t_f[V(t')]} dt' \tag{8}$$

in an example that was solved exactly in Kijima et al. (1988). The example has

$$Q(x | V) = e^{-aV}(1 - e^{-bx}) + (1 - e^{-aV})(1 - e^{-bx}), a, b > 0. \tag{9}$$

In this case  $t_f$  can be solved from Equation 5 in a closed form

$$t_f(V) = \int_0^\infty [1 - Q(x | V)] dx = \frac{1}{a} e^{-aV} + \frac{1}{b} (1 - e^{-aV}), \tag{10}$$

which is a function of time through  $V = \alpha t$ . With  $F(t) = Q(x | 0)$  Equation 8 can also be integrated as

$$W(t) = 1 - e^{-at} + bt + \frac{b^2}{\alpha a(b-a)} \ln \left[ \frac{a + (b-a)e^{-a\alpha t}}{b} \right]. \tag{11}$$

To verify the accuracy of this formula it is compared in case  $\alpha = 1$  with the exact solution of Kijima et al. (1988) in Table 1 for the parameter values  $(a, b) = (1.5, 1)$  and  $(1, 2)$ .

The derivative  $w(t) \cong a$  can be observed for small  $t$  and  $w(t) \cong b$  for large  $t$ . The approximation overestimates in case of increasing hazard rate ( $b > a$ ) and underestimates in the opposite case ( $b < a$ ). It can be shown that in both cases the integral hazard  $H[V(t)]$  is less accurate than the suggested approximation (Eq. 8).

Table 1. Expected number of failures in time  $t$  for two cases.

t	a = 1.50, b = 1.00		a = 1.00, b = 2.00	
	W(t) exact	W(t) approx.	W(t) exact	W(t) approx.
0.10	0.1498	0.1495	0.1002	0.1002
0.30	0.4458	0.4403	0.3037	0.3040
0.50	0.7330	0.7155	0.5150	0.5172
0.70	1.0091	0.9748	0.7368	0.7436
0.90	1.2737	1.2206	0.9704	0.9855
1.10	1.5274	1.4555	1.2165	1.2439
1.50	2.0067	1.9017	1.7465	1.8099
2.50	3.1003	2.9464	3.2722	3.4609
3.50	4.1277	3.9565	5.0135	5.3162
4.50	5.1352	4.9587	6.8840	7.2605
5.50	6.1371	5.9592	8.8229	9.2396
6.50	7.1376	6.9593	10.7954	11.2319
7.50	8.1387	7.9594	12.7834	13.2291
8.50	9.1378	8.9594	14.7783	15.2280
10.00	10.6378	10.4594	17.7756	18.2275
12.00	12.6378	12.4594	21.7748	22.2274
14.00	14.6378	14.4594	25.7747	26.2274
16.00	16.6378	16.4594	29.7747	30.2274
18.00	18.6378	18.4594	33.7747	34.2274
20.00	20.6378	20.4594	37.7747	38.2274
23.00	23.6378	23.4594	43.7747	44.2274

### 3.2 Finite repair times with ageing during repairs

In this section each repair takes a finite time  $\tau$ , and the unit ages also during repair. The effect of repairs is as follows. The  $n$ th repair reduces the latest accumulated age  $X_n + \tau$  to  $\alpha(X_n + \tau)$ . Then the virtual age immediately after repair completion at  $t$  is again  $V(t) = \alpha t$ , no matter how many failures occurred before. It is now possible to find the exact integral equation for  $w(t)$ :  $w(t)dt$  is the sum of the expected first failure and failures at  $t'$  repaired at  $t' + \tau < t$  with the next failure at  $(t, t + dt]$ . Thus,

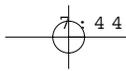
$$w(t) = f(t), \text{ for } 0 < t \leq \tau, \tag{12a}$$

$$w(t) = f(t) + \int_0^{t-\tau} w(t')h[t - (t'+\tau) + V(t'+\tau)]e^{-H[t - (t'+\tau) + V(t'+\tau)] + H[V(t'+\tau)]} dt', \tag{12b}$$

$t > \tau$ .

This yields Equation 14 of Kijima et al. (1988) as the special case ( $\tau = 0$ ). The integral of 12 is

$$W(t) = F(t) \text{ for } t \leq \tau, \tag{13a}$$



$$W(t) \equiv F(t) + \int_{\tau}^t \frac{F(t')}{\{t_{av}[V(t')] + \tau\}} dt', t > \tau, \quad (13b)$$

where  $t_{av}$  can be  $t_f[V(t')]$  or  $t_m[V(t')]$ .

### 3.3 Finite repair times without ageing during repairs

If the unit does not age during repair, the virtual age after a repair completion of  $n$ th failure at time

$$t = \sum_{k=1}^n (X_k + \tau)$$

is  $V(t) = \alpha(t - n\tau)$ . Now  $n$  is a random number at a fixed time  $t$ , and  $V(t)$  is a random function not known in advance. The average age after repairs completed around  $t$  is approximately

$$V(t) = \alpha[t - W(t)\tau]. \quad (14)$$

Then Equations 5 and 6 yield times  $t_f$  and  $t_m$  that may be used to calculate the expected number of failures up to time  $t$  from 13. Now  $W(t)$  appears on both sides of 13 and it is necessary to use a numerical procedure.

## 4 NUMERICAL PROCEDURE AND AN EXAMPLE

A numerical procedure to solve  $W(t)$  based on Equations 13 & 14 for  $t_i = i\Delta$ ,  $i = 0, 1, 2, \dots$  with small  $\Delta \ll \tau$  is as follows:

0° Initial values:  $W_0 = 0, u_0 = 0, V_0 = 0$ ;

1° For  $t_i \leq \tau$ :  $W_i = u_i = F(t_i)$ ;

For  $t_i > \tau$ :

$$W_i = W_{i-1} + F(t_i) - F(t_{i-1}) + \frac{F(t_i)\Delta}{t_m(V_{i-1}) + \tau};$$

$$u_i \text{ from Equation 2, or } u_i = (W_i - W_{i-1})\tau/\Delta;$$

2°  $V_i = \alpha(t_i - W_i\tau)$ ;

3° Solve  $t_m(V_i)$  from Equation 7; In case of Weibull model

$$t_m(V_i) = [1 + (\frac{V_i}{\alpha})^\beta]^{1/\beta} \eta - V_i;$$

4°  $i \rightarrow i + 1$ , return to 1°.

The availability  $A(t) = 1 - u(t)$  is presented in Figure 1 in case of Weibull hazard (7) with values  $\alpha = 0.25$ ,  $\beta = 3.0$ ,  $\tau = 0.05$ ,  $\eta = 1$ . The expected number of failures  $W(t)$  is presented in Figure 2. An alternative is to solve  $t_f(V_i)$  from Equation 5 and use it in place of  $t_m(V_i)$  in steps 3° and 1°.

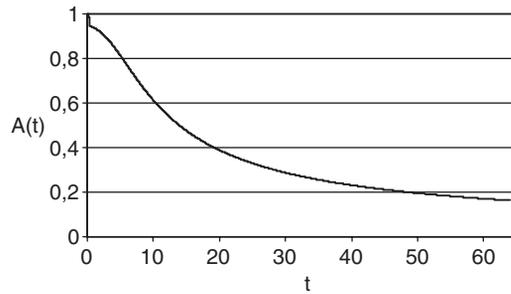


Figure 1. Availability with Weibull hazard;  $\alpha = 0.25$ ,  $\beta = 3.0$ ,  $\tau = 0.05$ ,  $\eta = 1$ .

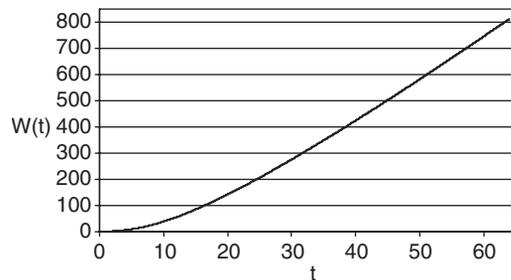


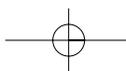
Figure 2. Expected number of failures with Weibull hazard;  $\alpha = 0.25$ ,  $\beta = 3.0$ ,  $\tau = 0.05$ ,  $\eta = 1$ .

## 5 CONCLUSIONS AND DISCUSSION

Analytical and numerical techniques have been developed to determine the failure intensity and the availability of a unit when repairs take time and reduce the virtual age. An exact Volterra integral equation and approximate solutions were provided when repairs take time and component ageing continues during repairs. A numerical technique was developed and illustrated when ageing stops during repairs. The approximations are reasonable when the component lifetime variance is not very small.

One advantage of this technique is to avoid iterative techniques and Monte Carlo simulations that would be expensive or prohibitive for large systems with hundreds of components. Analytical expressions are also useful when one needs to estimate parameters for the model. For large  $t$  and increasing  $h(t)$  studies so far indicate that  $W_i(t) \approx H(\alpha t)/\alpha$  (in case of instantaneous or fast repair). This could be fitted to the observed number of failures  $N(t)$  as a “quick and easy” estimation of  $\alpha$  when the parameters (e.g.  $\eta$  and  $\beta$ ) of a new unit are known.

The principle of the suggested method can be used for imperfect repair models other than Kijima types.



For example, if minimal repairs are performed during a warranty period  $0 < t < T_w$ , one can use Equation 1 for this period. If repairs after that bring the unit always to age  $V_w$ , slightly modified Equations 8 or 13 may be used for  $t > T_w$ , with  $V(t')$  replaced by  $V_w$ .

Numerical examples have indicated that the suggested approximations may have some bias. With increasing  $h(t)$  they tend to overestimate  $W(t)$  because they underestimate the times between failures around  $t$ . The intensity at  $t$  is more related to the hazard rate and age at an earlier point in time, roughly at  $t - t_f$  or  $t - t_m$ . Such improvements and the relative merits of  $t_f(t)$  and  $t_m(t)$  in the current formalism remain subject to future work.

## REFERENCES

- Vaurio, J.K. 1997. Reliability characteristics of components and systems with tolerable repair times. *Reliability Engineering and System Safety* 56: 43–52.
- Kijima, M., Morimura, H. & Suzuki, Y. 1988. Periodical replacement problem without assuming minimal repair. *European Journal of Operational Research* 37: 194–203.

## APPENDIX

### Theorem A.

If  $h(t)$  is non-decreasing for  $t$  larger than some  $t^*$ , then bounds of  $t_m = t_m(t)$  for virtual age  $V = V(t) > t^*$  are

$$\frac{1}{h(V)} \geq t_m \geq \frac{1}{h[V + \frac{1}{h(V)}]}.$$

If  $V(t)$  and  $h(t)$  increase without limit for  $t \rightarrow \infty$ , the bounds are tight for large  $t$  and  $t_m \rightarrow 1/h[V(t)]$ .

*Proof:* From the definition  $H(t_m + V) - H(V) = 1$  and monotonic  $h(t)$  follows first  $h(V)t_m \leq 1$  (the first inequality) and  $h(V + t_m)t_m \geq 1$ ; then  $V + 1/h(V) \geq V + t_m$  leads to the second inequality. With increasing  $h[V(t)]$  the bounds merge for increasing  $t$ .

### Theorem B.

If  $h(t)$  is asymptotically constant for increasing  $t$  and  $V(t)$  is asymptotically increasing without limit or is asymptotically constant, then both  $t_m(t) \rightarrow 1/h[V(t)]$  and  $t_f(t) \rightarrow 1/h[V(t)]$  for large  $t$ .

*Proof:* The condition  $H(t_m + V) - H(V) = 1$  with asymptotically constant  $h[V(t)]$  yields  $h[V(t)]t_m \rightarrow 1$ .

The definition (Equation 5) of  $t_f(t)$  becomes asymptotically

$$t_f \rightarrow \int_0^{\infty} e^{-h(V)x} dx = 1/h(V).$$

For finite  $t$  it may be more useful to know the bounds of  $t_m$  and  $t_f$  if the bounds of  $h(t)$  are known:

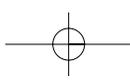
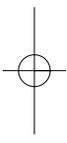
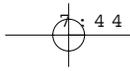
*Corollary:* If  $h(t)$  is known to be between some bounds  $h_a$  and  $h_b$  for all  $t > t^*$ , then both  $t_m$  and  $t_f$  are between  $1/h_b$  and  $1/h_a$  for  $V(t) > t^*$ .

*Proof:* This follows from the fact that there is a  $y$  such that  $H(V + x) - H(V) = h(y)x$  and  $V \leq y \leq V + x$ , and  $h(y)$  then is between  $h_a$  and  $h_b$  when  $V > t^*$ .

### Theorem C.

If  $h(t)$  is non-decreasing for  $t > t^*$ , then  $t_f(t) \leq 1/h[V(t)]$  for  $V(t) < t^*$ .

*Proof:* The non-decreasing  $h(t)$  means  $H(x + V) - H(V) \geq h(V)x$  for  $V \geq t^*$ . From the definition (Equation 5) then follows  $t_f \leq 1/h(V)$  for  $V > t^*$ .



## Quantification and uncertainties of common cause failure rates and probabilities

J.K. Vaurio

Fortum Power and Heat Oy, Loviisa, Finland & Lappeenranta University of Technology, Lappeenranta, Finland

**ABSTRACT:** Simultaneous failures of multiple components due to common causes at random times are modelled for standby safety systems by multiple-failure rates rather than probabilities per demand. Extensions and improvements are made to estimating such rates from single- or multiple-plant event data with uncertainties, and to determine basic common cause event probabilities for explicit fault tree models in terms of the rates, test intervals, test schedules and repair policies. Such models are needed especially in standby safety system reliability analysis, testing optimisation and in risk-informed applications. The probabilities are derived such that the correct time-average system unavailability can be obtained with a single fault tree quantification. Improvements are made in the rate estimation with generalised impact vectors, and the probabilities now include higher-order terms and are independent of the system logic (success criterion).

### 1 INTRODUCTION

Common cause events are defined as events that cause simultaneous failed states of multiple components due to a common cause. Such common cause failures (CCF) often dominate the unavailability of a standby safety system designed to react to a threatening incident. Most earlier CCF-models still in use are based on constant probabilities per demand, and generic ratios (alpha- or beta-factors or multiple Greek letters) between them. Failures that occur at random times in reality have to be modeled by general multiple-failure rates  $\lambda_i, \lambda_{ij}, \lambda_{ijk}, \dots$  etc., defined so that  $\lambda_{ijk} \cdot dt$  is the probability of event failing specific components  $i, j, \dots$  in a small time interval  $dt$ . These failures remain latent in a standby system until discovered by a scheduled test. Components are tested periodically to detect and repair possible failures. Because single failures and CCF can occur at any time, the system unavailability can be a complicated function of time in terms of the event rates, test intervals, test scheduling and repair policies. When a system fault tree is drawn and the system unavailability is computed step by step as a time-dependent function, the time-dependent CCF event probabilities can be determined as

$P[Z_{ij\dots}(t)] = \lambda_{ijk\dots}(t - T_t) =$  probability of failed states of components  $i, j, k, \dots$  at time  $t$  due to a common cause failing exactly these components simultaneously with rate  $\lambda_{ijk\dots}$ , when the last possible discovery (test) and repair of such failure was at  $T_t$ .

In fault tree models such basic events are input through OR-gates to components  $i, j, k, \dots$ , as illustrated in Figures 1 and 2. Modern computer codes for fault tree quantification should use such models and input data, especially for on-line monitoring of system unavailability or risk. This model properly describes the random entry of CCF's and provides correct quantification of the time-dependent and average unavailabilities of a system, as explicit functions of

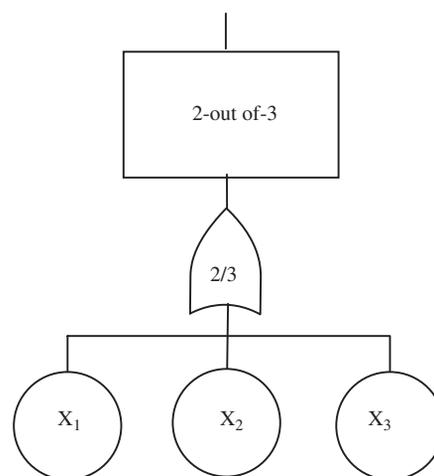


Figure 1. Component-level fault tree (example).

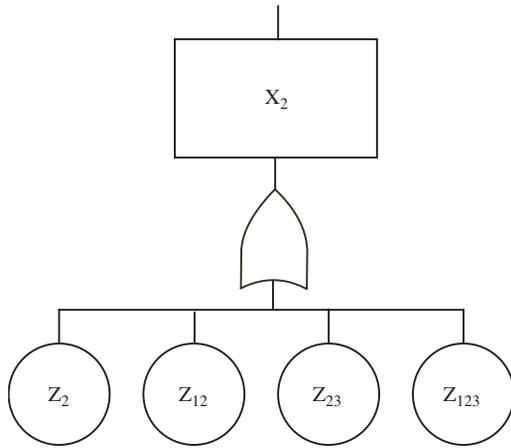


Figure 2. Component event  $X_2$  modelled by cause-events  $Z_{ij}$ .

test intervals and schedules. Unlike the probability-per-demand models, this model allows risk and cost based optimisation of test intervals.

The first topic of this paper deals with estimation of the rates  $\lambda_{ijk}$ ... under uncertainties associated with incomplete records and ambiguities of event observations and interpretations. The moments of the rates are obtained with a method that extends earlier results (Mosleh et al. 1989, 1993, Siu & Mosleh 1989, Vaurio 1994a) to more complex observations.

The second problem solved here is: how to define the input probabilities of a fault tree model so that the correct time-average risk or system unavailability can be obtained with a single fault tree computation, avoiding the multiple step-by-step calculations discussed above. The following features extend the earlier results of Vaurio (1994b):

- probabilities depend only on system (group) size  $n$  and not on the system success criterion;
- non-linear functions in terms of the test interval  $T$ ; an earlier method produced only linear terms;
- probabilities for general groups of  $n$  non-identical components and non-symmetric probabilities.

Three testing and repair policies are considered: consecutive testing, staggered testing with extra tests, and staggered testing without extra tests.

1.1 Notation

$\lambda_{k/n}$  = rate of CCF events failing specific  $k$  trains or channels (and no others) in a system with  $n$  redundant trains or channels;  $\lambda_{k/n}dt$  is the probability of a CCF event in a small time interval  $dt$ ;  $k = 1, 2, \dots, n, n = 2, 3, 4$

$\lambda_{ij}$ ... = rate of CCF events failing exactly components  $i, j, \dots$ ; due to space limitations results are

presented here only for the symmetric case  $\lambda_i = \lambda_{1/n}, \lambda_{ij} = \lambda_{2/n}$  for all  $i, j, \dots$ , etc.

$k/n$ -event = an event able to fail exactly  $k$  trains in a system with  $n$  trains

$\Lambda_{k/n}$  = rate of CCF events failing exactly  $k$  (any  $k$ ) trains per event in a group of  $n$  trains,

$$\Lambda_{k/n} = \binom{n}{k} \lambda_{k/n} \tag{1}$$

$N_{k/n}$  = number of  $k/n$ -events in exposure time  $T_n$

$T$  = test interval; duration of each test and repair is assumed  $\ll T$ , and  $\lambda_{ij} \dots T \ll 1$  for all rates

$T_n$  = observation time for a group of  $n$  trains.

2 UNCERTAINTY ANALYSIS

This section addresses data uncertainties in standby systems where failures are discovered mostly by periodic tests. For example, when four failures are discovered in a test cycle, they could be due to a single 4/4-event, or a coincidence of 3/4- and 1/4-events, or two 2/4-events, or even more overlapping events. Consequently, we do not truly know the number of events (“shocks”) associated with a single observation (test cycle). It makes a difference to uncertainty assessment whether there is a single  $k/n$ -event in two observations or two  $k/n$ -events in a single observation. There is a need to accept impacts with the possibility 0, 1 or 2  $k/n$ -events at least (of the same multiplicity) in a single observation. Since failures are rare events in the sense that the probability of occurrence in a single test interval is small compared to unity, the probability of more than two  $k/n$ -events in one interval is assumed to be negligible: not more than two  $k/n$ -events of the same multiplicity  $k$  can be associated with any observation  $i, i = 1, 2, \dots, N$ . The number of events is a random number while the number of observations (e.g. test cycles),  $N$ , is fixed or known. Allowing impact vector component values 0, 1, 2, the assessor has to estimate the following weights for each observation (test)  $i$  and failure multiplicity  $k$ :

$w_{i,\delta}(k/n)$  = the probability (conditional on the symptoms and characteristics seen by the assessor) of exactly  $\delta$  ( $\delta = 1, 2$ )  $k/n$ -events in observation  $i$  ( $i = 1, 2, \dots, N$ ).

Multiple events of different multiplicities  $k/n$  are allowed in one observation. Actually  $w_{i,0}(k/n)$  does not affect the rate estimation. For given multiplicity  $k/n$  the estimator  $\Lambda_{k/n}$  has a gamma distribution with mean  $(N_{k/n} + 1/2)/T_n$  and variance  $(N_{k/n} + 1/2)/T_n^2$  when  $N_{k/n}$  is known. But now  $N_{k/n}$  is unknown due to the assessment uncertainties. The following mean and variance can be obtained for the  $k/n$  -event rates (Vaurio 2002a).

$$E(\Lambda_{k/n}) = \frac{E(N_{k/n}) + 1/2}{T_n} \quad (2)$$

$$\sigma^2(\Lambda_{k/n}) = \frac{E(N_{k/n}) + \sigma^2(N_{k/n}) + 1/2}{T_n^2} \quad (3)$$

where the moments of  $N_{k/n}$  are

$$E(N_{k/n}) = \sum_{i=1}^N w_{i,1}(k/n) + 2 \sum_{i=1}^N w_{i,2}(k/n) \quad (4)$$

$$\sigma^2(N_{k/n}) = \sum_{i=1}^N w_{i,1} + 4 \sum_{i=1}^N w_{i,2} - \sum_{i=1}^N (w_{i,1} + 2w_{i,2})^2 \quad (5)$$

These results combine assessment uncertainties with statistical uncertainties.

Moments for the CCF –rates of *specific* k components are, based on Equation 1,

$$E(\lambda_{k/n}) = E(\Lambda_{k/n}) / \binom{n}{k}, \quad \sigma(\lambda_{k/n}) = \sigma(\Lambda_{k/n}) / \binom{n}{k} \quad (6)$$

$E(\Lambda_{k/n})$  is the best estimate and both moments together define the uncertainty distribution.

### 3 CCF PROBABILITIES FOR FAULT TREE MODELS

The task in this Section is to show how the rates  $\lambda_{k/n}$  can be used to determine probabilities of a fault tree model so that correct time –average risk or system unavailability can be obtained with a single fault tree computation, avoiding multiple step-by-step calculations as a function of time.

#### 3.1 Simultaneous or consecutive testing

When parallel trains of a system are tested simultaneously or consecutively and the test duration is small compared to T, the average residence time of failures occurring with any rate  $\lambda_{k/n}$  is approximately  $1/2T$ . However, using the average failed state probabilities  $1/2\lambda_{k/n}T$  for the basic events does not generally yield the correct time-average unavailability for the system. Correct values can be obtained by first calculating the time-average joint unavailabilities of the trains under the shocks, and then transforming these to the probabilities of explicit events  $Z_{ij} \dots$ . These transformations have been introduced at ESREL 2000 and more thoroughly later (Vaurio 2002b). Through the system fault tree these transformations yield correct explicit-event

probabilities independent of the system success criterion. The probabilities are

$$n \geq 1: z_i = 1/2 \lambda_{1/n} T, \quad i = 1, 2, \dots, n$$

$$n = 2: z_{12} = 1/2 \lambda_{2/2} T + 1/12 (\lambda_{1/2} T)^2$$

$$n = 3: z_{12} = z_{13} = z_{23} = 1/2 \lambda_{2/3} T + 1/12 (\lambda_{1/3} T)^2$$

$$z_{123} = 1/2 \lambda_{3/3} T + 1/4 (\lambda_{2/3} T)^2 + 1/4 (\lambda_{1/3} T)(\lambda_{2/3} T)$$

$$n = 4: z_{ij} = 1/2 \lambda_{2/4} T + 1/12 (\lambda_{1/4} T)^2, \quad 1 \leq i < j \leq 4$$

$$z_{ijk} = 1/2 \lambda_{3/4} T + 1/4 (\lambda_{2/4} T)^2 + 1/4 (\lambda_{1/4} T)(\lambda_{2/4} T) \\ 1 \leq i < j < k \leq 4$$

$$z_{1234} = 1/2 \lambda_{4/4} T + 1/3 (\lambda_{3/4} T)(\lambda_{1/4} T) + (\lambda_{3/4} T)(\lambda_{2/4} T) + \\ + 1/2 (\lambda_{3/4} T)^2 + 1/4 (\lambda_{2/4} T)^2 - 1/120 (\lambda_{1/4} T)^4 \quad (7)$$

These improve earlier results (Vaurio 1994b) in two ways:

1. the values depend on system size n but not on system success criterion;
2. non-linear terms are included, improving the accuracy.

Using only linear terms the system unavailability could be underestimated by a factor of 3.

#### 3.2 Staggered testing with extra tests and repairs

Uniformly staggered testing of n components means that there is a time delay T/n between the tests of components 1, 2, ..., n, and each component is tested at intervals T. Figure 3 illustrates the time-dependent

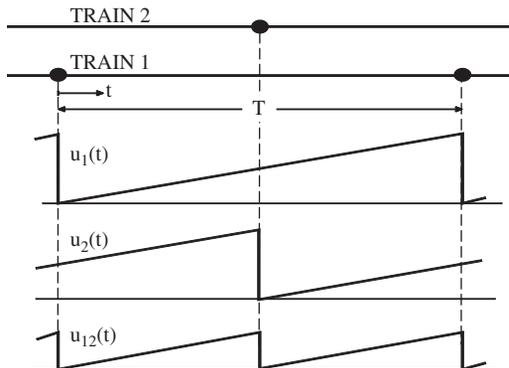


Figure 3. Staggered testing scheme for n = 2 trains. Single failure unavailabilities  $u_1(t)$  and  $u_2(t)$ , CCF unavailability  $u_{12}(t)$ .

unavailabilities in case  $n = 2$ . With such staggering the average residence time of a CCF is generally shorter than with simultaneous testing. Consider the following *Extra Testing and Repair Rule (ETRR)*:

Whenever a component is found failed in a test, the other  $n-1$  trains are also tested or inspected, and any failed components are repaired.

The joint unavailabilities of components can be solved analytically under a slightly different assumption that only CCF-specific failures are repaired at the extra tests. Transforming the joint unavailabilities to the probabilities of explicit events  $Z_{ij\dots}$  yields the following results, only slightly conservative for ETRR:

$$n \geq 1: z_i = \frac{1}{2} \lambda_{1/n} T, \quad i = 1, 2, \dots, n$$

$$n = 2: z_{12} = \frac{1}{4} \lambda_{2/2} T - \frac{1}{24} (\lambda_{1/2} T)^2$$

$$n = 3: z_{12} = z_{13} = z_{23} = \frac{5}{18} \lambda_{2/3} T - \frac{1}{36} (\lambda_{1/3} T)^2$$

$$z_{123} = \frac{1}{6} \lambda_{3/3} T - \frac{1}{12} \lambda_{2/3} \lambda_{1/3} T^2 - \frac{1}{108} (\lambda_{2/3} T)^2$$

$$n = 4: z_{12} = z_{14} = z_{23} = z_{34} = \frac{5}{16} \lambda_{2/4} T - \frac{1}{96} (\lambda_{1/4} T)^2$$

$$z_{13} = z_{24} = \frac{1}{4} \lambda_{2/4} T - \frac{1}{24} (\lambda_{1/4} T)^2$$

$$z_{ijk} = \frac{3}{16} \lambda_{3/4} T + \frac{5}{256} (\lambda_{2/4} T)^2 - \frac{1}{16} (\lambda_{2/4} T)(\lambda_{1/4} T) \\ 1 \leq i < j < k \leq 4,$$

$$z_{1234} = \frac{1}{8} \lambda_{4/4} T + \frac{1}{128} (\lambda_{3/4} T)^2 - \frac{1}{16} \lambda_{3/4} \lambda_{2/4} T^2 \\ - \frac{7}{96} \lambda_{3/4} \lambda_{1/4} T^2 - \frac{9}{128} (\lambda_{2/4} T)^2 - \frac{1}{1920} (\lambda_{1/4} T)^4 \quad (8)$$

These improve earlier results by the non-linear terms and by being independent of system success criteria.

### 1.3 Staggered testing without extra tests

Another possibility with staggered testing is the following *Individual Testing and Repair Policy (ITRP)*:

Components are tested and repaired individually with intervals  $T$ . No other component is tested immediately even if one is found to be failed.

Exact analysis is rather complicated because a triple failure changes to a double failure in one test/repair, and a double failure to a single failure. This is why higher order rates appear in lower order joint probabilities. Transforming the time-average joint probabilities to explicit event probabilities yields

$$n = 2: z_i = \frac{1}{2} \lambda_{1/2} T + \frac{1}{4} \lambda_{2/2} T, \quad i = 1, 2$$

$$z_{12} = \frac{1}{4} \lambda_{2/2} T - \frac{1}{24} (\lambda_{1/2} T)^2$$

$$n = 3: z_i = \frac{1}{2} \lambda_{1/3} T + \frac{1}{9} (4\lambda_{2/3} + \lambda_{3/3}) T, \quad i = 1, 2, 3$$

$$z_{ij} = z_{12} = z_{13} = z_{23} = \frac{1}{9} \lambda_{3/3} T + \frac{5}{18} \lambda_{2/3} T - \frac{1}{36} (\lambda_{1/3} T)^2$$

$$z_{123} = \frac{1}{6} \lambda_{3/3} T - \frac{17}{108} (\lambda_{2/3} T)^2 - \frac{1}{12} (\lambda_{1/3} \lambda_{2/3} T)^2$$

$$n = 4: z_i = \frac{1}{2} \lambda_{1/4} T + \frac{1}{16} (10\lambda_{2/4} + 5\lambda_{3/4} + \lambda_{4/4}) T$$

$$z_{12} = z_{14} = z_{23} = z_{34} = \frac{5}{16} \lambda_{2/4} T + \frac{1}{16} (4\lambda_{3/4} + \lambda_{4/4}) T$$

$$z_{13} = z_{24} = \frac{1}{4} \lambda_{2/4} T + \frac{1}{8} \lambda_{3/4} T$$

$$z_{ijk} = \frac{3}{16} \lambda_{3/4} T + \frac{1}{16} \lambda_{4/4} T, \quad 1 \leq i < j < k \leq 4$$

$$z_{1234} = \frac{1}{8} \lambda_{4/4} T$$

(9)

Only linear terms have been solved for  $n = 4$  in this case. Also these results improve the earlier ones by non-linear terms (for  $n = 2, 3$ ) and by being independent of system success criteria. Note that some probabilities for  $n = 4$  are not symmetric ( $z_{12} \neq z_{13}$ ) even when the rates are symmetric ( $\lambda_{12} = \lambda_{13} = \lambda_{2/4}$ ).

## 4 QUANTIFICATION PROCEDURE

A suggested comprehensive CCF quantification procedure is presented in Figure 4. It starts with a collection of available generic CCF-event data sources, including data for the plant under study. For a specific system and component type the target plant has a certain number of components,  $n$ . Option 1 is to select plants (systems)  $v$  with the same  $n$ , and determine the impact vector weights  $w_{i,\delta}(k/n)$  for all events  $i$  observed over the times  $T_n(v)$  of those plants. For each plant individually one can estimate the moments of the rates using Equations 2 through 6, and then use the mean values  $E(\lambda_{k/n})$  to determine the best-estimate CCF-event probabilities through Equations 7, 8 & 9.

One can also estimate "group rates" by adding up the observation times  $T_n(v)$  and the event moment Equations 4 and 5 for all plants with the same  $n$ , and use these in Equations 2 and 3. These would be valid under the assumption of completely identical plants.

However, because plants are individual and CCF are rare events, it is generally believed that one can improve the estimates by using an empirical Bayes method that uses data from many selected plants to generate a prior distribution (population distribution),

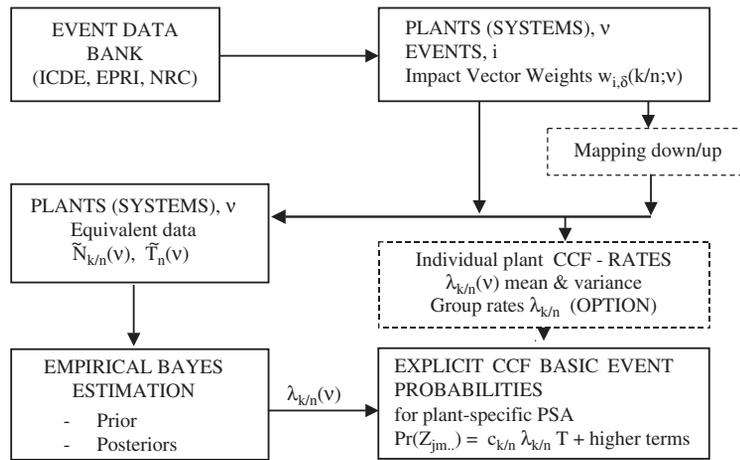


Figure 4. Common cause failure quantification procedure.

Table 1. Loviisa 1 posterior mean values of CCF –rates with two prior data sources [hr<sup>-1</sup>].

System and component	CCF–rate: $\Lambda_{2/4}$		$\Lambda_{3/4}$		$\Lambda_{4/4}$	
	Data Source: EPRI	ICDE	EPRI	ICDE	EPRI	CDE
HP safety injection pumps	5.48E-07	4.62E-07	3.04E-07	2.73E-07	0.91E-07	0.56E-07
LP safety system pumps	2.96E-0	0.33E-07	0.91E-07	0.42E-0	0.91E-07	0.56E-07
Service water pumps	2.28E-07	1.35E-07	0.91E-07	0.76E-07	0.91E-07	0.63E-07
Component cooling pumps	0.77E-07	0.40E-07	0.91E-07	0.44E-07	0.91E-07	0.44E-07
Diesel generators	8.92E-07	10.8E-0	0.95E-07	4.21E-07	29.1E-07	35.0E-07

and then get plant-specific posterior rates for the interesting plant. Such methods use input data in the form of pairs  $(\tilde{N}_{k/n}, \tilde{T}_n)$  for each plant, where  $\tilde{N}_{k/n}$  is a Poisson distributed number of events in observation time  $\tilde{T}_n$ . Due to the assessment uncertainties such known  $\tilde{N}_{k/n}$  are not available. But one can determine effective event statistics, values  $\tilde{N}_{k/n}$  and  $\tilde{T}_n$  that yield the same moments as Equations 2 & 3, i.e. satisfying the conditions

$$\frac{\tilde{N}_{k/n} + 1/2}{\tilde{T}_n} = \frac{E(N_{k/n}) + 1/2}{T_n}, \tag{10}$$

$$\frac{\tilde{N}_{k/n} + 1/2}{\tilde{T}_n^2} = \frac{E(N_{k/n}) + 1/2 + \sigma^2(N_{k/n})}{T_n^2}. \tag{11}$$

Using such data  $(\tilde{N}_{k/n}, \tilde{T}_n)$  as input to the empirical Bayes process one can obtain a common prior distribution and plant-specific posterior distributions for all CCF –rates of interest. The mean values are then used for the best-estimate CCF –event probabilities in Equations 7, 8 & 9.

This method has been demonstrated using international common cause failure data (Vaurio & Jänkälä 2002) in case  $\delta < 2$ . Examples of posterior CCF –rates for groups of  $n = 4$  pumps and diesel generators at Loviisa 1 power plant are given in Table 1 using two data sources, EPRI and ICDE.

Another option is indicated in Figure 4 by the box “Mapping down/up”. It is a way to utilise data from plants that have a group of  $n' \neq n$  similar components in a CCF group, transforming the weights  $w_{i,\delta}(k'/n')$  to the weights  $w_{i,\delta}(k/n)$  suitable for the target plant. Rules that have been recommended for mapping down are based on the assumption  $\lambda_{k/n} = \lambda_{k/n+1} + \lambda_{k+1/n+1}$ . This assumption is inherent in many earlier CCF models (Vaurio 1994b) but has not been empirically validated. Nevertheless, it yields the mapping down rule  $w(k/n) = [(n + 1 - k)w(k/n + 1) + (k + 1)w(k + 1/n + 1)]/(n + 1)$ . Mapping up may be based on assuming some generic ratio  $\rho = \lambda_{m+1/m+1}/\lambda_{m/m}$ .

It is worth noticing that the current model and quantification does not need any other parametric models or ratios (alpha- or beta-factors, multiple Greek letters

or binomial parameters) as intermediate steps: the CCF rates can be estimated directly from observed event data and used directly to create numerical input probabilities for the basic CCF –events in fault tree models or other logic representations of a system. It is possible to calculate such ratios and parameters afterwards, if the system analysis software so requires. Ratios can be calculated for the rates ( $\lambda_{k/n}$ ) or for the basic event probabilities ( $z_{k/n}$ ), depending on the requirements of the software in use. There are no universal generic ratio-parameters anymore, because they are different for different testing schemes and intervals, even in the same system.

If the plant under study is new and has no operating experience, one can use the prior (population) mean values in this process, and prior distributions in uncertainty studies.

It is also possible to use data collected from plants (systems) that have a different number of components than the plant under study. But then one has to assume some transformation rules for mapping up or down the impact vector weights (or the rates) to be applicable to the plant under study.

## 5 CONCLUSIONS

Simultaneous failures of multiple components due to common causes at random times have been modelled for standby safety systems by general multiple-failure rates (GMFR) rather than probabilities per demand. This is considered more realistic than many traditional probability-per-demand models. Actual event evaluations have demonstrated that many causes of CCF enter between tests rather than due to tests or true demands. Some of the other features and advantages are:

- Correct time-dependent system risk/unavailability can be obtained with the GMFR –model
- GMFR parameters can be estimated directly from multiple-failure event data over a specified time,
  - there is no need to know the total number of demands
  - there is no need to tie the GMFR parameters to single-failure rates (that generally have different causes than CCF)
  - assessment uncertainties and statistical uncertainties can be synthesised
  - empirical Bayes method is available to utilise uncertain data from multiple plants
- GMFR does not need to assume or calculate any ratios between the rates of different multiplicities, or artificial mapping down or mapping up equations
- The probabilities obtained here for the basic events for steady-state calculation
  - yield correct average system risk/unavailability in a single system quantification

- are explicitly dependent on test intervals and testing schemes, facilitating optimisation of these based on risk and/or cost
- depend on the system/group size but are independent of the system success criterion

In this paper improvements were made to the procedure for estimating CCF –rates from single- or multiple-plant event data with uncertainties, allowing more than one CCF event of a certain multiplicity in a single observation (test episode). This required use of generalized impact vectors. Advancements were also made to determine basic common cause event probabilities for explicit fault tree models of standby systems in terms of the rates, test intervals, test schedules and repair policies. These probabilities yield the correct time-average system unavailability with a single fault tree quantification. The probabilities obtained are now independent of the system success criterion and include non-linear terms.

Future efforts should be directed towards effective CCF event data collection and evaluation. Quantitative analysis of the efficiency of various defences against CCF, including redundancy, diversity and programmable digital systems, is a worthy objective for future research.

## REFERENCES

- Mosleh, A., Fleming, K.N., Parry, G.W., Paula, H.M., Worledge, D.H. & Rasmuson, D.M. 1989. Procedures for Treating Common Cause Failures in Safety and Reliability Studies. NUREG/CR-4780 (EPRI NP-5613). U.S. Nuclear Regulatory Commission.
- Mosleh, A., Parry, G.W. & Zikria, A.F. 1993. An Approach to the Parameterization of Judgement in the Analysis of Common Cause Failure Data. *Proceedings of PSA '93, Clearwater Beach, January 26–29, 1993*: 818–822. American Nuclear Society.
- Siu, N. & Mosleh, A. 1989. Treating Data Uncertainties in Common Cause Failure Analysis. *Nuclear Technology* 84: 265–281.
- Vaurio, J.K. 1994a. Estimation of Common Cause Failure Rates Based on Uncertain Event Data. *Risk Analysis* 14: 383–387.
- Vaurio, J.K. 1994b. The Theory and Quantification of Common Cause Shock Events for Redundant Standby Systems. *Reliability Engineering and System Safety* 43: 289–305.
- Vaurio, J.K. & Jänkälä, K.E. 2002. Quantification of Common Cause Failure Rates and Probabilities for Standby-System Fault Trees Using International Event Data Sources. In E.J. Bonano et al. (eds), *Proceedings of PSAM 6 Conference, San Juan, Puerto Rico, 23–28 June 2002*. Elsevier.
- Vaurio, J.K. 2002a. Extensions of the Uncertainty Quantification of Common Cause Failure Rates. *Reliability Engineering and System Safety* 78: 63–69.
- Vaurio, J.K. 2002b. Treatment of General Dependencies in Fault Tree and Risk Analysis. *IEEE Trans. Reliability* 51: 278–287.

## Risk assessment for offshore installations in the operational phase

J.E. Vinnem

*Stavanger University College/Preventor, Bryne, Norway*

T. Aven

*Stavanger University College, Stavanger, Norway*

H. Hundseid

*DNV, Høvik, Norway*

K-A. Vassmyr

*Acona Group, Stavanger*

F. Vollen

*Safetec Risk Management, Trondheim*

K. Øien

*SINTEF Industrial Management, Trondheim, Norway*

**ABSTRACT:** Risk assessments for offshore petroleum installations have for more than 20 years focused on development of new installations or major modifications, using both qualitative and quantitative risk assessments. The risk assessments have often, especially the quantitative studies, placed an emphasis on major hazards. There is now focus on how risk assessments may be used most efficiently for installations in the operational phase. In this paper we review the challenges for use of risk assessment studies for installations in the operational phase, with the main emphasis on quantitative studies. The focus should mainly be on aspects that are available for influence in the operations phase, so-called free variables. When these are of a different nature from those that apply in the development phase, this should have strong impact on the studies being conducted. However, these changes to analytical approach have yet to be fully implemented.

### 1 INTRODUCTION

#### 1.1 Background

##### 1.1.1 Historical review regulations

The Norwegian safety regime for offshore petroleum installations and operations is founded on internal control. The licensees have the full responsibility for ensuring that the petroleum activities are carried out in compliance with the conditions laid down in the legislation, and the authorities' supervisory activities aim to ensure that the licensee's management systems are adequately catering for the safety and working environment aspects in their activities.

The initial petroleum legislation from the 1970s was technically oriented, with detailed and prescriptive requirements to both safety and technical solutions. The authorities, with the Norwegian Petroleum Directorate (NPD) in a key role, have gradually changed the legislation to a functional or goal-based orientation. Although regulations concerning internal control and safety were issued as early as 1985, the majority of the "new generation" regulations were issued in the early 1990s. From 1.1.2002 a substantial rationalization was implemented with 14 regulations reduced to 4.

Quantitative risk assessment (QRA) techniques were first given wide application in Norwegian offshore oil and gas industry in the early 1980s. Of particular importance were the NPD regulatory guidelines for concept safety evaluations (CSE) studies, which were introduced in 1980. The guidelines introduced a quantified cut-off criterion related to the impairment frequency for nine types of accidents that could be disregarded in further evaluation processes, the so-called  $10^{-4}$  criterion (i.e. a criterion of  $10^{-4}$  per year for the so-called Main Safety Functions and for each accident type, and a total risk of up to nearly  $10^{-3}$  per year). Introduction of this criterion, which in practice was implemented as a risk acceptance criterion, attracted considerable attention worldwide. Until then, there were few attempts by authorities to approach the sensitive issue by making risk visible and subject to open debate.

The development of the Norwegian legislative regime was prompted by several serious accidents in the Norwegian Sector, culminating with the Alexander Kielland capsized in 1980, which resulted in 123 fatalities. A similar development of regulations occurred about 10 years later in the UK, based upon the Piper Alpha inquiring report (Lord Cullen, 1990) following

the catastrophic explosion and fire in 1988 with 167 fatalities.

In the Norwegian regulations relating to implementation and use of risk analyses, which came into force in 1990, focus was on the risk analysis process. The scope of application of the regulations was extended compared to the CSE guidelines. Provisions were laid down for a more integrated and dynamic use of risk analyses, with suitable quality controls on the process, covering the whole life cycle of the petroleum activities.

Pursuant to the regulations, risk analyses are to be carried out in order to identify the accidental events that may occur in the activities. Further to evaluate the consequences of such accidental events for people, for the environment and for assets and financial interests. The purpose of the risk analyses is to provide a basis for making decisions with respect to choice of arrangements and risk reducing measures. The operator is to define safety objectives and risk acceptance criteria. The objectives express an ideal safety level. Thereby they ensure that the planning, maintaining and the further enhancement of safety in the activities become a dynamic and forward-looking process. This means that accidental events must be avoided, the level of risk is kept as low as reasonably practicable (ALARP), and attempts are made to achieve reduction of risk over time, e.g. in view of technological development and experience. The need for risk reducing measures is assessed with reference to the acceptance criteria, for which the basis shall be documented in an auditable manner.

In 1992 NPD also issued a regulation on emergency preparedness (safety barriers). The most important elements of this regulation was that:

- The emergency preparedness of the activity in question shall be established on the basis of some defined situations of hazard and accident (i.e. scenarios definitions).
- The operator shall define specific requirements relating to the effectiveness (performance standards) of the emergency preparedness measures.
- Analyses shall be carried out as a basis for the design of the emergency preparedness system.

New regulations replaced the old in 2002, but the main requirements related to risk analysis remained unchanged. However, a stronger focus has been placed on the context and the use of risk analysis, as well as on assessment and monitoring of barrier performance.

It has been recognized that current practices for quantitative studies have several deficiencies in relation to the requirements in the new regulations.

### 1.1.2 Challenges

Both qualitative and quantitative risk assessments are being used, for different purposes. This paper, however, has the main emphasis on quantitative studies. Further,

major hazards as well as more limited, occupational hazards are being considered. The risk assessments have often, especially the quantitative studies, placed an emphasis on major hazards.

There has been in recent years focus on how risk assessments may be used most efficiently for installations in the operational phase. Qualitative studies may be used much in the same way as in the development phase. The transfer of the quantitative studies from the approach used in the development phase has been seen as a challenge, and a commonly accepted approach has yet to be developed. The focus of such studies should be on aspects that are available for influence in the operational phase, such as operational and maintenance measures. These are often called “free variables”, and are different in the operational phase from the development phase. The analytical approach should be tailored to the free variables. When these are of a different nature from those that apply in the development phase, this should have strong impact on the studies being conducted. However, these changes to analytical approach have yet to be fully implemented. Quantitative studies for installations in the operational phase are still being conducted in much the same way as in the development phase.

The protection against major hazards in the offshore petroleum industry is based on the “defence in depth” concept, with multiple barriers, (see Reason, 1997). Maintenance of the integrity of barriers is therefore an important aspect for risk management in the operational phase. This also implies that risk assessments in some cases will need to model how integrity of barriers may be impaired and what effect this will have on the risk levels.

Another important aspect in the operational phase is the performance of activities of short duration, with associated high risk levels, often in combination with special conditions and premises.

The above challenges are not only relevant for the oil and gas industry in Norway. In for example UK and Australia the safety regime is similar to the Norwegian, and the use of risk analysis in the operational phase is also in these countries a topic for further research and development.

## 1.2 R&D context

The Norwegian Government has initiated a research program to improve the safety level offshore. The program is led by the Norwegian Research Council and a network of Norwegian institutions has been established to realize the program. The ambition is to obtain more adequate risk analysis tools, in general and for the operational phases in particular. The present work is a part of this program.

In coordination with this research program the Association of Norwegian oil companies has initiated

a development activity to establish models of the safety barriers. Together these initiatives are considered to give a strong push forward for the application of risk analyses in the operational phase.

The first phase of this work considered needs for risk assessments as input to decision-making, and was conducted in 2002, see Acona Group (2002) and DNV/ScP (2002).

### 1.3 Purpose of paper

The purpose of the paper is to provide the following documentation:

- Review current status, use and experience
- Describe objectives for use of operational risk assessment (ORA)
- Identify areas for further improvement
- Suggest possible new approaches

Use of risk assessment for other purposes, like risk based inspection, reliability centered maintenance, etc. is not covered.

## 2 OBJECTIVES OF USE OF OPERATIONAL RISK ASSESSMENT

### 2.1 Overall objectives

Proposed objectives for operational risk assessment are as follows:

- Assess overall risk level in the operational phase, reflecting modifications and operational status (such as activity level and manning)
- Identify important improvement areas for operation
- Provide input to operational decisions relating to risk issues
- Identify how operational tasks and special operations may be safely carried out
- Identify adequate maintenance strategies
- Assess barrier performance and demonstrate effects on the risk level of barrier deterioration
- Communicate risk results and important factors to the workforce.

“Operational risk assessment” (ORA) is possibly more a “family of methods”, rather than one single method, in contrast to Design risk assessment (DRA), by which most people will understand a specific analysis, usually referred to as “TRA”, “QRA” or “PRA” in the nuclear power generation industry. The difference between ORA and DRA has been illustrated as shown in Figure 1 (Veire, 2002).

DRA studies are often relatively coarse, also due to the fact that not all details are known in the development phases. DRA studies have the main emphasis on main concept issues, and do not need to be very detailed.

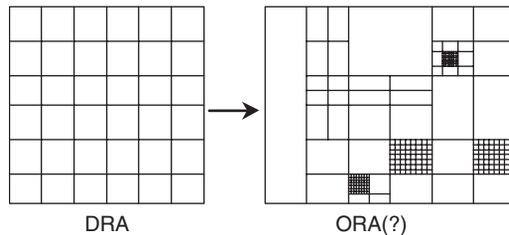


Figure 1. Difference between Design risk assessment and Operational risk assessment.

ORA studies are indicated as rather different from this, very detailed in some selected areas, but could be even more coarse than DRA studies in other respects. The areas where fine details are analyzed may change over time, depending on what the needs are, according to the operational decisions that require input from the ORA study.

### 2.2 What is a good risk analysis?

The purpose of risk analysis is to provide support for decision-making, by producing descriptions of risk for alternative concepts, arrangements, systems, activity levels and measures. Furthermore, the analyses provide insights into the phenomena being studied and this can be used to improve the design and operation. The analysis can also be used to identify contributing factors to risk. Further, intermediate results may be used for dimensioning of capacities of emergency systems and functions. The analyses give support for choosing among alternatives, and they provide basis for deciding on risk being acceptable or not, and on the need for risk reducing measures.

A risk analysis is considered generally good if it can meet these objectives. The question is how we can judge that these objectives are met; and to what degree?

Basically, we see six main elements for being able to perform such a judgment and thus obtain a high quality of the analysis:

1. The degree that the user of the analysis is satisfied with the analysis as a basis for making decisions
2. The fulfillment of requirements set by the risk analyst discipline for an analysis to be good
3. The analysis team's understanding of the phenomena being analyzed and the decision making process and context
4. The analysis team's competence on risk analysis; principles, methods and models
5. The ability of the analysis to produce intermediate results for input to planning and emergency procedures
6. The accuracy and quality of the results of the analysis.

These aspects are discussed in more detail in Vinnem et al. (2003b).

### 2.3 Qualitative or quantitative analysis

The scope of work in the OLF project (see Acona Group, 2002; DNV/ScP, 2002) was focused on both qualitative as well as quantitative studies. It has been a typical situation that all risk assessment studies that are performed with direct application in the operational phase (except updating of Design QRA studies) have been qualitative studies.

This is considered to be a reflection of unsuitable methodologies for quantitative studies for operational matters, rather than a reflection of correct use of methodologies. In fact some of the authority requirements actually call for quantitative studies in areas where the normal approach currently is basically qualitative studies.

One of the purposes of the paper is to define the distinctions between applications of qualitative and quantitative studies. Qualitative and quantitative studies are therefore discussed separately in Section 3–4 below.

There are roughly two stages of risk assessment for offshore activities:

- Risk assessment during planning of offshore activities. This is normally undertaken onshore, but with participation of key offshore personnel.
- Risk assessment just prior to execution of an activity. This is undertaken using the Work Permit System, Procedures and Safe Job Analysis.

## 3 USE OF QUALITATIVE STUDIES

For offshore operations, the use of qualitative studies has increased significantly over the last decade. In particular, the introduction of risk based safety management systems has encouraged the use of qualitative studies, both prior to specific offshore operations, and more recently, during all aspects of “management of change”.

This section concentrates on the use of qualitative studies for **offshore activities** in the Norwegian sector of the North Sea. Maintenance and inspection planning to ensure adequate integrity of safety barriers have not been evaluated.

### 3.1 Offshore activities

Some categories of offshore activities may from time to time be subjected to some form of qualitative studies:

- Drilling and well services
- Production, maintenance and minor modifications
- Marine operations
- Transportation
- Organizational changes

Within these 5 categories, there are a number of specific activities that are either executed as a single activity or as part of several activities that are undertaken simultaneously. The risk associated with these activities will be dependent on a number of parameters, such as:

- Type of activity
- Technical integrity of equipment and structure
- Available documentation
- Communication
- Organization
- Human Factors
- External Factors
- Extent of simultaneous activities

Each of the above parameters could be split into a number of sub-issues (e.g., competence, experience, complacency, stress, etc. for human factors). Thus, the overall risk picture for a specific activity can be rather complex. The above parameters are included in various checklists that are being used as guidewords to identify hazards during qualitative studies.

Current use of qualitative studies is briefly outlined in Vinnem et al. (2003b).

## 4 USE OF QUANTITATIVE STUDIES

### 4.1 Current use of quantitative studies

Quantitative Risk Assessment may include quantification of the probability and the consequences of accidental events with respect to one or several of the following risk dimensions; personnel, environment and assets. The study further includes a comparison with quantitative risk acceptance criteria established by the operator. This will typically include quantitative criteria for Fatal Accident Rate (FAR) and/or Individual Risk (IR) and quantitative criteria for safety functions like e.g., support structure, escape ways, evacuation, control room and sheltered area.

For effective planning, execution and use of risk analysis reference is given to NORSOK standard Z-013 (NTS, 2001). Current requirements set by the Norwegian Petroleum Directorate makes references to this NORSOK standard.

Current use of quantitative studies is briefly outlined in Vinnem et al. (2003b).

### 4.2 Decisions where quantitative input is required

The decision processes are complex and are normally related either to economic or safety related aspects. Either the offshore organisation or the onshore organisation takes the initiative to changes. Typical problems where decisions are required in the operational phase and where decision support from a well developed ORA will increase the probability for the “correct”

decision, are identified to be:

- Whether the activity should be carried out or not
- What restrictions and safety related aspects that should be taken care of in daily operation
- What the requirements to the equipment are
- What the requirements to the personnel and the competence are
- Whether the production should be shut down
- Whether the manning level must be changed
- What simultaneous operations that can be carried out
- Whether compensating measures are necessary and which of them are effective
- Whether maintenance and improvements could be delayed.

Several of the decisions related to the listed problems must be taken on a daily basis, and use of quantitative analyses as a decision support tool will in many situations not be optimal. This is discussed in more detail in Vinnem et al. (2003b).

#### 4.3 Shortfalls and deficiencies in QRA methodology application

There are several shortfalls and deficiencies in the QRA methodology with regard to decision support in the operational phase. They are identified among others to be:

- Focus on long term risk rather than short term risk which is necessary to consider in the operational phase.
- The acceptance criteria are often inappropriate for short term risk.
- Knowledge about QRAs is not sufficiently communicated to offshore personnel.
- QRA teams often consist of risk analysts only with negligible experience from operations. Operational personnel should be involved.
- Often the risk level is not presented in an understandable and trustworthy manner.
- To carry out a QRA is often time consuming and not necessarily adjusted to the time schedule for the decision processes in the operational phase (decisions to be taken on daily basis).
- Relevant data to carry out a QRA in the operational phase (such as data relating to operations) are often difficult to obtain.
- Today the QRA normally only includes technical aspects, but for operational aspects also human, organizational and cultural factors must be taken into account. Human reliability analyses (HRA) are rarely used in offshore QRAs, even though methods exist. It is important to make better use of existing HRA and also to improve these methods in order to succeed in development and use of QRAs in the operational phase.

## 5 ANALYSIS OF BARRIERS

### 5.1 *The barrier concept and barrier requirements*

The requirements for principles to be adopted for use of barriers are stated in the so-called management regulations (NPD, 2001).

Barrier is not a totally new concept in the petroleum industry, but the previous interpretation has usually been restricted to physical measures, e.g., as in MORT (Management Oversight and Risk Tree; Johnsen, 1980).

The management regulations (NPD, 2001) emphasize that barriers shall include administrative or organizational measures as well as physical measures, i.e. physical and non-physical barriers. Organizational barriers or safety measures are those measures that shall ensure continuous adequate performance of the technical and human barriers.

### 5.2 *Potential achievements using barrier analysis in ORA*

The management regulations' requirements on barriers may be broken down in the following parts:

1. Stipulate the strategies and principles on which the design, use and maintenance of barriers shall be based
2. Know what barriers have been established and which function they are designed for, and what performance requirements have been defined
3. Know which barriers are non-functional or have been impaired
4. Initiate necessary actions to correct or compensate for missing or impaired barriers.

Further discussion of these aspects is presented in Vinnem et al. (2003b).

### 5.3 *Future analysis and modeling of barriers*

A future development toward more detailed modeling of physical barriers (e.g., safety systems) in the risk analysis (ORA) will support the potential achievements mentioned in Section 5.2. This may enable one or several of the following, depending on future decisions about usefulness:

- Establishing safety system requirements based on risk assessment, i.e., the reliability of a particular safety system, may be used as a requirement when the safety integrity level (SIL) is determined for that system (in order to meet the overall risk acceptance criteria).
- Obtain information on risk status for safe daily operation using living risk assessment and RMS.
- Risk based configuration control, i.e. to manage and control concurrent unavailability of components, the

possibility of functional alternative components, the outage times of the unavailable components and the frequency of the critical configurations.

- Evaluation/rating of operational events, i.e. to carry out an operational events analysis in order to evaluate the safety significance of the events and to establish an event importance ranking.
- Establishing allowed outage times for safety systems in order to minimize the risk from equipment unavailability while maintenance is in progress.

A more detailed modeling of physical barriers may also support risk-informed decision making within maintenance management, e.g., RCM, in-service testing, in-service inspection, etc.

The broadening of the concept of barriers, including non-physical elements is in line with prevailing thinking about major accident prevention. The notion of organizational accidents (Reason, 1997) underlines the fact that most major accidents are not caused by simple technical failures or human errors but rather organizational deficiencies. To include models of non-physical barriers in risk assessments (e.g., in ORA, QRA, PRA, PSA, etc.) is, however, not an easy task (see e.g., Hale et al. 1998b). For qualitative assessments (audit type of methods) and accident investigations the inclusion of non-physical barriers is more manageable. This is also the area in which works already have been initiated in the petroleum industry, (ref. the TTS project and the MTO-method).

Another challenge for future analysis and modeling of barriers is the adequate treatment of dependencies. Some of the dependencies between similar physical components are accounted for in the models. However, dependencies between systems are rarely considered and this is of special relevance with respect to potential organizational dependencies (e.g., same maintenance team using the same (lack of) knowledge, (less than adequate) procedures, etc., working on different systems). This has been addressed by Relcon in a project for NPD (Bäckström & Vinnem, 2003).

## 6 ANALYSIS OF RISK TRANSIENTS

“Transient” in this context implies short duration activities, say from one hour up to several days duration, that imply increased risk during the time it takes to complete the activities in question.

### 6.1 Requirements

Section 14 of the “Management regulations” (NPD, 2001) requires quantitative assessment of risk in order to identify contributions to major hazard risk from hazards such as:

- Drilling and well operations

- Modifications, during and after implementation
- Helicopter transportation

Although not explicitly stated, the implicit requirement in this formulation is that transient risk levels need to be addressed.

The NPD requirement further state that the effect of these temporary activities on the total risk level shall be presented. It is therefore required that temporary risk levels and durations are analyzed and documented.

### 6.2 Objectives of activity based modeling

The objectives of adopting activity or condition based modeling are:

- To allow a representation of risk which shows clearly at least the main variations in risk levels according to the activities or conditions.
- To provide, through the representation of risk, an explicit demonstration of the effects of the dominating risk factors.
- To allow monitoring of risk to address instantaneous risk levels rather than average risk levels.
- To enable risk modeling to be used as a planning tool.

## 7 CONCLUSIONS AND RECOMMENDATIONS

### 7.1 Recommended use of qualitative studies – offshore operations

Qualitative studies have been established in most operator’s safety and risk management system. It is considered to be a practical and efficient tool to provide essential information for decision making of a practical nature. The method combines utilization of qualified personnel with a systematic approach to identify hazards, assess consequences and probabilities, and evaluate prevention and mitigation measures for the ongoing management of risk.

Qualitative studies are recommended for the following use:

- Practical risk evaluation during planning of major offshore activities
- Practical risk evaluation of simultaneous activities
- Practical risk evaluation of organizational changes

Qualitative approaches may not be suitable to evaluate barriers or maintenance strategies and intervals. Further, for design and process modifications, quantitative expressions are appreciated by many as it is easier to compare.

Thus, quantitative approaches should be developed to account for such issues, and are discussed in the following.

### 7.2 Recommended use of quantitative studies

As already argued, there are a number of decisions in the operational phase that need a quantitative basis for decision-making. This need appears to be agreeable to most HES management experts.

The next issue is whether the oil companies need to know the instantaneous risk level on their installations. It may be argued that this is implied by the new NPD management regulations (NPD, 2001), this would be however, a rather conservative interpretation of the requirements. Also the requirements for risk acceptance criteria in the NPD regulations indirectly call for such a detailed quantitative study, but should nevertheless also be open for debate and discussion. This is a separate subject for a future study.

After all, maybe a more cost effective and sufficient solution from a HES management perspective, is the approach indicated in Figure 1, whereby the "total risk" level in general is assessed relatively crudely, whereas a number of subjects are assessed in more detail, according to what the need may be. Not all of these detailed studies may be possible to integrate into an overall value, if they do not have a common expression of the consequence dimension.

Some of the areas where more detailed modeling often may be required, are:

- Modeling of barriers, their impact on the risk level and interactions with performance of operational and maintenance activities.
- Improved illustration of and insight into different aspects of the risk level.
- Improved modeling and illustration of operational, short term and local risk conditions.

When carrying out a quantitative study for the operational phase it is important that the team carrying out the work includes both onshore and offshore personnel covering all relevant aspects. The results must also be presented for the users in an understandable and trustworthy manner. Other decision support tools together with the QRA are also needed to develop a safe daily operation, and it is recommended to evaluate how the different decision tools better can be integrated with each other.

### 7.3 Analysis of barriers

The analysis of barriers is in need of substantial improvement with respect to:

- More explicit modeling of the various barrier elements, and their contributions to the overall barrier function.
- More explicit modeling of the performance of barriers, in relation to the relevant performance parameters.

- Modeling of barriers which allow dependencies and common causes to be explicitly addressed.
- Explicit modeling of the coupling between barriers and the performance of operational and maintenance activities.

### 7.4 Analysis of risk transients

It may be inferred from the discussions in Section 6 that a detailed quantitative analysis of all transients is required. But this is far from an obvious conclusion.

The opposite approach would be to perform an overall quantitative assessment which gives the opportunity to compare with general risk acceptance limits, addressing annual accumulated values (often referred to as "annual average values"), without considerations of transients.

But detailed assessment of some transients may be required for certain conditions:

- Particularly critical transient conditions (e.g. activities that have a high risk intensity, but a low contribution to annual fatality risk dose, because of short duration).
- Transients that are vital in order to identify risk reducing measures and/or actions (e.g. where risk reducing measures need to be defined relative to the transient conditions rather than "average conditions").

It is not obvious that risk acceptance criteria need to be available for analysis of such transients. The main conclusion offered here is that analysis of transients may be carried out also when risk acceptance criteria for transient are not introduced. The analysis results will in such cases be evaluated in a relative sense, as well as in an ALARP context.

### TERMINOLOGY

ALARP	As low as reasonably practicable
CSE	Concept safety evaluations
DRA	Design risk assessment
FAR	Fatal accident rate
FIREPRAN	Fire protection risk analysis
HAZID	Hazard identification
HAZOP	Hazard and operability study
HES	Health, environment and safety
HRA	Human reliability analyses
IR	Individual risk
MORT	Management Oversight and Risk Tree
MTO	Human Technology Organisation
NPD	Norwegian Petroleum Directorate
OLF	Norwegian Oil Industry Association
ORA	Operational risk assessment
PFD	Probability of Failure on Demand
PSA	Probabilistic safety assessment

QRA	Quantitative risk assessment
RMS	Risk Monitoring System
SAFOP	Safe Operations Analysis
SIMOPS	Simultaneous operations
SJA	Safe job analysis
TATO	“Take two” (“Ta to” in Norwegian)
TRA	Total Risk Analysis
TTS	State of Technical Safety

## ACKNOWLEDGEMENT

The authors are indebted to NFR for the funding of the work and their parent organisations for the permissions to publish this paper. During the preparation of the paper, a large group of specialists has been consulted at various stages, orally and in writing. We are obliged to all those that have provided comments, for the time they have taken to review and provide very valuable input to the process.

## REFERENCES

- Aven, T., 2003. Foundations of Risk Analysis. Wiley NY, to appear.
- Acona Group AS, *Operational Risk Analysis – Phase I*, Report AJ-10260, 2002.07.17.
- Bäckström, O., Vinnem, J.E., 2003. (to be presented)
- Bedford, T., Cooke, R., 2001. Probabilistic Risk Analysis; Foundations and Methods, Cambridge, UK.
- Bento, J-P., 1999. Human – Technology – Organisation; MTO-analysis of event reports. OD-00-2. (In Swedish). Restricted.
- Det Norske Veritas & Scandpower, *Operational Risk Analysis – Phase I*, DNV Report 2002-0717, 2002.10.04.
- Hale, A.R., Guldenmund, F., Smit, K., Bellamy, L., 1998. Modification of technical risk assessment with management weighting factors. In Lydersen, S., Hansen, G., Sandtorv, H. (eds) Safety and Reliability, Proceedings from ESREL'98, Rotterdam, Balkema, pp. 115–120.
- Hansen, G.K., Aarø, R., 1997. Reliability Quantification of Computer-Based Safety Systems. An Introduction to PDS. SINTEF report STF38 A97434.
- Husebø, T., Ravnås, E., Lauritsen, Ø., Lootz, E., Brandanger Haga, H., Haugstøyl, M., Kvitrud, A., Vinnem, J.E., Tveit, O., Aven, T., Haukelid og, K., Ringstad, A.J., (2002). *Utvikling i risikonivå-norsk sokkel. Fase 2 rapport 2001* (Oljedirektoratet, OD-02-07, www.npd.no).
- IAEA, 1998, IAEA, Draft-document, PSA Applications to Improve NPP Safety, IAEA-J4-97-CT-06876, February 1998, Vienna, Austria.
- IAEA (2001). IAEA-TECDOC-1200. Applications of probabilistic safety assessment (PSA) for nuclear power plants. ISSN 1011–4289. IAEA, Vienna, Austria.
- IEC 61508. “Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems”, part 1–7, Edition 1.0 (various dates).
- ISO, 2000. Petroleum and natural gas industry – Offshore production installations – Guidelines on tools and techniques for identification and assessment of hazards, ISO 17776.
- Johnson, W.G., 1980. MORT Safety Assurance Systems, Marcel Dekker, New York, USA.
- Kafka, P., 1994. Living PSA – Risk Monitor: Current Developments. IAEA TCM, Budapest 7–11 Sept. 1992, IAEA-TECDOC-737, March 1994, IAEA, Vienna, Austria.
- Lord Cullen, 1990. Inquiring into the Piper Alpha Disaster, HMSO 1990.
- NTS, 2001. NORSOK Standard Z-013, Risk and Emergency Preparedness Analysis, 2001.
- Norwegian Petroleum Directorate. (2001). Regulations relating to Management in the Petroleum Activities (the Management Regulations). ([http://www.npd.no/regelverk/r2002/frame\\_e.htm](http://www.npd.no/regelverk/r2002/frame_e.htm)).
- Norwegian Petroleum Directorate. (2002). Guidelines to Regulations relating to Management in the Petroleum Activities (the Management Regulations). ([http://www.npd.no/regelverk/r2002/frame\\_e.htm](http://www.npd.no/regelverk/r2002/frame_e.htm)).
- OLF guideline 070 on the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian Continental Shelf, OLF, Rev. 01, 26-01-2001; (see <http://www.itk.ntnu.no/sil>).
- Reason, J., 1997. Managing the Risks of Organizational Accidents, Ashgate, England.
- Sørum, M., Firing, F., Endresen, I., Øvrebø, R., Storhoug, O., Berg, F.R., Hvam, C., Holmboe, R.H., Austbø, J.S., 2002. Mapping of state of technical safety in Statoil; Main report. (In Norwegian). Restricted.
- Veire, G., 2002. Private communication with Gunnar Veire, Statoil.
- Vinnem, J.E., 1998. Use of performance indicators for monitoring HSE operating achievement. Proceedings of ESREL'98, Trondheim, Norway, 16–19 June: 127-35: Balkema.
- Vinnem, J.E., 1999. Risk Assessment of Offshore Platforms, Keynote note paper to ESREL 1999, Munich, October, 1999.
- Vinnem, J.E., 2000. Risk Monitoring for Major Hazards, SPE61283, SPE International Conference on Health, Safety and the Environment in Oil and Gas Exploration and Production in Stavanger, Norway 26–28 June 2000.
- Vinnem, J.E., Aven, T., Sørum, M., Øien, K., 2003a. Structured approach to risk indicators for major hazards, ESREL2003, Maastricht, 15–18 June, 2003 (to be published).
- Vinnem, J.E., Aven, T., Vassmyr, K-A., Vollen, F., Øien, K., 2003b. Risk Assessments for Offshore Installations in the Operational Phase, NFR report.
- Øien, K., Sklet, S., Nielsen, L., 1997. Risk Level Indicators for Surveillance of Changes in Risk Level. Proceedings of ESREL'97, Lisbon, Portugal, 17–20 June, Pergamon, pp. 1809-16.
- Øien, K., Sklet, S., Nielsen, L., 1998. Development of risk level indicators for a petroleum production platform. Proceedings of the 9th International Symposium of Loss Prevention and Safety Promotion in the Process Industries, 4–7 May, 1998, Barcelona, Spain, pp. 382–393.
- Øien, K., Sklet, S., 1999. Risk Control during Operation of Offshore Petroleum Installations. Proceedings of ESREL'99, Munich, Germany, 13–17 September, Springer, pp. 1297–1302.
- Øien, K., 2001. Risk Control of Offshore Installations – A Framework for the Establishment of Risk Indicators. NTNU 2001:04, Trondheim, May 2001.

## Structured approach to risk indicators for major hazards

J.E. Vinnem

*Stavanger University College/Preventor, Bryne, Norway*

T. Aven

*Stavanger University College, Stavanger, Norway*

M. Sørum

*Statoil, Stavanger, Norway*

K. Øien

*SINTEF Industrial Management, Trondheim, Norway*

**ABSTRACT:** Risk indicators for major hazards in offshore petroleum operations have not been widely used until quite recently, and the uncertainty about what is the preferred approach is considerable. This paper attempts to describe a structured approach to such indicators, and to recommend a consistent approach. Proposed terminology for barriers and indicators is given. General requirements for development of risk indicators are presented from a theoretical as well as a HES management perspective. These requirements are presented in relation to broad categories of use on a national level, a company/installation level and an equipment level. A basic approach for development of risk indicators is presented, relating to incidents, barrier performance, activity levels, causal factors, management systems and cultural aspects. Suggestions for loss related and process related indicators, as well as indicators relating to causal factors are presented.

### 1 INTRODUCTION

Risk indicators in the offshore petroleum industry have traditionally been based on occurrence of injuries to personnel. This implies that the indicators that may be possible to present, are:

- Trends in the occurrence of injuries to personnel and near-misses, classified according to severity or potential severity
- Injury causation statistics

Such indicators are suitable for performance monitoring in the context of workplace injury (consequence up to one fatality). It has been claimed that such indicators can provide information about all safety aspects of an installation, i.e. also aspects of major hazard risk.

It may be argued that there is considerable similarity between occupational and major accidents, when it comes to root causes of organisational nature. Otherwise, the similarity would be expected to be very limited. Therefore, indicators for personal injuries have very limited applicability for monitoring of major hazard risk.

This may be further emphasized as follows: A traditional focus on near misses and motivation is no guarantee for the functioning of normally dormant safety barriers. The indicators based on events and HES culture therefore need to be supplemented with indicators reflecting the status of safety barriers, in order to illustrate the total picture.

In the recent NPD management regulations (NPD, 2001a) there is a clear requirement to monitor risk and present trends in indicators, which shall illustrate the relevant aspects of major hazard risk.

#### 1.1 Objectives

The Norwegian Government has initiated a research program to improve the safety level offshore. The program is led by the Norwegian Research Council and a network of Norwegian institutions has been established in order to realise the program. The ambition is to obtain more adequate tools for risk assessment and support for decision-making, in general and for the operational phases in particular. The present work is a part of this program.

The purpose of the paper is to propose a structured approach to definition of suitable risk indicators for major hazards for the offshore petroleum industry, based on a brief review of current usage, development plans and experience from existing projects.

## 1.2 Terminology

### 1.2.1 Risk dimensions

There are three main dimensions of risk according to Norwegian regulatory requirements, which has the following main elements:

- Risk to personnel
  - Occupational accidents
  - Major accidents
  - Occupational diseases
- Risk to environment
  - Accidental spill
  - Continuous release
- Risk to assets and production/transportation capacity
  - Accidental disruption

Unplanned and planned maintenance are also contributions to disruption of production and transport. These contributions are normally considered within regularity analysis. Regularity analysis may be considered as part of risk assessment, if a wide interpretation of the term is used, but may be more efficiently considered a separate analysis.

The main focus in the paper is risk to personnel, in particular major hazard risk in offshore systems.

### 1.2.2 Proposed terminology for barriers

The new Norwegian regulations for offshore installations and operations make extensive references to the term “barriers”. This term is not defined, but comments given in the regulations (NPD, 2001a) imply that barriers are actions that are intended to reduce the probability that faults or hazards develop into accidents or to limit or reduce injury, damage and other unwanted effects.

ISO Standard 17776 defines barrier as follows: “measure which reduces the probability of realising a hazard’s potential for harm and of reducing its consequence. Barriers may be physical, (materials, protective devices, shields, segregation, etc.) or nonphysical (procedures, inspection, training, drills)”.

This implies that NPD has adopted the ISO definition. This definition is wide and general, and includes a wide range of actions which may be considered a barrier. More precise or limited definitions have been searched for by several specialists.

Another application of the barrier concept is in relation to MTO analysis of accidents and incidents in the offshore petroleum sector (Bento, 1999). The term “barrier” is in this application given a wide definition, in line with the ISO definition.

The following definitions are proposed as more precise definitions of barrier related expressions, within the general definition adopted from ISO 17776. These definitions are proposed in the context of the present paper, for use in relation to barriers for major hazards and indicators in relation to such risk elements. The term “major hazard barrier” has been proposed in order to give a more precise definition of the wide term “barrier”:

Major hazard barrier	“Line of defence” relating to overall functions, as explained below.
Barrier element	Part of barrier, but not sufficient alone in order to achieve the required overall function, as explained below.
[Barrier performance] Influencing factor	Factors that influence the performance of barriers.

The NPD management regulations (NPD, 2001a) makes a distinction between physical barrier [elements] and non-physical barrier [elements]. The former are the “hardware” systems, whereas the latter are organisational, procedural or human elements.

The influencing factors are particularly important for non-physical barriers.

Barriers may be regarded as “lines of defence”, as illustrated in Figure 1 below.

Each of these levels will consist of several barrier elements, for instance (but not limited to) the following for the ignition prevention barrier:

- Automatic gas detection
- Manual gas detection
- Shutdown logic
- Procedures to limit open flame exposure, such as hot work procedures
- Area classification rules affecting protection of electrical equipment

[Barrier performance] Influencing factors are factors that influence the performance of barriers. Consider as an example the manual gas detection performed by

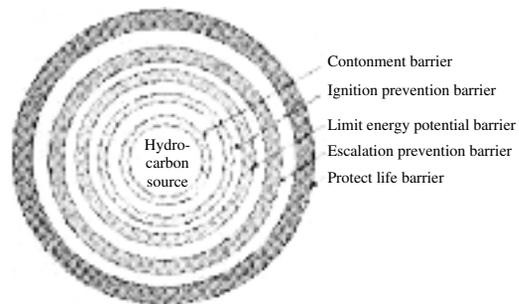


Figure 1. Illustration of “lines of defence” principle.

personnel performing manual inspection in the hydrocarbon processing areas. Factors that will influence the ability of such personnel to detect possible gas leaks are as follows:

- Procedures for manual inspections
- Organisation of work, work patterns
- Training of plant operators
- Experience of plant operators
- Motivation of plant operators
- etc.

Indicators may be defined for each of these factors, some of these are briefly suggested in Section 4 below.

Please note that what we here consider as influencing factors will often be considered as “barriers” according to the ISO or NPD definition as stated above.

### 1.2.3 Proposed terminology for indicators

This section proposes a structured terminology for indicators:

Risk indicator:	A measurable quantity which provides information about risk
Risk indicator related to activity:	A measurable quantity related to execution of defined operational activities, which provides information about risk
Risk indicator based on barrier performance:	A measurable quantity related to barrier performance, which provides information about risk
Risk indicator related to incidents:	A measurable quantity related to occurrences of accidents, incidents and near-misses, which provides information about risk
Risk indicator related to causal factors:	A measurable quantity related to causal factors for barrier performance, which provides information about risk
Risk indicator related to safety culture:	A measurable quantity related to safety climate/culture and its influence on the performance of barriers, which provides information about risk
Proactive (leading) risk indicator:	A measurable quantity which provides information about risk, explicitly addressing an aspect of future

performance (example; anticipated number of hot work hours next year)

Reactive (lagging) risk indicator:

A measurable quantity based on outcomes of accidents and incidents

It may be discussed whether “causal factors” and “influencing factors” are synonymous expressions, and to some extent they are. It may be argued that “influencing factors” is a wider term than “causal factors”, but little emphasis is placed on this here.

Sometimes the term “safety indicator” is used instead of or in addition to the term “risk indicator”. We use these terms as synonymous terms in this paper, meaning that safety indicator is a measurable quantity which provides information about safety. Both the terms safety and risk are used in a wide sense and for the purpose of this paper we have not distinguished between them. The term “risk indicator” is used throughout the paper.

## 2 RISK INDICATORS, OBJECTIVES AND REQUIREMENTS

### 2.1 Requirements to the use of risk indicators

#### 2.1.1 HES related requirements

The overall objectives may be broken down into specific requirements. Performance indicators for all types of offshore related accidents should meet the following requirements for indicator “goodness”:

- The total set of indicators should address a range of incidents, from the insignificant near-misses up to the most severe and complex accident sequences.
- If very different hazards are studied, an incident based indicator reflecting the potential for major accidents should be considered, alongside with individual indicators.
- Indicators such that they are discussed in this paper should primarily reflect aspects that are possible to influence from an operational point of view, although some indicators may not satisfy this requirement, but still be useful.
- Such indicators that are considered as intuitively important for personnel with practical operational/HES experience, should ideally be given priority.
- Indicators should give opportunities for risk reduction potentials that reflect physical accident mechanisms or causes which may be related to physical or non-physical aspects, as opposed to synthetic, simplified or artificial modelling parameters. Volume density of hydrocarbon processing equipment may illustrate such an artificial modelling parameter. Volume density is used as a parameter in escalation modelling. Volume density would be a rather useless risk indicator, as it is purely a synthetic modelling

parameter, which is not considered in design or operation [although there are aspects considered that implicitly have influence on the density].

The suitability of indicators is also dependent on which level the indicator is used for. This may also be related to the so-called “free variables”, i.e. quantities that are possible to change.

As an example, let us consider the activity risk indicator, the number of days with a certain [hazardous] activity, such as drilling. Clearly this indicator provides interesting information about risk, and consequently is a useful indicator, but it can be discussed to what extent it is related to a free variable. On the national level, the extent (or volume) of drilling activity may be considered a “free variable”, in relation to which regions or fields to be developed, whereas it is not at the same degree a free variable on the installation level as this activity in practice must be done, given the frame conditions for the activity on this installation.

On the installation level, more detailed indicators need to be added, to establish a proper set of indicators, and in order to reflect aspects that may be influenced through operational decisions. Such indicators include the type of drilling of well intervention activity, the number of effective barriers, porosity of the formation, the weight margin of the drilling fluid, etc.

Another aspect is related to whether to express annual values, or accumulated over the field lifetime. This is a general problem, but can be illustrated with reference to drilling. If a certain number of wells is needed in order to develop or maintain production, it will usually not imply overall reduced risk even if the drilling activities is spread out over several years, as opposed to completing the program in just one year.

One solution for this and similar cases is that the indicator reflects some kind of accumulated values. The disadvantage of such a solution will be a more complicated indicator, which will need to be considered over several years before conclusions may be drawn.

### 2.1.2 Formal requirements

There are a set of formal requirements that indicators should satisfy, in addition to the requirements relating to offshore petroleum HES management as outlined in Section 2.1.1 above. The indicators should satisfy the following formal requirements, and thus be (cf. Kjellén, 2000):

- observable and quantifiable
- sensitive to change
- transparent and easily understood
- robust against manipulation
- valid

It must be possible to observe and measure performance by applying a recognized data collection method and scale of measurement. Usually, the indicators are

expressed on a ratio scale of measurement, such as the Lost Time Injury (LTI) rate which expresses the number of injuries resulting in absence from work per one million hours of work. It is difficult to establish a data collection method that gives reliable data, i.e. the data corresponds to the quantity we would like to observe. For example, measuring the true number of LTIs is in practice often difficult. Recording of the events may be poor, and the data may be contaminated by extraneous factors such as rumours and direct manipulation.

Psychological and organizational reasons could in many cases result in a too low reporting. An example, we may think of an organizational incentive structure where absence of injuries is rewarded. Then we may experience that some injuries are not reported as the incentive structure is interpreted as “absence of reported injuries”.

A risk indicator must be sensitive to change. It must allow for early warning by capturing changes in an socio-technical system that have significant effects on accident risks. Clearly, the number of accidents leading to fatalities would not normally be sufficiently sensitive to change. The LTI rate is more sensitive, but also this indicator could be considered to be too insensitive for changes.

The “good” set of indicators will reflect changes in risk as well as point to aspects where improvements should be sought.

The risk indicators must also be robust against manipulation. The point is that the indicator should not allow the organisation to “look good” by for example changing reporting behaviour, rather than making the necessary basic changes that reduce accident risk.

This leads us to the requirement of validity, which is a critical point in the evaluation of the goodness of an indicator. Is the indicator a valid indicator for the accident risk? Does the indicator actually measure what we intend to measure? Consider for example the indicator defined by the number of lost time injuries. Clearly, this indicator say something about accident risk, but of course, the accident risk is more than the number of lost time injuries, so we cannot use just this indicator to conclude on development in the accident risk level as a whole. The validity of a statement concerning the accident risk based on observations of the injury rate only, would thus in most cases be low. But restricting attention to this specific type of injuries, there should be no validity problem, in this respect. But still we have problem in concluding on any development in the injury risk based on the observations from the indicator. This is discussed further in Aven (2003), Section 2.1.

### 2.2 Use of major hazard indicators at different levels

The following levels are discussed below:

- National level for offshore petroleum industry

- Company/Installation level
- Equipment level

One aspect which is valid on all levels is the need to address variations between the best and the worst units in addition to average levels.

It should also be noted that development of indicators on a higher level, may in theory be done by aggregating from a lower level. This is in practice seldom so simple, because other indicators may be more relevant on a higher level than just summing up from a lower level.

### 3 BASIC APPROACH – INDICATORS FOR MAJOR HAZARDS

#### 3.1 *Classification of indicators*

There are various ways to classify indicators, two classification schemes that are discussed in this paper, are the following:

- Classification of indicators reflecting how the data is collected
- Classification of indicators reflecting steps in the “accident chain”

Kjellén (2000) has classified indicators as:

- Loss based indicators
- Process based (i.e. accident sequence) indicators
- Indicators based on causal factors (including indicators related to safety “climate”)

Only for quite frequent occurrences indicators may be based on recording of actual losses, otherwise indicators for risk will have to be based on hydrocarbon processing parameters or causal factors.

Based on the discussion in the previous sections, the following types of indicators are required for major hazards:

- Incident indicator
- Barrier indicator
- Activity indicator
- Indicators related to causal factors (including indicators related to safety “climate”)

Incident indicators are based on occurrence of accidents, incidents and near-misses, and are as such reactive indicators. This type of indicator is nevertheless needed, as they give important information of what has occurred in the past. Indicators based on occurrence of accidents are loss related indicators, whereas indicators based on near-misses and similar are process related indicators.

Activity indicators are almost entirely proactive indicators, which are required in order to manage actively planning of activities on the installations and thereby minimise major hazard risk. Activity indicators

have not been utilised to any significant extent so far, but shall reflect major hazard risk due to execution of operational activities on the installations.

Indicators related to causal factors are a separate category by both classifications. This category will naturally include safety “climate” indicators.

#### 3.2 *Use of indicators and risk assessments*

The following principles are used as basis for development of risk indicators for major hazards:

- The main perspective is to provide tools for expressing quantities which provide information about future risk exposure, with basis in current status and past performance, in order to provide input to decision-making.
- Risk indicators should have the main emphasis on illustrating effect on risk of variable parameters.
- A mix of proactive and reactive indicators may be required in order to give a comprehensive presentation of risk levels.

The results from risk analysis may be used to give weights to different risk indicators, and such use is valuable. It is on the other hand not recommended to use risk indicators in a “mechanistic” updating of overall expressions of risk levels. Indicators, usually based on observations, will have to be combined with adjustments and evaluations, if an evaluation of the risk level shall be produced. If this is done in a justifiable manner, then risk indicators may be used for updating overall estimations of risk levels.

The risk assessment results may also be used for identification of and setting of priorities for different risk mechanisms, based on their contribution to total risk. The risk assessment results may also be used as a basis for establishing weights for the different contributions, if they are being added up to some kind of total value.

#### 3.3 *Accidents, incidents and near-misses*

Loss based indicators will imply indicators reflecting occurrence of accidents. This requires as mentioned above, that the volume of accidents is sufficiently high for the extent of installations and operations being considered, in order to establish an indicator based on such events. This will usually be the case, if at all, for only some kind of hazards, for instance occupational injuries.

But even if the number of occupational injuries may be substantial, it will rarely be sufficient accident data to establish an indicator for fatality risk due to occupational hazards.

Indicators based on incidents and near-misses (process related indicators) are therefore required.

All these indicators are based on actual occurrences, where the valuable information will be much more than just the number of occurrences. Actual cases may also give very valuable qualitative information about mechanisms, causal factors, etc.

Indicators based on accidents, incidents and nearmisses may be weighted and normalised as follows:

Weighted	Rating of types or categories of events according to severity, thereby implying that weighted indicators may be combined in order to create overall indicators of different kinds.
Normalised	Rating of indicators (may be regarded as weighting) in relation to volume of exposure measured according to a relevant parameter reflecting the type of risk exposure.

### 3.4 Barrier performance

Indicators that are reflecting barrier performance (in a wide sense) belong to the category “process related indicators”, together with indicators based on occurrence of incidents and near-misses as well as activity indicators. The performance should cover the following barriers:

- Physical barriers
- Non-physical barriers (organisational, administrative, procedural, etc)

The performance should in general cover a wide range of capabilities (cf. NPD, 2001b):

- Functionality and effectiveness
- Reliability and availability
- Robustness (antonym to vulnerability)

In certain circumstances incident indicators and indicators related to barrier performance may be combined into an overall indicator (see further discussion in Section 4).

### 3.5 Activity level

A review of hydrocarbon leaks on the Norwegian Continental Shelf in 2001 and 2002 has revealed (Husebø et al., 2003) that less than one third of the leaks occur during normal operations, whereas a dominating majority occurs when special operations are being carried out, such as maintenance, inspection, manual intervention, trips etc. This situation emphasises the need to develop risk indicators that reflect major hazard risk as a function of the activities being carried out.

Activity indicators are almost entirely proactive indicators. The basis for development of activity indicators has not yet been developed extensively. The basis

will have to reflect risk exposure due to:

- Performance of single activities, and/or
- Performance of simultaneous activities, and/or
- Absence of completed maintenance activities on safety critical equipment according to plan.

Activity indicators may be used in order to estimate the expected risk exposure according to activity plans and combinations, and also for optimisation of operational plans. A development project has been launched as part of the programme outlined in Section 1.1.

### 3.6 Causal factors

Indicators for causal factors may cover a wide range of aspects, relating to causes of incidents and nearmisses, as well as failure of physical barriers (technical safety systems) and non-physical barriers (human, administrative and organisational functions).

One example of causal factors behind occurrence of incidents can be the split of ongoing operations at the time of occurrence of hydrocarbon leaks, as referred to in Section 3.5. Other examples may include records showing the percentage of personnel having participated in vital safety training or safety motivation courses or campaigns.

To establish accurate models of how causal factors relate to possible accidents and losses, is difficult – the uncertainties are very large. Extensive R&D efforts are required to obtain models with sufficient credibility. Data directly supporting the models will seldom be present, and extensive assumptions need to be made to establish the models. Nonetheless, such models may be useful to get insights – what are the critical factors and how do different factors correlate? – and study the impacts on risk of various theories and hypotheses related to the importance of causal factors. The models should be seen as instruments for structuring knowledge and uncertainties, more than accurate tools for prediction.

Causal factors also include what could be called management system factors and cultural aspects.

## 4 RECOMMENDED INDICATORS

There are few hazards where major hazards related indicators based on actual loss may be used, implying that indicators for most of the hazards have to be based on process related indicators. Indicators for these two hazards on a national level may be found in the NPD annual report for risk level on the Norwegian Continental Shelf, see Husebø et al. (2002).

There are few loss based indicators that are possible for major hazards. There are therefore many indicators for major hazards that need to be based on modelling of losses.

Causal factors for major hazards are limited to performance of barriers for major hazards. Potential causes for major hazards may be classified as:

- Technical
- Human performance
- Organisational

## 5 CONCLUSIONS

The following indicators are required for a comprehensive risk monitoring of major hazard risk:

- Incident indicator
- Barrier indicator
- Activity indicator
- Indicators related to causal factors, including indicators related to safety “climate”

Few loss related indicators are feasible for major hazards, only on the national level. For major hazard risk, most of the indicators will have to be of the process related type and causal indicators.

The recommendations for use of loss related indicators, process related indicators and indicators relating to causal factors are briefly indicated in Section 4.

## TERMINOLOGIES

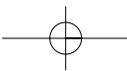
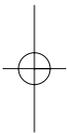
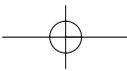
HSE	Health and Safety Executive
HES	Health, Environment and Safety
ISRS	International Safety Rating System
KPI	Key Performance Indicator
LTJ	Lost Time Injury
MTO	Man, Technology, Organization
NFR	Norwegian Research Council
NPD	Norwegian Petroleum Directorate
PFEER	Prevention of Fire and Explosion, and Emergency Response
QRA	Quantified Risk Assessment
RNNS	Risk level on the Norwegian Continental Shelf (“Risikonivå norsk sokkel”)
TTS	Technical condition of safety systems (“Teknisk Tilstand Sikkerhet”)

## ACKNOWLEDGEMENT

The authors are indebted to NFR for the funding of the work and their parent organisations for the permissions to publish this paper. During the preparation of the paper, a large group of specialists has been consulted at various stages, orally and in writing. We are obliged to all those that have provided comments, for the time they have taken to review and provide very valuable input to the paper writing.

## REFERENCES

- Aven, T., 2003. Foundations of Risk Analysis. Wiley, N.Y. to appear.
- Bento, J-P., 1999. Human – Technology – Organisation; MTO-analysis of event reports. OD-00-2. (In Swedish). Restricted.
- Husebø et al., 2002. RNNS report 18.4.2002.
- Husebø et al., 2003. RNNS report April 2003 (to be published).
- Kjellén, U., 2000. Prevention of Accidents Through Experience Feedback. Taylor & Francis, London & NY.
- NPD, 2001a. Regulations relating to the management in the petroleum activities, (The management regulations), issued 3.9.2001.
- NPD, 2001b. Guidelines to the management regulations, issued 3.9.2001.
- The learning lab, 2002. [http://www.laeringslaben.no/index\\_english.php?side=2](http://www.laeringslaben.no/index_english.php?side=2)
- Statoil. 2002. “Technical safety Conditions in Statoil, Main report”, Statoil F&T MST 2001-0181, January 2002
- Vinnem, J.E., 2000. Risk Monitoring for Major Hazards, SPE61283, SPE International Conference on Health, Safety and the Environment in Oil and Gas Exploration and Production in Stavanger, Norway, 26–28 June 2000.
- Vinnem, J.E., Tveit, O.J., Aven, T., Ravnås, E. 2002. Use of risk indicators to monitor trends in major hazard risk on a national level, ESREL 2002, Lyon, France, 18–21 March 2002.
- Øien, K., Sklet, S., 1999. Risk indicators for the surveillance of the risk level on Statfjord A. (In Norwegian. Confidential). SINTEF Report STF38 F98435, Trondheim: SINTEF Industrial Management, Norway.
- Øien, K., Sklet, S., 2001. Risk Analyses during Operation (The Indicator Project) – Executive Summary. SINTEF Report STF38 A01405, Trondheim: SINTEF Industrial Management, Norway.



## A contribution to vehicle life cycle cost modelling

Z. Vintr & R. Holub

*Military Academy in Brno, Czech Republic*

**ABSTRACT:** This article deals with a method of maintenance concept optimization that allows reduction of life cycle costs (LCC) of a vehicle on the basis of knowledge of operating reliability data. The authors present a theoretical model of optimization, describing the basic relationships between the LCC of the main vehicle's sub-systems and the frequency of their scheduled (preventive) repairs. This article describes in detail an applied mathematical model and it also analyses the possibilities and conditions of its practical use for optimization of the conception of vehicle maintenance. Practical application of the proposed method is demonstrated on an example of optimization of the period of replacement of the vehicle drive train subsystem that is performed as a part of its preventive maintenance.

### 1 INTRODUCTION

In the Army of the Czech Republic, a large number of heavy military vehicles were observed in service over a long time period to collect data on their reliability and maintainability, including relevant economic data. The data obtained were used for determination of basic dependability characteristics of the vehicle and its main sub-systems and for analysis of the vehicle's LCC. Among other findings, the results of this analysis showed an unsatisfactory level of the costs associated with maintaining the vehicle. For this reason, it was decided to look for ways to reduce maintenance costs through a change of the maintenance concept of the vehicle.

The solution was limited by the requirement not to change the basic principles of the maintenance concept, which are determined by the general maintenance policy of the army. This meant that the improvement desired could be achieved only through a change in the frequency of preventive maintenance. The original maintenance concept of the vehicle included in addition to classical preventive maintenance actions, scheduled repairs with the aim to replace or repair the stated vehicle's sub-systems and parts whose life cycle is shorter than the expected vehicle life cycle. The accomplishment of these scheduled repairs is very expensive and represents a decisive part of preventive maintenance costs of the vehicle. For these reasons, it was decided to analyze especially the influence of these repairs' frequency on the amount of maintenance costs.

As a solution to the above-mentioned tasks, the article's authors created a mathematical model describing relationships between the overall life cycle costs (LCC) of the vehicle and frequency of the prescribed maintenance actions. This model allows us to determine the frequency of repairs in which LCC of the vehicle reaches the minimal level.

### 2 NOTATION

$c(t)$	average unit cost during operating time $t$ ;
$C(t)$	cumulative cost during operating time $t$ ;
$u(t)$	instantaneous unit cost in the operating time instant $t$ ;
$u_R(t)$	instantaneous unit cost for repairs in the operating time instant $t$ ;
$t$	operating time;
$t_{opt}$	optimal length of maintenance period;
$C_C$	total life cycle cost of the subsystem;
$c_C(t)$	average unit cost of life cycle;
$c_{C min}$	minimized average unit cost of life cycle;
$C_B$	acquisition price and costs related to subsystem replacement;
$c_B(t)$	unit acquisition cost related to the operating time $t$ ;
$C_M$	total cost for preventive maintenance;
$C_M(t)$	cumulative cost for preventive maintenance during the operating time $t$ ;
$c_M(t)$	average unit cost for preventive maintenance during the operating time $t$ ;

- $C_R$  total cost for repairs of the subsystem;
- $C_R(t)$  cumulative cost for repairs during the operating time  $t$ ;
- $c_R(t)$  average unit cost for repairs during the operating time  $t$ ;
- LCC life cycle cost.

### 3 DESCRIPTION OF VEHICLE LIFE CYCLE COSTS

To express the dependencies under research, the presented mathematical model employs three different methods to describe the LCC of the vehicle. The model expresses the costs as cumulative or average unit costs, or so-called instantaneous unit costs are used.

#### 3.1 Cumulative costs

At each instant of time, the cumulative costs represent the sum of all costs of a given type from the beginning of service up to that certain instant of time. In general, these costs gradually increase with the operating time. In experiments (in service), the cumulative costs are usually the easiest to identify, as it is the most often evaluated economic value. Dependency of cumulative costs upon the operating time usually does not have a continuous character, and therefore various mathematical models often substitute for this dependency.

#### 3.2 Average unit costs

At a given instant of a time  $t$ , average unit costs are defined as the quotient of cumulative costs expended during the operating time  $t$  to the operating time  $t$ :

$$c(t) = \frac{C(t)}{t} \tag{1}$$

Average unit costs express the average costs attributed to the unit of operating time in any instant of operating time  $t$ .

#### 3.3 Instantaneous unit costs

Instantaneous unit costs are defined by the following relationship (if the appropriate derivative exists):

$$u(t) = \frac{dC(t)}{dt} \tag{2}$$

Instantaneous unit costs in each instant of time characterize "speed" with which the pertinent costs are expended. It is obvious from the above-mentioned relationship that:

$$C(t) = c(t) \cdot t = \int_0^t u(x) \cdot dx \tag{3}$$

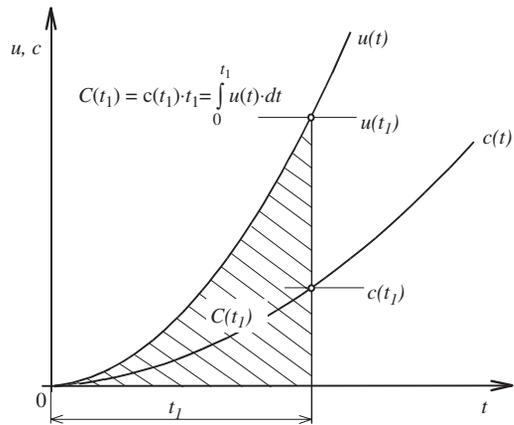


Figure 1. Graphical presentation of relationship between unit costs and instantaneous cost rate.

Graphical presentation of dependencies expressed by Equation 3 is shown in Figure 1.

### 4 OPTIMIZATION OF MAINTENANCE PERIOD MODEL

Consider a vehicle in the design of which a certain subsystem is used, and a periodic replacement is carried out as a form of preventive maintenance.

The subsystem's faults detected in service are corrected by repair of the subsystem. In addition, the subsystem under research undergoes a scheduled preventive maintenance consisting of a simple checkout and setting-up. The aim of optimization is to determine a period of replacement for the subsystem so as to minimize the vehicle unit life cycle costs. Let us assume that all necessary subsystem technical-economic data are known.

The proposed optimization model disregards those components of LCC which are not influenced by the scheduled maintenance action and that cannot influence our optimization. In this case, it is possible to express the total LCC of the subsystem by:

$$C_C = C_B + C_M + C_R \tag{4}$$

It is further assumed that the subsystem acquisition price is constant and does not depend on the operating time and that preventive maintenance costs and subsystem repair costs depend on the operating time. Based on these assumptions and using Equation 4, the average unit LCC of the subsystem can be expressed as a function of the operating time:

$$c_C(t) = \frac{C_B}{t} + \frac{C_M(t)}{t} + \frac{C_R(t)}{t} \tag{5}$$

All terms of the sum at the right-hand side of Equation 5 have the character of average unit costs of the respective type. For further solution, it is assumed that term which expresses the average unit costs for preventive maintenance is constant:

$$\frac{C_M(t)}{t} = c_M \tag{6}$$

Detailed justification of this assumption is provided in the next section. With this presumption, we can adjust Equation 5 into the following form:

$$c_C(t) = \frac{C_B}{t} + c_M + \frac{C_R(t)}{t} \tag{7}$$

The aim of optimization is to find, for a subsystem under research, the length of the maintenance period – operating time to replacement of the subsystem  $t$  – which will ensure that the unit costs expressed by Equation 5 will be minimized. Our solution of this optimization task consists in identification of local minimum of the function  $c_C(t)$ . For that, Equation 7 should be differentiated with respect to time:

$$\begin{aligned} \frac{dc_C(t)}{dt} &= \frac{d\left(\frac{C_B}{t}\right)}{dt} + \frac{dc_M}{dt} + \frac{d\left(\frac{C_R(t)}{t}\right)}{dt} \\ &= -\frac{C_B}{t^2} + \frac{\frac{dC_R(t)}{dt} \cdot t - C_R(t)}{t^2} \end{aligned} \tag{8}$$

Using the Equations 1 and 2, which define unit costs and instantaneous costs rate, for further solutions, the following values can be established:

– average unit cost for acquisition of the subsystem:

$$c_B(t) = \frac{C_B}{t} \tag{9}$$

– average unit cost for repairs of the subsystem:

$$c_R(t) = \frac{C_R(t)}{t} \tag{10}$$

– instantaneous unit cost for repairs:

$$u_R(t) = \frac{dC_R(t)}{dt} \tag{11}$$

Using these values, the Equation 8 has the form:

$$\frac{dc_C(t)}{dt} = \frac{-c_B(t) + u_R(t) - c_R(t)}{t} \tag{12}$$

Setting Equation 12 equal to zero yields:

$$u_R(t) = c_B(t) + c_R(t) \tag{13}$$

From this equation, it is evident that optimum length of maintenance period of the subsystem is the value of  $t$  for which the instantaneous unit costs for repairs equals to the sum of average unit costs for subsystem repairs and acquisition.

Figure 2 shows a graphical representation of the mathematical model above described. From Figure 2, it is obvious that optimization condition expressed by Equation 13 is met for a maintenance period of  $t_{opt}$ , where the function  $c_C(t)$  attains its minimum (point D

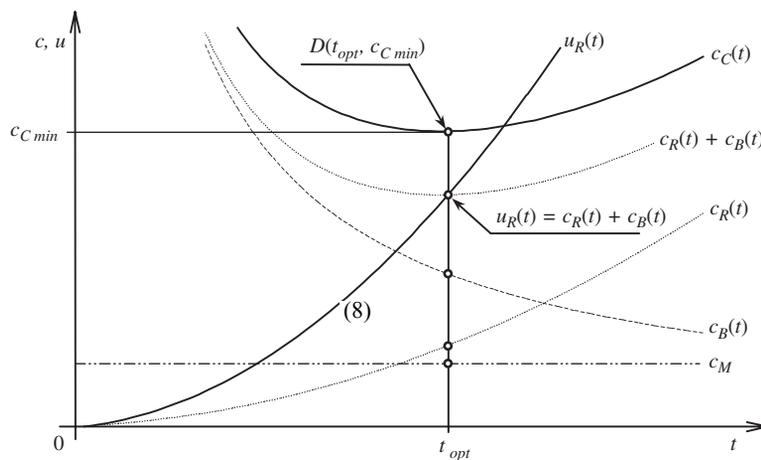


Figure 2. Graphical representation of optimization model.

on the graph of this function). Thus, if the subsystem under research will always be disassembled after the operating time  $t_{opt}$  and replaced by a new one, the unit LCC of the subsystem will be minimized:

$$c_C(t_{opt}) = c_{C \min} \quad (14)$$

## 5 ANALYSIS OF THE OPTIMIZATION MODEL

A basic condition for application of the described optimization method is to have a suitable (convex) shape of the curve  $c_C(t)$ . An important condition for optimization is a sufficiently strong local minimum in point D ( $t_{opt}$ ;  $c_{C \min}$ ), which will enable relatively precise identification of a location of this point even if the technical-economic data are not complete.

This section provides a more detailed discussion about the character of individual elements of costs (functional dependencies), which are included in the optimization model and a possibility of how to determine them.

### 5.1 Average unit cost for acquisition of a subsystem

Function  $c_B(t)$  expressing a dependency of average unit costs for acquisition of a subsystem upon the operating time is defined by Equation 9. Graphical representation of this function is an equilateral hyperbola. The value of this function decreases with extending of operating time.

### 5.2 Average unit cost for preventive maintenance

The function  $c_M(t)$  expresses the dependency of unit costs for preventive maintenance upon the operating time:

$$c_M(t) = \frac{C_M(t)}{t} \quad (15)$$

where  $C_M(t)$  expresses the sum of all costs connected with execution of subsystem preventive maintenance during the operating time  $t$ . Material, wage and support equipment costs connected with maintenance execution are included. The presented optimization model is based on the assumption that preventive maintenance is carried out in accordance with a schedule and consists in execution of periodic stated maintenance actions. The extent of individual preventive maintenance actions does not substantially vary with operating time, thus the average unit cost for preventive maintenance can be considered constant:

$$c_M(t) = c_M \quad (16)$$

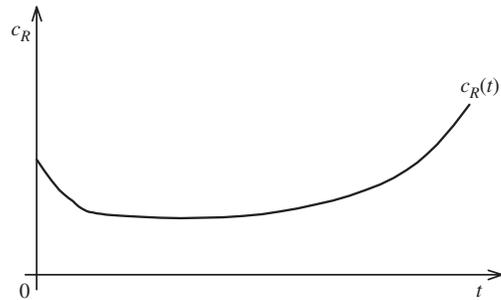


Figure 3. Example of actual course of unit repair costs.

This conclusion implies that knowledge of costs for execution of preventive maintenance is not necessary for optimization. In other words, the preventive maintenance costs affect the value of total life cycle cost of a subsystem – see Equation 5, but they do not influence the value of the optimum maintenance period  $t_{opt}$  – see Equation 13.

### 5.3 Average unit cost for repairs of the subsystem

Equation 10 expresses the dependency of the average unit cost for repairs of a subsystem upon its operating time. A graph of the function  $c_R(t)$  shown in Figure 2 intersects the co-ordinate origin and it increases within the whole scope of studied values of operating time of functions. This interpretation is rather simplified because a real course of the function  $c_R(t)$  usually includes three different parts – running in, phase of constant failure rate a phase of wear-out failures. A possible actual course of the function  $c_R(t)$  is depicted in Figure 3.

Despite all mentioned deviations of the theoretical model from reality, it is obvious that the assumption about the increasing character of the function  $c_R(t)$  is quite acceptable and not in contradiction with reality. If this precondition is not met in certain portions of service time, the optimization model will be affected negligibly.

However, knowledge of the function  $c_R(t)$  is a precondition for optimization. The presented model assumes that the course of this function will be based on the results of observation of a group of vehicles in service (several hundreds of vehicles). The whole time of subsystem service will be divided into a final number of the same time periods and in each of these periods, the cumulative costs expended for repairs of a given subsystem in all vehicles will be observed.

From these costs, the average cost per vehicle in each period of service can be easily established, and from them, a number of discrete values representing the time development of cumulative costs for repair of the subsystem can be determined. These discrete values can

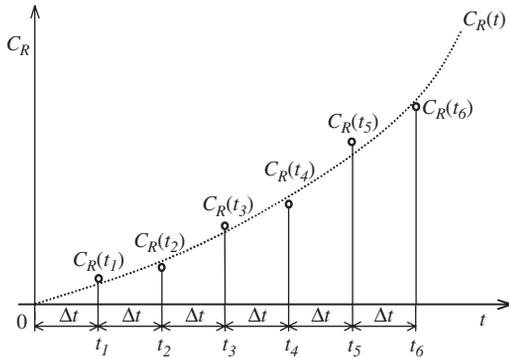


Figure 4. Approximation of discrete values by a suitable function.

be, for the purpose of further solution, approximated by a suitable function  $C_R(t)$  (e.g. by a method of least square). This function can be used to obtain the average unit repair cost  $c_R(t)$  and the instantaneous unit cost for repairs  $u_R(t)$ . Figure 4 shows an example of using discrete values to develop the cumulative costs for repairs function.

### 6 EXAMPLE OF PRACTICAL APPLICATION OF THE OPTIMIZATION MODEL

The proposed mathematical model was used for optimization of the maintenance concept of military heavy tracked vehicles fielded in the Army of the Czech Republic. In this section the process of optimizing the maintenance period for the vehicle drive train is presented. The applied concept of vehicle maintenance required performing a scheduled preventive repair, consisting in a given subsystem replacement, after covering 12,000 km.

Based on long-term observation of a great number of vehicles, the costs related to repairs of failures of this subsystem were evaluated. The subsystem life cycle was divided into 12 sections (1000 km each), and for each section of service, the average costs attributed to the subsystem repairs were determined. The observation results are shown in Table 1.

From these data, the values characterizing a time development of cumulative costs for the subsystem repairs were calculated. Table 1 provides a survey of the calculated values. The method of least squares was applied to these discrete values to develop a third-order polynomial approximation of the cumulative repair costs of the subsystem (Fig. 5). Then, by suitable conversion of this polynomial function, a course of the average unit cost for repairs and the instantaneous unit cost for repairs was obtained. A mileage of 1 kilometer was used as a unit of service to which the

Table 1. Survey of observation results and calculated results.

Interval of operating time (km)	Average repair costs (\$)	Time development of cumulative repair costs $C_R$ (\$)
0–1000	333	333
1000–2000	260	593
2000–3000	242	835
3000–4000	307	1142
4000–5000	326	1468
5000–6000	296	1764
6000–7000	287	2051
7000–8000	361	2412
8000–9000	338	2750
9000–10,000	412	3162
10,000–11,000	503	3665
11,000–12,000	661	4326

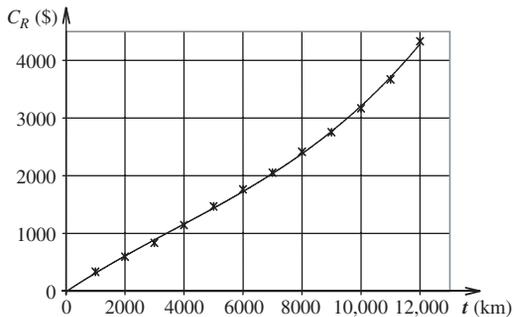


Figure 5. Approximation of the time development of cumulative costs for repairs.

unit costs are related. From the subsystem acquisition price of \$12,000, a time dependency of the average unit cost for subsystem acquisition was also derived.

Graphical presentation of the resulting dependencies is shown in Figure 6. As evident from the charts in Figure 6 the subsystem is replaced much sooner than its optimum period of service is achieved. If the subsystem was not replaced and left in the vehicle for further use (until its optimum length of operating time is achieved), then the total unit costs would continue to decrease. Thus, replacement of the subsystem after covering 12,000 km is not optimum in terms of cost efficiency.

In this case, it is not possible to establish an exact optimum maintenance period since no data about the behavior of the subsystem after 12,000 km are available. However, from the charts in Figure 6 it can be anticipated that optimum operating time will probably be within 15,000 – 17,000 km. In accordance with the above-mentioned conclusions, a change of operating

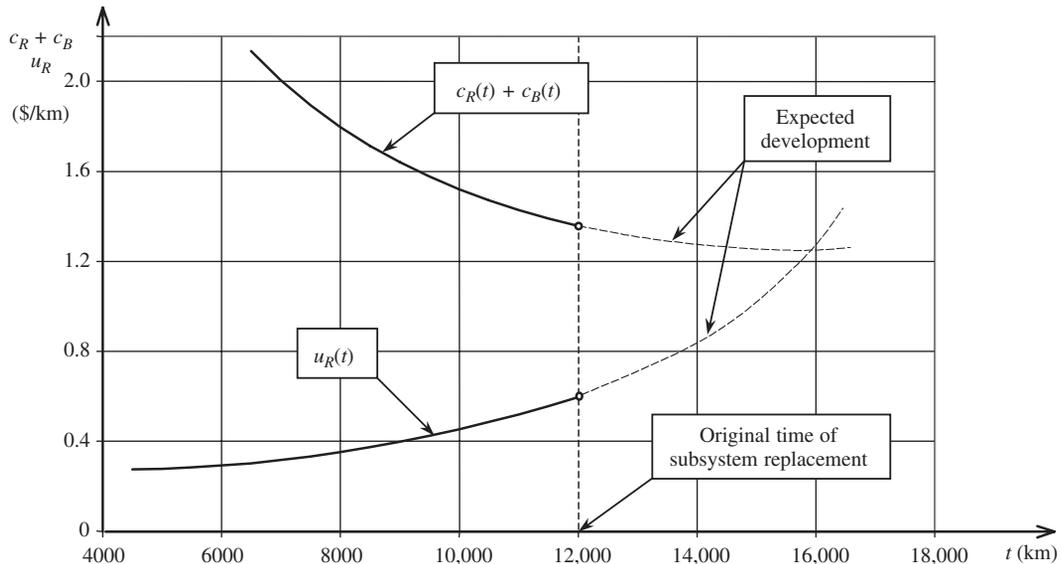


Figure 6. Graphical model of optimization.

time to the replacement of the observed subsystem from 12,000 km to 15,000 km was recommended. Using the described method, a suitable replacement time for all subsystems and vehicle parts where the applied concept of maintenance (replacement) is used was evaluated.

In cases when this evaluation revealed that the operating time to replacement of the subsystem or part is not optimum (it is shorter or longer), the appropriate changes were recommended. Justification of recommended changes in the conception of vehicle maintenance would be verified in the next observation of vehicles with modified periods of maintenance.

## 7 CONCLUSION

The presented method indicates that data from observation of vehicle operational reliability can be with success employed for optimization of conditions of their maintenance. By means of proposed model, it is relatively easy to find reserves in conception of vehicle maintenance and by using a simple measure – administrative change of maintenance periods – to attain significant savings in the vehicle LLC.

## ACKNOWLEDGEMENT

We are pleased to thank the Ministry of Defense of the Czech Republic that supported development of this method of optimization.

## REFERENCES

- Havlicek, J. et al. 1989. *Operating Dependability of Machines*. Prague: SZN. (in Czech)
- Vintr, Z., Holub, R. & Stodola, J. 2002. Optimization of Vehicle Life Cycle Costs with Usage of Operating Data. *Proceedings of 2002 FISITA – World Automotive Congress, Helsinki, 9–11 May 2002*. Helsinki: SALT. (CD-ROM).
- Vintr, Z. & Holub, R. 2003. Preventive Maintenance Optimization on the Basis of Operating Data Analysis. *Proceedings of Annual Reliability and Maintainability Symposium, Tampa, 27–30 January 2003*. Tampa: IEEE.
- Villemeur, A. 1992. *Availability, Maintainability and Safety Assessment*. New York: John Wiley & Sons.

## Method for correlation of failure data from durability tests and field of automotive engine parts with spontaneous failure mode

M. Vogt & H.R. Neu

*Robert Bosch GmbH, Schwieberdingen, Germany*

**ABSTRACT:** Determining of the level of fatigue present in components that were used in the field, is an important basis for the implementation of accelerated testing. This paper presents a method which enables fatigue determination of intact but pre-aged components that fail spontaneously. In the beginning components which have been field tested are exposed to additional laboratory testing. Then a fictitious lifetime is computed from the weighted sum of the field lifetime and the laboratory lifetime. These components are then compared against pure laboratory-aged, reference parts using the maximum-likelihood method as the comparison criterion. The weighting coefficient is then determined so that the distribution of the fictitious lifetime agrees well with that of the reference parts. Finally the ratio of the failures can be derived from the comparison of field-aged and laboratory tested parts.

### 1 INTRODUCTION

The modern automobile is becoming not only technologically more complex but also the customers expect their cars to last longer. For these reasons component and system reliability has high importance in the automotive industry. During the process developing products for the automotive industry, testing is becoming an increasingly time- and cost-consuming process. But the decreasing development time for new automotive products leads to minimized testing time being required. Additionally, legal and market requirements concerning warranty and life expectancy are rising. Especially the US-market demand of 240,000 km useful life has led to a new definition of testing conditions.

To determine the product lifetime accelerated testing is usually carried out. The purpose of accelerated testing is to find laboratory conditions which are most representative to field conditions that the components experience.

### 2 TESTING OF AUTOMOTIVE COMPONENTS

Automotive components can be fatigued by many different physical or chemical mechanisms (e.g. temperatures, temperature cycles, chemical media, water, salt spray, vibrations etc.). These mechanisms occur

with different stresses which can be quantified in the following units

- mileage in kilometers
- operating time in hours
- useful life in years
- number of starts  $n$
- number of cold starts  $m$
- ...

In reality these different influences arise coupled. But the aging of the component can usually be described with one main fatigue mechanism.

The method described in this paper is based on a classic Weibull Method (Fahrmeir et al. 1997; Hartung 1998; VDA (Hrsg.) 2002; Robert Bosch GmbH (Publ.) 2000), which is often used to evaluate failure data from technical parts. It is applied in the second order-parametric form. Therefore, the reliability  $R(t)$  of a part can be described by means of the time  $t$  by

$$R(t) = e^{-\left(\frac{t}{T}\right)^b} \quad (1)$$

with the characteristic lifetime  $T$  and the parametric variable  $b$ .

During laboratory testing methods are used to accelerate the component testing and aging are used. But first, theoretical methods must be used to derive

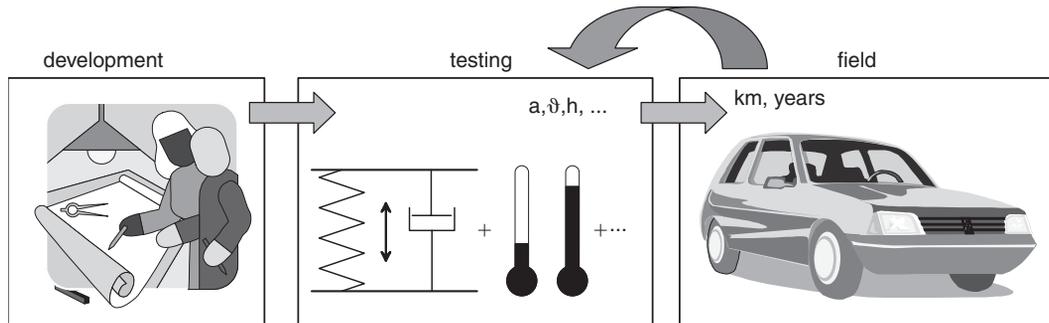


Figure 1. The influence of field experience on the testing of automotive parts.

the laboratory test conditions which best represent the loads components experience in the field. In practice, sometimes theoretically determined values used in laboratory testing does not quantitative correlate to actual load values seen in field service. Often field parts show substantially smaller fatigue or wear, then is expected based on the laboratory testing results. For this reason a method is required to provide a better correlation between laboratory and field results (Vogt & Neu 2002).

### 2.1 Survey of field data

It should always be taken into account that laboratory testing is always just a model of the field. From statistical point of view, the field itself is the best data source, due to the large sample population. Therefore, it is useful to analyze parts, which have seen field use in order to gain extra information. This practice also is a significant step required to fulfill the laws demanding that a product be observed over its entire lifetime in the field.

During the warranty period, there is usually a good basis for field data, in that all defective parts are registered and evaluated. But this data is often insufficient for developing an end-of-life test, because the parts usually exhibit no wear. These parts fail accidentally at a premature point in time. Data from the end-of-life is under-represented with only few data points from warranty information.

The access to fatigued parts from the field and the corresponding time of failure is difficult. The registration of all failed field parts during the vehicle and component lifetime would be very complex, especially for suppliers. As such the total number of parts that have failed in field, during the whole lifetime, is unknown. Therefore, as an alternative method to generate end-of-life data, intact parts are taken out of the field and their level of fatigue and remaining lifetime is determined.

### 2.2 Evaluation of intact field parts

The basis of the developed method is the collection of used field parts, which are intact and have not yet failed. The data

- mileage in kilometers
- first date of registration
- date taken out service or demounted
- vehicle type
- motor type

has to be known to interpret the results.

In the following example derivation, the mileage is used to represent load. But the variables for the number of starts, cold starts etc. which were described in part 2 could be used as well. The hours of service or operating time is used to describe the laboratory load. Alternatively, temperature or stress cycles could also be used. It is only important that component fatigue increases with increasing time or cycles.

The level of fatigue has to be determined exactly to obtain a quantitative connection between the laboratory and field data. The basic assumption is that the testing time  $t_L$  in laboratory leads to an equivalent level of fatigue  $S$  compared the mileage  $s_F$  in the field. If the fatigue of the part is measurable and quantifiable, this comparison will be simple. In this case a measurable characteristic exists. The comparison of parts aged in laboratory with those field aged leads to a quantifiable connection between laboratory testing time and mileage accumulated in the field.

This leads to the correlation coefficient  $c_K$  deduced from laboratory wear  $S_L$  and field wear  $S_F$  to

$$c_K = \frac{\Delta S_L}{\Delta t_L} \cdot \left( \frac{\Delta S_F}{\Delta s_F} \right)^{-1} \quad \text{with } [c_K] = \text{km/h} \quad (2)$$

with the mileage in field  $s_F$  and the testing time  $t_L$ . The degree of mechanical wear can be described with this method (Fig. 2).

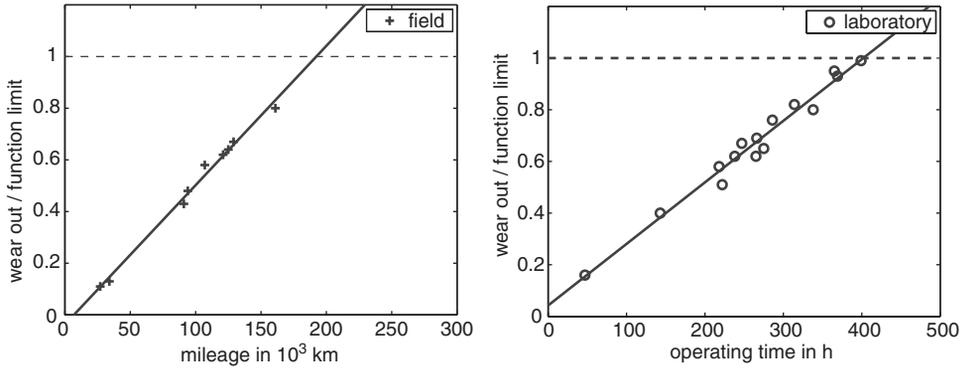


Figure 2. Scaled wear to correlate field and laboratory with variable characteristics.

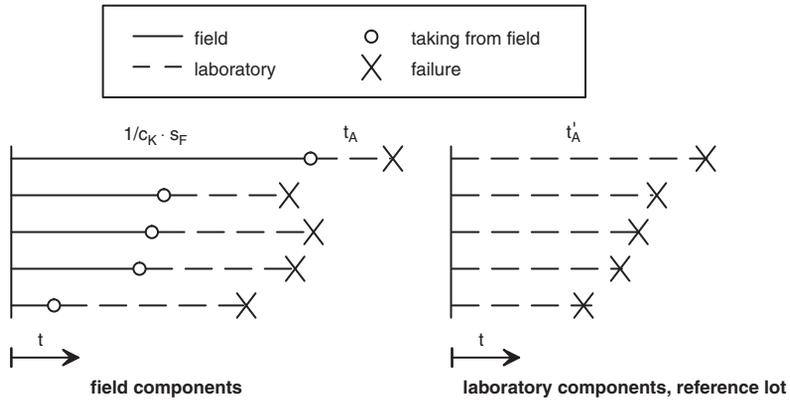


Figure 3. The principle of evaluating attributive characteristics.

The level of fatigue in many parts cannot be quantified, e. g. broken wires, or the short circuiting of isolators. The stress leads to a fatigue building up but with full functionality of the part still being maintained. Then, at the end of its lifetime the part fails spontaneously, but the point in time when this failure occurs is not predictable. The remaining lifetime of intact parts taken from field can not be given exactly, because of this spontaneous failure mechanism.

### 3 QUANTIFYING THE LEVEL OF FATIGUE

As the level of fatigue in parts returned from field service is not directly measurable, intact parts from the field are operated in laboratory until they fail (Fig. 3). These parts fail, spontaneously after the operating time  $t_A$ . This time is shorter than that of a new part  $t'_A$ , because the field part is pre-aged<sup>1</sup>.

These field-aged parts undergo an additional aging in laboratory are fatigued twice with two different levels of stress. To take this into account, the fatigue accumulation hypothesis analog to (Haibach 1989) that with the thesis of Palmgren/Miner is used. Under this premise, the sequence of loading is not significant. The sum of the wear and tear on the part  $S_{sum}$  is the sum of the individual fatigues. This leads to

$$S_{sum} = \sum_{i=1}^{\infty} S_i \tag{3}$$

with the individual fatigues  $S_i$  from laboratory and field.

The assumption that both experienced fatigues are interchangeable, leads to the fictitious summing of the operating time  $t_{sum}$  which can be defined as

$$t_{sum} = \frac{1}{C_K} s_F + t_A \tag{4}$$

<sup>1</sup>Reference values are marked with an apostrophe.

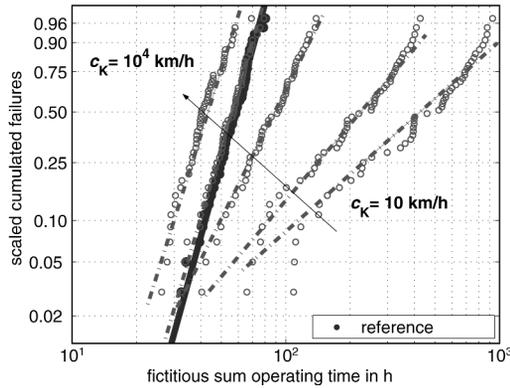


Figure 4. Weibull curves for different correlation coefficients  $c_K$ .

with the sum of mileage  $s_F$  in field converted into time and length of time operating in laboratory  $t_A$  until the point of failure. The correlation coefficient has the range  $c_K = 0 \dots \infty$  and is unknown at the beginning. For  $c_K = 0$  one extreme is defined as the length of time that the part was only aged by field stress. The other extreme  $c_K \rightarrow \infty$  is defined when the part is only fatigued by laboratory testing. The value of  $c_K$  increases with increasing stress in laboratory, such as e.g. elevated temperatures. As the factor relating to laboratory fatigue increases the sum total fatigue increases Proportionally. The value of the coefficient can be interpreted as a measure of the test acceleration.

To separate the factors of laboratory and field aging according to Eq. (4) and to determine the correlation coefficient, a reference value is needed. For this comparison new parts are used which are only fatigued in laboratory until they fail at the time  $t'_A$  (Fig. 3).

The previous mileage  $s_F$  and the time to failure  $t_A$  in the laboratory must be known. If the life expectancies of the components do not vary or deviate significantly, one field-aged part and one reference component would be enough to determine the unknown correlation coefficient  $c_K$  according to Eq. (4). But in practice, the component life-expectancy has a statistical distribution, so that a larger sampling of parts must be investigated to reliably determine this correlation coefficient.

Usually, the first step is a classic Weibull-analysis of component failure times  $t'_A$  using new, reference parts fatigued only in laboratory testing (VDA (Hrsg.) 2002; Ronninger 1999). This provides the two Weibull-parameters of characteristic lifetime  $T'_0$  and the gradient  $b'_0$  as reference values. With the assumption that field and laboratory stress are convertible, the fictitious lifetime of field parts with the characteristic Weibull-parameters

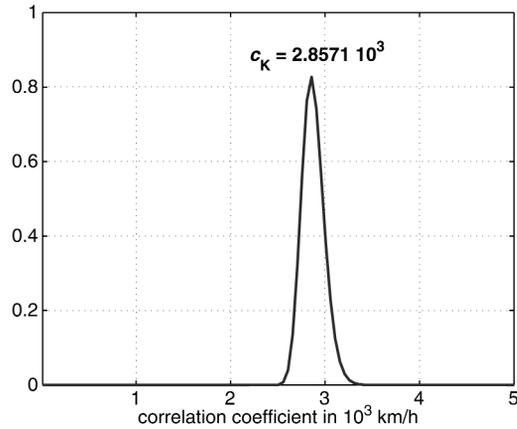


Figure 5. Scaled Maximum Likelihood Function  $L/L_0$  for different correlation coefficients  $c_K$ .

$$T, b = f(c_K) \tag{5}$$

has the same distribution, because the fatigue is equal and the parts identical. Thus the Weibull-parameters are assumed to be the same as

$$T(c_K) \stackrel{!}{=} T'_0 \wedge b(c_K) \stackrel{!}{=} b'_0 \tag{6}$$

those determined from reference parts  $t'_A$ . To solve this equation the correlation coefficient  $c_K$  is varied until such that the Weibull curves for the reference parts and field-aged parts, with their fictitious lifetime, fits one another as best as possible.

The maximum likelihood method according to (Hartung 1998; Fahrmeir et al. 1997) is used to describe the level of fit between both curves. The likelihood function  $L$  with

$$\begin{aligned} -\log L &= -\log \prod_{i=1}^n f(T'_0, b'_0 | t_{sum,i}) \\ &= -\sum_{i=1}^n \log f(T'_0, b'_0 | t_{sum,i}) \end{aligned} \tag{7}$$

will be maximum, if the distributions of fictitious lifetime  $t_{sum}$  and reference parts  $t'_A$  fit as well as possible. Eq. (6) and (7) lead to the desired correlation coefficient. The scaled value  $L/L_0$  is used to check the result (Fig. 5). For this scaling the Likelihood function  $L_0$  of the reference curve is used.

Finally, the correlation coefficient  $c_K$  gives the ratio between the field and laboratory stress, where

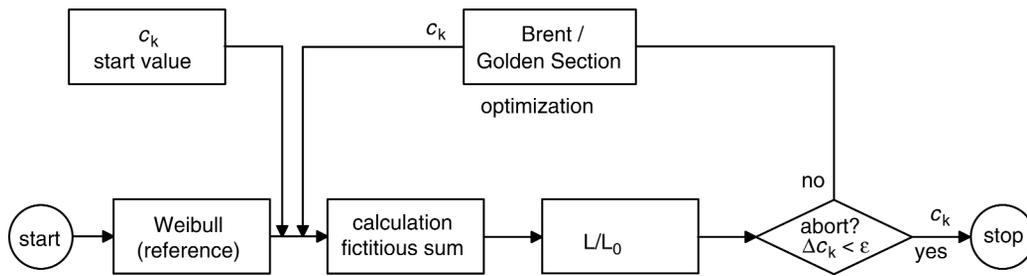


Figure 6. Sketch of optimization process to determine  $c_K$ .

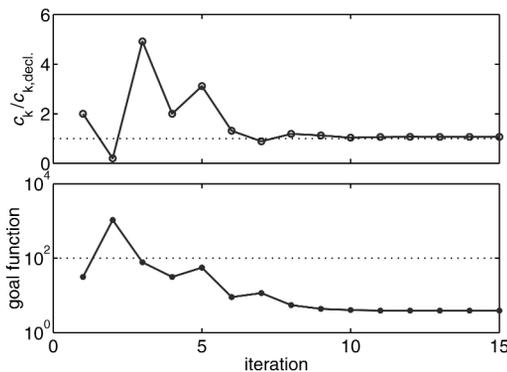


Figure 7. Correlation coefficient  $c_K$  and goal function during the optimization process.

the Likelihood function is maximum

$$L/L_0 \stackrel{!}{=} \max \tag{8}$$

as shown in Figure 5.

Because of the non-linear problem, an optimization algorithm is used to determine the optimum (Fig. 6). For this the Golden section and the Brent algorithm are implemented (The Mathworks Inc. 2000a; The Mathworks Inc. 2000b; Press et al. 1986). The negative logarithm of the Likelihood function is used as the goal function, which has to be minimized. The optimum is reached after 10 ... 15 iterations (Fig. 7). The automatic search is much more faster than a classic parametric study with approximately 100 points, which are necessary to determine the minimum.

#### 4 EXAMPLE OF USE

The developed method is demonstrated with an artificial example to test the implementation. The values

Table 1: Mileage  $s_F$  in  $10^3$  km and life span  $t_A$  in h of field parts up on failure in laboratory testing.

No.	1	2	3	4	5	...	50
$s_F$	134	159	78	120	127	...	15
$t_A$	18.1	3.1	13.3	27.9	20.1	...	37.3

Table 2: Life span of reference part up on failure  $t'_A$  in h to determine  $T'_0$  and  $b'_0$ .

No.	1	2	3	4	5	...	50
$t'_A$	47.1	55.1	58.4	65.0	65.9	...	56.4

are generated randomly, these then supposedly describe a failure behavior according to Weibull distribution. The numbers are generated with the assumption that the fatigue is caused by  $10^5$  km in field is equivalent to a fatigue level caused by 31.3 h in laboratory. This leads to  $c_K = 3200$  km/h.

##### 4.1 Scenario

To find the quantified connection  $n = 50$  intact parts with varying mileage are withdrawn from field use. These parts are operated in laboratory until they fail (Fig. 3). Simultaneously, new parts are tested to failure as a reference. The necessary data is shown in Tables 1 and 2.

The frequency distribution of the life span up on failure shows the characteristic way in which these parts fail (Fig. 8). The field parts are fatigued differently because of being their stochastic pre-aging and varying mileage. In this respect, the failure data is not distributed according to Weibull form (Fig. 8 a.). But the frequency distribution of the reference parts is conform to Weibull distribution (Fig. 8 b.). The average lifetime of the reference parts is longer then the average life span of the pre-fatigued parts.

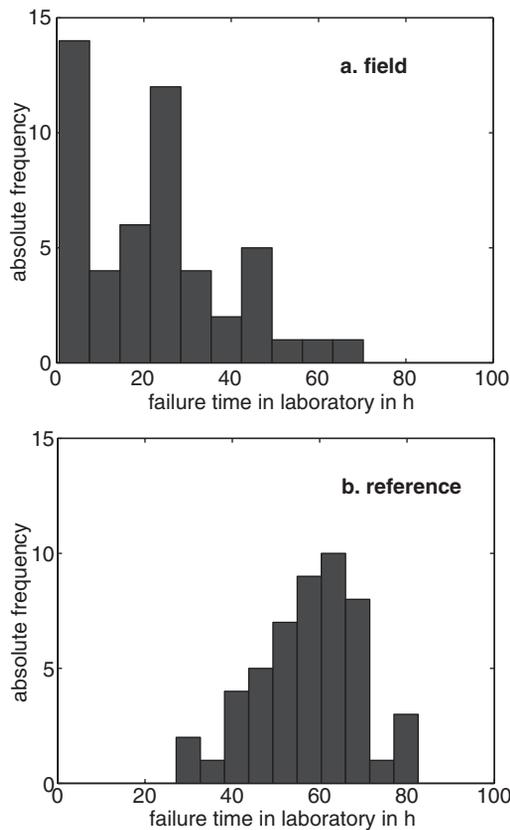


Figure 8. Absolute frequency of life span at laboratory failure of each 50 parts; a. field  $t_A$ , b. reference  $t'_A$ .

4.2 Determination of the correlation coefficient

The characteristic Weibull parameters are determined to  $T'_0 = 62 \cdot 10^3 \text{ km}$  and  $b'_0 = 4.8$ . These values then are the reference for the calculation of the desired correlation coefficient. The Likelihood function shows using Eq. (4) and (6) the maximum at  $c_K = 2840 \text{ km/h}$ . This value corresponds well with the value  $c_{K,decl.} = 3200 \text{ km/h}$  which was defined for checking the method. The Weibull parameters for the components possessing a fictitious lifetime are determined to be  $T = 61.7 \cdot 10^3 \text{ km}$  and  $b = 5.2$ .

Different scenarios with similar Weibull parameters and identical correlation coefficients lead to similar results (Tab. 3). The correlation coefficient is in the range of  $c_K = 2.84 \dots 3.52 \cdot 10^3 \text{ km/h}$ . These values agree well with  $c_{K,decl.} = 3200 \text{ km/h}$  which was used to create the artificial data. The calculated coefficient enables the conversion from field to laboratory conditions. Which allows one to make reliable statements to field behavior for the components in question.

Table 3: Results for different sample sizes  $n$ .

$n$	$T$ (h)	$b$	$c_K$ ( $10^3 \text{ km/h}$ )
defined	62.5	5.4	3.20
5	56.0	7.7	4.01
10	64.2	5.4	3.52
20	62.1	5.8	3.02
50	61.7	5.2	2.84
100	60.9	4.7	3.16

4.3 Influencing parameters

To determine the accuracy of the previously described methods, various different examinations have been carried out. But the most important question is the influence of the point in time when the field aged parts are demounting or removed from the field. To clarify this question the Monte-Carlo Method is used.

Several fictitious data sets were generated using random numbers with the same Weibull parameters and the same correlation coefficient  $c_{K,decl.}$ , using different lengths of field aging with the respective mileage and time periods. These data sets were examined with the method described. The correlation coefficient is calculated and compared with that which was used to generate the random numbers.

The examination is carried out with each 25 samples from field and as reference parts.

The result is defined as permissible if

$$\xi^{-1} \cdot c_{K,decl.} < c_K < \xi \cdot c_{K,decl.} \tag{9}$$

with  $\xi = 1.05 \dots 1.3$

used with the declared coefficient  $c_{K,decl.}$  and the deviation  $\xi$ . The result is the share of the simulations which fulfill the condition Eq. (9). This measure is used to determine the accuracy and the confidence of the calculation method. The Monte-Carlo simulations show, that the accuracy of the statement increases with increasing mileage (Fig. 9). For a deviation of 30% and a confidence of 80% a scaled demounting lifetime of 30% is satisfactory.

The described relationship is valid for the general conditions mentioned above. Additionally examinations with different Weibull parameters are still required.

4.4 Evaluation

The examples shown, which are based on Weibull distributed random numbers, deliver good results for the relationship between field and laboratory aging conditions developed with this method. Both the

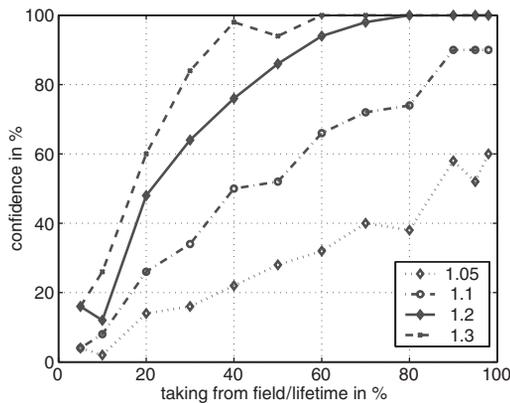


Figure 9. Confidence of calculations with different deviations  $\xi$ .

implementation of the algorithm and the duration of computation are well suitable in practice.

But reliability of the results obtained depend significantly up on the quality of field data. If outliers or false data occur, the result can be corrupted. Large dispersions in field stresses can also negatively influence the accuracy of the result. If the fatigue in field is considerably lower than those in laboratory, the deviation can be larger. For this reason, often the differences in fatigue levels that should be identified are veiled by the dispersion in laboratory conditions. In this case the testing parameter should be reassessed, as the testing conditions is much harsher than those experienced in the field. In the case of well correlated testing parameters the new method provides additional information about the expected lifetime in the field.

## 5 CONCLUSIONS

The method developed enables the quantification of fatigue levels present in intact components exhibiting a spontaneous failure mode. The examples shown, demonstrate good results in deriving a quantification

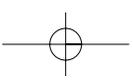
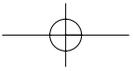
between laboratory and field conditions. An important basis is the field parts data set, which must be big enough. Additionally, initial investigations concerning the accuracy of the results have been carried out.

But the accuracy of the method must be investigated further. The quality of the results can be influenced significantly by several factors including: using different data sets, Weibull parameters, or changing the ratio between field and laboratory stresses. Further investigations to improve the accuracy are planned.

The developed method makes a significant contribution to better correlating field and laboratory testing. Additionally, this method contributes not only to a more efficient product development process but also can result significant savings in time and costs during the component testing period.

## REFERENCES

- Fahrmeir, L., R. Künstler, I. Pigeot & G. Tutz (1997). *Statistik – Der Weg zur Datenanalyse*. Springer-Verlag, Berlin u. a.
- Haibach, E. (1989). *Betriebsfestigkeit*. VDI-Verlag, Düsseldorf.
- Hartung, J. (1998). *Statistik – Lehr- und Handbuch der angewandten Statistik, 11. Aufl.* Oldenbourg Verlag, München.
- Press, W.H., B.P. Flannery, S.A. Teukolsky & W.T. Vetterling (1986). *Numerical Recipes, The Art of Scientific Computing*. Cambridge.
- Robert Bosch GmbH (Publ.) (2000). *Automotive Handbook*. 5th ed., Stuttgart.
- Ronninger, C.U. (1999). *Zuverlässigkeitsanalyse mit Weibull in Entwicklung und Serie*. ATZ 101 (99), pp. 942–949.
- The Mathworks Inc. (2000a). *Matlab, The Language of Technical Computing; Vers. 6*. Natick.
- The Mathworks Inc. (2000b). *User's Guide Statistics Toolbox, For use with Matlab; Vers. 3*. Natick.
- VDA (Hrsg.) (2002). *Qualitätsmanagement in der Automobilindustrie, Zuverlässigkeitsmethoden und -Hilfsmittel; Band 3, Teil 2, 3. Aufl.* Frankfurt.
- Vogt, M. & H. Neu (2002). *Auswertungsverfahren zur Korrelation von Felddaten und Erprobungsbedingungen von Kfz-Komponenten*. TTZ 2002, Zuverlässige Produkte, Düsseldorf, pp. 161–174.



## Time-dependent reliability analysis of coastal flood defence systems

H.G. Voortman

*ARCADIS Infra, Amersfoort, The Netherlands*

J.K. Vrijling

*Delft University of Technology, Faculty of Civil Engineering and Geosciences, Delft, The Netherlands*

**ABSTRACT:** Risk- and reliability-based design methods are useful tools in the design of coastal flood defence systems. Applications to date often neglect the effects of climate change on the optimal design of a flood defence structure. In the paper, a method is proposed to incorporate climate change in design optimisation. The method is based on the use of fragility curves to quantify the effects of climate change on the probability of failure of a flood defence structure. The combination of fragility curves with scenarios of climate changes then leads to an estimate of the hazard rate of the flood defence structure. A case study demonstrates the application of the proposed method.

### 1 INTRODUCTION

Risk- and reliability-based design methods prove to be useful tools in the design of flood defence systems. Uncertainties in load and strength of flood defences can be explicitly accounted for in the design by application of reliability-based methods. The consequences of flooding and the cost of protection form the basis for establishing an appropriate reliability level by application of risk-based optimisation.

Very often, in the application of reliability- and risk-based methods to the design of flood defences, it is implicitly assumed that the environmental conditions do not change over time. However, there are indications that the environmental conditions do change. The increase of the mean sea level along the Dutch coast is clearly present in observations of the water level. Furthermore, there are indications that world-wide climate change is imminent.

In this paper, a method will be proposed to deal with climate change in the risk-based design of flood defence systems. The method is aimed at application in practice, which implies that the method should be applicable to large-scale systems. To this end, the risk-based design strategy proposed by Voortman and Vrijling (2001) will be used (see also Voortman, 2002).

### 2 PROBLEM OUTLINE

The level of protection provided by a flood protection system is ideally obtained by balancing the cost of

protection with the obtained reduction of the flooding risk in the protected area. Based on this idea, risk-based design methods for flood defences have been developed, starting with the economic optimization of the safety level of Dutch dikes by Van Dantzig (1956). Van Dantzig's analysis considered the water level in front of the protection system as the only random variable.

In the 1960s and 1970s, probabilistic methods were developed in the realm of structural engineering (see for instance Turkstra, 1962, 1970). This development took place largely independent of the aforementioned risk-based design method for flood defences. In the late 1970s and 1980s, probabilistic methods were again recognised as important tools for design in coastal engineering (Vrijling & Bruinsma, 1980; Bakker & Vrijling, 1980). Recently, the concepts of risk-based optimisation have been integrated with up-to-date probabilistic methods, resulting in a method for risk-based design of large-scale flood defence systems (Voortman, 2002).

The risk-based design method as shown in Voortman (2002) implicitly assumes an unchanging natural environment for which the defence structure is designed. Recent research appears to indicate that major climate changes are imminent (Intergovernmental Panel on Climate Change, 2001; Dutch Meteorological Institute, 2001). Since a flood defence system should be designed for the future, a method needs to be found in which future climate changes can be incorporated in the risk-based design method.

### 3 ECONOMIC OPTIMISATION OF FLOOD DEFENCES

#### 3.1 Time-independent formulation

As stated before, risk-based design aims at achieving an appropriate balance between the cost of the protection system and the consequences of flooding. A variety of monetary and non-monetary costs and consequences may be relevant to the decision on the design safety level of a flood protection system. See Voortman (2002) for an overview.

In this paper, the decision problem will be limited to monetary aspects of the decision only, which results in economic optimisation of the protection level. Mathematically, an optimally designed flood protection system is achieved by solving:

$$\min_{P_{flood}} C_{life}(P_{flood}) \quad (1)$$

Where  $C_{life}$  denotes the life-cycle costs of the flood defence and  $P_{flood}$  the flooding probability. The life-cycle costs of the protection system are given by:

$$C_{life}(P_{flood}) = I(P_{flood}) + \dots + \int_0^T P_{flood} \left( \frac{1+r_e+i}{1+r} \right)^t (b_0 + d_0) dt \quad (2)$$

Where  $I$  denotes the direct cost of protection,  $b_0$  the loss of production capacity in case of flooding,  $d_0$  the material damage in case of flooding,  $r_e$  the rate of economic growth,  $i$  the inflation,  $r$  the market interest rate and  $T$  the planning period.

Every value of the flooding probability  $P_{flood}$  corresponds to a geometry of the protection system that can be constructed on site. Thus, the process of economic optimisation has a strong link with the actual design practice of flood defences. The cost of the protection system can be found by estimating the direct cost of the system as a function of the geometry of the flood defence. Monetary consequences of flooding follow from an inventory of the value of the protected area. The rates of interest, inflation and economic growth may be estimated from historic data. In the formulation of equation 2, fixed values are assumed for these three parameters.

#### 3.2 Time-dependent formulation

Economic optimisation as formulated in the previous section assumes an unchanging value of the flooding probability over time. This can only be achieved if:

- The properties of the climate and of the structure do not change over time, or

- The changes in the structure exactly balance the changes of the climate.

Both options are unlikely, so that in general changes of the flooding probability over time need to be accounted for in a risk-based design approach. In principle this is achieved by replacing the flooding probability in equation 2 with the hazard rate  $h$ :

$$C_{life}(P_{flood;0}) = I(P_{flood;0}) + \dots + \int_0^T h(t, P_{flood;0}) \left( \frac{1+r_e+i}{1+r} \right)^t (b_0 + d_0) dt \quad (3)$$

Where  $P_{flood;0}$  denotes the flooding probability immediately after construction (design flooding probability).

The cost of construction is a function of the flooding probability just after construction. The hazard rate is a function of time and of the design flooding probability. Once a flood defence structure is constructed, it will respond autonomously to changes in climate. The flooding risk over time can in principle be influenced only through the value of the design flooding probability  $P_{flood;0}$ .

### 4 THE HAZARD RATE OF A COASTAL FLOOD DEFENCE SYSTEM IN A CHANGING CLIMATE

#### 4.1 General

The hazard rate of a flood defence system is influenced both by time-dependent changes of the structure and by time-dependent changes of the climate. In this paper, only changes of the climate will be considered, but the proposed method can also be applied to quantify the consequences of changes of the structure.

Sea level rise and its effects on the optimal design of flood defences were studied by Vrijling and Van Beurden (1990). This work considered only the water level as a random variable.

In practice, the water level in front of a coastal flood defence depends on two important influences:

- The mean sea level and the tidal amplitude;
- The wind field over the neighbouring water body.

Especially in shallow seas like the North Sea, strong winds may cause a considerable increase in the water level. This increase due to the wind is denoted "wind setup". Furthermore, the wind field is responsible for the intensity of the wave attack on coastal flood defences.

It is often suggested that climate changes not only cause a rise of the mean sea level, but also lead to an increase of the frequency and intensity of storms.

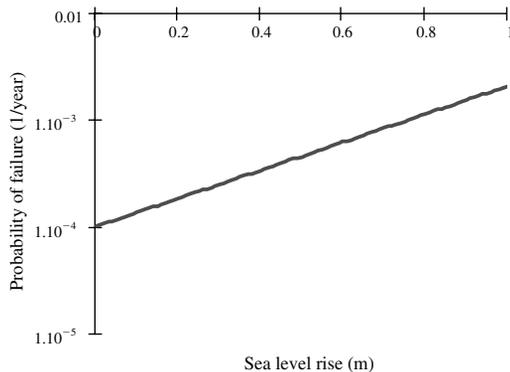


Figure 1. Example of a fragility curve for sea level rise.

If this is true, the extreme water levels will show a larger increase than the mean sea level, due to increased wind setup. Furthermore, increased intensity of storms will cause an increase of wave attack. In summary: an analysis of the effects of sea level rise only is insufficient to fully appreciate the effects of climate change on the level of flood protection.

#### 4.2 The use of fragility curves

Fragility is defined by Casciati and Faravelli (1991) as the probability of failure conditional on a specific value of the loading. Dawson and Hall (2001, 2002) used fragility curves to characterise the quality of a flood defence structure without the necessity to analyse the loading conditions.

Fragility curves can also be used to quantify the effects of changes in the loading due to climate change. In that case, the fragility is given as a function of changes in the parameters of the probability distributions of the loading. Figure 1 shows an example.

The fragility curve in figure 1 shows the probability of failure of the flood defence for given values of the initial (design) failure probability and a given value of the sea level rise. Sea level rise changes the mean of the astronomic tide in front of the structure and thus influences the loading.

#### 4.3 Uncertainties in climate change

The fragility curve in the previous section shows the probability of failure for a given value of the sea level rise. However, in the design stage of a flood defence, future sea level rise is unknown. At best, estimates are available of the temporal development and the uncertainty of the sea level rise. A scenario for sea level rise thus provides a probability distribution of the sea level rise a number of years in the future. Figure 2 shows an example where the assumption is made that

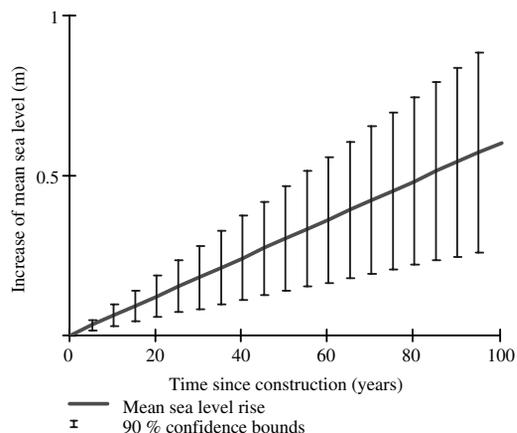


Figure 2. Example of a scenario for climate change including uncertainty.

the sea level rises linearly over time but the rate of sea level rise is uncertain.

The rate of the sea level rise is assumed to be normally distributed with fixed values of the mean and standard deviation. The effect is that both the mean and the standard deviation of the sea level rise increase over time. Thus, the climate scenario provides estimates of the distribution of future sea level rise. The probability of failure at a time in the future is then given by:

$$h(t) = \int_{-\infty}^{+\infty} f_{\Delta h}(\eta, \mathbf{p}(t)) P_{f|\Delta h}(\eta) d\eta \quad (4)$$

Where  $\mathbf{p}$  is a vector of parameters that change as a function of time. Equation 4 is easily extended to incorporate other aspects of climate change.

## 5 TIME-DEPENDENT RELIABILITY OF A FLOOD DEFENCE ALONG THE SOUTHERN NORTH SEA COAST

### 5.1 General

The analysis of the time-dependent reliability of a coastal flood defence will be demonstrated in a case study taken from Voortman (2002). Figure 3 shows the location of the case study area.

In the case study, the probability of failure of a coastal flood defence system in the Dutch province of Groningen is calculated with the wind speed and the astronomic tide as dominant input variables. Assumptions will be made regarding the effect of climate change on the probability distribution of the astronomic tide and the probability distribution of wind speed. The assumptions do not affect the generality of the method.



Figure 3. Case study location in the southern North Sea.

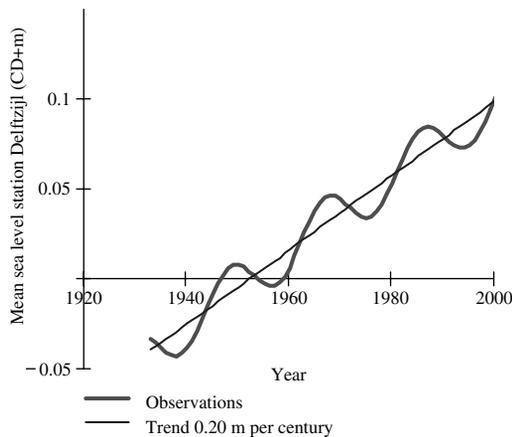


Figure 4. Yearly averaged sea level observed at the water level station Delfzijl (information obtained from the Dutch Institute for Coastal and Marine Management).

5.2 Sea level rise

In observations of the water level along the Dutch coast, an 18.6-year cycle and a trend are clearly observed. (See Table 4).

The mean long-term sea level rise amounts to 0.20 m per century. The cycle is a well-known tidal phenomenon (Godin, 1972).

For policy studies, the Dutch Institute for Coastal and Marine management uses three deterministic scenarios and one scenario including uncertainty. Table 2

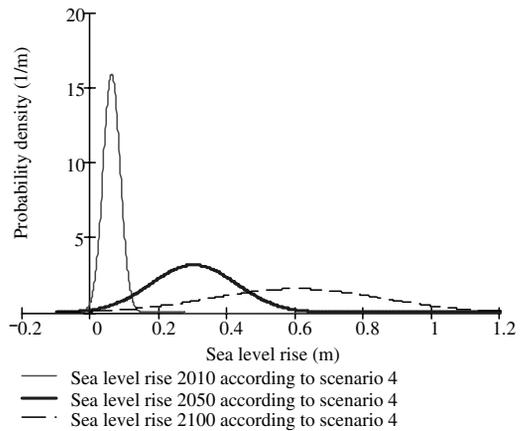


Figure 5. Distribution of future sea level rise according to climate scenario 4.

Table 1. Probability distribution of five-hour averaged wind speed in the case study area (Voortman, 2002).

Property of distribution	Value
Distribution type	Weibull
Shift parameter	19.8 m/s
Scale parameter	2.83 m/s
Shape parameter	1.2

shows an overview. Based on the indicated values of sea level rise and wind speed change in the year 2100, in this paper functions are proposed for the time-dependent changes of the climate. Sea level rise will be modelled as a linear function of time, according to:

$$\Delta h(t) = a_h t \tag{5}$$

The value and distribution of the parameter  $a_h$  depends on the scenario considered. Figure 5 shows the probability distribution of sea level rise at different times in the future according to scenario 4.

5.3 Change of wind climate

Based on the work of Wieringa and Rijkoort (1983) and on an analysis of 20 years of wind observations, Voortman (2002) derived the distribution of the five-hour averaged wind speed at the case study location. Table 1 provides an overview.

It is suggested that climate change may increase the frequency and the intensity of storms over the North Sea, but information is highly limited. The Dutch Institute for Coastal and Marine Management suggests

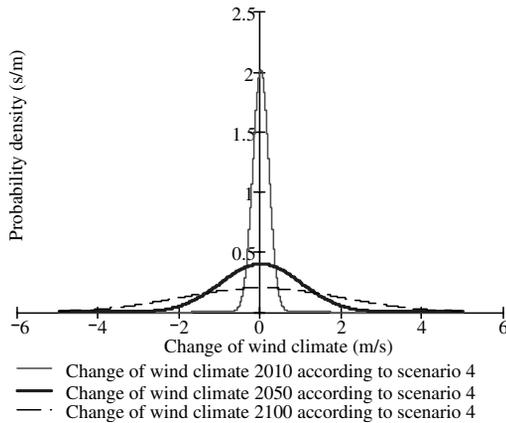


Figure 6. Distribution of future changes in wind speed according to climate scenario 4.

an increase of the wind speed in storms of 10%. In this paper, the increase of the wind speed will be assumed to influence the shift parameter of the wind speed distribution in the case study area. The shift parameter is assumed to increase linearly over time according to:

$$\Delta u(t) = a_u t \tag{6}$$

The distribution and parameter values of  $a_u$  depend on the scenario considered. Figure 6 shows an example for scenario 4.

#### 5.4 Deriving the fragility curve

Voortman (2002) derived optimal geometries for the flood defence structure for failure probabilities ranging from  $10^{-1}$  per year to  $10^{-6}$  per year, using four different failure modes and six different design variables for a dike cross section. The effect of sea level rise and increased wind speed are quantified by calculating the probability of failure for combinations of structure geometry, sea level rise and wind speed increase in a level II method, using the optimal geometries derived by Voortman (2002). The results of the model runs can be summarised by a parametric model of the following form:

$$\log(P_f) = \log(P_{f,0}) + a \cdot \Delta h + b \cdot \Delta u \tag{7}$$

Where  $P_{f,0}$  is the design flooding probability,  $\Delta h$  the sea level rise,  $\Delta u$  the change of the wind climate and  $a$  and  $b$  model parameters.

The values of the parameters of the model are derived using the least-squares method. The fitted

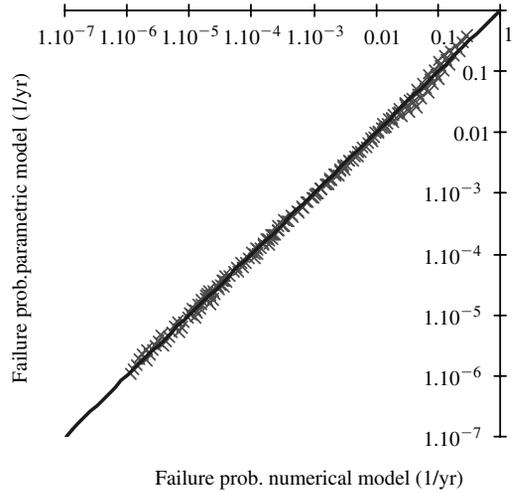


Figure 7. Comparison of parametric fragility curve with results of numerical model.

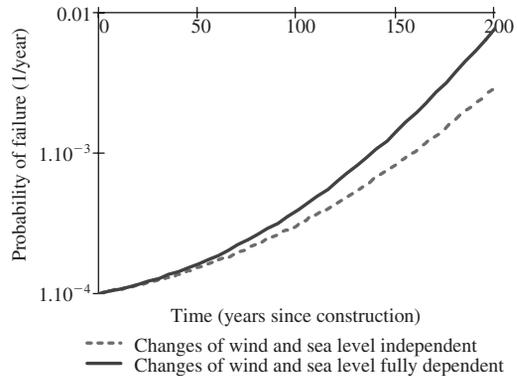


Figure 8. Hazard rate calculated for two cases of dependence between climate changes.

model shows a satisfactory match with the data (figure 7).

#### 5.5 Calculation of the hazard rate

Combining the climate scenarios with the fragility curve provides the hazard rate for the flood defence structure. Not only the marginal distributions of the climate changes but also the dependencies between them influence the final result. Figure 8 shows the hazard rate calculated for a structure with an initial probability of failure of  $10^{-4}$  per year using scenario 4. The hazard rate is calculated for two cases of dependence;

independence between sea level rise and wind climate change and full dependence between sea level rise and climate change.

As expected, dependence between sea level rise and wind climate change leads to a larger increase of the flooding probability over time than independence. Since the changes of sea level and wind climate both stem from the same cause, some degree of dependence appears to be realistic. In the following, full dependence will be assumed. Figure 9 shows the hazard rate for the four scenarios shown in Table 2.

Up to 150 years after construction, the maximal scenario (scenario 3) leads to the highest values of the hazard rate. After 150 years, scenario 4 leads to the highest values of the hazard rate. The reason for this is that in scenario 4, the uncertainties on the climate changes increase over time. For times after construction longer than 150 years, the increased uncertainty in scenario 4 dominates over the larger increase of the mean climate change in scenario 3.

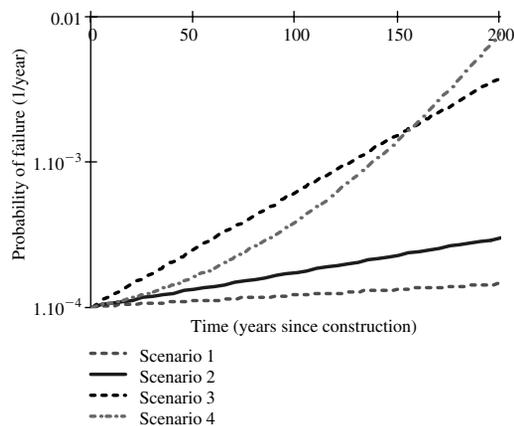


Figure 9. Hazard rate of the flood protection system for four different scenarios of climate change.

## 6 OPTIMISATION OF A FLOOD DEFENCE IN A CHANGING CLIMATE

### 6.1 General

With the hazard rate calculated in the previous section, the risk-based optimisation of the flood defence system can be performed for different scenarios of climate change. In this section economic optimization of the flood defence system is performed for several scenarios for climate change.

### 6.2 Input data

The construction cost of the coastal flood defence system as a function of the flooding probability is derived in Voortman (2002) by reliability-based optimisation. The construction cost is given by the following function:

$$I(P_{f,0}) = 10^{a \log(P_{f,0}) + b} \quad (8)$$

Where  $P_{f,0}$  is the design flooding probability and  $a$  and  $b$  are parameters. The costs are given in euro.

The damage in case of flooding consists of material losses and loss of production capacity in the protected area. The economic input used in the optimization is shown in Table 3.

### 6.3 Results of the optimisation

Figure 10 shows the life-cycle cost of the flood defence system for the four scenarios of climate change in comparison to the case without climate change. The influence of climate change on the lifecycle cost and on the optimal flooding probability is clearly visible. A summary of the optimal designs for the five cases is given in Table 4.

As expected, climate change lowers the optimal design flooding probability. This implies an increase of the direct cost of protection by at maximum 10% in scenario 3. The expected value of the future flooding

Table 2. Climate scenarios used by the Dutch Institute for Coastal and Marine Management (2000).

Scenario	Description	Distribution of climate changes	Mean sea level rise in 2100 (m)	Standard deviation of sea level rise in 2100 (m)	Mean increase of wind speed in 2100 (m/s)	Standard deviation of increase of wind speed in 2100 (m/s)
1	Minimal scenario	Deterministic	0.2	n.a.	0	n.a.
2	Middle scenario	Deterministic	0.6	n.a.	0	n.a.
3	Maximal scenario	Deterministic	0.85	n.a.	1.98	n.a.
4	Probabilistic scenario	Normal	0.6	0.25	0	1.98

Table 3. Input for economic optimisation of the flood defence system.

Parameter	Description	Value	Remark
$a$	Slope of investment function	0.18	Voortman (2002)
$b$	Intercept of investment function	8.81	Voortman (2002)
$d_0$	Monetary value of the area	G€34,-	Taken from PICASO study*
$b_0$	Yearly gross domestic product	G€14.40	Value of 1998 <sup>#</sup>
$r$	Interest rate	0.07 per year	Average over 1960–2001 <sup>#</sup>
$re$	Rate of economic growth	0.03 per year	Average over 1960–2001 <sup>#</sup>
$i$	Inflation	0.02 per year	Average over 1960–2001 <sup>#</sup>
$T$	Reference period	100 years	Assumed value

\* RWS, 2001.

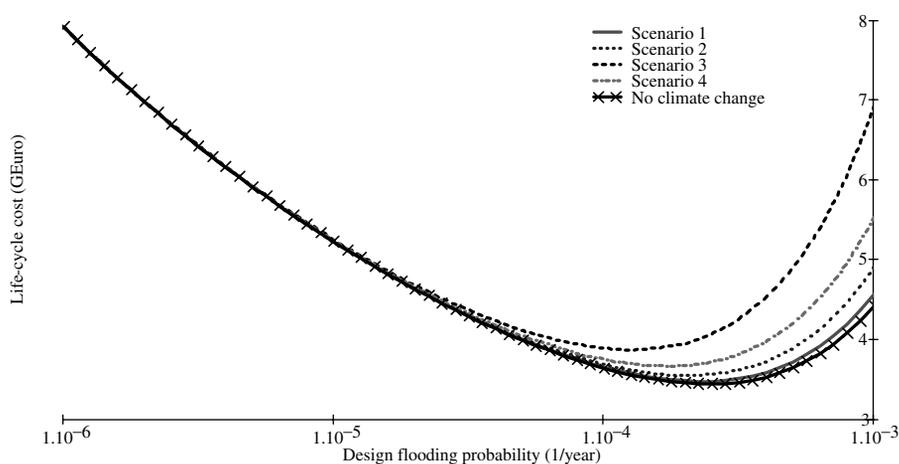
<sup>#</sup> Data obtained from the database of the Dutch Central Bureau of Statistics.

Figure 10. Life-cycle costs of the flood protection system as a function of design flooding probability.

Table 4. Results of risk-based optimisation for different scenarios for climate change.

Scenario climate change	Optimal flooding probability ( $10^{-4}$ /year)	Direct cost of protection (G€uro)	Expected future flooding damage (G€uro)	Life-cycle cost (G€uro)
1	2.1	2.99	0.48	3.48
2	1.9	3.04	0.51	3.55
3	1.3	3.26	0.61	3.87
4	1.7	3.12	0.55	3.66
None	2.2	2.98	0.47	3.44

damage (flooding risk) also shows an increase in comparison to the case without climate change.

## 7 DISCUSSION

A method has been presented to incorporate climate change in reliability- and risk-based design of flood

defences. Uncertainty in climate changes is dealt with in a consistent way.

The analysis as it is presented is aimed at application in the design stage of a flood defence. Historic information may be used to establish scenarios for climate change. The final decision on the optimal design incorporates the knowledge of climate changes at the design stage.

As time after construction passes, more and more knowledge on the actually occurring climate changes comes available. This information can then be used to update the initial scenarios for climate changes. Bayesian methods may be applied for this purpose.

The methods as presented can not only be used to quantify the effects of climate changes, but also to quantify the effect of time-dependent changes in the structure itself. Like in the case of climate change, a scenario may be defined that describes the ageing process of the defence structure and the uncertainty around it.

The information on the state of the structure and the state of the climate can be combined to support decision-making on upgrading or replacement of older deteriorated flood defences.

## 8 CONCLUSIONS

Recent climate research indicates that important changes in the world climate are to be expected. Climate change will influence the loading and thus the reliability of coastal flood defences.

Because flood defences are built for the future, design choices should reflect the knowledge of future climate changes. A method is proposed to incorporate climate scenarios in a risk-based approach to flood defence design.

In a case study, economic optimisation of a flood defence system in the southern North Sea is performed. Inclusion of scenarios for climate change leads to lower optimal design flooding probabilities than in the case where climate change is neglected. Consequently, the direct cost of protection and the life-cycle costs of the protection system increase.

The proposed method may also be used in combination with deterioration models for flood defences, in which case also the resistance of the structure is a function of time. Finally, during the life of the protection system, observations may be used to constantly update the climate scenarios using Bayesian methods. Thus, the model can be used to support decisionmaking on upgrading of older deteriorated flood defences.

## ACKNOWLEDGEMENT

The basis of the work in this paper was established while the first author was employed as research assis-

tant at Delft University of Technology. The fruitful cooperation with Dr. P.H.A.J.M. van Gelder is gratefully acknowledged.

## REFERENCES

- Bakker, W.T. & Vrijling, J.K., 1980, Probabilistic design of sea defences, *Proceedings of the International Conference on Coastal Engineering (ICCE)*.
- Casciati, F. & Faravelli, L., 1991, *Fragility analysis of complex structural systems*, Taunton: Research Studies Press.
- Dawson, R.J. & Hall, J.W., 2001, Improved condition characterization of coastal defences, *Proceedings of the conference "Coastlines, structures and breakwaters"*, London: Institution of Civil Engineers.
- Dawson, R.J. & Hall, J.W., 2002, Probabilistic conditions characterisation of coastal structures using imprecise information, *Proceedings of the International Conference on Coastal Engineering (ICCE)*.
- Dutch Institute for Coastal and Marine Management, 2000, *Third report on coastal development, tradition, trends and future (in Dutch)*.
- Godin, G., 1972, *The analysis of tides*, Liverpool University Press, Liverpool.
- Intergovernmental Panel on Climate Change (IPCC), 2001, *IPCC Third Assessment Report – Climate Change 2001*, www.ipcc.ch.
- Royal Dutch Meteorological Institute, 2001, *Weather and water in the 21st century, a summary of the third IPCC climate report for water management in the Netherlands (in Dutch)*.
- Turkstra (1962, 1970), *Theory of structural design decisions*, University of Waterloo.
- Van Dantzig, D., 1956, Economic decision problems for flood prevention, *Econometrica*, Vol. 24, pg. 276–287.
- Voortman, H.G. & Vrijling, J.K., 2001, A risk-based optimization strategy for large-scale flood defence systems, *Proceedings IABSE-conference Safety, Risk and Reliability – Trends in Engineering*.
- Voortman, H.G., 2002, *Risk-based design of large-scale flood defence systems*, Phd-thesis, Delft: Delft University of Technology.
- Vrijling, J.K. & Bruinsma, J., 1980, Hydraulic boundary conditions, *Symposium on hydraulic aspects of coastal structures*.
- Vrijling, J.K. & Van Beurden, I.J.C.A., 1990, Sea level rise: a probabilistic design problem, *Proceedings of the International Conference on Coastal Engineering (ICCE)*.
- Wieringa, J. & Rijkoort, P.J., 1983, *Wind climate of the Netherlands*, Royal Dutch Meteorological Institute (in Dutch).

## Adding a new perspective to the existing results by baseline NPP PSA model: parameters uncertainty implementation

Ivan Vrbanić

*Nuclear Power Plant Krško, Vrbina, Krško, Slovenia*

Romana Jordan Cizelj

*“Jožef Stefan” Institute, Reactor Engineering Division, Jamova, Ljubljana, Slovenia*

**ABSTRACT:** The paper describes the ongoing project of introducing parameters' uncertainty into the baseline PSA model of Nuclear Power Plant Krško (NEK). Up to now, the values of parameters in PSA model were expressed as point estimates. As more and more stress has been put to the importance of uncertainty analyses when using PSA in risk-informed applications, the decision was made to incorporate parameter uncertainty analysis into NEK PSA model for internal events. The major categories of parameters that are treated in this paper are probabilities of components' failure per demand, failure rates and unavailability due to test and maintenance (TM). Uncertainty distributions of these types of parameters have been introduced into the model and uncertainty has been propagated to the core damage frequency (CDF) level. The paper presents uncertainty distribution of CDF and provides a discussion on some relevant issues associated with the subject.

### 1 INTRODUCTION

The PSA model of Krško Nuclear Power Plant (NEK) was developed during the early nineties following the US IPE (United States' Individual Plant Examination) methodology (US NRC 1988) and in accordance to the International Atomic Energy Agency (IAEA) guides (IAEA 1992). The results (core damage frequency, various systems unavailability, etc.) were expressed as point estimates. To address the impact of potential uncertainty of data on PSA results, various sensitivity cases were run and evaluated. This served the primary purpose of IPE-type analysis, which was focused on evaluation of existent plant design. Upon the completion of IPE, NEK started to use the PSA model for various applications. As the usage of PSA in NEK increased with time, so did the awareness of need to perform uncertainty analysis as an integral part of the baseline PSA model and its applications. In order to facilitate the Living PSA program and applications, NEK subsequently performed the transfer of initial IPE PSA model into Risk Spectrum, an integral PSA tool, which, among other advanced features, supports uncertainty analyses.

During the recent past years, the PSAs became worldwide recognized tools for various risk-informed applications in the field of nuclear power plants

operation and design. Guides have been developed as an attempt to achieve certain level of standardization in PSA applications (e.g. ASME 2002 and US NRC 1998), which also put additional stress to the importance of uncertainty analyses.

Consequentially to these issues and concerns came a decision to incorporate parameter uncertainty analysis into NEK PSA model for internal events. It is performed in two phases. The first phase of project is coming to a conclusion (Jordan Cizelj & Parzer 2002, Vrbanić et al. 2003 in prep.). The major categories of parameters that were treated in the first part of the uncertainty analysis are probabilities of components' failure per demand, failure rates, unavailability due to TM and some special parameters, for example exposure times.

Categories such as initiating events' frequencies and human error probabilities are being treated in the second phase of the project. The uncertainty distributions for the parameters from the first phase have been established and introduced into the baseline PSA model. The uncertainty has been propagated to CDF, based on Monte Carlo simulations built into the Risk Spectrum. The paper presents CDF uncertainty distribution and discusses some relevant issues associated with the subject.

## 2 UNCERTAINTY ANALYSIS OF PARAMETERS IN PSA MODEL

The PSA model of concern is a Level 1 model with internal initiating events (Westinghouse-NEK 1994). The top event represented is a core damage due to internal initiating events. So, the model is used to calculate the frequency of occurrence of core damage event (i.e. core damage frequency or CDF). There are 16 categories of initiating events with corresponding 16 event trees, each one representing a plant response to the given initiator. Responses of plant systems that take part in event trees' sequences are presented by means of fault trees. The overall model relies on the fault tree linking methodology, meaning that support systems' fault trees are linked into the fault trees of frontline systems, which in turn are linked into the event tree sequences.

The model contains, roughly, some 2500 fault tree gates. In the fault tree structure there is approximately 1500 basic events, not accounting those representing common cause failures (CCF). (The CCF-type basic events are created in an automated manner on the basis of specified CCF groups, whenever a minimal cutset analysis is being performed.)

The probabilities of these 1500 basic events are calculated by means of more than 350 parameters. A rough breakdown of types of parameters contained in NEK PSA model for internal initiating events is presented by Table 1.

Out of 350 parameters from Table 1, the uncertainty distributions have been defined and introduced in the PSA model for categories 1 (probabilities of failures per demand), 2 (failure rates) and 3 (unavailability due to test or maintenance), which makes somewhat more than half of the overall parameters' population. Uncertainty distributions for remaining categories will be added in the second phase.

Uncertainty of various exposure times included in the model was also evaluated during the first phase. However, in the runs considered in this paper these parameters were treated as point estimates. It is also noted that the Table 1 does not contain frequencies of initiating events. As already mentioned, there are 16 initiators. Eleven of them are presented by means of basic events (frequency-type) while remaining are modeled as fault trees. Uncertainties of parameters representing initiating events' frequencies will be treated and introduced in the model in the second phase also.

The CDF, as calculated from minimal cutsets generated prior to introduction of any parameter uncertainty, was  $3,17E-05/\text{yr}$  (Vrbanić et al. 2002). Absolute truncation value applied was  $1E-10$  (/yr).

Uncertainty distributions for probabilities of failures per demand and failure rates were established by combining generic and plant specific data input, in accordance with well-known practices (e.g. Hickman, J. W.,

Table 1. Breakdown of parameters in PSA model of concern (Level 1, internal initiating events).

Parameter type	Number of par. (approximately)
1. Prob. of Failure per Demand	90
2. Failure Rate	60
3. TM Unavailability	40
4. Human Error Probability	90
5. Recovery and Phenomena	30
6. Common Cause Factors (MGL)	40
Total Number of Parameters:	350

et al. 1983, Bari, R. A et al. 1985). Binomial and Poisson likelihood functions were applied for demand-related probabilities and failure rates, respectively. Obtained posterior distributions were fit to analytical probability distributions allowed by Risk Spectrum. In almost all of the cases this resulted in lognormal distributions that were incorporated into the model. Uncertainty distributions of equipment unavailability due to TM were defined as lognormal distributions directly. Details on the determination of uncertainty distributions are provided in the report (Jordan Cizelj & Parzer 2002) and series of papers (Jordan Cizelj & Vrbanić 2001, Jordan Cizelj & Vrbanić 2002a,b, Jordan Cizelj et al. 2002).

Upon introducing parameter uncertainties into the model, the first step was to re-generate minimal cutsets under the pre-defined conditions and to obtain a "new" point estimate of CDF. In the case of parameters with newly defined distributions a point estimator of parameter of concern is mean value of specified distribution. Point estimate of CDF obtained was  $3,13E-05/\text{yr}$  (Vrbanić et al. 2003 in prep.), which is only slightly different from old point estimate value of  $3,17E-05/\text{yr}$ . The difference was generally attributable to differences introduced between distributions' mean values and "old" point estimates, due to numerical Bayesian integration. Both point estimates were obtained by 3rd order approximation (Berg & Sardi 1994).

The same set of minimal cutsets was then used as a basis for uncertainty propagation to CDF. Figure 1 shows CDF uncertainty distribution curve from a series of ten runs with number of Monte Carlo simulations growing from 1000 to 10000 (maximum allowed by Risk Spectrum).

As it can be seen, the distribution curve becomes relatively smooth at 8000–9000 simulations. Figure 2 presents characteristic values (5th and 95th percentiles, mean and median) of the same set of distribution curves. The 5th percentile is approximately at  $2,0E-05$  /yr, while the 95th percentile fluctuates around the values of  $5,6E-05$  to  $5,7E-05/\text{yr}$ .

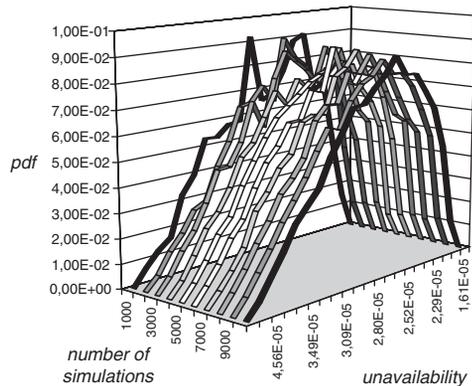


Figure 1. Core damage frequency distribution curve with growing number of simulations.

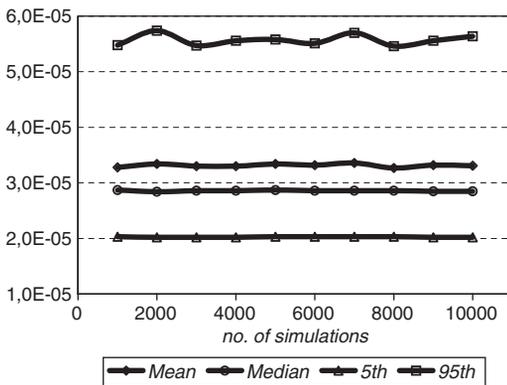


Figure 2. Characteristic values of CDF distribution curves from Figure 1.

It is important to note that in an uncertainty analysis Risk Spectrum quantifies minimal cutsets using so called “min cut upper bound approximation” (Berg & Sardh 1994), which yields somewhat higher results than 3rd order approximation.

Table 2 presents the mean values of CDF curves obtained in series of ten successive uncertainty propagations with 9000 Monte Carlo simulations each.

The average value taken from the ten results is 3,31E-05/yr. On the other hand, the min-cut-upper-bound-approximation of CDF based on point estimates on the same set of cutsets is 3,26E-05/yr. Thus, introduction of parameters’ uncertainty distributions (for, roughly, one half of parameters’ population) results in a slight shift in CDF value. This shift is generally explainable by the effect of coupling of parameters, which is discussed in the section that follows.

Table 2. Series of ten propagations of uncertainty to CDF-level.

Run #	CDF (/yr)
1	3,33E-05
2	3,29E-05
3	3,31E-05
4	3,32E-05
5	3,34E-05
6	3,28E-05
7	3,33E-05
8	3,34E-05
9	3,28E-05
10	3,28E-05
Average	3,31E-05

### 3 COUPLING THE FAILURE PROBABILITY

In Risk Spectrum code (Berg, U. & L Sardh. 1994), the uncertainty propagation is based on the set of pre-generated minimal cutsets (Berg, U. & L Sardh. 1994). The data for basic events and parameters included in minimal cutsets are read from the project data base. In the simulation process, the top event result is calculated specified number of times. In each of those simulations, all of the parameters are looped through. For each parameter, a value is simulated from parameter’s uncertainty distribution.

One important effect of simulating at the parameter level (rather than at the basic event level) is that parameter dependencies (“coupled failure data”, “state-of-knowledge-dependence”) are taken into account (Berg & Sardh. 1994). As noted earlier, the quantification of minimal cutsets in individual simulation is carried on by using the “min cut upper bound approximation”.

To demonstrate an impact of coupling the parameters’ values in uncertainty propagation, a simple example was designed and carried out. It is based on evaluating two hypothetical redundant components *A* and *B* that appear in the minimal cutset *M*:

$$M = A B \tag{1}$$

It is assumed that components have identical failure probability, i.e.  $P_A = P_B = q$ . Assuming, further, that basic events *A* and *B* are independent from each other (common cause failures are left out from this example), the probability of the minimal cutset *M* is:

$$P_M = P_A P_B \tag{2}$$

In the case that no parameter uncertainty is taken into the account, the probability of *M* is obtained by means of point estimate, which is:

$$P_M = q^2 \tag{3}$$

When consideration of parameters' uncertainty is introduced, parameter  $q$  becomes a random variable ( $Q$ ) subjected to a specified uncertainty distribution with mean value  $q$ . Probability of minimal cutset  $P_M$  becomes a random variable itself, which distribution is determined by sampling out the values of  $Q$ . In this example, sampling is done in two ways:

- 1) with "uncoupled" failure probabilities, and
- 2) with "coupled" failure probabilities.

In the case of uncoupled failure probabilities, the sampling is performed at the basic event level, i.e. probabilities  $P_A$  and  $P_B$  are random variables  $P_A = Q_A$ ,  $P_B = Q_B$ , which are sampled independently. The expected value of minimal cutset probability  $P_M$  that would be obtained by this kind of sampling is:

$$\begin{aligned} E[P_M] &= E[P_A P_B] = E[Q_A Q_B] = \\ &= E[Q_A] E[Q_B] = q^2 \end{aligned} \quad (4)$$

In other words, the expected value equals the point estimate value that existed before the introduction of uncertainty considerations.

On the other hand, when coupling of failure probabilities for this example is applied, the sampling is performed at the parameter level. This means that probabilities  $P_A$  and  $P_B$  are represented by the same random variable  $Q$ , i.e.  $P_A = P_B = Q$ . The expected value of probability of minimal cutset,  $P_M$ , when this type of sampling is applied, is:

$$\begin{aligned} E[P_M] &= E[P_A P_B] = E[Q^2] = \\ &= E^2[Q] + V[Q] = \\ &= q^2 + V[Q] \end{aligned} \quad (5)$$

This means that the value of minimal cutset probability, as obtained by sampling, would be higher by the value of variance  $V[Q]$  than the value obtained from point estimate (Eq. 3).

Assuming that random variable  $Q$  is subjected to lognormal distribution with mean  $q$  and error factor  $EF$ , variance  $V[Q]$  is expressed as:

$$V[Q] = q^2 \left[ \exp \left[ \left( \frac{\ln EF}{1,645} \right)^2 \right] - 1 \right] \quad (6)$$

where 1,645 is 95th percentile of standard normal distribution. The expected value of minimal cutset probability is then equal to:

$$E[P_M] = q^2 \exp \left[ \left( \frac{\ln EF}{1,645} \right)^2 \right] \quad (7)$$

Table 3. Calculated values of factor  $z$  (Eq. 8) vs. corresponding risk spectrum estimates (coupled failure probabilities).

EF	Calculated	Risk spectrum
1	1,00	1,00
1,5	1,06	1,07
2	1,19	1,20
2,5	1,36	1,36
3	1,56	1,56
3,5	1,79	1,76
4	2,03	2,01
4,5	2,31	2,32
5	2,60	2,74
5,5	2,93	2,83
6	3,28	3,38

Thus, mean value of minimal cutset probability obtained by sampling from coupled failure probability would be higher than point estimate by factor:

$$z = \frac{E[P_M]}{q^2} = \exp \left[ \left( \frac{\ln EF}{1,645} \right)^2 \right] \quad (8)$$

which increases exponentially with squared error factor.

Calculated values of factor  $z$  for error factors ranging from 1 to 6 are presented in the second column of Table 3. An appropriate example has been simulated by Risk Spectrum in order to obtain estimates of  $z$  for the same values of error factors. It consisted of hypothetical two redundant components (AND-ed together in a trivial fault tree) with assigned coupled failure probability subjected to lognormal distribution with mean value of 1,0E-04. For each assumed error factor value from Table 3, ten successive uncertainty analyses were performed based on 10000 Monte Carlo simulations (samplings). In each analysis a value of factor  $z$  was calculated by dividing the obtained mean value of minimal cutset probability distribution with  $q^2$  (i.e. 1,0E-08). Average values taken from sets of ten results for each error factor from Table 3 are provided in the third column in the table.

Comparison between calculated values of  $z$  and estimates from Risk Spectrum is shown in Figure 3.

As could be seen, values obtained on the basis of runs follow very closely the calculated values.

Risk Spectrum sampling and uncertainty propagation to  $P_M$  has also been performed for the same example (two redundant components with failure probability subjected to lognormal distribution with mean value of 1,0E-04) for the case of uncoupled failure probabilities. In this case, the expected value of  $z$  (Eq. 4 and Eq. 8) is:

$$z = \frac{E[P_M]}{q^2} = 1 \quad (9)$$

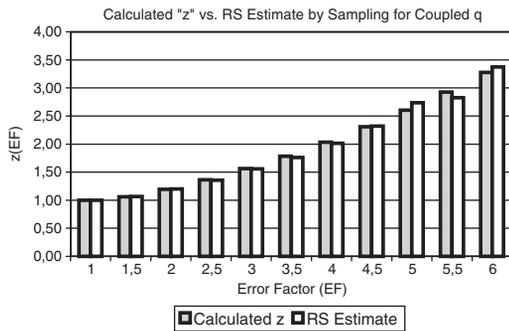


Figure 3. Comparison of calculated values of z vs. estimates based on risk spectrum simulations.

Table 4. Risk spectrum simulations of factor z (Eq. 9) for the case of uncoupled failure probabilities.

EF	Simulation of z
1,5	1,000
2	1,000
2,5	1,007
3	0,998
3,5	0,995
4	1,003
4,5	1,008
5	1,007

In the manner similar to the above, for each assumed error factor value ten successive uncertainty analyses were performed based on 10000 samplings. In each analysis a value of z was calculated by dividing the obtained mean value of  $P_M$  distribution with  $q^2$  (i.e. 1,0E-08). Average values taken from sets of ten results for error factors ranging from 1,5 to 5 are provided in Table 4.

As can be seen from the Table 4, Risk Spectrum performs uncoupled sampling in the way that is in very good agreement with Equation 9.

Thus, coupling of parameters can have very significant effect on the result in the case of redundant components, i.e. the case when representative basic events appear in the same minimal cutset(s).

The coupling does not have such an effect in the case when the components appear “in series”, which means that the representative basic events do not appear in the same minimal cutsets. This is particularly the case when rare event approximation applies, which mostly is the case with PSA models. For the above example this would mean:

$$P_M \approx P_A + P_B \tag{10}$$

Table 5. Simulation of top event probability with 2 identical components in series for coupled and uncoupled parameters.

EF	Coupled ( $\times 10^{-04}$ )	Uncoupled ( $\times 10^{-04}$ )
1,5	2,000	1,999
2	1,996	2,001
2,5	1,995	2,005
3	2,010	2,004
3,5	2,001	1,998
4	2,006	2,014
4,5	1,999	2,005
5	2,001	2,000

Point estimate of top event probability  $P_M$  is:

$$P_M \approx 2q \tag{11}$$

In the case of uncoupled sampling, the expected value of  $P_M$  is:

$$\begin{aligned} E[P_M] &\approx E[P_A + P_B] = E[Q_A + Q_B] = \\ &= E[Q_A] + E[Q_B] = 2q \end{aligned} \tag{12}$$

while the expectation in the case of coupled sampling would be:

$$\begin{aligned} E[P_M] &\approx E[P_A + P_B] = E[2Q] = \\ &= 2 E[Q] = 2q \end{aligned} \tag{13}$$

Thus, in the case of rare event approximation, both uncoupled and coupled sampling would result in a mean value that equals point estimate. This has also been simulated by Risk Spectrum in an example similar to the one above. It consisted of hypothetical two identical components OR-ed together in a trivial fault tree, with assigned failure probabilities subjected to lognormal distribution with mean value of 1,0E-04. Thus, the point estimate of assumed top event probability equaled 2,0E-04. (Second order term is negligible.)

For a set of error factor values ranging from 1.5 to 5 uncertainty analyses were performed with uncoupled as well as with coupled failure probabilities. For each error factor, in each of the two cases ten successive uncertainty runs were performed based on 10000 samplings.

Average values taken from sets of ten results for each error factor (for the case with coupled as well as uncoupled parameters) are provided in Table 5.

As can be seen, the simulations yielded expected results.

#### 4 EFFECT OF MOST IMPORTANT PARAMETERS

In order to get more insight on the impact of introducing parameters' uncertainty distributions and sampling at parameter level on the CDF result, an analysis of importance of parameters was performed.

Parameter importance lists based on Risk Increase Factor (RIF) and Fractional Contribution (FC) were examined and a group of parameters from the top of both lists was selected (Table 6), based on the following considerations.

- Parameter must be defined with an uncertainty distribution. Parameters that appeared at the top of any list, but were, otherwise, represented as point estimates were ignored.
- For convenience, parameter's uncertainty distribution must be lognormal. This lead to exclusion from the list of only one parameter.
- Parameter must contribute to the coupling effect. This lead to removing from the list some parameters that were related to single basic events (e.g. failures of AF TDP, which is a single component of a kind).
- Retained in the list were parameters with RIF > 1000 or FC > 2%.

On this basis, the list of 22 influential parameters was obtained, which is presented in Table 6. To observe the impact of their uncertainty on the estimate of mean CDF value, sensitivity cases were designed with

increased values of error factors of these parameters' distributions. In a specific case, all 22 error factors were multiplied by a factor *k*. In four cases analyzed, values of *k* were being increased from 1 (i.e. nominal error factors) to 3. In all cases the mean parameters' values were left unchanged.

The results are presented in Table 7 and illustrated by Figure 4. For each case from Table 7, a series of ten uncertainty propagations, based on 9000 Monte Carlo simulations, was performed. Mean CDFs given in Table 7 represent averaged values taken from ten results.

As it could be seen, increasing the error factors in uncertainty distributions of only a limited set of 22 parameters (out of, roughly, 190 parameters with uncertainty distributions introduced) can have a significant effect on the estimate of CDF mean value due to the coupling effect.

#### 5 CONCLUSIONS

In the PSA model considered, introducing uncertainty distributions for probabilities of failure per demand, failure rates and TM unavailabilities (which is approximately one half of all parameters in PSA model) introduced only a slight shift (of the order of 1-2%) in mean CDF value, with respect to existing point estimate.

Table 6. Top parameters in RIF and FC lists.

Parameter	Equipment	RIF	FC (%)	EF
1 R-411	AC Buses	3,4E +5	-	10
2 R-58	MOVs	3,0E +5	-	3
3 R-83	AC Buses	3,1E +4	-	5
4 Q-64	Check Val.	1,2E +4	3,0	3
5 R-84	Circ. Break.	9,0E +3	-	3
6 R-182	CCW Pumps	5,7E +3	6,5	2,73
7 R-67	MDP	5,3E +3	-	10
8 Q-114	Spec. Valv.	5,2E +3	4,1	1,75
9 Q-191	Relays	5,0E +3	-	10
10 R-180	ESW Pumps	4,1E +3	2,1	3,75
11 R-141	Relays	-	3,7	10
12 Q-55	MOVs	2,2E +3	7,9	1,5
13 R-90	DC Invert.	1,4E +3	-	3
14 Q-138	Relays	1,4E +3	-	10
15 R-73	DGs	-	22,2	2,19
16 Q-72	DGs	-	18,7	1,5
17 Q-85	Circ. Break.	-	6,5	10
18 Q-179	ESW Pumps	-	2,7	2,5
19 Q-181	CCW Pumps	-	2,7	2,99
20 Q-99	Air Compr.	-	2,4	3
21 Q-165	AFW MDP	-	2,3	2,64
22 Q-51	AOVs	-	2,2	1,31

Table 7. Mean CDF sensitivity cases with Increased error factors of 22 parameters.

k	Mean CDF
1	3,31E-05
1,5	3,54E-05
2	3,69E-05
2,5	3,92E-05
3	4,21E-05

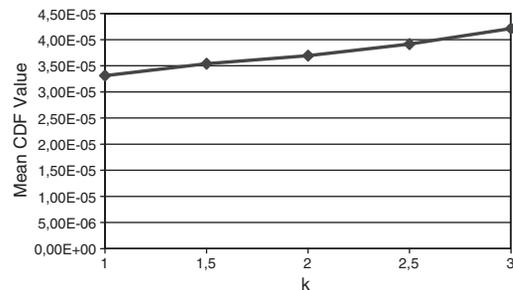


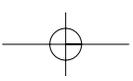
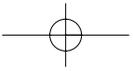
Figure 4. The effect of increasing the error factors of influential parameters on mean CDF value.

The effect of parameters' coupling can have significant impact in the case of components appearing in the same minimal cutsets (e.g. redundant components).

The error factors of influential parameters, such as those from the top of parameter importance lists, can have significant impact on the estimate of mean CDF value.

## REFERENCES

- ASME 2002 Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME RA-S-2002, The American Society of Mechanical Engineers.
- Bari, R. A., Buslik, A. J., Cho, N. Z., El-Bassioni, A., Fragola, J., Hall, R. E., Ilberg, D., Lofgren, E., O'Brien, J., Papazoglou, I. A., Samanta, P. K., Teichmann, T., Vesely, W., Unione, A. and Youngblood, R. 1985 *Probabilistic Safety Analysis Procedures Guide*. NUREG/CR-2815. Upton, USA: Brookhaven National Laboratory.
- Berg, U. & Sardh, L. 1994 Risk Spectrum User's Manual. Relcon Teknik AB, Sundbyberg, Sweden.
- Hickman, J. W., et al. 1983 PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants. NUREG/CR-2300. USA: Nuclear Regulatory Commission, 1983.
- IAEA 1992 Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1). Safety Series No. 50-P-4. Vienna, Austria: International Atomic Energy Agency.
- Jordan Cizelj, R. & Parzer, I. 2002 Uncertainty Analysis of NEK IIE PSA Component-related Parameters, IJS-DP-8634, Institut "Jožef Stefan", Ljubljana, Slovenija.
- Jordan Cizelj, R. & Vrbanić, I. 2001 Parameter Estimation of Component Reliability Models in PSA Model of Krško NPP. *Nuclear Energy in Central Europe 2001*, Portorož, Slovenia Ljubljana: Nuclear Society of Slovenia.
- Jordan Cizelj, R. & Vrbanić, I. 2002a Modelling Uncertainties When Estimating Component Reliability (Unpublished).
- Jordan Cizelj, R. & Vrbanić, I. 2002b Transformation of Bayesian Discrete Posterior Distribution into a Continuous Distribution, International Conference "Nuclear Energy for New Europe", September 9–12, 2002, Kranjska Gora, Slovenia.
- Jordan Cizelj, R., Vrbanić, I., and Mavko, B. 2002 Uncertainty Analysis of Fault Tree Parameters, International Topical Meeting on Probabilistic Safety Assessment, American Nuclear Society, October 6–9, Detroit, Michigan, USA.
- US NRC 1988 NRC GL 88-20: Individual Plant Examination for Severe Accident Vulnerabilities – 10 CFR 50.54(f) With Supplements.
- US NRC 1998 An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, Revision 0. Regulatory Guide 1.174.
- Vrbanić, I. & Jordan Cizelj, R. 2002 Uncertainty Analysis of Component Failure Model Parameters in PSA: A Case Study. *PSAM 6*, San Juan, Puerto Rico, USA.
- Vrbanić, I., Kaštelan, M. & Košutić, I. 2002 NEK Baseline PSA Model "NEKC18", *NEK ESD TR-07/01*, Revision 0.
- Vrbanić, I., Košutić, I. & Jordan-Cizelj, R. 2003. Propagation of Parameters' Uncertainty from Task 1 in Baseline NEK PSA Model, *NEK ESD TR-20/02* (in preparation).
- Westinghouse-NEK 1994 Probabilistic Safety Assessment of Nuclear Power Plant Krško, Level 1 Report, Volumes 1–14, Westinghouse Electric Corporation – NEK.



## Impact of river morphology on extreme flood level prediction: a probabilistic approach

S. van Vuren, M. Kok & S.J. Ouwerkerk

*Delft University of Technology, Section of Hydraulic Engineering, Delft, Netherlands*  
*HKV Consultants, Netherlands*

**ABSTRACT:** The dike rings along the Rhine in the Netherlands have a level of protection of 1/1250 per year. The design water levels are estimated on the basis of one random variable: the river discharge. Van Vuren & Van Breen (2003) show the existence of large spatial and temporal variation in bed level position in the river Waal. In this paper the impact of river morphology on extreme flood level predictions is investigated. Therefore, the method to compute design water levels is extended with another random variable: the river morphology. The results show that the impact of river morphology on design water levels is limited. A random bed level prior to the design water level computations leads to small changes (order of 0.01–0.06 m) in design water levels. The impact of seasonal variations in the river morphology and morphological changes during the flood wave can be neglected.

### 1 INTRODUCTION

The Netherlands is unique in the fact that a large part of it exists solely because of the presence of dikes along the coast and rivers, (TAW, 1998). Flood protection is therefore embedded in many laws, but is summarized in the Flood Protection Legislation. According to this Legislation the Netherlands is divided in 53 dike ring regions of which each has its own level of protection. The dike rings along the Rhine branches have a level of protection of 1/1250 per year. This means that river dikes are designed for water levels with a yearly exceedance probability of 1/1250 – the design water level (DWL).

So far, the DWLs are estimated on the basis of one random variable: the design discharge. A 1D hydrodynamic model for the Dutch Rhine branches (Van der Veen, 2001) is used to compute the DWLs. A margin is applied to account for among others wave and wind set-up. The DWLs do not only depend on this discharge and the set-up factors. Uncertainties in the DWLs are introduced with among others the schematization of the hydrodynamic model and the specification of the model input (boundary conditions, initial conditions and model parameters). For example, uncertainties in the model calibration (hydraulic roughness modeling) and the geometrical river schematization (morphological state) may affect the computed DWLs. Each uncertainty source will contribute differently to the

exceedance probability of the water levels. Accordingly, each uncertainty source will affect differently the computed DWLs.

In this paper we investigate the impact of river morphology in the river Waal on extreme flood level predictions. Therefore, the DWL computation method is extended. The present situation in the Waal without any additional human intervention is considered. The extended method includes the contribution of two random variables in the DWL computation: the river discharge and the river morphology. The method contains different steps. With the help of Monte Carlo simulation with a 1-D morphodynamic model, a large number of possible morphological states are simulated. These morphological states form the basis of a large number of water levels computations: for each simulated morphological state, water levels are computed for a range of steady discharges. Numerical Integration combines the likelihood of the simulated morphological state and the discharge levels to estimate the probability of the computed water levels. The set of outputs resulting from all computations is used to determine per location along the river a curve showing the exceedance probability of water levels. On the basis of this curve the “new” water level with a probability of occurrence of 1/1250 per year can be derived. This can be compared with the DWL that is derived with the traditional method using only one random variable:  $DWL_0$ . Also, this curve can be used to estimate the “new” exceedance probability of the  $DWL_0$ .

Concerning river morphology two aspects are considered:

1. The effect of variation in the morphological state prior to DWL computations.
2. The impact of morphological changes during the flood wave.

## 2 DESIGN WATER LEVELS AND MORPHOLOGY

### 2.1 *Design water levels*

In the Netherlands, the dike rings along the Rhine branches have a protection level of 1/1250 per year (Flood Protection Legislation, 1996). Every five years, the DWLs are revised to adapt for changes in the design discharge, in the river morphology, in the discharge distribution at bifurcation points and in the lateral discharges of tributaries.

Flood protection measures are taken on the basis of the revised DWLs. In the past the dikes were strengthened and heightened in order to protect the Netherlands from flooding. Recently, a new flood protection policy, called Room for the Rivers, has been implemented for the Dutch rivers. Measures other than dike strengthening are considered in order to increase the flood conveyance capacity of the river. Examples of such measures are lowering groynes, repositioning river dikes, establishing detention basins, lowering floodplains and removing summer dikes.

The estimation of DWL is embedded with a number of uncertainties, as shown for instance by Kok et al. (2003). Apart from statistical uncertainties which are caused by the limited amount of observed river discharges, also model uncertainties (caused by the fact that the actual probability density from which "nature generates its realisations" is unknown) can lead to uncertainties of the design river discharges of up to 20% (Van Gelder, 2000). The DWL computation method is only stochastic in a certain way: a design discharge with a yearly probability of 1/1250 is applied. The inclusion of more than one random variable in the DWL computation method may result in a change in the DWLs. In this paper the importance of river morphology on flood level prediction is investigated.

Van Vuren & Van Breen (2003) show the existence of large spatial and temporal variation in bed level position in the river Waal. The river's geometrical schematization (morphological state) in the hydrodynamic model used for the DWL computation is derived on the basis of annual bathymetric soundings in the period between April and November – a series of snapshot taken at different points in time. This means that the sampling has a seasonal bias. The geometrical schematization might therefore be an arbitrary choice,

as the bed level state in September can be different from the one in February.

Moreover, the riverbed can be very active in the Waal during floods. This leads to a large uncertainty range in the bed level, which affects the predicted height of the flood wave. This important role of morphological changes at high discharge conditions is encountered in many rivers. In the Yellow River, for instance, it is impossible to accurately predict the flood levels without accounting for the morphological changes during the flood (Kemink, 2002).

### 2.2 *Morphodynamic sobek rhine branches model*

The morphodynamic Rhine branches model (Jesse & Kroekenstoel, 2001), a 1-D Sobek model (WL, 2001), is used to simulate the morphological response and to compute the DWLs. This morphodynamic model solves the 1-D cross-sectionally integrated shallow water equations, distinguishing between the main channel, the flow conveying floodplain and the storage area. In addition the sediment transport rate and the sediment balance equations are used to determine the morphological changes.

In reality many irregularities occurs in the river Waal, such as variations in geometry, in floodplain width, in floodplain vegetation type, in the presence or absence of summer dikes, flood-free areas and storage and conveying parts in the floodplains. Each irregularity acts as a generator for new bottom waves. Irregularities such as variations in river geometry, bottom groynes (Erlecom) and fixed bottom layers (Nijmegen and St. Andries) are included in the Sobek Rhine branches model. The morphological model is calibrated on the basis of bathymetric data in the period between 1987 and 1997. The model predicts for the period between 1997 and 2097 erosion in the upper part (867 km–915 km) and large-scale sedimentation in the lower part (915 km–963 km) of the Waal. Although some sedimentation is expected because maintenance dredging is not incorporated in the model, the sedimentation cannot be completely explained by the neglect of dredging. The sediment transport is likely underestimated. Therefore, in this study only the upper part of the Waal – Waal section between Pannerdensed Kop (km 886) and Tiel (km 915) – is considered next.

### 2.3 *Design flood wave*

The DWLs are estimated on the basis of the design discharge that has a yearly probability of occurrence of 1/1250. The design discharge is derived with a statistical analysis on yearly peak discharges out of a range of 100 years of daily discharge measurements at Lobith, where the Rhine enters the Netherlands. This time series is homogenized to compensate for the river

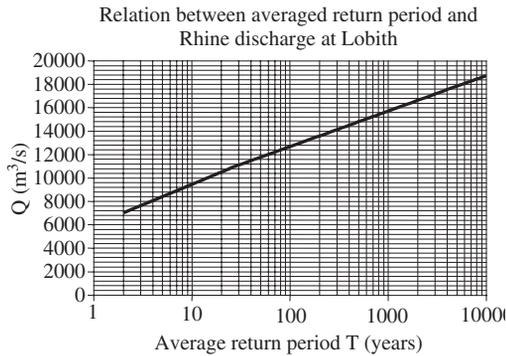


Figure 1. Relation between river discharge at Lobith and the averaged return period.

regulation works in Germany (canalization works and the placement of weirs). A combination of three probability distributions (a Gumbel distribution, a Pearson-III distribution and a lognormal distribution) is applied to derive the design discharge (Parmet, et al. 2002).

The design discharge is revised every five years, recently in 2001. The time series is extended with peak discharges in the period between 1992 and 1998. As a consequence of extreme discharges in 1993 (11,039 m<sup>3</sup>/s) and 1995 (11,885 m<sup>3</sup>/s) the design discharge has gone up to 16,000 m<sup>3</sup>/s. The relation between the averaged return period T and the river discharge – Q [m<sup>3</sup>/s] – at Lobith is described by:

$$\begin{aligned}
 Q &= 1517.8 \cdot \ln(T) + 5964.6 & 2 \leq T \leq 25 \\
 Q &= 1316.4 \cdot \ln(T) + 6612.6 & 25 \leq T \leq 10,000
 \end{aligned}
 \tag{1}$$

The wave shape of the design flood wave is derived by upscaling 21 historical flood waves (Klopstra & Duits, 1999). The discharge levels of each flood wave are multiplied with the ratio discharge/peak discharge of the flood wave. The average wave shape (Figure 2) of the resulting 21 upscaled flood waves is used for the traditional DWL computation method.

2.4 River morphology in the waal

Van Vuren & Van Breen (2003) investigated the bed level variation in the Waal in the present situation without additional human interventions. A short summary of their findings is given in this section. The morphological response in the river Waal (Figure 3) is analysed with a 1D-morphodynamic Sobek model of the Dutch Rhine branches (Jesse & Kroekenstoel, 2001). The model shows further evolution of the system without any additional human intervention.

The morphological computations are affected by various uncertainties, including uncertainties in the model schematization and uncertainties in the

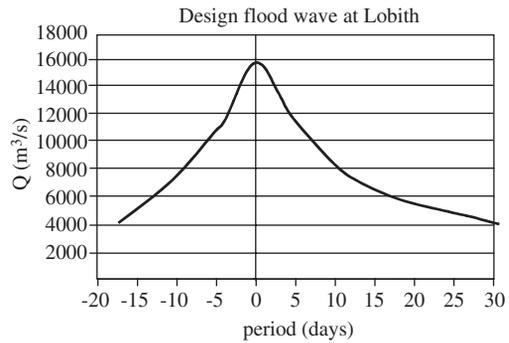


Figure 2. Design flood wave at Lobith.



Figure 3. The river Waal in the Netherlands.

specification of the model input. Monte Carlo simulation is applied to quantify the uncertainties in the morphological response. Van der Klis (2003) and Van Vuren et al. (2002) showed that the relative contribution of an uncertain discharge to the uncertainty in the morphological response is one of the most relevant factors. Therefore, the effect of an uncertain river discharge on the uncertainty in the morphological response is analysed. Uncertainties introduced by the model schematization are not considered.

Monte Carlo simulation (Hammersly and Handscomb, 1964) involves a large number of model simulations with statistically equivalent inputs. For each 1D Sobek model simulation a discharge time series of a hundred years duration is randomly generated according to the prescribed probability distribution. This distribution accounts for the seasonal dependency of the discharge and the correlation of the discharge in successive periods. On the basis of the outputs of 500 of these model simulations, the morphological response statistics (e.g. the expected value and 90% confidence band of the bed level change) are analysed.

The results show that a large variation in bed level uncertainty exists in the river Waal: in space (due to irregularities in the river geometry) and in time (due to seasonal variation in discharge).

Figure 4 shows the spatial variation of the morphological response statistics in the main channel after 100 years in January. This figure presents the mean bed level changes and the (size of the) 90% confidence interval of the bed level changes in the Waal section between the Pannerdende Kop (km 886) and Tiel (km 915). The 90% confidence interval means that with a probability of 90% the bed level changes are within this range.

Figure 4 illustrates that the irregularities in the river, such as width variation and man-made structures (such as riverbed protection), in combination with an uncertain river discharge lead to an uncertain morphological response. Each irregularity in the river acts as a generator of new bottom waves. At locations with large discontinuities, a local increase in bed level variability is observed – reflected by an increase in the 90% confidence band in the panel of Figure 4.

At Erlecom (km 873–876) submerged groynes and at Nijmegen (km 882–885) an armoured layer are present in the bend of the riverbed. These constructions are designed for navigation purposes. In the model the river bed constructions are schematized as fixed bed layers imposing a lower bound on the bed level. At both locations the morphological response after 100 years shows a bar in the riverbed and a reduction of the confidence band. The fixed layers prevent further erosion, while they lead to extra erosion and bed level variability downstream.

Figure 4 indicates the locations with large variation in the floodplain width: Hiensche waarden and Affendensche waarden (km 898–901); Ochtense Buitenpolder (km 902–906) and Willemspolder and Drutense waard (km 906–913). At these locations an increase in the size of the confidence band is noticed. E.g. a large open water area exists between km 906 and km 908 in the floodplain “Willemspolder” (Figure 5). An increase in floodplain width results in sedimentation. A decrease leads to erosion. At the transition points this results in an increase in bed level variability and hence to a larger size of the confidence band.

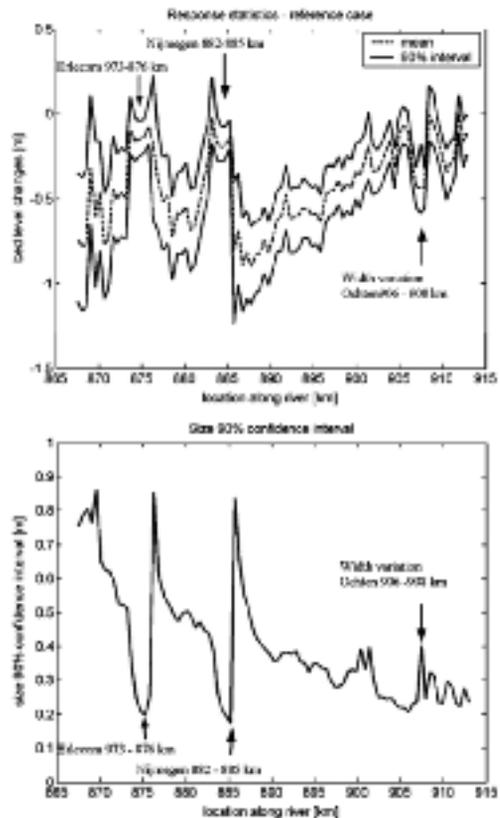


Figure 4. Spatial variation of statistical properties of the bed level change after 100 years in the Waal section between Pannerdende Kop (km 886) and Tiel (km 915).



Figure 5. River section “Willemspolder” (km 906–908) with large variation in the floodplain width (courtesy of DON).

In Figure 6 the temporal variation of location 907.4 km in the floodplain “Willemspolder” is shown. At this location, the temporal variation in morphological response statistics is considerable. This temporal variation reflects the seasonal variation of the river discharge. At this transition from a narrow to a wide

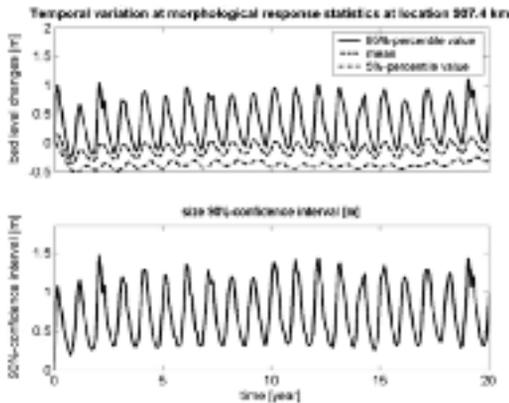


Figure 6. Temporal variation of statistical properties of the bed level change in the Waal at location 907.4 km in the Willemspolder.

cross section (see Figure 5) sedimentation in the main channel takes place. The seasonal fluctuation of the 90%-confidence band is significant. The largest 90% confidence interval is found in the high water period. The smallest interval is found in the low water period. The 95%-percentile strongly oscillates, while the 5%-percentile is more or less constant. This can be explained by the fact that during discharges higher than the bankfull discharge bottom waves (sedimentation) are initiated in the main channel. These bottom waves migrate downstream and (partly) decay during discharges lower than the bankfull discharge. Therefore, the seasonal variation in the 5%-percentile is limited. At other locations along the river with small irregularities this temporal variation is less (or hardly noticeable).

Van Vuren and Van Breen (2003) concluded that large-scale floodplain lowering in combination with summer dike removal lead to more bed level variability than in the present situation without any additional human interventions.

### 3 METHOD

#### 3.1 Proposed methodology for DWL computation

The extended method not only includes the discharge as a random variable. It includes the “uncertain” river morphology as well. The method covers that a peak discharge in combination with a particular morphological state may result in water levels that are higher or lower than the DWLs derived with the traditional computation method. The extended method involves the following steps (Figure 7):

1. With the help of Monte Carlo simulation with the 1-D morphodynamic Sobek model for the Rhine

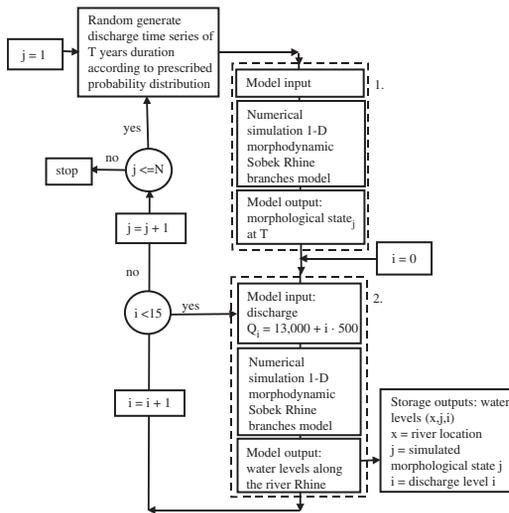


Figure 7. Design water levels: computation method with the random variables: discharge and bed level.

branches, a large number of morphological states are simulated (similar to section 2.4). In this study 500 morphological simulations are performed.

2. The simulated morphological states form the basis of a large number of water level computations with the 1-D morphodynamic Sobek Rhine branches model. For each simulated state, water levels are computed for a range of steady discharges between 13,000 m<sup>3</sup>/s and 20,000 m<sup>3</sup>/s, with a discretisation step of 500 m<sup>3</sup>/s. This results in 15 water level computations per simulated morphological state:

$$Q_i = 13,000 + i \cdot 500 \quad \text{for } i = 0, \dots, 14 \quad (2)$$

3. Numerical Integration combines the probability of the two random variables. The likelihood of the simulated morphological state and the discharge levels is combined to estimate the probability of the computed water levels. The probability of each simulated morphological state is the same:

$$P(\text{Morphological State}_j) = \frac{1}{N} \quad \text{for } j = 1, \dots, N \quad (3)$$

in which N is the number of morphological simulations with the Sobek Rhine branches model (in the Monte Carlo simulation). The probability of the discharge level  $Q_i$  is derived with the help of formula (1):

$$T(Q) = \exp\left(\frac{Q - 6612.6}{1316.4}\right)$$

$$F_Q(Q) = P(Q \leq Q) = \frac{1}{T(Q)} = \exp\left(\frac{Q - 6612.6}{1316.4}\right) \quad (4)$$

$$P(Q_i) = F_Q(Q_i + 250) - F_Q(Q_i - 250)$$

The multiplication of the probability of the simulated morphological state  $j$  and the probability of the discharge level  $Q_i$  lead to the combined probability of the water level computation:

$$P(\text{Water level}(i, j)) = P(\text{Morphological State}_j) \cdot P(Q_i) \quad (5)$$

Equation (5) holds since the morphological state  $j$  is considered independent of the discharge  $i$ .

- The set of outputs resulting from all computations is used to determine per river location a curve showing the exceedance probability of water levels.

On the basis of the exceedance probability curve the “new” water level with yearly a probability of occurrence of 1/1250 can be derived. This can be compared with the DWL that is derived with the traditional method using only one random variable:  $DWL_0$ . Also, this curve can be used to estimate the “new” exceedance probability of the  $DWL_0$ .

### 3.2 Cases

Three cases are considered to analyse the impact of river morphology on extreme flood level prediction.

In Case 1 “Long-term variation in morphology” the impact of stochastic morphological changes over a longer period – years – is considered. The model scheme in Figure 7 is run through for different points in time  $T$ :

$$T = t_0 + k \cdot \Delta T \quad \text{for } k = 1, \dots, 4$$

in which  $t_0$  is the starting point of the morphological simulation,  $\Delta T$  is a period of 5 years. The morphological changes during floods are not included. The simulated bed level state at time  $T$  is held fixed during the water level computations.

In Case 2 “Seasonal variation in morphology” the impact of seasonal variation in the morphological state prior to the water level computation is considered. The model scheme in Figure 7 is run through for different points in time  $T$ :

$$T = t_0 + 5 + k \cdot \Delta T \quad \text{for } k = 1, \dots, 12$$

in which  $t_0$  is the starting point of the morphological simulation,  $\Delta T$  is a period of 1 month. Similar to Case 1, the morphological changes at high water conditions is not considered.

Case 3 “Morphology during floods” is similar to Case 1. The morphological changes during flood circumstances are considered in this case. The simulated bed level state at time  $T$  is not held fixed during the water level computations, but morphodynamic changes at high water conditions are included.

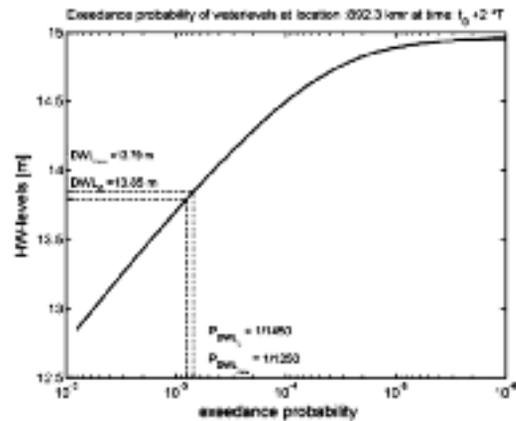


Figure 8. Exceedance probability of water levels at location 892.3 km at time  $t_0 + 2 \cdot T$  for Case 1.

## 4 RESULTS

For the three cases the model scheme in Figure 7 is used. For each case this resulted per future moments in a set of computed water levels and corresponding probabilities. These are used to derive a curve showing the exceedance probability of water levels per river location, see for example Figure 8.

The  $DWL_0$  in this curve represents the design water level at time  $t_0$  that is derived with the traditional method using only one random variable. The curve is used to derive the “new” water level with a yearly exceedance probability of 1/1250 and “new” exceedance probability of the  $DWL_0$ . In Figure 8 it is shown that the DWL (at location 892.3 at time  $t_0 + 2 \cdot T$ ) will decrease with 0.06 m. The exceedance probability of the  $DWL_0$  decrease from 1/1250 to 1/1450.

### 4.1 Case 1: “Long-term variation in morphology”

The results of case 1 (Figure 9 and Figure 10) shows us that the influence of a random bed level on the DWL is not high. This is partly the result of a negative trend in the bed level: it is expected that in the future the bed level will be lower than the current situation (Figure 11). This trend has a positive impact on the DWL: these water levels will also be lower. The uncertainty in the bed level can, however, increase the DWL. In the calculations we combine these two affects.

Figure 9 and 10 show that the influence of the random bed level results in higher safety, but this depends on the location along the river. The maximum change is 0.08 m, and this influence is not very large.

Figure 12 shows the  $DWL_{\text{new}}$  derived with the extended method and some DWL computations derived with the traditional method (using only one random variable, the design discharge) for single simulated

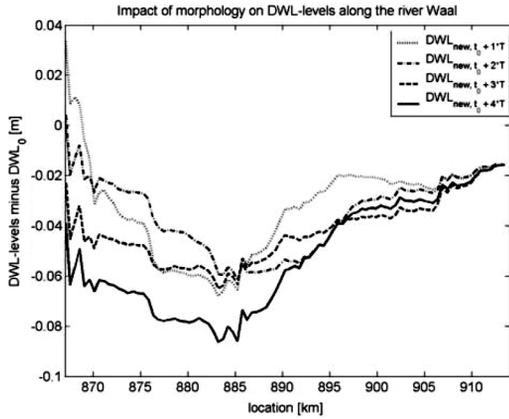


Figure 9. Impact of morphology of DWL-levels along the river Waal: change in DWL level with respect to  $DWL_0$ .

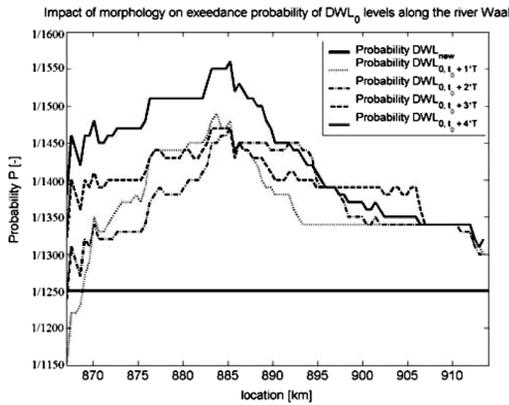


Figure 10. Impact of morphology on exceedance probability of the  $DWL_0$  levels along the Waal.

morphological states at time  $t_0 + 3 \cdot T$ . The figure illustrates that each simulated morphological state results in slightly different DWLs. The difference depends on the location along the river and is in the order of 0.01 m.

4.2 Case 2 “Seasonal variation in morphology”

Figure 13 shows the impact of seasonal variation in morphology on DWL computations. The figure illustrates that the impact of seasonal variation in morphology is small: order of less than 0.01 m. It seems that the seasonal bias in the morphological river state does affect the DWL computation.

4.3 Case 3 “Morphology during floods”

The morphological changes during floods have little impact on DWL computations. Figure 14 shows

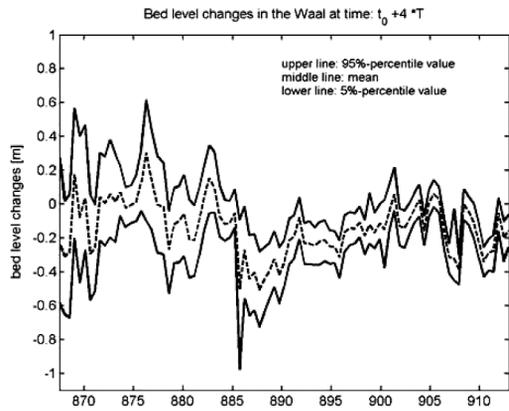
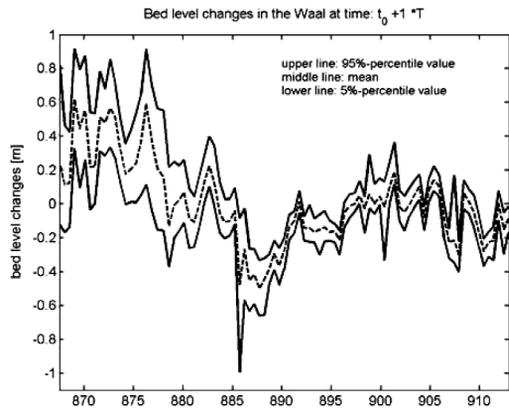


Figure 11. Spatial variation of the statistical properties of the morphological response in the Waal at time  $t_0 + T$  and  $t_0 + 4 \cdot T$ .

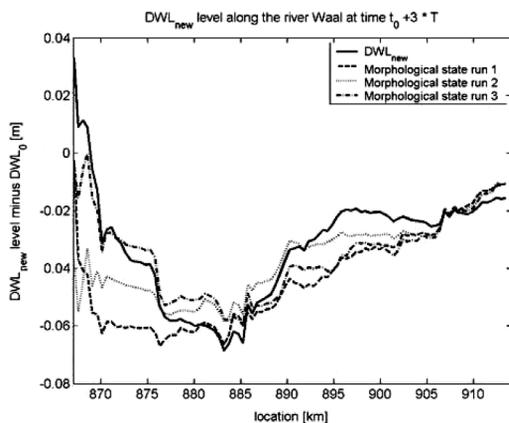


Figure 12. Impact of morphology of DWL-levels along the river Waal: change in  $DWL_{new}$  levels and DWL levels of single morphological simulations with respect to  $DWL_0$ .

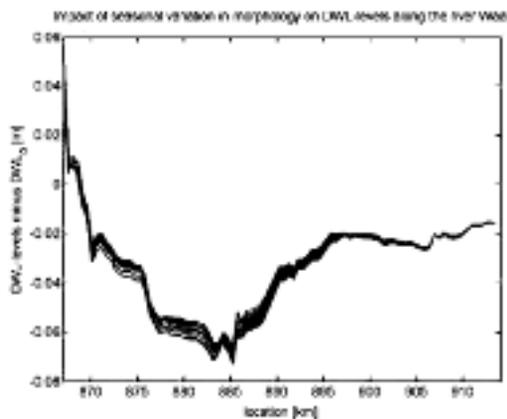


Figure 13. Impact of seasonal variation in morphology on DWL computations: each line represents the change in DWL with respect to  $DWL_0$  in one month after 5 years.

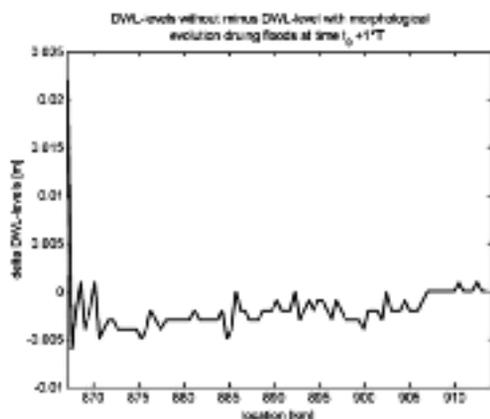


Figure 14. Impact of morphological changes during flood circumstances: difference between DWL levels if morphological changes during floods are neglected and considered.

difference between the computed DWL levels if morphological changes during floods are neglected and if they are considered in the DWL computation. Considering morphological changes at high water conditions results in slightly higher DWLs – order of less than 0.01 m.

## 5 CONCLUSIONS

In this paper the traditional DWL computation method is extended. The extended method includes the contribution of a second random variable: the river morphology. The impact of a random bed level on the

DWL is not high. The large spatial and temporal variation in the bed level position, investigated in Van Vuren & Van Breen, depends very much on the location along the river. The contribution of the uncertainty in these local bed level patterns to DWLs is reflected smoothly. The large-scale negative trend in the bed level has more impact on extreme flood levels.

This paper shows that:

- Each morphological state prior to DWL computations results in DWLs that differ in the order of 0.01–0.06 m.
- Over a longer period – years – a negative trend in the bed level in the Waal section between Panterdense Kop (km 886) and Tiel (km 915) has a positive impact on the DWLs in this section. The DWLs will decrease.
- The impact of seasonal variation in the morphology can be neglected. In the traditional DWL computation method the geometrical river schematization is derived on the basis of annual bathymetric soundings. These soundings have a seasonal bias. However, this will hardly affect the DWL computations.
- The impact of the morphological changes during floods on DWL computations is hardly noticeable.

In this paper we investigated the impact of one random variable (the variability of the discharge) on the bed level. Other random variables such as the uncertainty in the morphological process equations and the influence of the bed level might also be important. We recommend to investigate these influences on the variability of the bed level and the resulting consequences on the DWLs.

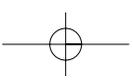
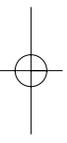
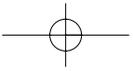
## ACKNOWLEDGEMENT

This paper is embedded in the project “Stochastic modeling of low-land river morphology no. DCB 5302” funded by the Foundation for Technical Sciences (STW). The authors wish to acknowledge the Institute for inland water management and wastewater management (RIZA) for the permission to use the Rhine-branches model. They also would like to thank Professor Huib de Vriend of Delft University of Technology for his valuable input in this project.

## REFERENCES

- Hammersly, J.M. & Handscomb, D.C., 1964. Monte Carlo Methods. Methuen & Co Ltd., London.
- Jesse, P. & Kroekenstoel, D.F., 2001. 1-D Morphodynamic Rhine branches model. RIZA rapport 2001.040. ISBN 9036953952 (in Dutch “1-D Morfologisch model Rijntakken”).

- Kemink, 2002. Flood management in the lower reach of the Yellow River. MSc thesis. Delft University of Technology. Civil Engineering. Section hydraulic Engineering.
- Klopstra, D. & Duits, M.T., 1999. Methodiek voor vaststelling van de vorm van de maatgevende afvoergolf van de Maas bij Borgharen. HKV Consultants in opdracht van WL|Delft Hydraulics en Rijkswaterstaat RIZA. Lelystad, maart 1999.
- Kok, M., Stijnen, J.W. & Silva, W., 2003. Uncertainty Analysis of river flood defense design in the Netherlands. ESREL 2003.
- Parmet, B.W.A.H., Van de Langemheen, W., Chbab, E.H., Kwadijk, J.C.J., Diermanse, F.L.M. & Klopstra, D., 2001. Design discharge of the Rhine at Lobith. Rapport 2002.012. ISBN 9036954347 (in Dutch "Analyse van de maatgevende afvoer van de Rijn te Lobith").
- TAW – Technical Advisory Committee on Water Defences in The Netherlands, 1998. Fundamentals on Water Defences. English translation of the Dutch Guidelines "Grondlagen voor Waterkeren".
- Van der Klis, H., 2003. Stochastic morphology. PhD-thesis Delft University of Technology. Civil Engineering. Section hydraulic Engineering.
- Van Gelder, P.H.A.J.M., 2000. *Statistical Methods for the Risk-Based Design of Civil Structures*, PhD-thesis (249 pp), Delft University of Technology, ISBN 90-9013452-3.
- Van Vuren, S. & Van Breen, L.E., 2003. Morphological impact of floodplain lowering along a low-land river: a probabilistic approach. XXX-IAHR Congress water engineers and research in a learning society: Modern Developments and Traditional Concepts in Thessaloniki in Greece, 24–29 August 2003.
- Van Vuren, S., Van der Klis, H. & De Vriend, H., 2002. Large-scale floodplain lowering along the River Waal: a stochastic prediction of morphological impacts. In: River Flow 2002 – Volume 2 edited by D. Bousmar and Y. Zech. A.A. Balkema Publishers. ISBN 905809 516 9. pp. 903–912.
- WL, 2001. *Sobek River Estuary, User manual. Technical report*. WL | Delft Hydraulics.



## Efficiency and accuracy of Monte Carlo (importance) sampling

P.H. Waarts

TNO, The Netherlands

**ABSTRACT:** Monte Carlo Analysis is often regarded as the most simple and accurate reliability method. Besides it is the most transparent method. The only problem is the accuracy in correlation with the efficiency. Monte Carlo gets less efficient or less accurate when very low probabilities are to be computed in combination with limit state functions that use a lot of computational time. The efficiency of Monte Carlo simulations can be improved by means of importance sampling. This however requires pre-information on the state function that may affect the accuracy. Several Monte Carlo simulation methods are compared with respect to efficiency and accuracy: Crude Monte Carlo, Importance Sampling, Increased Variance Sampling, and Directional Sampling. Furthermore a comparison is made with a special kind of response surface method.

### 1 BASIC FORMULATION OF THE RELIABILITY PROBLEM AND REQUIRED ACCURACY

A reliability problem is defined by a limit state function  $g(\underline{x})$  and a set of  $n$  random variables  $\underline{x}$ . Failure is defined by the event  $g(\underline{x}) \leq 0$ . The equality  $g(\underline{x}) = 0$  is called the limit state equation, the corresponding surface is called the failure surface. The failure probability can be formally expressed as:

$$P_f = P[g(\underline{x}) \leq 0] = \int_{g(\underline{x}) < 0} f_{\underline{x}}(\underline{\xi}) d\underline{\xi} \quad (1)$$

$f_{\underline{x}}(\underline{\xi})$  is the joint probability density function of  $\underline{x}$ .

The primary purpose of reliability methods is to evaluate integral (1).

How accurate the calculation of this reliability index should be is debatable. In Waarts (2000)  $V(\beta) = 0.05$  is chosen as the limit for a sufficient accurate result. The reliability index  $\beta$  is defined as:

$$\beta = \Phi^{-1}(P_f) \quad (2)$$

In this paper the amount of samples that are needed by the reliability methods to meet this accuracy will be used as a measure for the efficiency.

In this paper the methods will be compared using standard normally distributed variables. Each set of  $n$  basic random variables ( $x$ -space) can namely be transformed into a set of  $m$  ( $m \leq n$ ) independent standard normal variables ( $u$ -space). The (dependent) basic

random variables are first remodelled into standard normal variables by equating the cumulative distribution functions for the basic random variable and the standard normal variable:

$$\Phi(u_i) = F_{x_i}(\xi_i) \longrightarrow u_i = \Phi^{-1}[F_{x_i}(\xi_i)] \quad (3)$$

$\Phi(\cdot)$  is the standard normal distribution function.

Correlated variables may have to be transformed into non-correlated variables. There are several methods for the transformation of correlated variables into uncorrelated variables. The Rosenblatt transformation (Rosenblatt 1952) is the most used. Other methods proposed for transformation are proposed in (Nataf 1962), and (Johnson 1972).

### 2 STANDARD MONTE CARLO TECHNIQUES

#### 2.1 Crude Monte Carlo sampling

Well-known and straightforward Monte Carlo (MC) sampling techniques (Rubinstein 1981) are known to be accurate. Errors can only be caused by a too low number of simulations in MC.

The Monte Carlo technique consists of sampling random  $x$ -values from their distributions  $f(x)$  and calculating the relative number of simulations for which  $g(\underline{x}) < 0$ :

$$P_f = \frac{N_f}{N} \text{ or } P_f = \frac{\sum_{i=1}^N I(g(\underline{x}))}{N} \quad (4)$$

where  $N$  is the total number of simulations;  $N_f$  the number of simulations in the failed state ( $g(\underline{x}) \leq 0$ );  $I(g(\underline{x})) = 1$  if  $g(\underline{x}) \leq 0$  and  $I(g(\underline{x})) = 0$  if  $g(\underline{x}) > 0$ .

The minimum required number of samples in Monte Carlo sampling, given a target for  $V(P_f)$ , can be calculated from (Vrouwenvelder 1994):

$$N > \frac{1}{V(P_f)^2} \left( \frac{1}{P_f} - 1 \right) \tag{5}$$

For  $\beta = 4$ , the coefficient of variation of the reliability index  $V(\beta) = 0.05$  can be translated into the coefficient of variation of the probability of failure estimate  $V(P_f) = 0.57$ . The number of samples is then equal to  $N > 3/P_f \Rightarrow N > 3 \cdot 10^4$ .

The number of samples depends on the probability of failure and is independent of the number of random variables. The lower the probability of failure, the more samples have to be used.

### 2.2 Crude directional sampling

Deák (1980) first suggested the method of transforming the normal coordinates (u-space) into polar coordinates. The basic idea is to remodel the basic variables  $\underline{u}$  into polar co-ordinates  $(\lambda, \underline{\theta})$ . The unit vector  $\underline{\theta}$  defines the direction and a scalar quantity  $\lambda$  defines the length of the vector in u-space. Equation (1) is altered into:

$$P_f = \int_{g(\underline{x}) \leq 0} dF(\underline{x}) = \int P(g(\lambda \underline{\theta}) \leq 0) f(\underline{\theta}) d\underline{\theta} \tag{6}$$

where  $f(\underline{\theta})$  is the (constant) density on the unit sphere.

For each direction  $\underline{\theta}_i$  the value of  $\lambda_i$  is determined for which the limit state function equals zero:

$$g_i = g(\lambda_i \underline{\theta}_i) = 0 \tag{7}$$

In other words  $\lambda_i$  is a measure of the distance from the origin to the limit state in the direction defined by the vector  $\underline{\theta}_i$ . The factor  $\lambda_i$  is found via an iteration procedure and requires several Limit State Function Evaluations (LSFE). An estimate of the probability of failure  $P_f$  can be obtained by performing  $N$  directional Monte Carlo simulations of the  $\underline{\theta}$ -vector. Every simulation results in a sample value  $P_i$ :

$$P_i = P(g(\lambda_i \underline{\theta}_i) < 0) = 1 - \chi_n^2(\lambda_i^2) \tag{8}$$

Where  $\chi^2(\cdot)$  is the chi-squared distribution function;  $n$  is the number of random variables in the limit state function.

An estimate for the probability of failure is calculated as the mean value of the sample values  $P_i$ :

$$E(P_f) = \frac{1}{N} \sum_{i=1}^N P_i \tag{9}$$

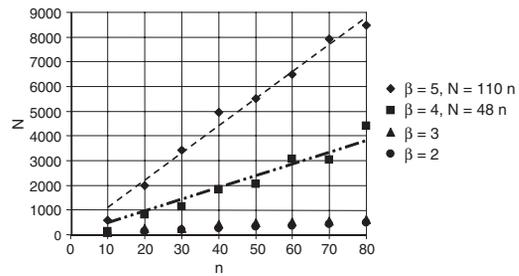


Figure 1. Required number of samples  $N$  before the estimator is sufficiently close to the criterium.

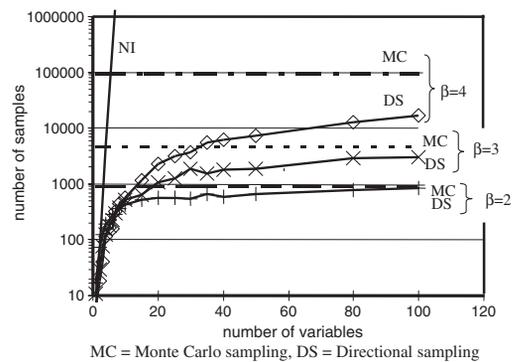


Figure 2. Required numbers of samples, all variables have equal importance in the limit state function (eq. 9).

An estimate of the standard deviation is given by Ditlevsen (1988):

$$\sigma^2(P_f) = \frac{1}{N(N-1)} \sum_{i=1}^N \{P_i - E(P_f)\}^2 \tag{10}$$

When the number of samples  $N$  is sufficiently large, the estimator for  $P_f$  is assumed to be normally distributed. The confidence intervals of the probability of failure are calculated from:

$$E(P_f) + k \sigma(P_f) < P_f < E(P_f) - k \sigma(P_f) \tag{11}$$

According to Ditlevsen (1988), the probability of failure lies between the confidence limits with a probability approximately equal to  $1 - 2\Phi(k)$ .

Figure 2 shows the required number of samples  $N$  for a coefficient of variation  $V(\beta) = 0.05$ , for reliability indices  $\beta = 2, 3$  and  $4$ . This required number of samples is calculated as the mean of 50 numerical experiments on a linear limit state function  $g$ , where all (standard normal) variables  $u_i$  have equal importance:

$$g = \beta - \sum_{i=1}^n u_i \tag{12}$$

The number of necessary samples  $N$  increases with the number of variables  $n$  in the limit state function and with increasing  $\beta$ .

### 2.3 Comparison of the efficiency of the crude MC and directional sampling

Figure 2 shows the required number of samples for the level III standard reliability methods. The number of samples (under constraint of  $V(\beta) = 0.05$ ) is shown for MC and DS. The directional sampling procedures converges into an increase of samples linear to the number of variables. For  $\beta = 4$ , the required number of samples for directional sampling approximates  $N = 160n$ . For  $\beta = 4$  and 100 random variables Monte Carlo simulation requires  $10^5$  samples, where directional sampling requires  $1.6 \cdot 10^4$  samples. Bear in mind that Monte Carlo simulation uses one Limit State Function Evaluation (LSFE) per sample, where directional sampling uses approximately 4 LSFE per sample (for use of iteration). The difference is therefore approximately a factor 2 in the number of LSFE. The profit of directional sampling grows as less random variables are applied in the limit state function.

It is concluded that for problems with less than 100 random variables, directional sampling performs best. Monte Carlo simulation becomes appropriate only for high ( $n > 100$ ) dimensional problems.

## 3 IMPORTANCE SAMPLING

### 3.1 Monte Carlo importance sampling

The Monte Carlo procedures can be speeded up by means of importance sampling. A sampling density  $h(\underline{x})$  is used instead of the actual probability density function  $f(\underline{x})$ . For Monte Carlo importance sampling the probability of failure is calculated by:

$$P_f = \frac{\sum_i^N I(g(\underline{x})) \frac{f(\underline{x})}{h(\underline{x})}}{N} \quad (13)$$

In practice, importance sampling usually means that the sampling is concentrated in the area with a high likelihood of failure (see left part of Figure 3, where the dotted line equals the original distribution  $f(\underline{x})$  and the solid line the sample distribution  $h(\underline{x})$ ). The problem is that prior knowledge is needed of the failure area, which in most cases is not available. A reliable procedure, for most cases where no prior knowledge exist on the influence of variables on the limit state function, is to increase the variance of all variables to  $\sigma_h$  (see right part of Figure 3): Increased Variance sampling (IV).

The number of samples is calculated here, by means of numerical experiments on limit state function (12).

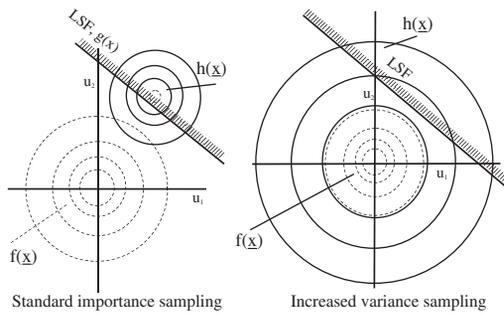


Figure 3. Importance sampling.

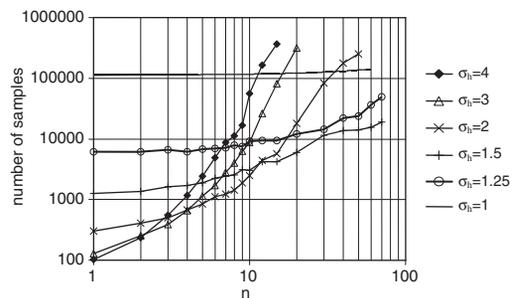


Figure 4. Required number of samples by Monte Carlo Increased Variance sampling (IV), all variables have equal importance to the limit state function (eq. (12),  $\beta = 4$ ).

A normal distribution with  $\sigma_h > 1$  is used in the importance sampling density  $h(\underline{x})$ . Figure 4 shows the required number of samples as a function of the number of variables  $n$  and the importance sampling standard deviation  $\sigma_h$ . The situation with  $\sigma = 1$  is equal to crude Monte Carlo sampling (without importance sampling). The required number of samples for this case is in line with equation (5). Figure 4 shows that a small increase of  $\sigma$  results in a considerable decrease of the required number of samples. It shows furthermore that the required number of samples increases with the number of variables.

The optimal importance sampling strategy ( $\sigma_h$ ) depends on the number of variables. On the basis of the simulation results, an empirical relation has been derived. The optimal  $\sigma_h$  is approximately equal to:

$$\sigma_h = \beta n^{-0.4} \quad (14)$$

Figure 4 shows that for this optimal  $\sigma_h$  in relation with the number of variables  $n$ , the number of samples equals approximately  $N = 300n$ . This means that the proposed Monte Carlo importance sampling,

requires more samples than crude directional sampling (Figure 2). Directional sampling uses approximately 4 LSFE per sample, where Monte Carlo simulation uses only one LSFE per sample. A disadvantage, however, is that an estimate of the reliability index  $\beta$  has to be known on forehand in order to choose an optimal  $\sigma_h$ . The amount of samples can be higher than without importance sampling when a non-optimal  $\sigma_h$  is chosen.

It can be observed from Figure 4 that a slight deviation in  $\sigma_h$  easily leads to a factor 2 increase of the required number of samples  $N$ . For example for DS,  $N_{LSFE} = 160 n * 4 = 640 n$  and for  $MC_{IV} = 300 n * 2 = 600 n$ .

It is therefore expected that Monte Carlo importance sampling and crude directional sampling are approximately equally efficient.

### 3.2 Directional importance sampling

For directional sampling, basically, sampling in  $u$ -space is replaced by sampling in a limited number of directions. Equation (8) is rewritten as:

$$P_f = \int P\{g(\lambda \underline{\kappa}) \leq 0\} \frac{f(\underline{\kappa})}{h(\underline{\kappa})} h(\underline{\kappa}) d\underline{\kappa} \quad (15)$$

$h(\underline{\kappa})$  is the importance sampling density of the vector  $\underline{\kappa}$ .

An estimate of the probability of failure is calculated from sample values:

$$P_i = P\{g(\lambda_i \underline{\kappa}_i) \leq 0\} \frac{f(\underline{\kappa}_i)}{h(\underline{\kappa}_i)} = (1 - \chi_n^2(\lambda_i^2)) \frac{f(\underline{\kappa}_i)}{h(\underline{\kappa}_i)}, \quad (16)$$

$$E(P_f) = \frac{1}{N} \sum_{i=1}^N P_i \quad (17)$$

The distribution  $f(\underline{\kappa})$  uniform density. The density of  $h(\underline{\kappa})$  can be computed numerically. The computation of  $f(\underline{\kappa})/h(\underline{\kappa})$  requires considerable computational effort. Performing this operation for high  $n$  is therefore discouraged.

Several authors have suggested methods for importance sampling in combination with directional sampling (Bjerager 1988, Ditlevsen 1988 and 1990, and Kijawatworawet 1992). All methods require prior knowledge on the influence of variables on the limit state function. In general, in structural reliability, there is little prior knowledge on the influence of variables on the limit state function. Even little knowledge may however speed up the computations considerably. In general there are five methods of importance sampling:

- Decrease variance of unimportant variables.
- Truncate distribution function of variables with known importance to the limit state function.

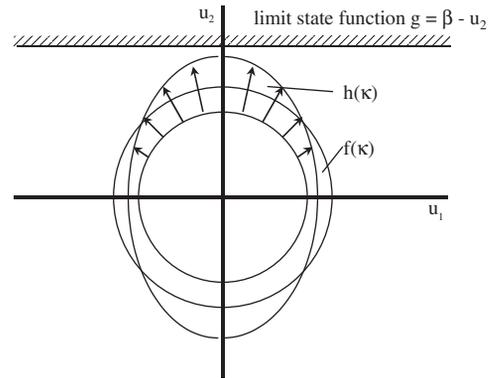


Figure 5. Decreasing the standard deviation of non-dominating variables.

- Apply weighting functions.
- Skip unimportant variables.
- Shift variables.

#### 3.2.1 Decrease the variance of unimportant variables

Decreasing the variance of non-dominating variables can be performed in combination with a shift of the mean value. This procedure should help to increase the number of samples to important directions. This requires that non-dominating variables are known on forehand, or are recognized by the procedure itself. Choosing a variable to be non-dominant where in fact it is dominant leads to an erroneous result. The procedure can therefore only be generally accurate when a possible incorrect choice of non-dominating variables is recognized and adjusted. Figure 5 shows an example with two standard normal variables. An importance sampling density  $h(\underline{\kappa})$  is used instead of the original sampling density  $f(\underline{\kappa})$ . The importance density is based on a reduced variance of variable  $u_1$ , which is totally unimportant to the limit state function.

Figure 6 shows the results (required number of samples) of an example with two standard normal variables  $u_1$  and  $u_2$ , using a limit state function  $g = 4 - u_1$ . Variable  $u_2$  is totally unimportant to the limit state function. Here, a required accuracy of  $V(\beta) = 0.005$  is used instead of  $V(\beta) = 0.05$ , because  $V(\beta) = 0.05$  would give a number of samples which is too low to show the influence of decreasing the variance.

### 3.3 Truncate the variable distribution

Truncating might be useful when it is known that only the positive side of the distribution is of importance to the limit state function. In most cases the important direction of only a part of the variables is known. It can

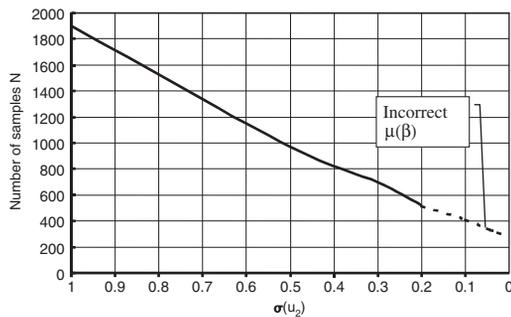


Figure 6. Number of samples needed for  $V(\beta) = 0.005$ , 2 variables,  $g = 4 - u_1$ .

be shown that the number of samples approximately reduces by a factor 2 for each truncated variable. Given 10 truncated variables, the reduction is maximum factor  $2^{10} = 1024$ . The correct result can even be found if an incorrect truncation is used. The condition is that some samples (approximately 10% of the total number of samples) are chosen in the truncated directions. Sampling is continued until  $V(\beta)$  is sufficiently low. The fact that only few samples are performed in the correct direction leads consequently to many required samples.

#### 4 RELIABILITY METHODS USING RESPONSE SURFACES

The previous chapter indicated that a fast reliability method can be searched in directional sampling or Monte Carlo importance sampling. Several authors (Faravelli 1989, Bucher 1988) claim that response surface techniques are the only possible way to compute the probability of failure when response is only available from experiments or complex computations (like structural FE computations). An analytical limit state function replaces the real response function. The main idea is that the response consisting of a complex function of input variables is approximated by a simple function of the input variables. In combination with Finite element analysis, the RSM technique is used by, for instance, Faravelli (1989) and Bucher (1988). The standard procedure is as follows:

1. Select the most important random variables on the basis of engineering judgment;
2. The value of each important random variable is varied individually and a real LSFE is performed (the other variables remain unchanged);
3. A response surface is constructed through the response data;
4. A reliability calculation is carried out using the response surface instead of the real response.

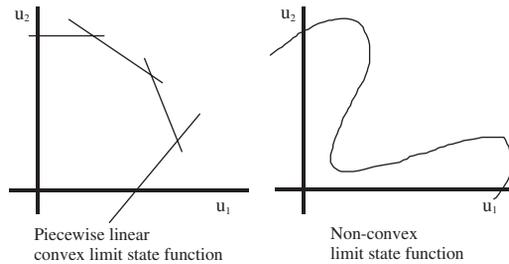
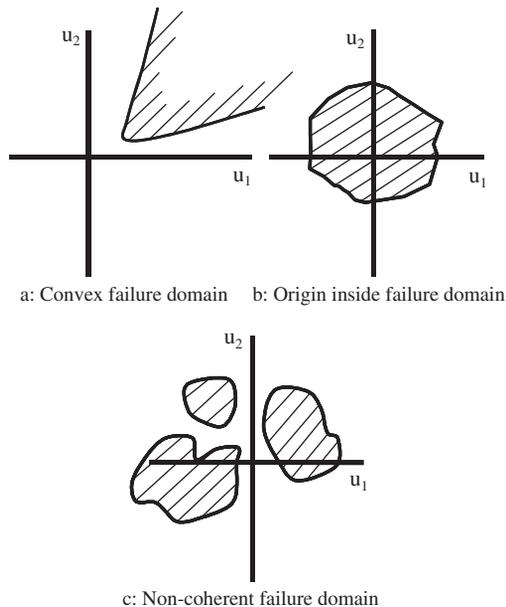


Figure 7. Non-linear limit state functions.

The type of reliability method used is of little importance since the time consuming LSFE are replaced by analytical expressions. Of main importance to the question whether every important random variable has been taken into consideration and whether the response function is accurate enough in the neighbourhood of the estimated design-points. In the simplest case, the value of each random variable is varied individually in positive and negative direction with a factor  $f\sigma$ . As a result, the sampling points are located at  $\mu_i + e_i \sigma_i$ , where  $\underline{e}$  is the vector  $(0, 0, 0, 0, \dots, \pm f, \dots, 0)$ . The factor  $f$  is advised to be equal for all variables (Box 1978). Bucher (1990) suggests fitting a quadratic function without cross terms to these sample points. This yields that the fitted response surface is sensitive to the choice of the coordinate axes. Several authors suggest therefore to include the cross terms. This way, the interaction between variables is taken care of. This so-called "Central Composite Design" requires  $2^n + 2n$  LSFE. For a high number of variables, this leads to an enormous increase of the required number of sample points and is therefore not advisable. Improving the first step with relevant samples near the limit state is probably a far better option. In fact, samples should be searched on the limit state surface and close to the origin in the  $u$ -space. This is equivalent to the finding of the parameter  $\lambda$  in the directional sampling procedure. Special care should be taken in case of non-convex limit state functions and limit state functions that have cross terms only. In these cases the response surface may not find all important regions (see Figure 7).

In this section a procedure is suggested and demonstrated, combining the advantages of directional sampling, response surface and importance sampling. In the previous section the following starting procedure was suggested for the response surface method:

1. Increase the value of each random variable individually until the limit state is reached;
2. Fit a quadratic response surface;
3. Perform the reliability analysis on the fitted response surface.



In short the total procedure is:

- 1 Perform Axis Directional Integration (ADI)
  - 2a Fit response surface on data  $(0, 0, \dots, f, \dots, 0)$ , using  $f = \pm 3$  and  $f = \pm \lambda$  (when available)
  - 2b Perform coarse directional sampling on the response surface
 

if $\lambda_{RS} < \lambda_{min} + \lambda_{add}$	- Calculate $P_i(FE) = \chi^2(\lambda_{i,FE}, n)$
	- Update the response surface with new (LSFE) data, using only the point on the limit state ( $g(\lambda, \theta) = 0$ ), when available
else	- Calculate $P_i(RS) = \chi^2(\lambda_{i,RS}, n)$ .

Figure 8. Failure domains that are not supported in the adaptive response surface sampling procedure.

Step 1 can be seen as a coarse directional integration procedure. Since the sampling is only performed in the coordinate axis directions in the  $u$ -space, it is called Axis Direction Integration (ADI). The ADI result already gives an estimate of the failure probability. A LSFE is performed in the origin of the  $u$ -space  $(0, 0, 0, \dots, 0)$  and the point  $(0, 0, f, 0, \dots, 0)$ . The factor  $f$  is set equal to the expected reliability index  $\beta^*$ . Mostly after approximately 4 iterations LSFE the root is found.

Consequently, a response surface can be fitted to the data points. It has been chosen to fit the response surface to the data in:

- origin  $(0, 0, \dots, 0)$
- the points  $(0, 0, \pm 3, \dots, 0)$
- the roots  $(0, 0, \pm \lambda, \dots, 0)$  (when available).

These data points are most times sufficient to fit a quadratic response surface to. Otherwise a linear surface has to be fit to the data.

The Directional Sampling (DS) procedure can now be performed on the response surface. Only in directions with, according to the response surface, a relatively high probability  $P_i$  an LSFE is used instead of the response surface to compute the distance  $\lambda$ . Consequently, the accuracy of the DS procedure is high in important regions and low in non-interesting regions. The question whether or not a failure probability is relatively high can be transformed into a measure  $\gamma$  on the minimum found distance  $\gamma_{min}$  (a direction is not important when  $\lambda_{RS} > \gamma \lambda_{min}$ ). Harbitz (1986) proposes in to skip a direction when  $\lambda > \lambda_{min} + \lambda_{add}$ , with  $\lambda_{add} = 3$ . Contrary to this proposal, the direction here is not skipped but the real  $\lambda_{LSFE}$  is replaced with  $\lambda_{RS}$ . The proposed directional sampling procedure can not be applied under the following circumstances:

- The failure domain is highly convex (see a);
- The origin in  $u$ -space is inside the failure domain (see b);
- The failure domain is non-coherent (see c).

A more general explanation of the method can be found in (Waarts 2000 and Waarts & Vrouwenvelder 2001).

## 5 COMPARISON OF THE RELIABILITY METHODS

### 5.1 Evaluation criteria

In the previous sections the following reliability methods were discussed:

- Crude Monte Carlo simulation (MC),
- Monte Carlo importance sampling (MCI)
- Crude Directional Sampling (DS),
- Directional Adaptive Response surface Sampling (DARS).

By way of evaluation, in this section, all methods are compared based on relatively simple artificial limit state functions, most of them found in literature. In order to judge the different reliability methods, the following criteria are used from (Engelund 1993) to select the artificial limit state functions:

1. Robustness against multiple critical points;
2. Robustness against noisy boundaries;
3. Capability to handle unions and intersections;
4. Efficiency and accuracy with respect to:
  - a) the number of variables (space dimension);
  - b) the probability level;
  - c) strong curvatures of the limit state function;

The reliability methods are compared on the basis of artificial limit state functions, summarised in Table 1, Figure 9 and Figure 10. The limit state functions are chosen in such a way that it is expected that the reliability methods may have difficulties. The efficiency is

Table 1. Artificial limit state functions (all variables are normally distributed).

Case	Random variables	ref
A LSF with 25 quadratic terms $g = R - \sum_{i=1}^{25} S_i^2/i$	$R \sim N(0.5, 0.1)$ $S_i \sim N(0.2, 0.1)$	
B Convex failure domain $g = 0.1*(u_1 - u_2)^2 - (u_1 + u_2)\sqrt{2} + 2.5$	$u_i \sim N(0,1)$	Borri et al. (1997)
C Oblate spheroid $g = R - \sum_{i=1}^{10} S_i^2/(1 + i/10)$	$R = 10$ $S_i \sim N(0,1)$	
D Saddle surface $g = 3 - u_1 u_2$	$u_i \sim N(0,1)$	
E Concave failure domain $g = -0.5(u_1 - u_2)^2 - (u_1 + u_2)/\sqrt{2}$	$u_i \sim N(0,1)$	Katsuki et al. (1994)

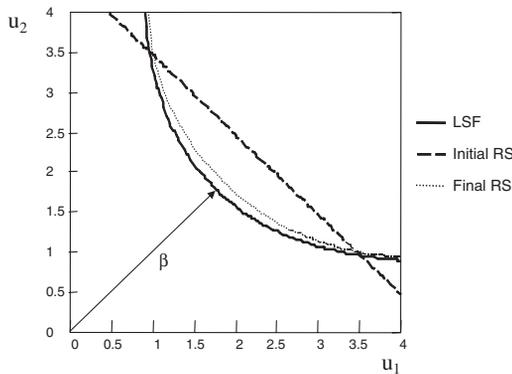


Figure 9. Convex failure domain (case B).

expressed as the number of limit state function evaluations (LSFE). The results are presented in Table 2.

5.2 Evaluation procedure and used reliability methods

The crude directional sampling (DS) result is considered to be the “exact” result when the theoretical reliability is not available. The crude Monte Carlo

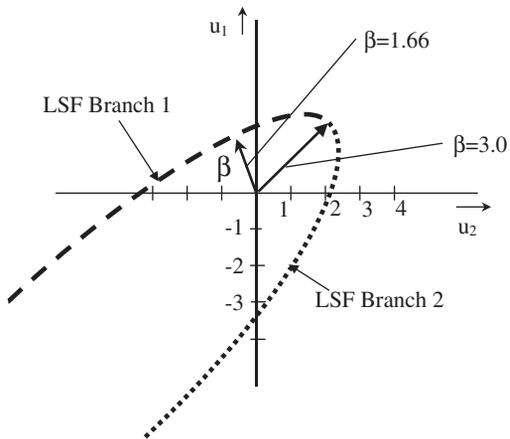


Figure 10. Concave failure domain (case E).

technique has been applied only in case the various methods give different results. The results of the crude directional sampling procedures are the mean of 5 arbitrary runs. The coefficient of variation of the probability of failure  $V(P_f)$  is chosen such that  $V(\beta) = 0.05$ . The efficiency of Monte Carlo importance sampling (MCI) depends on the number of variables and the

Table 2. Number of LSFE needed by the various reliability methods.

	MC	adsamp <sup>§</sup>	MCI	DS	DARS
25 quadratic terms	10 <sup>3</sup>	#	6501	2540	188
Convex failure domain	10 <sup>3</sup>	10 <sup>5</sup>	513	208	47
Oblate Spheroid	10 <sup>2</sup>	#	1682	170	160
Saddle surface	10 <sup>2</sup>	#	385	299	225
Concave failure domain	10 <sup>2</sup>	10 <sup>5</sup>	1172	260	240

# erroneous answer without error message ( $\Delta\beta > 0.08\beta$ );

§ adaptive sampling is performed with  $N = 10^5$

correctness of the estimate of  $\beta$ . Since  $\beta$  is not known beforehand, here the importance sampling is optimised for  $\beta = 4$ . As a result, for other outcomes of the reliability index  $\beta$ , the importance sampling will not be optimal. The COMREL code offers the opportunity for adaptive Monte Carlo sampling (adsamp). This is a kind of adaptive importance sampling. The mean value of the sampling density  $h(\underline{x})$  is chosen in the point that has the absolute minimum g-value. The number of samples has been set equal to  $10^5$  in all cases.

In the DARS procedure, the limit state function results are used when according to the response surface the vector length  $\lambda$  is less than the minimum value found so far plus 3 ( $\lambda_{\text{add}} = 3$ ) otherwise  $\lambda_{\text{RS}}$  is used.

The results (except importance sampling) are summarised in Table 2 as a reference. Detailed information on the limit state function and results is found in (Waarts 2000). Table 2 shows a wide range of required LSFE.

Level III methods can not give an error message. As a result, it is not sure whether DARS finds the correct answer. The results in Table 2 show however little reason for doubt. All level III procedures lead to the correct answer where DARS is the best in efficiency.

## 6 CONCLUSIONS

Summarising the previous sections the following number of Limit state function evaluations (LSFE) are needed in the methods:

- Crude Monte Carlo simulation: 3/Pf
- Monte Carlo importance sampling: 600 n
- Crude Directional sampling: 640 n
- DARS: 28 n

Directional sampling is often forgotten as option for Monte Carlo sampling. For a low number of variables ( $< 100$ ) it is much faster than standard Monte Carlo sampling. Importance Monte Carlo sampling should be dealt with carefully. Increased Variance sampling is a good and robust method. DARS is a good

option, certainly for cases where limit state evaluations per sample take much computational effort.

## REFERENCED LITERATURE

- Borri, A., Speranzini, E., Structural reliability analysis using a standard deterministic finite element code, *Structural safety*, Vol. 19, No. 4, 1997.
- Box, W.G., Hunter, J.S., *Statistics for experimenters, An introduction to design data analysis and model building*, John Wiley & Sons, 1978.
- Bucher, C.G., Adaptive sampling – an iterative fast Monte Carlo procedure, *Structural Safety*, Vol. 5, No. 2, 1988.
- Bucher, C.G., Bourgund, U., 1990, A fast and efficient Response Surface approach for structural reliability problems, *Struct. Saf.* Vol. 7, 1990.
- Deak, I., 1980, Three digit accurate multiple normal probabilities, *Num. Math.*, 35, 369–380.
- Ditlevsen, O., Melchers, R.E., Gluwer, H., 1990, General multi-dimensional probability integration by directional simulation, *Comp. & Struct.* Vol. 36, No. 2.
- Ditlevsen, O., Bjerager, P., Olesen, R., Hasofer, A.M., 1988, Directional simulation in Gaussian process, *Prob. Eng. Mech.*, Vol. 3, No. 4.
- Engelund, S., Rackwitz, R., A benchmark study on importance sampling techniques in structural reliability, *Structural Safety*, Vol. 12, 1993.
- ENV 1991-1: Eurocode 1: Basis of design and actions on structures –Part 1: Basis of design, CEN 1994.
- Faravelli, L., 1989, Response Surface Approach for Reliability analysis, *J. Eng. Mech. ASCE*, 1150(12), 1989.
- Harbitz, A., 1986, An efficient sampling method for probability of failure calculations, *Structural Safety*, Vol. 3,
- Johnson, N.L., Kotz, S., *Continuous multivariate distributions*, John Wiley & Sons, New York, 1972.
- Katsuki, S., Frangopol, D.M., 1997, Advanced hyperspace division method for structural reliability, *proceedings of ICOSAR '97, Structural safety and reliability*, Shiraisa, Shinozuka & Wen, Eds., november, Balkema, Rotterdam.
- Kijawatworawet, W., 1992, *An efficient adaptive importance directional sampling for nonlinear reliability problems*, Universität Innsbruck.
- Nataf, A., 1962, Détermination des distribution don't les marges sont données, *Comptes rendus de l'academie des sciences*, vol. 225, pp 42–43.
- STRUREL users manual, RCP, Munchen, 1997.
- Rosenblatt, M., *Remarks on a Multivariate Transformation*, The annals of Mathematical Statistics, Vol. 23, pp 470–472, 1952.
- Rubinstein, R.Y., 1981, *Simulation and the Monte Carlo method*, John Wiley and Sons, New York, 1981.
- Vrouwenvelder, A.C.W.M., Vrijling, J.K., 1994, Probabilistisch ontwerpen, Lecture notes b3, Delft University of Technology, The Netherlands.
- Waarts, P.H., 2000, *Structural reliability using Finite Element Analysis, – An appraisal of DARS: Directional Adaptive Response surface Sampling*, Thesis Delft University of Technology, Delft University Press.
- Waarts, P.H., Vrouwenvelder, A.C.W.M., 2001, Structural reliability using the finite element method, *Proceedings of ASRA*, Glasgow.

## Optimizing software system design with recovery blocks considering reliability estimation uncertainty

N. Wattanapongsakorn

*King Mongkut's University of Technology Thonburi, Bangkok, Thailand*

D.W. Coit

*Rutgers University, New Jersey, USA*

**ABSTRACT:** In this paper, we consider software system optimization design with Recovery Blocks considering uncertainty in component reliability estimate. The design objective is to maximize an estimate of system reliability and also minimize the variance of the reliability estimate. Recovery Block is one of the most common fault-tolerant system architectures, and it is applied for system redundancy, if needed, in this system optimization research effort. We present an optimization model where the system has a serial configuration, and each of the subsystems has choices of with or without RB/1/1 redundancy; a single software fault and a single hardware fault are tolerated. The model is designed under cost constraints. Our model can be easily applied for other types of fault-tolerant system architecture. This is the first time that a technique to optimize reliability of a system using multiple software versions with different reliabilities and correlated failures is proposed. We believe that our reliability optimization of redundant systems consists of realistic assumptions of failure correlation between/among software versions.

### 1 INTRODUCTION

In software system design, very often the information of available components, such as component reliability, is not known but can be approximated with a degree of uncertainty. This is the case, particularly when the system consists of new components with few failure data recorded. Therefore the system/component reliability is uncertain and can only be approximated. Mean and variance of the system/component reliability estimate are considered as reasonable parameters to represent the reliability estimate and its confidence interval (Coit & Jin 2001). Selecting components with high reliability uncertainty would result in a designed system with high reliability uncertainty. This is undesirable because system designers and users seek an optimal system design choice with high reliability estimate, while the reliability uncertainty is low.

This paper describes an optimization model for software system design with recovery blocks considering reliability estimation uncertainty. Recovery Block (RB) (Laprie et al. 1990) is one of the most common fault-tolerant software system architectures, where component redundancy is applied. This model is an extended

work from Wattanapongsakorn and Levitan (2001) where component reliability is exact and known.

We consider software systems that consist of both software and hardware components. Failures of software components/versions are the major causes of system failures. To provide fault-tolerance to a system, component redundancy is one of the most common approaches. Thus, multiple software versions and hardware components are considered in our optimization model.

Unlike most research papers, we provide a technique to optimize system reliability considering software versions with different reliabilities and correlated failures. For many experimental studies, multiple software versions, which are functionally equivalent, do have failure correlation even if they have been independently developed (Dugan 1994, Eckhardt et al. 1985 & Eckhardt et al. 1991). The failure correlation may come from faults in the software specification, faults from the voting algorithm, and or related faults from any two software versions. Our approach considers this correlation of failures in formulating our optimization model.

The systems that we model are series-parallel fault-tolerant systems. The redundancy allocation problem

for series-parallel systems is known to be difficult (NP-hard). Many researchers have proposed a variety of approaches to solve this problem using, for example, integer programming, branch-and-bound, dynamic programming, mixed integer and nonlinear programming. Recent optimization approaches are based on heuristics such as Genetic Algorithms (GA), and Tabu Search (TS). All of these approaches were developed for either optimizing reliability for software systems or hardware systems. In this paper, we consider systems consisting of both software and hardware components. The software failure behavior, which is different from the hardware failure behavior, is considered.

GA is used as the optimization approach. The term "genetic" derives from the roughly analogous natural re-producing new-born population by crossover and mutation. There are competitions among the population; the stronger ones will survive to the next generation and the weak ones will soon die out. GA is a heuristic optimization model that has been applied effectively to solve many difficult problems in different fields such as scheduling, facility layout, and graph coloring/graph partitioning problems. It is a stochastic algorithm with performance depending on the solution encoding, crossover breeding operator, elitist selection and mutation operator.

Our optimization model is developed to select both software and hardware components and the degree of redundancy to optimize the overall system reliability, with a total cost constraint. In the system, there are a specified number of subsystems in series. For each subsystem, there are several hardware and software choices to be made. The system is designed using components, each with estimated reliability, but with known cost.

This paper is organized as follows. The assumption and notation used in this paper are listed next. In section 2, the software system design with recovery block architecture is discussed. Section 3 provides the concept of reliability estimation uncertainty. Section 4 presents our optimization model to maximize reliability considering uncertainty. Section 5 discusses the GA as our optimization approach. In section 6, we demonstrate our model with an example system, where reasonable and interesting results are obtained and discussed.

### 1.1 Assumptions

- 1) Each software component, hardware component or the system has two states: functional or failed
- 2) Reliability of each software or hardware component is unknown, but estimable
- 3) There is no failure repair for each component or system
- 4) Hardware redundancy is in active mode (i.e. hot spares)
- 5) Failure of individual hardware components are statistically independent

### 1.2 Notation

RB/ $i/j$	system architecture RB with $i$ hardware faults tolerated and $j$ software faults tolerated
$n$	Number of subsystems in the series system
$m_i$	Number of hardware component types available for subsystem $I$
$p_i$	Number of software versions available for subsystem $I$
$R$	Estimated reliability of the distributed system
$R_i$	Estimated reliability of the subsystem $I$
$R_{hw_{ij}}$	Reliability of hardware component $j$ at subsystem $i$
$R_{sw_{ik}}$	Reliability of software component $k$ at subsystem $i$
$Chw_{ij}$	Cost of using hardware component $j$ at subsystem $i$
$Csw_{ik}$	Cost of developing software version $k$ at subsystem $i$
Cost	Maximum allowable cost (constraint)
$P_x$	Probability that event $X$ occurs
$Q_x$	Probability that event $X$ does not occur; $Q_x = 1 - P_x$
$Pv_i$	Probability of failure of software version $I$
$Prv_{ij}$	Probability of failure from related fault between two software versions, $i$ and $j$
$P_{all}$	Probability of failure from related fault among all software versions, due to faults in specification
$Pd$	Probability of failure of decider or voter
$Ph_i$	Probability of failure of hardware component $i$ . If only one hardware is applied, $Ph_i = Ph$ for all $i$

## 2 SOFTWARE SYSTEM DESIGN WITH RECOVERY BLOCKS

### 2.1 Recovery Block (RB): RB/1/1 architecture

The RB model consists of an adjudication module called an *acceptance test*, and at least two software components, called alternates (Laprie et al. 1990, Lyu 1996), as indicated in Figure 1. At the beginning, the output of the first or primary alternate is tested for acceptance. If it fails, the process will *roll back* to the beginning of the process, and then let the second alternate execute and test its output for acceptance again. This process continues until the output from an alternate is accepted or all outputs of the alternates have been tested and fail.

RB/1/1 has a single hardware fault tolerated and a single software fault tolerated. The system consists of two hardware components, each running two independent software versions; primary and secondary. The primary version is active until it fails, and the secondary version is the backup spare. System failures occur when both versions fail, or both hardware components fail.

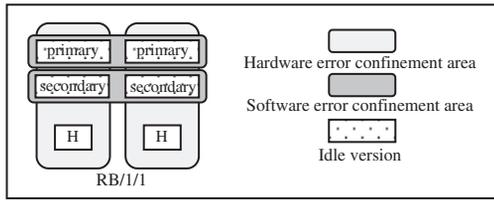


Figure 1. RB/1/1 fault-tolerant architecture.

Table 1.  $a_i, k_{ij}$  and  $h_{ij}$  expressed in a matrix form for RB/1/1 architecture.

$k_{ij}$						$h_{ij}$								
i	j=1	2	3	4	5	6	i	j=1	2	3	4	5	6	$a_i$
1	1	0	0	0	0	0	1	0	0	0	0	0	0	1
2	0	1	0	0	0	0	2	1	0	0	0	0	0	1
3	0	0	1	0	0	0	3	1	1	0	0	0	0	1
4	0	0	0	0	0	2	4	1	1	1	0	0	0	1
5	0	0	0	1	1	0	5	1	1	1	0	0	0	1
6	0	0	0	1	1	2	6	1	1	1	0	0	0	1

The probability that an unacceptable result occurs during a single task iteration, P is presented by Equation 1 where  $a_i, k_{ij}$  and  $h_{ij}$  values for RB/1/1 architecture are listed in Table 1.

$$P = \sum_{i=1}^s \left( a_i \prod_{j \in C_i} p_j^{k_{ij}} q_j^{h_{ij}} \right) \tag{1}$$

where,  
 $s$  = number of additive terms when all failure probabilities have been enumerated;  $s = 6$  for this RB1/1 architecture  
 $a_i$  = integer coefficient  
 $C_i$  = component type set for  $i$ th additive term  
 $k_{ij}$  = power coefficient for  $j$ th component reliability in set  $C_i$   
 $h_{ij}$  = power coefficient for  $j$ th component unreliability in set  $C_i$   
 $p_j$  = unreliability of  $j$ th type of component  
 $q_j$  = reliability of  $j$ th type of component,  $p_j + q_j = 1$  for all  $j$   
 $p_j$  and  $q_j$  definitions and comparisons with notation from Wattanapongsakorn and Levitan (2001) are as follows,

- $p_1 = Prv$        $q_1 = Qrv$
- $p_2 = Pd$        $q_2 = Qd$
- $p_3 = P_{all}$      $q_3 = Q_{all}$
- $p_4 = Pv_1$      $q_4 = Qv_1$
- $p_5 = Pv_2$      $q_5 = Qv_2$
- $p_6 = Ph$        $q_6 = Qh$

With RB/1/1 architecture, we develop an optimization model for a fault-tolerant embedded system considering reliability estimates with uncertainty. The components, which are available for the system design, each has reliability estimation uncertainty measured by the variance of the reliability estimate.

In the next section, we formulate equations for system reliability estimate and variance for the reliability estimate for the RB/1/1 fault-tolerant architecture. These equations will be used in our optimization model, discussed later in section 4.

### 3 RELIABILITY ESTIMATION UNCERTAINTY

Usually the exact component unreliability,  $p_j$ , or reliability,  $q_j$ , is not known. They are estimated from life test data or field failure records. The estimated  $\hat{p}_j$  or  $\hat{q}_j$  are used to replace the true but unknown in Equation 1.

$$\hat{P} = \sum_{i=1}^s \left( a_i \prod_{j \in C_i} \hat{p}_j^{k_{ij}} \hat{q}_j^{h_{ij}} \right) \tag{2}$$

Direct calculation of  $E[\hat{P}]$  and  $Var(\hat{P})$  are difficult due to the coupling of  $\hat{p}_j$  and  $\hat{q}_j$ . Therefore, Equation 2 has been rearranged, as follows.

$$\hat{P} = \sum_{i=1}^s \left( a_i \prod_{j \in C_i} (1 - \hat{q}_j)^{k_{ij}} \hat{q}_j^{h_{ij}} \right) \tag{3}$$

Equation 3 can be rearranged by expanding  $(1 - \hat{q}_j)^{k_{ij}}$  terms, resulting in Equation 4.

$$\hat{P} = \sum_{i=1}^s \left( b_i \prod_{j \in C_i} \hat{q}_j^{n_{ij}} \right) \tag{4}$$

where  
 $t$  = number of additive terms after expansion,  $t > s$   
 $b_i$  = integer coefficient  
 $t$  is the number of terms after the expansion.  $b_i$  and  $n_{ij}$  are determined by grouping similar terms. This expansion procedure is conducted automatically using Matlab code based on the parameters in Table 1. Due to the length of the expansion, detailed computational procedure is omitted. Table 2 lists all the expansion results.

From the table,  $t = 25$ . Based on the coefficients  $n_{ij}$ ,  $b_i$  and component reliability information, Equation 4 can be used to obtain the mean and the variance of unreliability  $\hat{P}$ . Together with the higher-order moment information of component reliability estimates, the mean and the variance of unreliability  $\hat{P}$ , can be obtained as follows (Jin & Coit 2001).

$$E[\hat{P}] = \sum_{i=1}^I \left( b_i \prod_{j \in C_i} E[\hat{q}_j^{n_{ij}}] \right)$$

$$\begin{aligned} \text{Var}(\hat{P}) = & \left( \sum_{i=1}^I \left\{ b_i^2 \left( \prod_{j \in C_i} E[\hat{q}_j^{2n_{ij}}] - \prod_{j \in C_i} (E[\hat{q}_j^{n_{ij}}])^2 \right) \right\} \right) + \\ & 2 \sum_{i < m}^I \left\{ b_i b_m \left( \prod_{j \in C_{im}} E[\hat{q}_j^{n_{ij} + n_{mj}}] - \prod_{j \in C_{im}} E[\hat{q}_j^{n_{ij}}] E[\hat{q}_j^{n_{mj}}] \right) \right\} \end{aligned} \tag{6}$$

Table 2.  $n_{ij}$  and  $b_i$  Expressed in a matrix form for RB/1/1 architecture.

$n_{ij}$							$b_i$
i	j = 1	2	3	4	5	6	
1	0	0	0	0	0	0	1
2	1	0	0	0	0	0	1
3	1	1	0	0	0	0	1
4	1	1	1	0	0	0	1
5	1	1	1	0	0	0	1
6	1	1	1	0	0	0	-1
7	1	0	0	0	0	0	-1
8	1	1	0	0	0	0	-1
9	1	1	1	0	0	0	-1
10	1	1	1	0	0	1	-2
11	1	1	1	0	0	2	1
12	1	1	1	1	0	0	-1
13	1	1	1	0	1	0	-1
14	1	1	1	1	0	0	1
15	1	1	1	0	1	0	1
16	1	1	1	0	0	1	2
17	1	1	1	0	0	2	-1
18	1	1	1	1	1	0	1
19	1	1	1	1	1	0	-1
20	1	1	1	1	0	1	-2
21	1	1	1	1	0	2	1
22	1	1	1	0	1	1	-2
23	1	1	1	0	1	2	1
24	1	1	1	1	1	1	2
25	1	1	1	1	1	2	-1

where  $C_{im} = C_i \cup C_j$

To show the relationship of reliability estimate and variance of reliability estimate for each component, we provide a few numerical examples. Table 3 lists component reliability estimates or unreliability estimate values. These data are selected directly from Wattanapongsakorn and Levitan (2001). Equations. 5 & 6 are also valid, as long as high moments of component reliability estimates are known. Without loss of generality, it is assumed Bernoulli test and applied binomial distribution theory was used to estimate high moments (Jin & Coit 2001).  $\eta = [\eta_1, \eta_2, \eta_3, \eta_4, \eta_5, \eta_6, \eta_7]$  is a variance-factor vector, and  $\eta_i = \text{integer}$ . For example, when  $\eta = [6, 4, 2, 2, 4, 3, 6]$ , the corresponding component variances are given in Table 3.

Table 4 lists four results with respect to different component variance. It is shown that system unreliability is unchanged even if component variances vary as  $\eta$  changes. It can be observed that as component variances become small, the overall variance of the system unreliability estimate  $\hat{P}$  also decreases.

#### 4 OPTIMIZATION MODEL

In this section, we present our optimization model for reliability of software systems. The objective is to find the optimal set of software and hardware allocations

Table 3. Parameters and definition of component's variance of reliability estimate.

Unreliability estimate	Reliability estimate	Variance of reliability estimate
Prv = 0.004	Qrv = 0.996	Var(Prv) = (Prv × Qrv)/ $\eta_1$ = 0.000664
Pd = 0.02	Qd = 0.98	Var(Pd) = (Pd × Qd)/ $\eta_2$ = 0.0049
P <sub>all</sub> = 0.005	Q <sub>all</sub> = 0.995	Var(P <sub>all</sub> ) = 0.0024875
Pv <sub>1</sub> = 0.035	Qv <sub>1</sub> = 0.965	Var(Pv <sub>1</sub> ) = (Pv <sub>1</sub> × Qv <sub>1</sub> )/ $\eta_4$ = 0.016
Pv <sub>2</sub> = 0.046	Qv <sub>2</sub> = 0.954	Var(Pv <sub>2</sub> ) = (Pv <sub>2</sub> × Qv <sub>2</sub> )/ $\eta_5$ = 0.012
Pv <sub>3</sub> = 0.09	Qv <sub>3</sub> = 0.910	Var(Pv <sub>3</sub> ) = (Pv <sub>3</sub> × Qv <sub>3</sub> )/ $\eta_6$ = 0.03
Ph = 0.03	Qh = 0.970	Var(Ph) = (Ph × Qh)/ $\eta_7$ = 0.004

Table 4. Parameters of components and system unreliability  $P$ , system unreliability estimate  $E[\hat{P}]$ , and system variance of unreliability estimate  $\text{Var}(\hat{P})$ .

$\eta$	$P$	$E[\hat{P}]$	$\text{Var}(\hat{P})$
[1, 1, 1, 1, 1, 1, 1]	0.05571	0.03716	0.03578
[2, 2, 2, 2, 2, 2, 2]	0.05571	0.06317	0.02801
[8, 8, 8, 8, 8, 8, 8]	0.05571	0.06068	0.00777
[12, 12, 12, 12, 12, 12, 12]	0.05571	0.05925	0.00521

for all subsystems (with or without RB/1/1 redundancy). The problem formulation is to maximize the system reliability estimate, subjected to a specified cost constraint, *Cost*. The system has all subsystems connected in series. This model is suited for systems that handle relatively critical tasks. The problem formulation for this model allow each subsystem to have RB/1/1 redundancy allocation as its reliability estimate and variance of the reliability estimate, calculated according to the RB/1/1 redundancy configuration. The parameters considered for the reliability of the RB/1/1 architecture are available as component reliability estimate and variance of reliability estimate. Each allocated software version is allowed to have a different reliability estimated value, unlike several proposed models where all of the software versions have the same reliability value (Lyu 1996).

The problem formulation is to maximize system reliability estimate with its variance of reliability estimate by choosing the optimal set of hardware and software components for each subsystem by:

$$\begin{aligned} & \text{Max}\{\hat{R}(x) - \text{penalty}(\text{Var}(\hat{R}(x)))\} \\ \text{Subject to } & \left( \sum_{j=1}^m X_{jy} = 1 \text{ and } \sum_{k=1}^n Y_{ik} = 1 \right) \text{ or } \left( \sum_{j=1}^m X_{jy} = 2 \text{ and } \sum_{k=1}^n Y_{ik} = 2 \right) \\ & \sum_{j=1}^m X_{jy} C_{jy} + \sum_{k=1}^n Y_{ik} C_{ik} \leq \text{Cost} \\ & X_{jy} = 0,1,2 \quad Y_{ik} = 0,1 \quad i=1,2,\dots,n \quad j=1,2,\dots,m \quad k=1,2,\dots,n \end{aligned}$$

where

$$\begin{aligned} \hat{R}(x) &= \prod_{i=1}^n (\hat{R}_i(x)) \\ \text{Var}(\hat{R}(x)) &= \text{Eq. (8)} \\ \left. \begin{aligned} \hat{R}_i(x) &= \sum_{j=1}^m \sum_{k=1}^n X_{jy} Y_{ik} \hat{R} h w_{jy} \hat{R} s w_{ik} \\ \text{Var}(\hat{R}_i(x)) &= \text{Eq. (9)} \end{aligned} \right\} \text{ if } \sum_{j=1}^m X_{jy} = 1, \quad \sum_{k=1}^n Y_{ik} = 1 \\ \left. \begin{aligned} \hat{R}_i(x) &= 1 - \text{Eq. (5)} \\ \text{Var}(\hat{R}_i(x)) &= \text{Eq. (6)} \end{aligned} \right\} \text{ if } 2 \sum_{j=1}^m X_{jy} = 2 \quad \sum_{k=1}^n Y_{ik} = 2 \end{aligned}$$

The design objective is to identify solutions with very high reliability, but also with a low variance of the reliability estimate. If the decision maker is risk-neutral, then the design objective is to maximize the reliability estimate. If the person is risk-averse, where the worst case with high variance of the reliability estimate is unacceptable (i.e., highly critical & life-dependent systems), then minimizing the variance is also an important design objective. One approach is to consider the problem as a multi-criteria optimization: to maximize the system reliability estimate and at the same time minimize the variance. This approach was proposed by Coit and Jin (2001). Another approach, which is our approach, is to penalize the estimation uncertainty by penalizing the system reliability estimate with its estimation variance. The “penalty” is a tunable parameter

based on a system designer’s tolerance for risk, i.e. actual reliability deviation from the estimate. By penalizing the variance, the final solution represents a compromise between high reliability and low variance.

## 5 GENETIC ALGORITHM OPTIMIZATION APPROACH

GA requires that the system design (phenotype) be encoded as a solution vector (genotype). Then, genetic operators (crossover, mutation) are applied over successive generations until the GA converges to a solution or a pre-determined maximum number of generations is reached.

### 5.1 Encoding

For an embedded (hardware and software) system with *n* subsystems connected in series, the string encoding can be represented as:

$$H1 S1 | H2 S2 | H3 S3 | \dots | Hn Sn$$

where *Hi*, with  $0 \leq i \leq n$  is the selected hardware component for subsystem *i*, and *Si* is the selected software component/version for the specified subsystem.

### 5.2 Initial population

We set the initial population by randomly generating a set of chromosomes consisting of genes, and calculate their fitness value according to the fitness function.

### 5.3 Selection

The chromosomes or population are sorted by their fitness values. The top 85% of the population with high fitness values are selected for the crossover process.

### 5.4 Crossover

We randomly select two systems or chromosomes from the current population for crossover, to produce two new chromosomes. Also we randomly select a subsystem for crossover. The positions P1 and P2 are labeled with bold font for crossover.

Example: 1 2 | 1 3 | 1 1 | 3 4  
 1 1 | 2 3 | 3 5 | 4 4  
 Random subsystem = 3, P1 = 1, P2 = 2  
 Results: 1 2 | 1 3 | **3 5** | 3 4  
 1 1 | 2 3 | **1 1** | 2 4

We select the highest 15% of the population with the maximum fitness values from the current population generation and combine with the best 85% from the crossover to be the next population generation.

### 5.5 Mutation

The current population generation is initially sorted by fitness values. Then, each chromosome in the generation, except the best 5%, is mutated with a mutation rate which is usually less than 10%. The chromosomes resulted from mutation are combined and considered as the chromosomes in the current population generation.

### 5.6 Penalty function

A dynamic penalty function is an effective approach to deal with problems with cost constraint (Coit et al. 1996). It is applied to the selected chromosomes that violate the constraint (i.e. infeasible solution). For example, if the system cost is not greater than the "Cost" constraint, no cost penalty is applied, else the cost penalty would be applied to the objective function. Doing this, the selected infeasible solution search space is explored and considered as local or temporary solutions which may lead in finding feasible global solutions.

## 6 AN EXAMPLE SYSTEM: DESIGN AND SIMULATION RESULT

We select the problem originally solved in Watanapongsakorn and Levitan (2001) to provide an

example problem considering the reliability estimate and variance of reliability estimate as multiple objectives. This example reliability optimization problem is a series system with six subsystems, having  $n = 6$ ,  $m_i = 3$ , and  $p_i = 4$ . As an extension of the previous work, the known component reliabilities used in the previous paper are now considered as reliability estimates with an associated variance. The component costs are unchanged and considered in this optimization problem. Table 5 shows the reliability estimate and its variance as well as cost of all the available components.

We apply this input data to our optimization model with various system design cost constraints at 180, 320, 460 and also with unlimited cost constraint. The penalty value (variance penalty), which is the weight of the variance of reliability estimate is set arbitrarily to 0.01, 0.1, 1, 2, 3, 4, 5, 10 and 100 for various system design cost constraint i.e. 180, 320, 460 and unlimited. Other design conditions are Prv = 0.004, Pall = 0.005 and Pd = 0.002, with the corresponding variance-factors ( $\eta$ ) each is equal to 20. We apply a genetic algorithm as our optimization approach. The simulation results, each is based on 10 runs, are presented in Tables 6–11.

From the GA results presented in Table 6 at various system cost constraints, we can see that with no cost constraint, each model can offer the highest system

Table 5. Available components and their reliability estimates, variances, and costs.

Inputs							
(i, j)	HW Cost <sub>ij</sub>	HW $\hat{R}_{ij}$	HW Variance-factor $\eta_{ik}$	(i, k)	SW Cost <sub>ik</sub>	SW $\hat{R}_{ik}$	SW Variance-factor $\eta_{ik}$
11	30.0	0.995	4	11	30.0	0.950	3
12	10.0	0.980	5	12	10.0	0.908	2
13	10.0	0.980	4	13	20.0	0.908	4
				14	30.0	0.950	2
21	30.0	0.995	2	21	30.0	0.965	1
22	20.0	0.995	3	22	20.0	0.908	3
23	10.0	0.970	1	23	10.0	0.887	3
				24	20.0	0.908	2
31	20.0	0.994	4	31	20.0	0.978	4
32	30.0	0.995	1	32	30.0	0.954	1
33	100.0	0.992	2	33	20.0	0.860	2
				34	30.0	0.954	3
41	30.0	0.990	2	41	20.0	0.950	1
42	10.0	0.980	4	42	10.0	0.908	2
43	10.0	0.985	1	43	20.0	0.910	3
				44	20.0	0.950	7
51	30.0	0.995	3	51	30.0	0.905	2
52	20.0	0.980	10	52	20.0	0.967	8
53	30.0	0.995	1	53	10.0	0.967	1
				54	30.0	0.905	5
61	30.0	0.998	3	61	10.0	0.908	1
62	20.0	0.995	4	62	30.0	0.968	2
63	20.0	0.994	2	63	20.0	0.968	3
				64	20.0	0.955	2

reliability estimate and the lowest variance of the reliability estimate compared to all the solutions with low or high cost constraints. With a very tight cost constraint, where cost = 180, the best possible obtained solutions are not as good as when the cost constraint is relaxed to 320 or 460. With a more relaxed cost constraint, better solutions can be obtained. The selected component allocations for the corresponding cost constraints are depicted in Table 7. Better solution means

Table 6. Optimization results from GA with variance penalty = 1.0.

Estimate	Cost = 180	Cost = 320	Cost = 460	Cost = Unlimited
$E[\hat{R}(x)]$	0.632460	0.862231	0.909249	0.914257
$Var(\hat{R}(x))$	0.090987	0.019648	0.006210	0.005914

the solution with higher reliability estimate and lower variance of the reliability estimate.

From Table 7, at cost 180, no component redundancy can be obtained, indicated by a software version and a hardware component selected for each subsystem. At higher cost constraints, the results show replicated software and hardware components allocated, for examples, at subsystems 1, 2, 4, and 5.

The GA optimization results with arbitrary values of variance penalty at system cost constraints equal to 180, 320, 460 and unlimited are depicted in Tables 8, 9, 10, and 11, respectively. From the results, at a certain cost constraint, the GA seeks for solutions with less variance of the reliability estimate when the variance penalty is set higher. However, these solutions also have lower reliability estimate as well. In other words, system design choice with high reliability estimate also has high variance. The design choice with high reliability estimate can be obtained when the uncertainty or

Table 7. Component allocations for the results shown in Table 6.

Cost	Subsystem 1 i = 1		Subsystem 2 i = 2		Subsystem 3 i = 3		Subsystem 4 i = 4		Subsystem 5 i = 5		Subsystem 6 i = 6	
	HW j =	SW k =										
180	2	2	3	3	1	1	2	4	2	3	2	3
320	2	2,3	2	2,3	1	1	2	2,4	2	2,3	2	3
460	2	1,4	2	1,3	1	1,4	2	1,4	2	2,3	2	3,4
unlimited	1	1,4	2	1,2	1	1,4	2	1,4	1	2,3	2	2,3

Table 8. Optimization results from GA with various variance penalties at cost = 180.

Variance penalty	$E[\hat{R}(x)]$	$Var(\hat{R}(x))$
0.01–0.1	0.635687	0.090987
1–3	0.632460	0.085178
4	0.632460	0.085178
5	0.632460	0.085178
10	0.632460	0.085178
100	0.604499	0.083446

Table 10. Optimization results from GA with various variance penalties at cost = 460.

Variance penalty	$E[\hat{R}(x)]$	$Var(\hat{R}(x))$
0.01–0.1	0.909249	0.006210
1–3	0.909249	0.006210
4	0.908004	0.005898
5	0.908004	0.005898
10	0.908004	0.005898
100	0.906183	0.005796

Table 9. Optimization results from GA with various variance penalties at cost = 320.

Variance penalty	$E[\hat{R}(x)]$	$Var(\hat{R}(x))$
0.01	0.862231	0.019648
0.1	0.862231	0.019648
1–3	0.862231	0.019648
4	0.862231	0.019648
5	0.847706	0.015310
10	0.847706	0.015310
100	0.847706	0.015310

Table 11. Optimization results from GA with various variance penalties at cost = unlimited.

Variance penalty	$E[\hat{R}(x)]$	$Var(\hat{R}(x))$
0.01	0.914486	0.006675
0.1	0.914257	0.005914
1–3	0.914257	0.005914
4	0.914257	0.005914
5	0.914257	0.005914
10	0.913637	0.005779
100	0.909938	0.005572

variance of the reliability estimate is affordable i.e. when the variance penalty is not significant.

## 7 CONCLUSION

This paper analyses and identifies system design choices when component reliability information is available in the forms of reliability estimate and variance of the reliability estimate. The system design objectives are to maximize the system reliability estimate, and at the same time, minimize its variance. These multiple objectives are in contrast with one another. When one objective is more importance than another one, a certain design choice is suggested. Therefore the system design decision depends on the degree of importance of the objective function.

## REFERENCES

- Coit D.W. & Jin T. 2001. Multi-Criteria Optimization: Maximization of a System Reliability Estimate and Minimization of the Estimate Variance, *Proceedings of the European Safety & Reliability International Conference (ESREL)*, Turin, Italy.
- Coit D.W., Smith A. & Tate D. 1996. Adaptive Penalty Methods for Genetic Optimization of Constrained Combinatorial Problems, *INFORMS Journal on Computing*, Vol. 8, NO. 2, pp. 173–182.
- Dugan J.B. 1994. Experimental Analysis of Models for Correlation in Multiversion Software, *Proceedings of the International Symposium on Software Reliability Engineering*, Los Alamitos, CA, pp. 36–44.
- Eckhardt D.E., Caglayan A.K., Knight J.C., Lee L.D., McAllister D.F., Vouk M.A. & Kelly, J.P. 1991. An Experimental Evaluation of Software Redundancy as a Strategy for Improving Reliability, *IEEE Transactions on Software Engineering*, Vol. 17, NO. 7, pp. 692–702.
- Eckhardt D.E. & Lee L.D. 1985. A Theoretical Basis for the Analysis of Multiversion software Subject to Coincident Errors, *IEEE Transactions on Software Engineering*, Vol. 11, pp. 1511–1517.
- Jin T. & Coit D.W. 2001. Variance of System Reliability Estimates with Arbitrarily Repeated Components, *IEEE Trans on Reliability*, Vol. 50, NO. 4, pp. 409–413.
- Laprie J. C., Arlat J., Beounes C. & Kanoun K., July 1990. Definition and Analysis of Hardware- and Software-Fault-Tolerant Architectures, *IEEE Computer*, pp. 39–51.
- Lyu M.R. (Editor in Chief) 1996. *Handbook of Software Reliability Engineering*, IEEE Computer Society Press, McGraw-Hill.
- Rubinstein R., Levitin G., Lisnianski A. & Ben-Haim H. 1997. Redundancy Optimization of Static Series-Parallel Reliability Models Under Uncertainty, *IEEE Transactions on Reliability*, Vol. 46, NO. 4, pp. 503–511.
- Wattanapongsakorn N. & Levitan S.P. 2001. Reliability Optimization Models for Fault-Tolerant Distributed Systems, *Proceedings of Annual Reliability & Maintainability Symposium*, pp. 193–199.

## The fireworks disaster in Enschede: overview, reconstruction, safety and pyrotechnics

J.Weerheijm, R.M.M. van Wees & L.H.J. Absil  
*TNO-PML, Rijswijk, The Netherlands*

P.C.A.M. de Bruyn & J.W. Karelse  
*NFI, Rijswijk, The Netherlands*

**ABSTRACT:** Saturday afternoon May 13, 2000 a major fireworks incident occurred at the company S.E. Fireworks in the city of Enschede, the Netherlands. Twenty-two people were killed and more than seven hundred were injured. Within a radius of hundreds of meters houses were destroyed by the blast and debris generated by the explosions and burnt because of the scattered fireworks.

The possible causes, safety regulations and safety control were investigated. By order of the Public Prosecutor, the Netherlands Forensic Science Institute (NFI) and TNO Prins Maurits Laboratory (TNO-PML) performed the forensic and technical investigations into the reconstruction and the cause of this disaster.

Within an hour the incident developed from a moderate fire and some initiated fireworks in one of the buildings into a series of three explosions of increasing violence. Many people witnessed the accident (at distance) and numerous video recordings from different angles were made. After the disaster an extensive investigation was started. The observed explosion effects, the inventory of the damage in the area and all the forensic evidence were analysed. They form the basis for the reconstruction of the disaster. Scenarios for possible causes of each of the events were developed and analysed. In addition, the most probable chain of events and the lessons to be learned concerning the (bulk) storage of pyrotechnics in general and fireworks specifically were dealt with.

### 1 INTRODUCTION

Saturday afternoon May 13, 2000 a major fireworks accident occurred at the company S.E. Fireworks in the city of Enschede, the Netherlands. Within an hour the incident escalated from a moderate fire and some initiated fireworks in one of the buildings into a series of three explosions of increasing violence. The first was a relatively small explosion in a container. Within a minute seven garage boxes (prefab concrete storage facilities) exploded. This was followed 66 seconds later by a further explosion of storage cells in the central storage building, whereby the most violent explosion occurred in storage cell C11. The resulting blast wave was comparable to an explosion with a mass between 4000 and 5000 kg TNT. The possible causes, safety regulations and safety control were investigated.

The observed explosion effects, the inventory of the damage in the area and all the forensic evidence were analysed by NFI and TNO. They form the basis for the reconstruction of the disaster. In this paper the observed facts and identification of the main, crucial elements in

the chain of disastrous events will be described. For the major events, the possible initiation mechanisms and possible consequences will be discussed. Lessons and general conclusions are drawn from these analyses. The paper only gives a summary of the research and highlights the main research steps. The research is reported in Bruyn & Karelse (2000) and Weerheijm et al. (2000). It should be noted that there is no complete certainty about the stored quantities and type of fireworks. The licensed quantities are given in the paper.

### 2 SITUATION MAY 13, 2000

May 13, 2000 was a warm sunny day. Many people were outside enjoying the weather and attracted to the S.E. Fireworks (SEF) area due to the increasing firework effects. The SEF firework depots were situated in a residential area of the city of Enschede. The location and the layout of the SEF-depot is given in Figure 1. Figure 2 gives the identification numbers of all storage cells. The company S.E. Fireworks performed firework

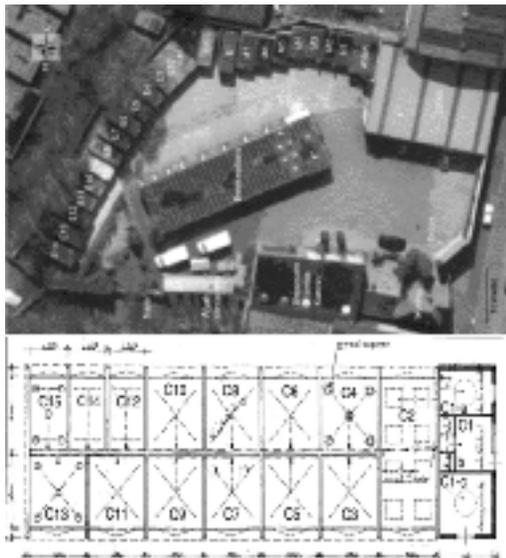


Figure 1. The layout of SE Fireworks and the central storage building (Delta photo, Enschede, adaptations NFI).

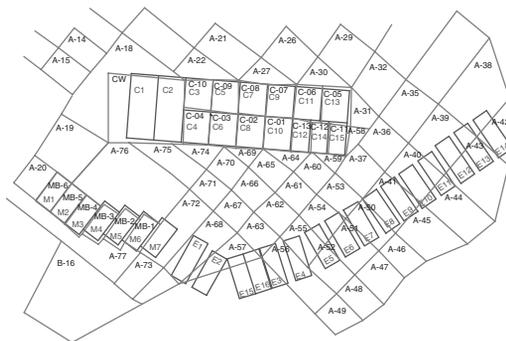


Figure 2. Scheme of the storage cells and containers of S.E. Fireworks.

displays and shows, imported fireworks and did some trade in fireworks. The depot consisted of a central storage building (cells C2–C15), seven prefab (garage) boxes and 14 ISO-containers. The central building had wooden doors and was constructed in cast, reinforced concrete with a wall and roof thickness of 20 cm. Cell 2 was the fireworks preparation and repair room, the internal dimensions of the cells C12, C14 and C15 were  $2.5 \times 4.0 \times 2.8 \text{ m}^3$  (width  $\times$  depth  $\times$  height). The other, larger cells had a width of 4 m.

The walls and roof of the prefab concrete garage boxes had a thickness of 50 mm. The dimensions of the boxes M1–M6 were  $2.6 \times 5.2 \times 2.3 \text{ m}^3$  (volume  $30.4 \text{ m}^3$ ). M7 was slightly larger and had a wooden

Table 1. Licensed storage capabilities.

Location:	Gross mass per cell (kg)	Transport classification
Central building		
Cells C3–C11	7000	1.4S/1.4G
Cell C13	500	1.3G
	or 7000	1.4S/1.4G
Small cells C12, C14, C16	500	1.3G
	or 5000	1.4S/1.4G
Preparation room C2	500*	1.4S/1.4G
Garage boxes M1–M7	3500	1.4S/1.4G
Containers E1–E14	3500	1.4S/1.4G
Total	158.500	1.4S/G
	or 136.500	1.4S/G and 2.000 1.3G

\* only during working hours.

door, the others had the original thin, corrugated steel sheet doors.

In order to prevent direct flame contact between cell doors in case of fire, the walls in the central building and the garage boxes were extended externally by 50 cm. The ISO containers were standard 20 ft transport containers, with wooden floors and no additional fire protective measures were applied.

The total licensed quantities for storage were 158.500 kg (gross mass) of 1.4S or 1.4G fireworks. In some cells firework of the class 1.3G was allowed to be stored. The license permitted in total a maximum of 2000 kg 1.3G, while 136.500 kg of the class of 1.4 could be stored. The maximum and class (transport classification) of fireworks are given in Table 1.

### 3 SEQUENCE OF EVENTS

Due to the many people that were attracted to the accident, several video recordings from various angles are available. For learning and evaluation purposes, one member of the fire brigade was specially tasked to record fire fighting actions. Especially his recordings of the events have been very helpful in the reconstruction of the disaster.

The global time frame was:

14:45	Firework effects witnessed
15:00	Fire reported to fire brigade
15:08	Reconnaissance SE Fireworks terrain
15:16	Fire in C2 under control
15:24	Smoke and fire effects from C4
15:33	Smoke from container E2 visible (video recording, time referenced to seismic recordings of the massive explosions)
15:34	Small explosion, massive deflagration of contents E2

- 15:34:40 Massive explosion garage storage boxes M7-M1  
 15:35:46 Explosion C11 (central building). Almost simultaneously the other cells and a number of containers exploded.

The Figures 3 and 4 illustrate the situation and the escalation of the firework reactions in the period of 15.16–15.33 hours. The pictures of Figure 4 and 5, respectively, show the final explosion (from a distance of about 600 m) and a top view of the explosion area with search sections taped out for the forensic investigation. The detailed time scheme and extensive event and damage descriptions are given in (Weerheijm et al. 2000). In this paper only the headlines are given.

### 3.1 Initial fire in cell C2

From the chronological accident facts, the paramount question emerges about the cause of the fire in the workshop, preparation cell C2 of the central storage building. Extensive forensic investigation was performed to examine the possibilities of:

- Sabotage, arson or improvised explosive devices;
- Malfunctioning, defects of the electrical and gas-installation or other equipment;
- Fire caused by human activities at the S.E. Fireworks terrain;
- (Self) ignition of firework articles, pyrotechnics or other fuels caused by instability or external effects.

In spite of the extensive forensic effort no definite proof was found for one of these scenarios. It should be noted that the strength of the final explosions had a devastating effect and most of the evidence of the initial fire was destroyed. Other forensic investigation concerned the possible traces of high explosives and ammunition. No traces of high explosives were found, therefore the explanations for the cause and the development of the disaster had to be found in the stored fireworks and storage conditions.

### 3.2 Observed explosion effects

The major explosion effects are the crater, fireball, blast and debris. The video recordings and the damage at the explosion area showed that the major three explosions, respectively container E2, garage boxes and the central building, had an increasing strength. Consequently the final explosion destroyed evidence and traces of the preceding explosions and hampers the detailed analysis. Nevertheless the following conclusions could be drawn from remaining evidence.

#### 3.2.1 Firework reactions in container E2

No crater or evidence for blast damage due to the E2 explosion was found. A very severe firework fire and



Figure 3. Situation at 15.16 hours.



Figure 4. The escalation between 15.24 and 15.33 hours (pictures R. van Willegen).



Figure 5. Final explosion (taken from 600 m).

the projection of firework articles characterise the “explosion” in E2. The observed effects correspond to fireworks of transport classification 1.3G, see also Merrifield and Myatt (2001).

#### 3.2.2 Explosion in garage boxes M7–M1

The second major event occurred in the garage boxes. From the video recordings it is seen that the fireball of the explosion swells to a diameter of about 85 m in

0.3 s. The explosion appeared to be a sympathetic reaction of the contents of the boxes from M7 towards M1. The boxes were completely destroyed, no remaining debris could be recollected. The video recordings show debris launch velocities of the order of 200 m/s. The reactions were severe but a detonation definitely did not occur. The concrete floors show severe cracking, and the floor slab of M7 was moved more than 1 m horizontally and a large depression of the soil at the original location was found. No crater was formed. The walls of the boxes were clearly sheared off and the direction of the deformed reinforcement bars formed clear evidence for the propagation direction of the sympathetic reactions in the cells (M7 towards M1). In most cases the blast strength of an explosion can be quantified from the building damage in the surroundings and especially from the window breakage. The final explosion destroyed most of this evidence. At one video recording of the second explosion, however, window and roof tile damage is visible. More information about the strength of the explosion is obtained from the seismic signals that were recorded of both major explosions. The ratio of the signals, the local damage and the blast damage to the surrounding area concluded that the explosion had a strength of about 800 kg TNT equivalence. The radius of the fireball corresponds to 17.000 kg propellant.

### 3.2.3 Final explosion

The relation between the events in E2, the garage boxes and the central building is described in (Weerheijm et al. 2000). The strength of the explosion in the garage boxes was by far sufficient to blow the wooden doors into the cells of the central building and the fireball engulfed the whole building. The contents of all cells were probably ignited. The central building was completely destroyed, see Figures 6 and 7. Sympathetic reactions occurred but the explosion in the central building was clearly dominated by the C11 reaction. This emerges from the facts that:

- In C11 a crater was formed with a depth of 1.3 m. The crater extended to the other cells and was clearly the result of one explosion event;
- the floors of the other cells show no damage of independent, severe explosion reactions, only the edges of the cell floors adjacent to C11 are severely damaged and contribute to the crater (see Figure 7);
- the remaining reinforcement stubs of the floor-wall connections of all cells show deflection directed away from cell C11.

Debris from the central building caused many casualties and severe damage to buildings. Debris was found up to a distance of 580 m (see Figure 8). The angle of impact, the throw distance of the major debris were related to the “required” launch velocity. Because the

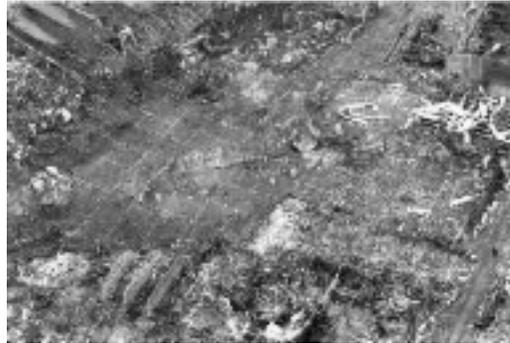


Figure 6. Explosion area after the accident (SFOB).



Figure 7. Damage central building.

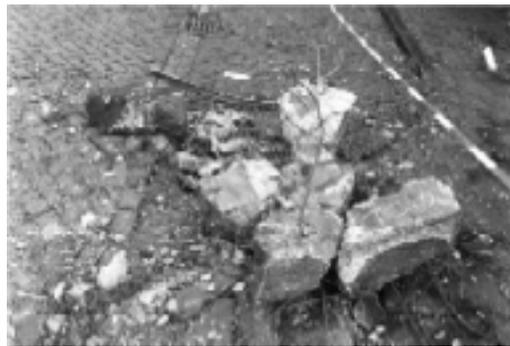


Figure 8. Debris at 165 m.

launch angle is unknown, only an approximate range of launch velocities could be determined. Most of the collected debris had a launch velocity in the range 30–100 m/s. Maximum reconstructed velocity was 150 m/s. It should be noted that most of the debris that could be collected was most probably not from C11 or the adjacent cells, because these were broken in small pieces due to the high explosion pressures in the cells.

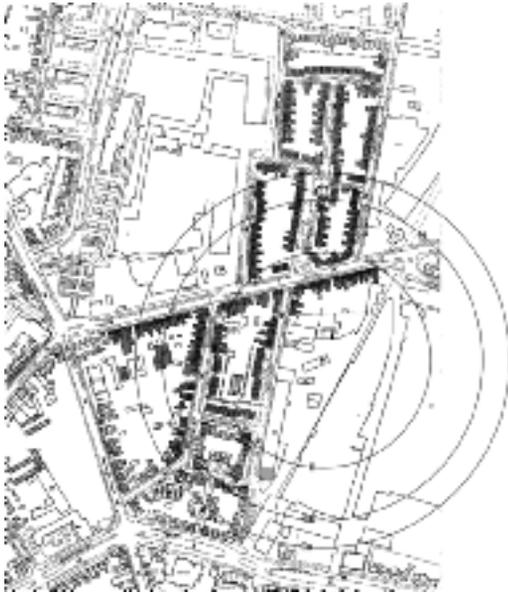


Figure 9. Damaga radii.

Most evidence for the final explosion strength was obtained from the window breakage and the observed damage in the surroundings. Window breakage was inventoried in three different directions up to a distance of 850 m. The distance, position, dimensions and breakage percentage of about 700 houses served as input for the calculation of the source strength. The methodology to determine the failure probability coupled to the dynamic load is given in Weerheijm et al. (2000). The damage to the houses, within the radius of 500 m, were categorized to levels A, B, Cb, Ca, or D. These categories were developed during the second World War II and are commonly accepted. The zones are given in Figure 9 with the radius for damage level Ca is about 230 m.

The final, devastating explosion proved to be in the range of 4000–5000 kg TNT equivalence. The size of the fireball was 135 m, corresponding to 86.500 kg propellant. It is evident that these effects are not caused by the contents of cell C11 alone. Sympathetic reactions of the other cells and also the containers contributed to the observed effects. On the video recordings the shape of the fireball shows clearly some additional “sub-sources” which may be caused by container reactions.

#### 4 THE EXPLOSION EFFECTS AND THE STORED FIREWORKS

For the lawsuit the question about the relation between the explosion effects that occurred and the



Figure 10. Effects during UN 6c test with report shells.

quantities and type of fireworks involved is paramount. Hitherto, no definite information is available of the quantities and type of fireworks that were stored in the different cells. Information is available from the sales list of SE Fireworks and the hearings. This information is insufficient to answer the question. It should be noted that the local damage to the floors, and the visual effects on the videos give us information about the firework reactions in the specific cells, while fireball, debris and damage is caused by the sum of all firework reactions (a combination of mild and very severe reactions).

The license show that only a limited amount of 1.3G class articles were allowed (2000 kg) to be stored in some specific storage cells of the central building. The bulk of the storage capacity (136.500 kg) concerned class 1.4 G articles. The safety regulations are based on the principle that the effects observed in the UN transport classification tests are also representative for the potential effects in (bulk) storage and transport conditions. Or in other words, the test conditions should cover the scale effect and confinement in storage conditions.

It is obvious that the effects in the Enschede disaster do not match with the 1.4G and 1.3G transport classification criteria. This means that large amounts of 1.3G, or even 1.1 articles were stored or the transport classification methodology is not well suited to cover bulk storage conditions and define storage safety regulations. Classification tests were performed on various kind of firework articles. Based on the sales list of SE Fireworks a selection was made of articles that could be of a class 1.3G or higher. Comparable, similar articles (display and sound effects) were purchased and tested for transport classification. The selection covered cakeboxes, roman candles, colour- and report shells as well as fountains and rockets. Especially the titanium report shells and the larger shells showed severe reactions. Some of the articles tested were classified as 1.1. Figure 10 illustrates one

of the 6c tests with report shells. The test series are given in Dirkse en de Jong (2000) and de Jong & Dirkse (2001). The tests learned that the selected items were of class 1.3G or 1.1. Because no definite information is available of the amounts and types of stored fireworks it cannot be concluded that the disaster was caused due to the kind of stored fireworks only. Scale effect and confinement conditions may have been of major importance.

## 5 INITIATION AND POSSIBLE CONSEQUENCES OF FIRE IN C2

In spite of the extensive forensic research and hearings no evidence is obtained for the cause of the fire in the firework preparation and reparation cell, C2. On Saturday 13th of May the company and the terrain were closed. Therefore we start with the facts that the fire was noticed at about 14:45 hour when activated firework was ejected and landed outside the S.E.F. premises. A small fire in a garden was reported. When the fire brigade arrived the doors of cell C2 were open at both sides and the plastic skylights were gone. Some fast pressure build up must have occurred because the doors on both sides were blown out. No external blast damage was noticed. The fire was fought at both sides of the central building. The firemen at the north side (side of garage boxes) were killed in the accident; no direct witness reports of the fire development at the north side are available.

The effects of the fire in C2 are:

1. Fire; heat loading on walls of adjacent cells;
2. Fire jet and heat radiation directed to the opposite garage boxes and containers;
3. Ejected fireworks, with possibility of fire ignition.

The following comments are made concerning these effects:

Ad 1: The wooden doors of the other cells were closed and locked; the internal walls of cast reinforced concrete had a thickness of 200 mm and were fire resistant. Only the wall between cells C2 and C4 had an opening (diameter 70 mm). Afterwards concrete samples were taken from the floor slabs of the central building. Laboratory research showed no evidence for heat loading. Combined with the fire brigade reports, the conclusion was drawn that the fire in the central building was not passed on to other cells except to C4. Fire in C4 started before 15:28.

Ad 2: Dependent on the content of C2 and the intensity of the flame jet and heat radiation, fire may be initiated in the opposite garage boxes with thin corrugated steel doors. However, there are no indications that the firemen observed any fire effects.

Ad 3: At the north side small fires were noticed and extinguished. Firemen reported that in between

the containers E1 and E2 smoke development was observed and fire was fought (15:28 hour).

On the S.E.F. premises the effects of the fire in C2 were most probably limited to the fire passed on to C4 and the initiation of small fires due to the ejected articles.

The effects of the fire in C4 are similar as reported for C2 with the comment that C4 was a storage cell, while C2 was the workshop with no licensed storage capacity after working hours.

The performed analyses confirmed that the building (cast concrete, 20 cm thick walls and roof) provided sufficient heat resistance between the storage cells. Of course openings between the cells are not allowed. The analyses also confirmed the requirement on fire resistance of doors. Automatic fire suppression systems like sprinklers should be a standard requirement.

Finally, one should be aware of the large area with potential fire hazards when the ejection of fireworks can occur. Requirements on fire resistance of other facilities are paramount as will be clear from the events in the container E2.

## 6 INITIATION AND POSSIBLE CONSEQUENCES OF REACTION IN E2

The following initiation mechanisms were examined theoretically:

- External fire;
- Fireworks on and, or under the container;
- Burning magnesium (ejected from the workshop) on top of container;
- Fireworks before door slit.

From previous research it was known that the resistance of steel ISO containers to the standardised fire loading is limited to a few minutes. However, in the current investigation the intensity, size and duration of the external fire were the parameters.

The TNO Centre of Fire Research performed theoretical calculations and the very poor fire resistance of the steel containers was stressed. Considering the timeframe, the very limited fire resistance of the container, the presence of an old small trailer with wooden floor between E1 and E2, a small fire was possible and sufficient to initiate a fire and fireworks in E2. The other potential initiation mechanisms appeared to be less likely and were rejected. The successive effects of the E2 reaction were: smoke from door slit, strong smoke development followed by intensive firework reactions, flame jet (in two pulses), ejected fireworks and very severe (external) massive reaction of firework. Similar effects were observed and reported by Merrifield and Myatt [1] with 1.3G fireworks tests. Figure 2 illustrates these effects.



Figure 11. Effects of E2 reaction (video by G.Poort, enhanced by NFI).

For the possible consequences of the E2 reaction the following effects were theoretically examined:

1. Ejection of debris (doors);
2. Failure of container (fragments and blast);
3. Flame jet (and possible external fireball);
4. Ejected fireworks.

Ad 1: If a container door is ejected from E2 and impacts on a door of the central storage building, this door will fail and cause damage to the stored firework packages. The successive fire jet and heat radiation could initiate the contents of the cell. The possible consequences were predicted assuming that the burning pyrotechnics led to an explosive reaction. The calculated local and structural failure modes however did not correspond to the observed effects and post accident damage.

Ad 2: The blast effects due to door failure or roof/wall failure were calculated. The blast level proved to be insufficient to cause damage to the doors of the garage boxes or central building.

Ad 3: The first jet had a duration of 2 s and a length of 17–30 m (distance to central building was 17 m, the jet was deflected upwards leading to a total length of 30 m and a diameter in the order of 20 m). A few seconds later the reaction intensified and a second jet was formed with a length of 35 m and duration of 1 s. The thermal loading on the doors of the other cells and the stored fireworks was calculated. Experiments were performed to determine the thermal load behind the steel sheet doors and the required duration to ignite the packages or fireworks. The required loading time proved to be in the order of 12 s. Consequently escalation of the accidents to the garage boxes or containers could be excluded. The possible escalation to the central building was rejected because of the considerations mentioned at “ad 1”.

Ad 4: The hearings learned that in E2 shells were stored of at least 6 inches. The video recordings confirmed the presence of mortar shells. The ejected fireworks caused fire and damage in a wide area. Because the accident escalated within a minute after E2, the possible local “breaching” damage of mortar shells to wooden and garage doors was examined experimentally. Note that the contents of E2 were unknown at the time of the experiments. 8 and 12 inch mortar shells and 3 inch titanium report shells were tested. The 12 inch shell had a devastating effect on both door types; the other shells caused severe damage but not complete failure. It is most likely that multiple hits and loading by the latter shells would lead to door failure and ignition of the cell contents.

Conclusion on E2 effects for the escalation of the accident is: No definite evidence is found for a fast escalation to the garage boxes. Most likely is the breaching of the M7 door by multiple shell reactions.

The performed analyses and tests confirmed and learned that:

- steel ISO containers have negligible fire resistance and are not suitable for storage or transport of flammable goods without additional counter measures,
- planning the lay out of a firework storage facility one should count with the combined threat of door debris and flame jet (1.3 bulk storage),
- when 1.3 G articles in a storage cell react, the pressure build up can be sufficient to throw the contents out which leads to extensive external effects and a considerable increase of the risks,
- The pressure effects at short distance of reacting shells can be sufficient for local damage and breaching of wooden or steel sheet doors is possible. Consequently the out throw of shells lead to new risks. Strength requirements for doors are recommended.

## 7 POSSIBLE CONSEQUENCES OF REACTION IN GARAGE BOXES M7-M1

The initiation possibilities in the garage boxes from the fire in the central building and the effects from E2 were already mentioned. In this section we focus on the sympathetic reactions in the garage boxes. Figure 12 gives two frames from the video recordings that illustrate the effects of the explosion.

The damage proofs that the most severe explosion occurred in M7, but the local damage clearly showed that no detonation occurred. The observed debris velocity of 200 m/s was related theoretically to the required reaction velocity of pyrotechnics and the local damage to the remaining floor slabs. These aspects could be related without any contradictions. It is evident that the "required reaction velocity" can be achieved by the properties of the pyrotechnic materials

themselves, and/or the number of ignition points and/or the 3D expansion of the reaction front and thus the length scale and size of the storage cell.

The next question was about the mechanism to initiate the contents of the other garage boxes. Most likely is that the 5 cm thick walls (of prefab box M7) failed and were launched with an initial velocity in the order of 100 m/s. The resulting severe crushing of the fireworks in M6 and thermal loading caused the sympathetic chain reaction of the fireworks in M6, and subsequently in the other cells. The reactions in the garage boxes occurred in the time frame of less than 0.5 seconds.

The effect of the explosion was a blast, equivalent to a TNT explosion of 800 kg. A fireball was formed with a radius of 85 m. The garage boxes were completely destroyed and fragmented into small debris. The combined blast and debris formed a severe loading for the

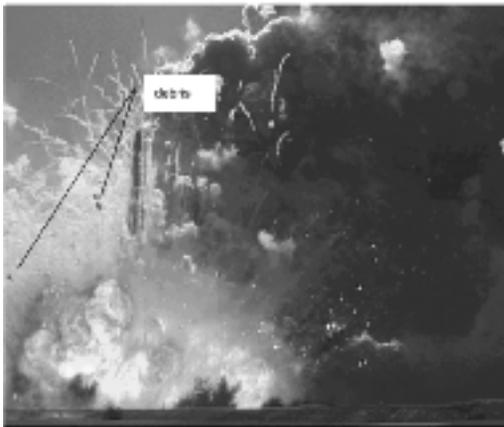


Figure 12. Effects of explosion in garage boxes (video by G.Poort, enhanced by NFI).



Figure 13. Mass explosion in central building (video by G.Poort, enhanced by NFI).

central building and the containers. In combination with the thermal loading and ejected burning firework articles escalation of the accident was inevitable.

Conclusions and discussion on the sympathetic reactions in the different cells are given in the next section about the explosion in the central storage building. Figure 13 illustrates some of the explosion effects.

## 8 INITIATION AND EXPLOSION EFFECTS OF EXPLOSION IN CENTRAL STORAGE BUILDING

Considering the central building, the strength of the explosion in the garage boxes was far sufficient to blow the wooden doors into the cells and the fireball engulfed the whole building.

The contents of all cells could have been ignited. The local damage however showed clearly that the explosion in storage cell C11 was most severe and dominant. A single explosion in C11 and the sequential sympathetic reactions in the other cells can explain the total damage. In analogy with the garage box analysis, the required local pressure and gas pressure were related theoretically to the required reacted mass of pyrotechnics per second to explain the observed damage and the sympathetic reactions in the adjacent cells.

Crucial in the explanation is the reaction velocity of the fireworks in C11. Hypotheses to explain the devastating mass explosion in C11 are:

1. Storage of firework of the transport class 1.1;
2. Combined storage of 1.3G and 1.1 fireworks;
3. Fireworks of the class 1.3G were stored, but due to door impact the packages were severely damaged and the firework obtained the 1.1 characteristics;
4. After initiation of the stored 1.3G class fireworks, temperature and confinement conditions accelerated the deflagration process towards a detonation-like reaction.

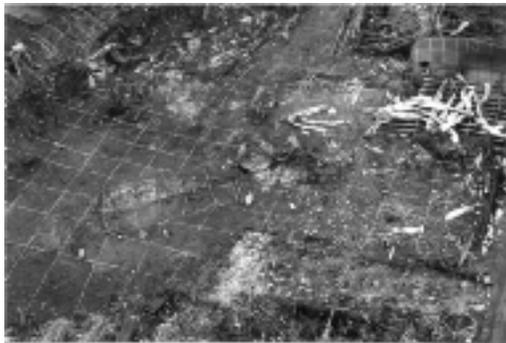


Figure 14. Overview explosion area (Picture SFOB).

None of these hypotheses was proven during the technical research program for the ministry of Justice. It should be noted that UN transport classification tests were performed on a selection of firework articles based on the sales list of S.E. Fireworks. Some of the tested fireworks obtained the 1.1 transport classification. The second comment is that the hearings learned that in C11 6-inch mortar and 6 inch titanium report shells were stored. The tested report shells were classified as 1.1.

In order to learn from the observed effects let us discuss the effects in storage cell C11 in more detail.

- Crater: The evidence for the local pressures is given by the crater. The crater extended to the adjacent cells but the shape of the crater showed that it was caused by a single explosion and that the reactions in the neighbouring cells did not contribute to the crater. Relating the strength of the explosion in C11 with a TNT detonation by the crater dimensions, the explosion strength is in the range of 750–2000 kg TNT equivalent. It should be noted that the concrete floor was not breached, so the local pressures in the firework reaction were much lower and not comparable with the pressures in a TNT reaction.
- Acceleration of walls and roof: Due to the shock wave of the explosion the roof will be torn from the walls and the walls from the foundation. Referring to the crack pattern and damage to the floor slab, the walls and roof were broken most probably into small debris. No good prediction of the debris velocities was possible. From explosion tests with concrete ammunition storage cells it is known that the velocities are in the range of 100–300 m/s. For the C11 reaction, the debris velocity had the same order of magnitude.
- The effect on the adjacent cells: The floor slabs were pushed downwards which proofs that the explosion pressure of C11 expanded through the failed walls to the adjacent cells. The required pressure to deform the floors was definitely sufficient to brake and eject the roofs and walls. However, the explosion pressure of C11 would never be able to throw the roofs of the next adjacent walls. Time is needed for the failure process and in the mean time the explosion pressure in C11 has vented through the door opening. Consequently, the conclusion must be that sympathetic reactions occurred in the adjacent cells.
- Blast pressure and damage: The explosion in C11 produced severe blast, but it must be excluded that the total blast damage in the surrounding living area (equivalent to damage of a 4000–5000 kg TNT explosion) was caused by the single explosion in C11. Referring to the licensed quantity to store 7000 kg gross weight (1.4G) fireworks,

- 50% net weight and estimating a TNT equivalence of 0.5 for the stored fireworks, a rough number for the (maximum) explosion strength is 1750 kg TNT.
- Fireball and firework projections: The observed fireball had a diameter of 135 m. The storage capacity of C11 was too limited that a single explosion in C11 could produce a fireball of this size.

It is clear that sympathetic reaction occurred in most of the cells in the central building (and containers). A likely but still unproven explanation emerge from the above given facts and observations. The explosion in C11 caused failure of the walls, these were blown into the adjacent cells (velocities in the order of 100 m/s). It is most likely that due to the impact, severe friction because of the non-uniformly distributed load, and also combined with the subsequent thermal load, large quantities of fireworks were initiated. High pressures were generated in short time leading to the break-up of the building and contributing to the total explosion blast and fireball.

From the firework disaster in Enschede and the observations made it emerges that international research effort is needed to understand and quantify the explosion effects of firework in bulk storage conditions. Consequences of mixed loading, confinement and scale have to be known to define safety regulations and evaluate the current UN transport classification methodology. It is mentioned that recently a joint research project of TNO, HSL (UK) and BAM (Germany) on these topics was granted by the European Commission.

## 9 CONCLUDING REMARKS

- The explosions at S.E. Fireworks in Enschede on May 13, 2000 caused 22 lethalties, 947 injuries, a complete residential area was destroyed. 500 houses were completely demolished and 1350 houses were damaged. The main cause of the damage in the neighbourhood was the massive conflagration of the old houses with wooden floors caused by the throw out of fireworks.
- The present paper was focussed on the observations and facts. Besides the initial fire in the central building, three crucial events are identified that dominate the escalation of the accident. These are the severe firework reactions in container E2, followed by the explosions in the garage boxes and finally the massive explosion in the storage cell C11 of the central building and the sympathetic reactions of the other storage cells and containers.
- In spite of the extensive forensic investigation no definite evidence for the initial cause of the chain of events was found. There was no indication of sabotage. No traces of high explosives

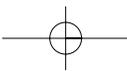
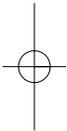
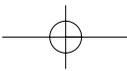
were detected; all traces indicated fireworks related substances.

- Window breakage, structural damage, crater dimensions, debris and the seismic signals enabled the quantification of the two major explosions. The explosion in the garage boxes had a strength of the order of 800 kg TNT equivalence while the strength of the final explosion is within the range of 4000–5000 kg TNT.
- Probably the classes of stored firework articles, quantities and storage conditions caused the initial fire to escalate into the disastrous explosions.
- If the situation at S.E. Fireworks would have been in conformity with the licenses, the fire in the workshop of the central storage building never could have escalated to the disaster May 13th, 2000.
- Much more firework of the class 1.3G was stored (and probably also class 1.1) than licensed. The facility was not suited to control and contain the effects.
- The minimal fire resistance of the containers and the lay out of the premises, containers and garage boxes at short distance and opposite to the central building, contributed to the escalation of the fire accident.
- The fireworks disaster is caused by the transition of firework fires into mass explosions. This happened in the garage box M7 as well as in the storage cell C11. Hypotheses were defined but could not be proven so far. Initiatives are taken to study the reaction characteristics of 1.4G and especially 1.3G fireworks in bulk storage conditions. If necessary the UN classification methodology for transport classification have to be modified in order to be suitable for safety regulations of bulk storage and bulk transport of fireworks.
- For the storage and transport of fireworks fire resistant containers have to be required.
- When 1.3G fireworks are stored, impact resistant doors are recommended in order to prevent demolition by close-in firework reactions.

## REFERENCES

- Bruyn, P.C.A.M. de and Karelse J.W., The forensic investigation Firework Disaster Enschede, *The Netherlands Forensic Institute*, report 2000.05.17.018.
- Commissie Preventie van Rampen door Gevaarlijke stoffen, "Methods for the determination of possible damage to people and objects resulting from release of dangerous materials". *Sdu Publishers*, CPR-16E, second edition, The Hague.
- Jong, E.D. de and Dirkse, M.W.L., Classification investigation on display fireworks of SE Fireworks, Part 2: Classification experiments, *TNO report 2001-C29*.

- Dirkse, M.W.L. and Jong E.G. de, The explosion at S.E. Fireworks, Part 2: Transportclassification judgement for confiscated firework, *TNO report* PML 2000-C121, vs 2.0.
- Merrifield, R. and Myatt, S.G., The effects of External Fire on Fireworks Stored in Steel ISO containers. *Journal of Pyrotechnics*, 2001.
- Weerheijm, J., Wees, van R.M.M., Doormaal, van J.C.A.M. and Rhijnsburger, M.P.M., The explosions at S.E. Fireworks; *TNO report*, PML 2000-C120 and C122. Part 1: The explosion strengths based on observed damage, Part 3: The reconstruction of the chain of events.
- Mercx, W.P.M. and Kodde, H.H., "The explosion of the display fireworks assembly plant 'MS Vuurwerk' on February 14, Culemborg, The Netherlands", *25th DoD Explosives Safety Seminar*, Anaheim, California, 18-20 August 1992.
- Vretblad, B., Weerheijm, J. en Guerke, G., "The KLOTZ group's debris dispersion program", *29th US DoD Explosives Safety Seminar*, 18-20 juli 2000, New Orleans, Louisiana.



## Consequence modelling of gas explosion scenarios in traffic tunnels

J. Weerheijm, A.C. van den Berg & N.H.A. Versloot

*TNO Prins Maurits Laboratory, Rijswijk, The Netherlands*

**ABSTRACT:** To be able to assess the social acceptability of hazardous materials transport through tunnels risk analysis is an appropriate technique. In order to be able to perform a sound hazard analysis two tools have been developed. A screening tool set to determine quickly the consequences in a wide spectrum of scenarios. A one-dimensional gas dynamic model of a gas explosion computes the pressure loading. This model requires input in terms of flame propagation behavior in tubes. Subsequently, damage criteria in pressure-impulse graphs determine the response of the tunnel structure. Secondly, a tool set for detailed numerical simulation. A three-dimensional CFD gas explosion simulator is capable of computing the consequences of gas explosion scenarios as well as the effects of any possible mitigating measure in detail. The resulting blast loading serves as input to an FE-model that is able to simulate dynamic response of the tunnel structure in any wanted detail.

### 1 INTRODUCTION

In the Netherlands, future road and rail infrastructure is increasingly projected underground or covered in. Consequently, risk assessment related to the transport of hazardous goods is an issue for the planning of new infrastructure, for the exploitation and maintenance of the tunnels, and the design and realisation of emergency counter measures. First responsibility for these tasks is with the government. Different ministries are involved, as there are the ministry of Housing, Spatial Planning and the Environment, the ministry of Transport, Public Works and Water Management and the ministry of the Interior and Kingdom Relations. Combined and conflicting interests of community, safety and economy require a sound tool for judgement and decision making.

Within the entire spectrum of risk of hazardous materials transportation, the probability of gas explosion in a tunnel may be relatively low but, on the other hand, the geometry of a tunnel constitutes optimal conditions for a gas explosion to develop devastating consequences. In the Netherlands the explosion scenario is not included or considered in the tunnel design. Consequently, a gas explosion is mostly fatal for the current tunnel structure as well as for all people present inside. With the increasing demand for underground infrastructure, it becomes inevitable and necessary to include the explosion scenario in the planning and design process.

To be able to assess the social acceptability of hazardous materials transport through tunnels risk analysis

is an appropriate technique. In order to be able to perform a sound hazard analysis, the TNO Prins Maurits Laboratory develops the proper tools and consequence models. These tools and models can also help to define the counter measures to limit the explosion effect and damage to an acceptable level.

This paper describes both a screening and a full scenario simulation approach. A simple one-dimensional gas dynamic model describes the explosion pressure in a tunnel. The load prediction forms the input for the dynamic response calculation and damage assessment given in PI-diagrams (iso-damage curves given as a function of Pressure and Impulse) for characteristic tunnel elements. This screening approach overestimates the consequences. More accurate load predictions are possible with the 3D-CFD gas explosion solver AutoReaGas™. The gas explosion modelling is supported by an experimental research programme in a small-scale model (1:20) of a traffic tunnel. At the TNO Prins Maurits Laboratory advanced numerical tools are available for the prediction of the dynamic response of concrete structures. In order to limit the scope, this aspect is not covered by the current paper. This paper summarises the characteristics and features of the CFD gas explosion solver and the screening tool.

### 2 EXPERIMENTAL PROGRAM

Hitherto, reliable data on gas explosions in tunnel geometries was lacking. To enable good and reliable

numerical simulation of gas explosions in traffic tunnels this data is essential. Therefore, TNO PML decided to perform an extensive experimental program. The experimental program has been performed in a steel channel of  $0.25 \times 0.5 \text{ m}^2$  cross section and 8 m long. This small-scale model (1:20) of a traffic tunnel was provided with a configuration of steel obstacles to simulate a standing traffic jam (Fig. 1). The channel was filled with a flammable gas-air cloud and ignited at a closed end, simulating central ignition in a two-sided open channel twice as long. The cloud length was varied as being  $1/4$ ,  $1/2$ ,  $3/4$  and  $1/1$  of the channel length. The fuels used were methane and propane at three different compositions.

The overpressure-time development was recorded at seven different stations positioned at more or less regular distances along the channel length. All the experiments were performed in triplicate. The full details of the experimental method and results are described by De Maaijer et al.(2002). This paper just summarises some data required for the calibration and validation of the gas explosion modelling.

### 2.1 Variation of cloud length

The maximum overpressures developed in the channel showed relatively little difference for cloud lengths of  $1/2$ ,  $3/4$  and  $1/1$  of the channel length. Contrarily, for a cloud length of  $1/4$  of the channel length, significantly lower overpressures were observed. Because the flammable mixture in front of the flame is set into motion, it mixes up with air and the flame, after having passed the  $1/4$  channel length position, propagates into leaner and leaner mixture. With cloud lengths of  $1/2$ ,  $3/4$  and  $1/1$  of the channel length, the flame does not run into substantially leaner mixture before the end of the channel with relatively less effect on the internal overpressure.



Figure 1. Scale model (1:20) of a traffic tunnel containing obstacles that simulate a standing traffic jam.

### 2.2 Variation of cloud composition

For a cloud length of  $1/1$  of the channel length both lean and rich mixtures developed substantially lower overpressures than the stoichiometric mixture, as to be expected. For a cloud length of  $1/4$  of the channel length, however, the rich mixture developed substantially higher overpressures than the comparable stoichiometric mixture. This is due to the fact that the mixture in front of the flame mixed up to stoichiometry before combustion, which resulted in a longer effective cloud length.

The data and phenomena are used as a reference for the gas explosion solver tool. Besides this advanced tool, interest was expressed in a tool for quick scans and rough parameter studies. For these purposes a screening tool was developed with simplifications, but with a sound basis of physics.

## 3 SCREENING TOOLS

### 3.1 Gas explosion loading

#### 3.1.1 Model

The pressure loading of a tunnel structure due to a gas explosion is approximated by the one-dimensional gas dynamics of a column of perfect gas. The gas dynamics is driven by an energy source, a flame that is propagated at any prescribed development of its speed. The heat of combustion is gradually added to the medium during the passage of a zone (flame) of a few cells thick (Fig. 2).

The gas dynamics is modelled by the Euler-equations for compressible inviscid flow and a conservation equation for the energy addition parameter. The equations are solved by means of a Flux-Corrected Transport scheme (Boris 1976) in a numerical mesh consisting of a row of cells. The entries at either end of the tunnel are simulated by imposing atmospheric pressure in the begin and end cells of the mesh. This simplified model of the gas dynamics of a gas explosion in a tunnel requires data for flame speed development as input.

#### 3.1.2 Model input

In a tube a gas deflagration develops a continuously increasing flame speed and pressure, if the tube is long



Figure 2. One-dimensional numerical model of a gas explosion in a tunnel. Flame propagation modelled as a moving zone in which the heat of combustion is added to a perfect gas. ( $Q$  = heat of combustion;  $b$  = flame front thickness; energy added to cell  $i = a/b * Q$ ).

enough resulting in transition to detonation. For simplicity a linear flame speed development was assumed in this model. Although deflagration–detonation transition (DDT) is characterised by highly probabilistic features, in this model a deterministic DDT-criterion was assumed. DDT was assumed to occur at a flame speed of 800 m/s. Deflagration to detonation transition is accompanied with an abrupt jump in the propagation velocity, which has been modelled by a sudden transition from 800 m/s to the Chapman-Jouguet wave speed. The CJ-wave speed is calculated from:

$$M_{CJ} \approx \sqrt{\frac{2Q(\gamma_1^2 - 1)}{c_0^2}} \quad (1)$$

where  $M_{CJ}$  = CJ-wave Mach number;  $\gamma_1$  = ratio specific heats combustion products;  $Q$  = heat of combustion (J/kg);  $c_0$  = ambient speed of sound (m/s).

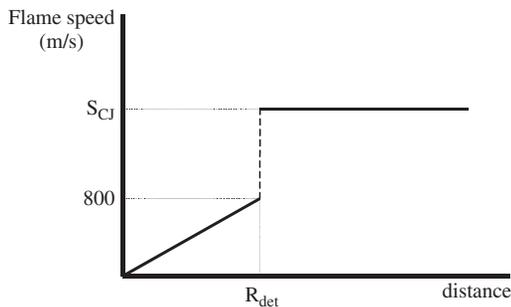
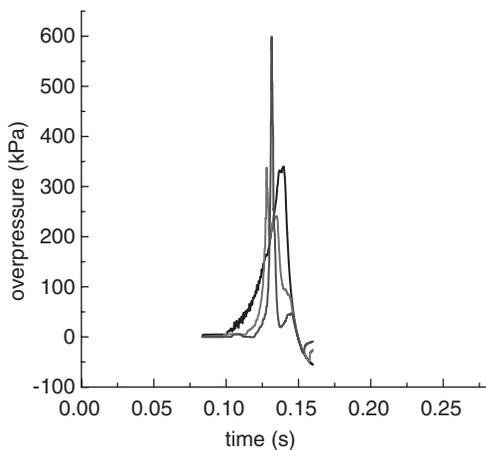


Figure 3. Schematised flame speed development in a tunnel tube.



The schematised development of a gas explosion in a tube, by which the one-dimensional gas dynamics is driven, is graphically represented in Figure 3.

Experimental data for gas explosion development in tubes completes the simplified gas explosion modelling:

- For empty tubes detonation runup ( $R_{det}$ ) distances are taken from Steen & Schampel (1983).
- For a tunnel containing a traffic jam, data on flame speed and overpressure development are taken from the experimental program addressed in section 2 (De Maaijer et al. 2002).

The small-scale experimental data were extrapolated to other flammable mixtures and to full-scale traffic tunnels on the basis of Karlovitz number similarity (Taylor & Hirst 1988, Catlin 1991, Catlin & Johnson 1992).

### 3.1.3 Model validation

To validate the model a test from the (1:20) scale experimental program was run. The tunnel tube of  $0.5 \times 0.25 \text{ m}^2$  cross-section was 8 m long and was provided with rows of obstacles at the floor to simulate a standing traffic jam. The tube was filled with a stoichiometric methane–air mixture and ignited at its closed end. Both, the computed and the observed overpressure-time development are represented in Figure 4.

The figure shows that the assumption of a linear flame speed development is not unreasonable. In addition, it shows that the gas dynamics and the pressure loading of the tunnel structure is properly reproduced. However, the cloud length in this case was equal to the channel length and the dilution of the flammable mixture in front of the flame during transport in the expansion flow was zero.

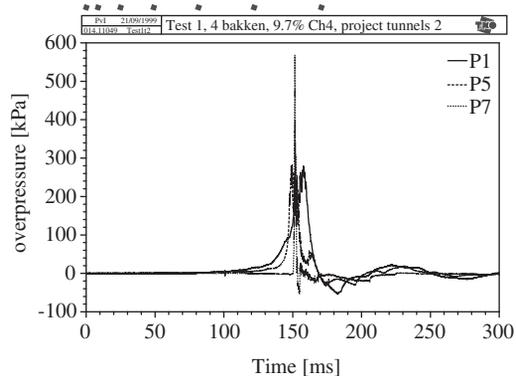


Figure 4. Computed (*left*) and observed (*right*) overpressure–time development in a 1:20 scale model of a tunnel containing a traffic jam (solid: closed channel end; dashed: halfway channel length; dotted: near channel exit).

The mixing of the flammable mixture with air in the expansion flow in front of the flame cannot be described in this simplified one-dimensional model of a gas explosion in a tunnel tube. Instead, the flammable mixture in front of the flame is simply transported and remains undiluted. In addition, the assumed linear flame speed development applies only to a flame propagating a homogeneous mixture. Therefore, this screening tool substantially overestimates the tunnel structure loading for clouds of limited length.

### 3.2 Structural response modelling

A basic and simple model for the dynamic response of structures is the Single Degree of Freedom (SDOF) system. With a dominant deformation mode, the structural deformation resistance represented by a “spring characteristic” and the equivalent mass to represent the inertia effect, the dynamic response can be calculated for dynamic loading. This basic technique is suitable for the screening tool when some conditions are fulfilled or simplifications are acceptable.

The main assumption (or condition) of the SDOF approach is that the dynamic response is dominated by one deformation mode. For the envisaged tunnel application, this condition should be valid for the whole response and damage range from elastic response to the stages of initial cracking and reinforcement yielding into the phase of final failure. Let us go step by step through the schematisation of the tunnel structure and see which assumptions and simplifications have to be made.

#### 3.2.1 Loading

Considering the duration of the gas explosion blast load, the duration is in the order of 0.2–0.6 seconds. The minimum length of the blast wave is in the order of 40–100 meter. The cross span of tunnels in the Netherlands is 9 or 12 meters wide. For the structural response the variation of the loading in axial tunnel direction is limited, therefore the cross section will be considered to determine the resistance of the tunnel to explosion load. With this simplification the load bearing capacity of the tunnel in axial direction is neglected and consequently, the result will be slightly conservative.

In the previous section, the blast load was calculated and the results show that the shape of the blast load depends on the ignition point, the cloud length but changes also along the tunnel. Because the shape of loading can influence the dynamic response considerably (see for instance Biggs 1964) we decided to schematise the load as depicted in Figure 5. The triangle shape of the load is characterised by the parameters  $P_{\max}$  (maximum pressure), the phase duration  $t_d$ , and the parameter  $\beta$  to characterise the rise time ( $\beta \cdot t_d$ ).

#### 3.2.2 Tunnel cross sections

The Ministry of Transport selected five characteristic, and representative tunnel cross sections. The cross sections were schematised to the set of basic elements. In Figure 6 an example of one of the five variants is given. It is a rectangular tunnel cross section with two traffic tubes. In the figure an explosion is sketched in one of the tubes. It is assumed that the roof and the intermediate wall are the two most critical components. The schematisation of these components is sketched at the right side of the figure. The connection between intermediate wall and roof is stiff enough to consider it as clamped. The intermediate wall is loaded with the dynamic gas explosion load only, while the roof is also loaded with an initial gravity load of the roof structure itself and the soil on top of it.

#### 3.2.3 Resistance curve

We assumed that the response of the cross section is dominated by the first response mode and bending failure will occur. Based on the moment–deformation curves ( $M$ – $\kappa$  diagrams) of the selected tunnels a resistance curve (spring characteristic) for the SDOF is calculated. An overview of the calculation process is given in Figure 7.

So, the resistance curve of the element cross section is given by a linear elastic response branch up to initial concrete cracking. Then the stiffness decreases given by the second linear branch. When the reinforcement starts to yield the additional load bearing capacity is

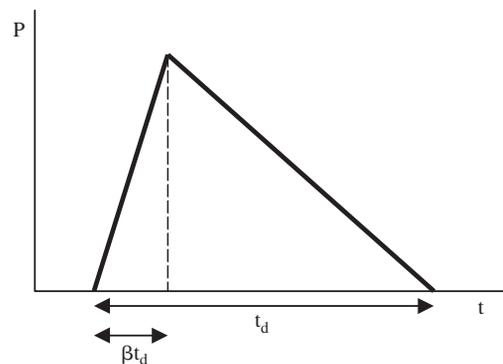


Figure 5. Schematised blast load from gas explosion.

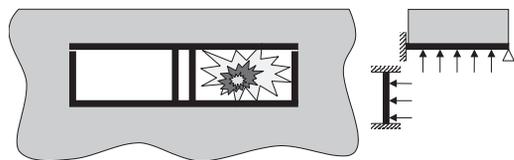


Figure 6. Basic elements of one of the five selected tunnel cross sections.

almost zero, which is represented by the third linear branch. The damage level in this last branch is characterised by the deformation angle  $\kappa$ . We decided to adopt the criterion of the TM 5-1300 (military guidelines for the design of protected structures) for complete failure given by a rotation angle of  $2^\circ$  at the clamped support. These resistance curves are combined with the structural response and (plastic) hinges of the element as illustrated in Figure 7.

Note that for the roof panel the influence of the soil cover on the inertia and the initial gravity loading is implemented in the SDOF model of the roof. Also the asymmetric reinforcement of the roof and its corresponding plastic hinges and resistance is accounted for.

### 3.2.4 P-I diagrams

For the given cross sections the SDOF models were constructed and the iso-damage curves were calculated for the different blast loads (characterised by the parameter  $\beta$ ) as a function of the maximum pressure

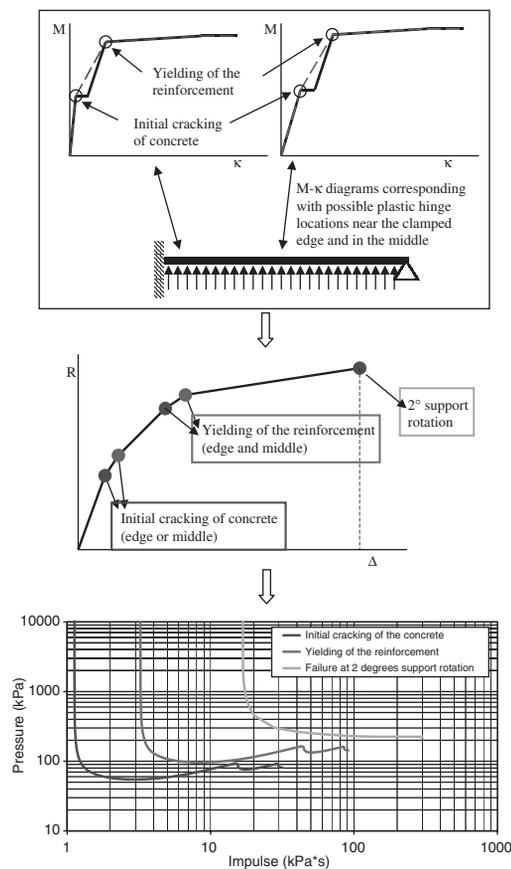


Figure 7. Typical calculation procedure of a tunnel roof structure.

level and the impulse. The results are given in P-I diagrams. Figure 8 gives two examples for the separation wall of the cross section with 12 meter span and  $\beta = 0.0$  and  $0.25$ .

### 3.3 Combination of load and response

With the simple load prediction the input is generated for the response calculations. The maximum pressure, the pressure rise times (given by the parameter  $\beta$ ) and the total impulse are calculated. In a study for the ministry of Ministry of Transport, Public Works and Water Management a whole range of scenarios was considered and quantified. For the tunnel cross sections as mentioned in the previous section the damage level was quantified. These calculations learned that for the predicted loads the response and damage thresholds were in the region of the pressure asymptote of the P-I diagram. These results show that for gas explosions the assumption that the response is dominated by the first eigenmode was good. For other situations where the load is more impulsive and the impulse asymptote becomes representative, more accurate analyses with FE calculations are recommended.

## 4 FULL SCENARIO SIMULATION

### 4.1 Gas explosion model

A gas explosion is a process of flame propagation through a flammable mixture. The increase of

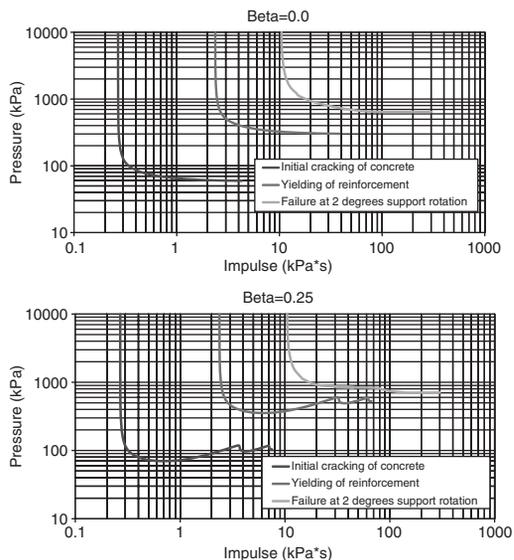


Figure 8. P-I-diagram with iso-damage curves for a tunnel separation wall with  $\beta = 0.0$  (top) and  $0.25$  (bottom) respectively.

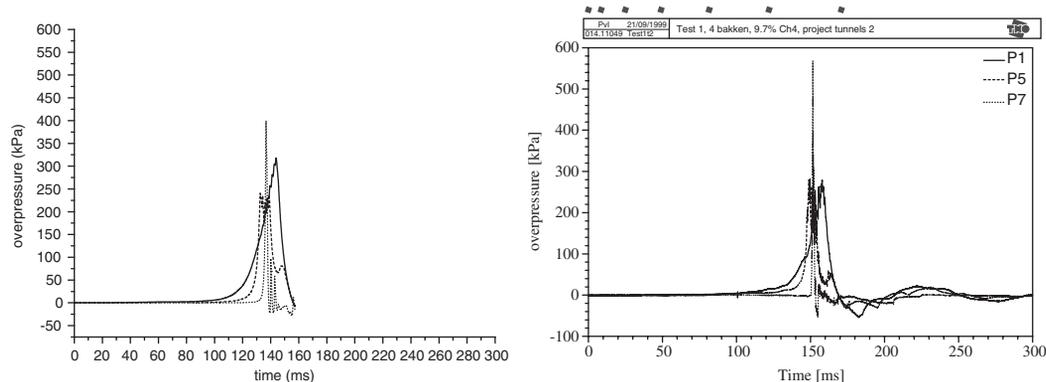


Figure 9. Numerically simulated (*left*) and experimentally observed (*right*) overpressure–time development at 3 stations along the channel length. Cloud of stoichiometric methane–air over  $1/4$  of the channel length (solid: closed channel end; dashed: halfway channel length; dotted: near channel exit).

temperature due to combustion induces an expansion flow in which the flame is carried along. The development of explosive combustion consists in the continuous interaction of the flame propagation process with its own expansion flow. The turbulent structure of the expansion flow, which is determined by the boundary conditions to the flow field, is the key factor in the development of this process. Full scenario simulation of a gas explosion requires, therefore, the three-dimensional simulation of all aspects of this complicated process: the gas dynamics, the (turbulent) flow structure and the flame propagation process.

In the gas explosion simulator AutoReaGas™ (TNO and CDL 2002), the full process of a gas explosion is modelled by a perfect gas that expands under energy addition through combustion:

- The gas dynamics of expansion is modelled by conservation equations for mass, momentum (Navier–Stokes equations) and energy.
- The turbulent flow structure is modelled by conservation equations for the turbulence kinetic energy and its dissipation rate.
- The flame propagation is modelled by a conservation equation for a reaction progress parameter in which the combustion rate is a source term.
- The composition of the diffusing cloud in the expansion flow is computed from a conservation equation for the mixture stoichiometry.

A special version of the AutoReaGas software was tailored to the problem of a gas explosion developing in a tunnel tube containing a standing traffic jam. The code was calibrated and validated on the results of the experimental program addressed in section 2 (De Maaijer et al. 2002).

The simulation of a realistic tunnel problem at full scale with presently available CPU, necessitates a

numerical mesh of approximately  $1 \text{ m}^3$  cell size. This is far too coarse to be able to resolve any physics of the flame propagation process. Therefore, the flame is modelled as a numerical interface, propagated at a burning speed that is prescribed through a theoretical relation with the characteristics of the turbulent flow structure (Peters 1999). In addition, special modelling was required to be able to simulate proper turbulence generation by coarsely resolved solid objects (the vehicles in the traffic jam).

#### 4.2 Model validation

To demonstrate the model's capabilities, two experiments from the experimental program in section 2.1 have been simulated. The channel including some open space around the exit was modelled in a numerical mesh of  $200 \times 20 \times 10$  cells of  $0.05 \text{ m}^3$ . A stoichiometric mixture of methane–air was specified over  $1/4$  and  $1/2$  of the channel length respectively and ignited in the centre of the closed channel end. The overpressure development was recorded at the same stations as in the experiments. The results are shown in Figures 9 and 10.

Figures 9 and 10 clearly demonstrate the capabilities of the software in various aspects. If the channel is filled with a stoichiometric cloud over  $1/4$  of the channel length, the overpressure runs up to more than 300 kPa and choking outflow conditions are met in the exit, witness the narrow pressure spike observed near the exit in Figure 9. If the cloud length is only  $1/4$  of the channel length, the overpressure developed is much lower and the outflow in the exit remains subsonic. Then the overpressure observed in the channel near the exit remains near-ambient.

The experiment with a cloud of  $1/4$  of the channel length (Fig. 10) is particularly significant because it

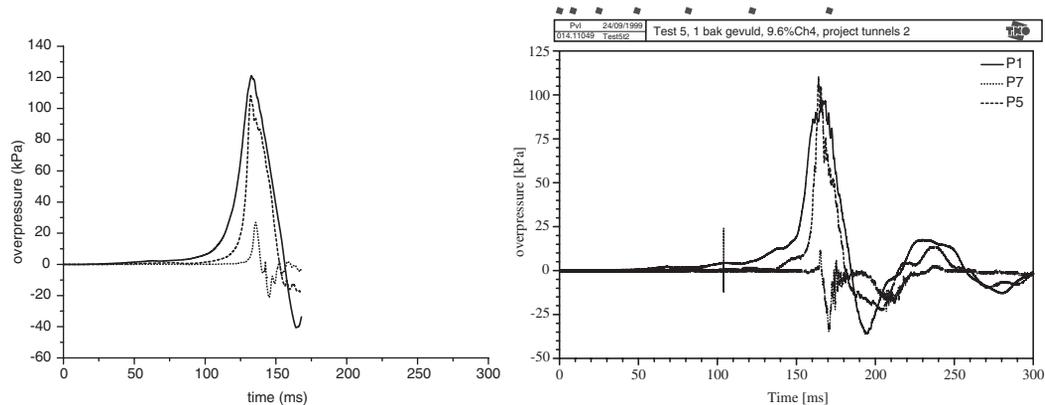


Figure 10. Numerically simulated (*left*) and experimentally observed (*right*) overpressure–time development at 3 stations along the channel length. Cloud of stoichiometric methane–air over  $\frac{1}{4}$  of the channel length (solid: closed channel end; dashed: halfway channel length; dotted: near channel exit).

covers various phenomena that play a determining role in the development of a gas explosion:

- The mixing of the flammable mixture with air in the expansion flow in front of the flame.
- The flame propagation in the continuously intensifying turbulent flow.
- The flame propagation through a non-homogeneous concentration field.

The computational results in Figure 10 show that the software is capable of a satisfactory simulation of the structure loading as a consequence of a realistic gas explosion scenario in a traffic tunnel.

## 5 CONCLUSIONS

A screening tool set to determine quickly the consequences in a wide spectrum of scenarios has been developed. A one-dimensional gas dynamic model of a gas explosion computes the pressure loading and, subsequently, damage criteria in pressure–impulse graphs determine the response of the tunnel structure. This tool requires input in terms of flame propagation behaviour in tubes.

As long as the flammable cloud length covers the greater part of the tunnel length, the simplified one-dimensional model of a gas explosion is capable of computing the pressure loading with a satisfactory accuracy. However, for smaller cloud lengths, the mixing of the flammable mixture in front of the flame becomes a significant phenomenon. Because the screening tool lacks the possibility to describe this phenomenon, it will substantially overestimate the pressure loading of the tunnel structure for smaller cloud length.

A tool set for detailed numerical simulation has been developed. A three-dimensional CFD gas explosion simulator is capable of computing the consequences of any gas explosion scenario as well as the effects of any possible mitigating measure in detail. The resulting blast loading may serve as input to a FE-model that is able to simulate the dynamic response of the tunnel structure.

The three-dimensional gas explosion simulator has shown to be able to reproduce the entire complex of phenomena that determine the development of a gas explosion in a satisfactory way. Combined with the screening approach a proper tool box is available to quantify the gas explosion loads in tunnels.

In analogy with the CFD explosion solver, the numerical response calculations with FE-codes will be applied when the global response schematisation is insufficient (e.g. dominant high frequency response; more accurate damage prediction required; 3D effects).

With the research into gas explosion phenomena in tunnels and the developed tools, TNO PML realised the required basis for sound hazard analysis for the transportation of hazardous materials through traffic tunnels. The gained expertise will also be applied for the development of explosion suppression equipment.

## REFERENCES

- Biggs, J.M. 1964. Introduction to structural dynamics. New York: McGraw-Hill Book Company.
- Boris, J.P. 1976. Flux-corrected transport modules for solving generalized continuity equations. *NRL Memorandum report 3237*. Washington D.C., USA: Naval Research Laboratory.

- Catlin, C.A. 1991. Scale effects on the external combustion caused by venting of a confined explosion. *Combustion and Flame* 83: 399–411.
- Catlin, C.A. & Johnson, D.M. 1992. Experimental scaling of the flame acceleration phase of an explosion by changing fuel gas reactivity. *Combustion and Flame* 88: 15–27.
- De Maaijer, M., Van den Berg, A.C. & De Bruijn, P.C.J. 2002. VOI – tunnel safety: Small-scale experiments and numerical simulation of gas explosions in tunnels. TNO-Prins Maurits Laboratorium report nr. PML 2002-IN##.
- Peters, N. 1999. The turbulent burning velocity for large-scale and small-scale turbulence. *Journal of Fluid Mechanics* 384: 107–132.
- Steen, H. & Schampel, K. 1983. Experimental investigation on the run-up distance of gaseous detonations in large tubes. *4th Int. Symp. on Loss Prevention and Safety Promotion in the Process Industries, 1983*. Symposium Series No.82: E23–E33. The Inst. of Chem. Engineers.
- Taylor, P.H. & Hirst, W.J.S. 1988. The scaling of vapour cloud explosions: a fractal model for size and fuel type. *Poster presented at the 22nd Int. Symp. on Combustion, Seattle, USA, 1988*.
- TNO & CDL, 2002. AutoReaGas™ – The interactive software for reactive gas dynamics and blast analysis. TNO Prins Maurits Laboratory and Century Dynamics Ltd.
- Van den Berg, A.C., Rhijnsburger, M.P.M. & Weerheijm, J. 2001. Guidelines for explosion loads and structural response of traffic tunnels (in Dutch). TNO Prins Maurits Laboratory report no. PML 2001–C121.

## Scenario Analysis for Road Tunnels

D. de Weger

*Civil Engineering Service, Ministry of Public Works and Water Management (Steunpunt Tunnelveiligheid),  
 LA Utrecht*

**ABSTRACT:** Risks of tunnel accidents are not only measured by probabilistic quantitative risk analyses, also more qualitative scenario analyses are an important contribution to achieving an optimal tunnel safety level. Scenario analyses may be carried out during all stages of the development process. Most of the experiences up to now result from scenario analyses during the design stage, at the point where only a limited number of tunnel design options have survived. The scenario analysis described in this paper aims at optimising the management of the processes occurring before, during and after an accident. The focus is on self rescue and emergency response. At an earlier stage, a scenario analysis may be useful when making an overview of the required safety measures for both large and small scale accidents. Furthermore, scenario analyses may be input to the decision making process regarding the construction of a tunnel.

In this paper, scenario analyses for road tunnels are described from the point of view of (i) the organisational and administrative environment, (ii) the differences between quantitative risk analyses and scenario analyses, (iii) the structure and elements of a scenario analysis. Furthermore, the first version of the Guideline Scenario Analysis for Tunnel Accidents and some preliminary application results are reported.

### 1 INTRODUCTION

Risk analysis in the Netherlands is carried out in two ways. In the early 1970's the Dutch government adopted the probabilistic risk evaluation as the leading philosophy for the Dutch safety policy. Quantitative risk analyses was strongly supported and widely applied as a decision making tool in land use and spatial planning. Especially risks of fixed industrial facilities were evaluated with a QRA (VROM, 1979).

The other view is advocated by those responsible for emergency response, such as the fire brigade, police and health department. Their interests lay not so much with the number of deaths but rather with the possibilities of casualty reduction, i.e. the number of wounded who can be rescued and transported to hospitals or other locations where they can receive proper treatment. According to this view, a risk evaluation should focus on optimising the emergency response processes, both technically and organisationally. This type of questions is concerned with specific accident scenarios, including the pre-accident events and the role played by the response services and the technical facilities. Probabilities are not of primary interest, or are even disregarded completely (Ministry of the Interior, 1995).

One could say that the quantitative risk analysis and the scenario analysis are located somewhere

between a full probability (or frequency) analysis and a consequence analysis (see Figure 1). Fortunately, in the Netherlands the contradictions between both views are losing ground in favour of the similarities, which is for example illustrated by the development of an integrated tunnel safety philosophy by the Dutch Civil Engineering Service (Centre for Tunnel Safety, 2001).

### 2 CURRENT STATUS OF SCENARIO ANALYSIS

#### 2.1 Scenario analysis during the design and construct process

Ask five tunnel safety experts to define a "scenario analysis" and you will probably get five different

Probability (frequency) analysis	Probabilistic approach (quantitative risk analysis)	Deterministic approach (scenario analysis)	Consequence analysis
--	--	---	-------------------------

Figure 1. QRA and scenario analysis at the scale between probability analysis and consequence analysis.

answers. The meaning of the term scenario analysis is strongly influenced by someone's perception of the moment in time when the scenario analysis is to be carried out, especially as related to the different tunnel design and construction stages.

In the earliest design phase, the general objective is to give a global definition of the required solution. A typical question at this stage would be "Are we going to build a bridge or a tunnel?" Part of answering such a question is a general risk inventory, which provides insight into the relevant risks of both alternatives and which may also help drawing up the guidelines for possibly required documents such as an Environmental Impact Assessment.

As the design process goes on, the selected options gradually will become more specific. Consequently, at the later stages the level of detail of the analyses increases ("from coarse to fine"). Prior to the actual design, the safety objectives have to be written down, which requires a very general scenario analysis. During the design process, a qualitative scenario analysis may be carried out, which may include a few indicative calculations. Typically, at this stage also a Quantitative Risk Analysis would be suitable.

When optimising the final design – which by that time has already passed the QRA-test – a more detailed Scenario Analysis is appropriate. At this stage, the technical and organisational safety measures have to be defined and agreed in detail.

Finally, during the construction and operation phases of the tunnel, design modifications may be implemented because of which a repeated QRA and/or SA is necessary.

## 2.2 Scenario analysis organisation

A striking difference between QRA and SA is their organisation. Generally speaking, a QRA will be carried out by one or more risk analysis experts who are supported by tunnel construction experts. In the Netherlands, the Terms of Reference of the QRA have to comply with official regulations. The analysis itself will to a great extent be carried out by dedicated experts on their own, while the other parties such as the tunnel owner and the authorities will be part of the steering committee which is only involved at certain moments in time.

For scenario analyses, things are different. A scenario analysis is acknowledged more and more as an essential part of the overall risk evaluation, complementary to the QRA. An SA is carried out by an analysis team that actively contributes during every stage of the analysis. A typical scenario analysis team will consist of the representatives of the local and regional authorities, the tunnel owner and operator, the emergency response services and one or more scenario analysis experts. Up to now, no official SA guidelines

exist. However, the Dutch Civil Engineering Service of the Ministry of Public Works has issued a first version of preliminary guidelines for road tunnels which are going to be tested in a few pilot studies this year (De Weger et al. 2003). Most of the current paper is built around material and experiences from the development of these preliminary SA guidelines.

## 3 QUANTITATIVE RISK ANALYSIS VS. SCENARIO ANALYSIS

A quantitative risk analysis (QRA) and a scenario analysis (SA) are strongly related to one another. In fact, they are variations of a combined, probability-and-consequence-analysis. Both consider the effects and consequences of unwanted events which are described as "accident scenarios", and in both analyses probabilities play a certain role. The differences between QRA and SA are e.g. that in a QRA probabilities are specifically taken into account, while a scenario analysis focuses on the consequences.

The probabilistic risk assessment is the basis for the Dutch external safety policy for both fixed industrial facilities and the transport of dangerous goods. Consequently, in a probabilistic tunnel risk assessment the probabilities and consequences of a large number of accident scenarios are calculated. The aggregated results are presented as a complementary cumulative frequency diagram (CCFD or fN-curve), representing societal (or "group") risk; alternatively, the risk may be presented as the expected value. The use of individual risk contours as a measure of internal tunnel safety is not very common; however, individual risk is used to indicate risk levels at both ends of the tunnel and alongside the tunnel area to evaluate the risks of severe accident (e.g. explosions) in the tunnel.

A Scenario Analysis, being a mere variation of a QRA, is built from the same elements as a QRA: (1) system description, (2) calculation of physical effects and damage (a.o. health effects), (3) calculation of frequencies and probabilities, and (4) risk presentation and evaluation. The focus of an SA is on optimising the accident process management. In an SA only a limited number of scenarios is analysed; however, each scenario is subject to a more thorough analysis than would be the case in a QRA. Especially, all accident processes, including population behaviour, status of tunnel safety measures, details of emergency response operations and of course the possible accident development scenarios are part of the analysis. Accident frequencies and accident development probabilities are for the greater part left out of the SA, which is an important contrast with a QRA. The results of an SA is not presented in graphs or diagrams but, depending on the required level of quantification, may be in a narrative form or as a combination of text

and (semi)quantitative information in a sequence of tables. Graphics may be used to illustrate the studied accident situations and their developments. If detailed calculations are carried out, their results will generally be presented in the analysis' appendices.

#### 4 ACCIDENT PROCESSES

A key concept in modern risk evaluation is the notion that an unwanted events does not arrive out of the blue but starts with some (often minor) disturbance of normal operation, which results in a minor or major accident, which in its turn may develop in several ways depending on the quality of the accident response, not only by the fire brigade and other emergency response services but also including human behaviour and technical and organisational safety measures. This concept has been developed in the process industries and is well known as the bow tie model (De Weger et al. 2001). In fact, the bow tie's knot in the middle represents the accident and links a fault tree at the left representing the cause part and an event tree at the right which stands for the consequence or "damage" part (see Figure 2).

The Bow Tie Model offers a widely accepted framework for risk reduction. It is immediately related to the accident chain, which in its simplest form consists of *cause – accident – consequence*, but in a more sophisticated way transforms into the emergency management sequence:

*prevention – preparedness –  
mitigation – response – recovery.*

One of the basic principles when applying the bow tie model is to look for safety enhancing measures in the front part of the accident chain. This principle expresses the preference of accident prevention. An important element in the bow tie model is the presence of Lines of Defence throughout the accident chain, each one of which serves as a starting point for safety measures. Examples of Lines of Defence to improve tunnel safety are automatic fire fighting systems such as sprinklers, automatic car or train speed detection, closed circuit television systems, communication equipment (telephones, public address systems), etc. But also incorporating safety into the car driving education programme or public awareness media campaigns will contribute to safety improvement and thus are some sort of line of defence.

The processes that are encountered before, during and after an accident are (De Weger et al. 2001):

1. disturbance of ordinary traffic;
2. incident;
3. incident detection and warning of operator and emergency response services;

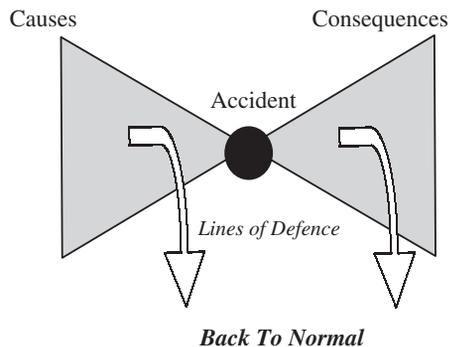


Figure 2. The Bow Tie Model.

4. self rescue by tunnel population;
5. response by fire brigade, police and health services.

Generally, stage 3 will be rather short. The start of stage 4 (self rescue) coincides with the start of stage 3. The response phase includes reconnaissance *i.e.* determination of the exact location of the incident, the number of vehicles involved, number of people in and outside the vehicles, and possibly present hazardous substances. As soon as all relevant information has been collected, the actual accident combatment will begin. This is for instance fire fighting, switching off electrical current (in case of train accidents), rescuing victims, and removing or covering hazardous substances.

During all stages, interaction occurs between all elements in the tunnel system. Traffic detection and regulation systems are meant to detect and if possible correct disturbances of the ordinary traffic conditions in order to prevent dangerous situations. Safety measures such as vehicle guiding barriers contribute to damage minimisation ("soft landings"). Self rescue is only possible if those present in the tunnel during or immediately after the accident are able to reach a safe haven, such as a rescue area or a tunnel tube which is not involved in the accident. Emergency response can only be successful if certain conditions are fulfilled, such as a quick alarm and proper communication with the tunnel operator.

A scenario analysis is carried out in order to find out whether the whole tunnel system, including all technical and organisational measures, is fit to deal properly with all relevant accidents and their possible developments and – if this is not yet achieved – which are the weak spots that have to be improved. This objective is different from that of a QRA, which is carried out to establish whether the tunnel meets the risk standards, as described in section 3.

## 5 SCENARIO ANALYSIS METHODOLOGY

A scenario analysis consists of the following elements:

- a. system description;
- b. selection of relevant scenarios;
- c. analysis of effects and consequences;
- d. evaluation of results and optimisation of design.

### 5.1 System description

Starting point of a scenario analysis is the preliminary design. This includes the tunnel itself, all mechanical and electrical installations like lighting, ventilation systems, communication equipment, traffic detection and warning systems, fire detection and fighting equipment, etc. The scenario analysis also comprises those parts of the tunnel operating organisation responsible for calamity response.

The public emergency response services can be activated by the tunnel operator, by a message from one of the tunnel users involved in an accident, or by a message from one of the other services. The tunnel operator is responsible for keeping all emergency pathways and doors accessible to the emergency response services. However, passing on the alarm to the responders on duty is the responsibility of the receiving party and does not belong to the tunnel organisation. Response service organisation is relevant insofar it directly influences the activities in the tunnel.

### 5.2 Scenario selection

Following the system description, the scenarios that are suitable for analysis are selected. For scenario selection a number of criteria have been determined. Scenarios should be realistic, test the system boundaries, and be representative and reproducible.

The first condition means that scenarios must be physically possible and acceptable to all parties involved. In order to reach agreement on the required safety level, all parties must support – or at least do not reject – the selected scenarios. Scenarios with extremely low probabilities or extremely high consequences should be selected only if all parties are convinced of their necessity, as too extreme scenarios will lead to oversized measures.

Maybe the most important criterium is that scenarios must test the system boundaries, because this is the actual goal of the scenario analysis: to find out whether the system's safety level is high enough, especially as far as the safety measures are concerned. This is best established by checking the performance of all system parts under unusual circumstances.

Thirdly, the set of scenarios must be representative and balanced. Scenarios should vary sufficiently in size and nature. The analysis should include “developing

scenarios” that start small, grow quickly and reach a full size calamity level. To limit the analysis effort, the number of selected scenarios should not exceed 5–10.

Finally, scenarios should be reproducible, *i.e.* the same scenario calculated for a different tunnel should lead to roughly comparable results.

To determine whether the criteria mentioned above have been met in an actual analysis, in the Guideline Scenario Analysis (see section 2) the user is offered a checklist referring to the tunnel and traffic properties are key factors in tunnel safety. The selected set of scenarios should cover all key safety parameters. The parameters have been derived from accident process descriptions, in which fault trees have been developed to identify the parameters that play a role in processes like the pre-accident phase, detection and alarm, incident, self rescue, and emergency response.

At a high level of abstraction the a set of scenarios would for instance be:

- car or train collision, train derailment;
- fire;
- release of hazardous materials.

Scenarios for road tunnels are different from those for train tunnels. Smaller fires, say below 10–20 MW, are distinguished from large fires, up to 300 MW in case of a fully loaded truck fire. In a road tunnel, the condition “congestion behind the accident” may severely increase the consequences especially in case of fire. An example of a set of scenarios that have been analysed for one of the new tunnels in the Netherlands is presented in Table 1.

### 5.3 Analysis of effects and consequences

Once the scenarios have been selected, the actual analysis can be carried out at a qualitative or at a quantitative level. The analysis framework is built around the accident processes mentioned before. Every process step relates to the transition from one time step to another. During the analysis, a “picture” is taken of every transition moment. Each picture gives an overview of the system status and in keywords, key-figures or brief text an account is given of

Table 1. Scenarios for road tunnels (Molag, 2001).

- |  |
|--|
| 1. Traffic disturbance without damage            |
| 2. Accident with material damage only            |
| 3. Accident with casualties (wounded)            |
| 4. Small car fire ( $\approx 5$ MW)              |
| 5. Bus fire, small truck fire ( $\approx 20$ MW) |
| 6. large truck fire (liquid, $< 300$ MW)         |
| 7. LPG BLEVE                                     |
| 8. LPG gas cloud explosion                       |
| 9. Accident with release of toxic liquids        |
| 10. Toxic gas release                            |

the system development in the previous accident development phase.

In the quantitative analysis, the “system pictures” are illustrated with calculated data like the number of people in the tunnel, the fire load, the effect distances and the numbers of casualties.

### 5.3.1 *Physical effect modelling*

The physical effects that may occur after an accident depend on the kind of accident and on the involvement of hazardous substances. The majority of accidents only causes material (vehicle) damage. Bigger accidents, for instance a fire, may occur in vehicles with or without dangerous substances. The absence of hazardous materials however, does not necessarily limit the accident consequences. Possibly the best known example of an “ordinary fire” with dramatic consequences is the Mont Blanc Tunnel Fire, where a truck loaded with flour and margarine caused a large fire with a lot of casualties (Ministère de l’Interieur, 1999); (Guigas, 2001). If a fire occurs, not only the skin burns due to direct heat radiation is important. Health damage may also be caused by high temperatures of the tunnel atmosphere (lung damage) and by exposure to the smoke which contains a cocktail of toxic compounds.

The accident development in terms of fire development, temperature increase, smoke dispersion and behaviour of other hazardous substances, may be calculated with the effect models that are well known from quantitative risk analysis (outflow, evaporation, dispersion, various types of explosions, etc). These models have been developed for application in the open air; for calculations in tunnels some of these models can be applied directly. Because of the properties of a tunnel, however, calculation of some of the substance behaviour phenomena requires specific models (Kootstra & Molag, 2003).

For instance, in ordinary outflow models a standard pool surface is assumed which is only dependent of the underground type (small, e.g. 1500 m<sup>2</sup> for permeable surfaces such as sand or little rocks, or 10,000 m<sup>2</sup> for a flat smooth surface). Modelling of liquid outflow in a tunnel has to take into account the slopes at both ends of the tunnel and the sewer facilities. A release at the entrance of the tunnel will flow downwards and form a large but shallow pool, from which the initial evaporation will be very high but during a short period of time. Pool formed at the bottom of the tunnel may be readily dispatched of by the sewers, which will result in smaller surface areas.

Another, more important difference between tunnels and open air is the modelling of smoke dispersion. In a contained space like a tunnel, hot gases will initially spread in the upper layer just below the tunnel ceiling. After some time the smoke will cool down and will mix with the cooler air layer in the lower part of the

tunnel. In case of a burning fire, an air flow is generated in the direction of the fire; the cooling smoke that mixes with the tunnel air will be transported towards the fire. This effect is not described by ordinary dispersion models. Furthermore, vehicles and other obstacles in a tunnel may significantly influence gas dispersion. For temperature development and smoke dispersion in complex environments like tunnels special models have been developed, varying from relatively simple zone models (Rylands et al. 1998) to sophisticated CFD models (Rhodes, 1998).

### 5.3.2 *Tunnel population modelling*

The number of victims is directly proportional to the number of people present in the tunnel, which in turn is a result of the in- and outflow. Increase of the tunnel population is caused by the continuous traffic flow. On the other hand, the tunnel population is reduced by “natural outflow” (cars downstream driving out of the tunnel), self rescue (drivers and/or passengers who may or may not be injured leaving the incident location on their own), and organised evacuation by tunnel personnel or emergency response services.

Incoming traffic may be stopped relatively easy. Car tunnels may simply be closed off by traffic lights or barriers at the tunnel entrances. This is in general the tunnel operator’s responsibility.

Trains on their way towards a tunnel can also be stopped easily. The tunnel operator or the emergency service in charge has to instruct the train traffic control centre. This is an additional communication step, which may cause some delay in the closing down procedure.

In the Guideline Scenario Analysis, “natural outflow” is only part of the evaluation if it is blocked by congestion downstream of the accident. The combination of fire and congestion may cause severe exposure of the people in the downstream part of the tunnel; if there are inadequate emergency exit facilities this will result in a significant increase of the number of casualties.

### 5.3.3 *Self rescue*

Self rescue may be measured by the total time required to reach a safe area. This time period is determined by (a) the wake-up period, *i.e.* the time needed for the tunnel users to realise the seriousness of the situation and take action, and (b) the fleeing period, which is directly dependent of the fleeing speed and distance to the next emergency exit. The total self rescue time appears to be dominated by the wake-up period. A large evacuation experiment carried out last year in the Dutch Benelux-tunnel in the Rotterdam Port area (Centre for Tunnel Safety, 2002) demonstrated that the wake-up period can last as long as 5–10 minutes, even if car drivers are watching the smoke coming out of a truck which is on fire. Furthermore, the experiments

demonstrated that the attention level and visibility of the emergency routes and exits may significantly influence the total self rescue time.

There are several other factors that influence the self rescue speed. If a tunnel is provided with a public address system, if good information texts have been prepared and if the operators are properly instructed about how to use the system, this may greatly improve the self rescue effectivity and efficiency. It is very important that messages are issued timely and repeated at regular intervals, that the texts are clearly audible and that the contents of the messages is consistent. Informing train passengers is easier than trying to reach car drivers. Furthermore, car drivers are more apt to stick to their vehicle, while it is easier to mobilise train passengers as they will be showing group behaviour. Apart from this, technical details like the width of the fleeing pathway, the percentage elderly and handicapped and the total number of fleeing persons will influence the self rescue performance of the whole system.

Self rescue models offer both qualitative and quantitative representations of human behaviour. Qualitative models are found in psychology and are descriptive models (Galea, 1999); (Steyvers, 1999); (Helbing, 2000); (Centre for Tunnel Safety, 2002). Quantitative models such as Exodus or Simulex calculate the escape time from parameters such as distance, walking speed and escape route capacity. There are three "sub-categories": rules of thumb, which are relatively simple, empirically based formulae; physical models in which population movement is modelled as particle flow; and computer simulation models, which combine elements from the previously mentioned categories. Every model category has its own advantages and disadvantages. Psychological models lack a firm quantitative basis. The basic assumption of particle flow models is that human behaviour much resembles ideal gas behaviour. In tunnel evacuation experiments however, strong evidence for deviating behaviour has been found. When escaping from a tunnel in dense smoke, exit visibility is an important factor for humans which is not accounted for by ideal gas models. Computer simulation models combine a sophisticated approach with a lack of transparency: the model relationships are often not specified in the programme documentation which gives these models much of a "black box-nature".

The (preliminary) conclusion that has been drawn for the Guideline Scenario Analysis is that at the moment the best possible self rescue predictions are offered by a combination of a qualitative (psychological) analysis and application of empirical models (rules of thumb). The latter produce mere indicative results that are at the same time a sufficient description of self rescue behaviour. Their greatest advantage is their simplicity. Approaches in the quantitative

models should be tested with a qualitative analysis. If it is assumed, for instance, that every person inside the tunnel will start escaping within 2 minutes after the accident, it should be demonstrated that the facilities enable such a quick response.

Computer models are an interesting, though expensive, alternative option. Most software programmes, however, lack the transparency which makes rules of thumb so easily accessible.

#### 5.3.4 Organised evacuation

Evacuation of the tunnel population by the emergency response services can only start after one of these services has arrived on the accident scene and has established which operations can be carried out safely (reconnaissance). Furthermore, roll-out of response equipment will take some time. Actual saving of people trapped in cars or trains may not start earlier than 20–30 minutes after the accident. Therefore, self rescue is seen as the primary source of casualty reduction (Bockholts et al. 1999). The emergency response operations contribute to fire fighting, clearing the tunnel and providing professional health care to the injured with zero or limited mobility.

#### 5.3.5 Health effect modelling

Health damage is evaluated from two points of view: the self rescue capacity and the need for health care. Firstly, health impairment will decrease the self rescue abilities and thus increase the number of victims. This is important in a scenario analysis, as safety measures like the number and spacing of emergency exits immediately affect the number of casualties.

Secondly, a scenario analysis will evaluate the planned health service capacity, *i.e.* will there be enough personnel to give first aid and preliminary treatment, and do the health services provide sufficient ambulances for transportation of the casualties to a hospital.

In the Guideline Scenario Analysis, two health effect classification systems are used. For self rescue evaluation, a classification system was adopted that has been developed by the American Industrial Hygiene Association (AIHA, 2002). It divides health effects into four categories (detectability, discomfort, disability and death). The transitions from one category to another are marked by the so called Emergency Response Planning Guidelines (ERPG-1, -2 en -3). The ERPG-1 is the maximum airborne concentration below which nearly all individuals could be exposed for up to one hour without experiencing other than mild transient adverse health effects or perceiving a clearly defined objectionable odor. The ERPG-2 is the maximum concentration below which exposure for up to one hour would cause no irreversible or other serious health damage or symptoms that could impair an individual's ability to take protective action.

Exposure to concentrations below ERPG-3 is tolerable for nearly all individuals for up to one hour without experiencing or developing life-threatening health effects. Above ERPG-3, life-threatening health effects are to be expected when exposure lasts more than an hour.

Because human responses do not occur at precise exposure levels – they can extend over a wide range of concentrations – the values derived for ERPGs should not be expected to protect everyone, but should be applicable to most individuals in the general population. For scenario analysis purposes, recalculation of ERPG-values for shorter exposure durations seems appropriate, since self rescue will start immediately after an accident and emergency response will in general start effectively some 20–30 minutes after the accident.

For health service response the so called triage classification methodology is used, which has already been in use with the military for a long time (De Boer, 2000). This classification system is based on health care urgency. There are three categories: T1-patients need immediate care; if treatment does not start within one hour, patients in this category will probably die. Patients who need treatment within 6 hours are classified as T2. For patients classified as T3, first aid is sufficient.

Concentrations below ERPG-1 or below ERPG-2 will not affect an individual's self rescue ability. Between ERPG-2 and ERPG-3 self rescue is reduced, and people exposed at levels above ERPG-3 will not be able to reach a safe haven without help.

As regards health care urgency, the triage categories do not relate directly to the ERPG-categorisation (Van der Torn, 2003). As for mechanical injuries, T1-victims may still have their full self rescue abilities. On the other hand, toxic T3-victims exposed to an organic substance with anaesthetic properties may have lost their self rescue abilities, while health care is not urgent at all.

## 6 EVALUATION AND OPTIMISATION

The results of the qualitative and quantitative analysis are evaluated against criteria on prevention, mitigation, self rescue and emergency response. This is consistent with application of the Bow Tie Model where safety measures are preferably taken early in the accident chain.

Evaluation of the safety performance of a tunnel is done by comparing the qualitative scenario descriptions of the different tunnel alternatives. In a full quantitative scenario analysis, the numbers of casualties that are expected to occur in the tunnel options may be compared with each other. A more sophisticated evaluation method is based on casualty distributions, which may be calculated from the distributions of the

underlying parameters, like spill volume development, fire growth, distance to accident, individual evacuation speed, exit door capacity, etc.

Currently, no generally accepted evaluation criteria have been found in the Dutch regulation or in literature. In recent studies, prevention, self rescue and emergency response were measured by means of qualitative histograms. In this approach, alternatives are compared without being judged as to their absolute safety performance. It is expected that upon issuing the Guideline Scenario Analysis tunnel-specific criteria will be established by those responsible for the scenario analysis. A view shared by participants of a working party during the development of the Guideline is, that (a) prevention, mitigation, self rescue and response must meet certain minimum standards, but (b) exchange between these four parameters is acceptable (De Weger, 2002). Consider for instance additional mitigation measures with a safety benefit of X at a certain cost; if additional response measures would result in a similar safety benefit against lower costs, this measure is to be preferred, provided that both mitigation and response meet the minimum standards.

## 7 CONCLUSIONS

Scenario analysis is a tool that fills the gap in the deterministic field next to quantitative risk analysis. In tunnel risk evaluation, scenario analysis can be used at different stages, both early and later on. Scenario analysis provides a qualitative description of the accident development at several critical stages. Models for the calculation of physical effects and casualties in most cases are not the same as models for risk calculation in an open environment. The results of behaviour models and health effect calculations have to be used cautiously. At the moment, given the current state-of-the-art, evaluation and optimisation have to be carried out based on tunnel-specific evaluation criteria.

## ACKNOWLEDGEMENTS

The work presented in this paper has been commissioned by the Netherlands Centre for Underground Constructions (*Centrum voor Ondergronds Bouwen*, COB) and was largely funded by the Civil Engineering Service of the Ministry of Public Works and Water Management.

## REFERENCES

- AIHA, 2002. Washington: American Industrial Hygiene Association, <http://www.aiha.org/publicationsadvertising/html/poerpgweels.htm>

- Bockholts, P. et al. (1999). *Integrated Safety Plan Westerscheldetunnel* (in Dutch). Terneuzen, NV Westerscheldetunnel.
- Centre for Tunnel Safety (2001). *Project Plan Integrated Safety Philosophy*. Utrecht: Civil Engineering Service, Rijkswaterstaat.
- Centre for Tunnel Safety (2002). *Safety Test*. Utrecht: Civil Engineering Service, Rijkswaterstaat.
- De Boer, J. (2000). Order in chaos: modelling medical management in disasters. In: De Boer, J. & Dubouloz, M. (eds), *Handbook of Disaster Medicine*. Utrecht: VSP International Science Publishers.
- De Weger, D., Hoeksma, J., Schaaf, J. van der (2001). *Process Descriptions MAVIT* (in Dutch). Utrecht: Bouwdienst RWS (Ministry of Transport, Public Works and Water Management, Civil Engineering Division).
- De Weger, D., Waterschoot, A. van. Vliet, C. van der, Jonkman, S.N. (2002). *Report of the Workshop Scenario Analysis Tunnels* (in Dutch). Utrecht: Bouwdienst RWS (Ministry of Transport, Public Works and Water Management, Civil Engineering Division).
- De Weger, D., Waterschoot, A. van. Vliet, C. van der, Jonkman, S.N. (2003). *Ontwikkeling Leidraad Scenario-analyse Tunnels* (Development of a Guideline Scenario Analysis in Tunnels, (in Dutch). Utrecht: Bouwdienst RWS (Ministry of Transport, Public Works and Water Management, Civil Engineering Division).
- Galea, E.R., Owen, M., Gwynne, S. (1999). Principles and Practice of Evacuation Modelling – A Collection of Lecture Notes for a Short Course. 2nd Edition 29
- Guigas, X., Weatherill, A., Trotter, Y. (2001) New Mont Blanc Tunnel Ventilation Systems. In: *Tunnel Management International* 4(1): 7–13.
- Helbing D., Farkas I., Vicsek T. (2000) Simulating dynamical features of escape panic. In: *Nature* 407, 487–490.
- Kootstra, F. & Molag, M. (2003). Applicability of Physical Effect Models for Accident Scenario's in Tunnels. Apeldoorn: TNO.
- Li, S., Harvey N. (2001). Simulation of escape from road and rail tunnels using SIMULEX. In: A.E. Vardy (ed.), *Proc. of Safety in Road and Rail Tunnels Madrid, Spain, 2–6 April 2001*: 323–334. Bedford: University of Dundee.
- Ministère de l'Intérieur, 1999. *Mission administrative d'enquête technique sur l'incendie survenu le 24 mars 1999 au tunnel routier du Mont Blanc*. [Http://www.equipement.gouv.fr/actualites/rapport\\_tmb.htm](http://www.equipement.gouv.fr/actualites/rapport_tmb.htm)
- Ministry of the Interior, 1995. *Fire Safety Concept*. The Hague: Ministry of the Interior, Directorate Fire Services and Crisis Management.
- Molag, M. (2001). *Scenario Analysis for the Leidsche Rijn Tunnel Options*. Apeldoorn: TNO.
- Rhodes, N. (1998). The accuracy of CFD modelling techniques for fire prediction. In: A.E. Vardy (ed.), *Proc. of the 3rd International Conference on Safety in Road and Rail Tunnels, 9–11 March, Nice*: 109–115. Bedford: ITC/University of Dundee.
- Rylands, S., Davis, P., McIntosh, A.C. & Charters, D.A. (1998). Predicting Fire and Smoke Movement in Tunnels Using Zone Modelling. In: A.E. Vardy (ed.), *Proc. of the 3rd International Conference on Safety in Road and Rail Tunnels, 9–11 March, Nice*: 127–138. Bedford: ITC/University of Dundee.
- Steyvers, F.J.J.M., Waard, D. de, Brookhuis, K.A. (1999). *General Aspects of Tunnel Use and Safety* (in Dutch). COV 99-09.
- Van der Torn, P.(to be publ.).
- VROM, 1979. *Omgang met Risico's* (Dealing with risks, in Dutch). The Hague: Ministry of Housing, Spatial Planning and the Environment.

## Risk based maintenance of civil structures

G.H. Wijnants

TNO Building Research Dept. Civil Infrastructure, Delft, Netherlands

**ABSTRACT:** The use of risk based maintenance approaches for civil structures today are limited to relatively few specific cases. Nevertheless, application of the methodology provides the means needed in present society where ageing constructions, multiple use of the built environment and increasing intensity of transport and travel introduce the need to reassess and manage the safety of the situation encountered.

This article presents the requirements that have to be met in order to incorporate enduring cost-effective risk-assessment procedures for the risk-management of large structures – with lots of components and approaches – by combining various approaches in one information model. The volatility of present cost-intensive risk-assessment methods, which disables many applications, is tackled by categorising the determining factors using “typicals”.

### 1 INTRODUCTION

#### 1.1 Risk management principle

The principle of risk management in order to manage both ongoing costs and failure probabilities is clearly gaining acceptance and interest. Important leaps are made in the last decade due to the awareness in Industry that risk based maintenance strategies provide a basis for knowledge management while complying with the need for cost-effective processes. The fact that approaches have been found in which encountered results can be reviewed using practical perspectives without “black-box” assessment types, finally has transformed scepticism into support for rational approaches.

In the process of civil maintenance management, nevertheless, the use of risk management concepts is still mostly limited to processes where priorities have to be set for quality management during construction and safety control. Explanations for the lack of use of risk concepts during the maintenance phase can be found in the fact that the failure probabilities are related to safety measures for structural failure and therefore set that low, that the effect of common maintenance procedures are hard to link to those probabilities. Besides, the empirical approach followed in most maintenance processes does not comply well with probabilistic approaches.

In order to integrate the benefits of rational risk based approaches in the empirical maintenance process, a couple of barriers have to be addressed and

tackled. One dominant barrier is the inaccessibility of deterioration models; another is the elaborateness of risk calculation procedures and the volatility in time of data incorporated. Nevertheless, due to the fact that it is only cost efficient for a few situations to require *detailed* analyses while most situations can adequately be approached using straightforward *first order* failure and risk predictions, an approach that combines the strengths of *both* approaches will provide clear yields. As a first step to such an approach, the requirements that have to be met are to be stated and integrated in one approach.

### 2 REQUIREMENTS

The requirements to be met by risk-based maintenance information models are stated. These requirements will be implemented by examples in section 3.

#### 2.1 Durability of input parameters

The circumstances of use that determine the deterioration mechanisms and the consequences of failure, vary with time. Since a durable approach that describes reality is needed, the parameters involved should have a specific durability for changes with time. This means that decisive parameters are to be categorised in clearly discerned groups in order to provide descriptions that are change resistant, easy to maintain and hence easy to maintain.

## 2.2 Mutual compatibility of multilevel approaches

The deterioration mechanisms present can be described accurately by incorporating much detailed influence factors while on the other hand in many cases effective values using integrating parameters provide sufficient accuracy. Therefore first order deterioration models should be applicable that are upgradeable to second and third order approaches when increased accuracy and detail is beneficial. Of course, in order to safeguard safety, the first order models should provide a more extreme image in comparison with the more detailed approaches.

## 2.3 Unambiguous risk assessment criteria

In order to provide unambiguous effect assessments in comparison with other risk assessment models used, the effects accounted for in the models should comply with the approaches used in the assessment of other safety systems. This implies that the most crisp consequence assessment methods will prevail above qualitative methods. In this case the IEC61508 assessment method is viewed to have the best qualifications for a leading role.

## 2.4 Delivery of an "HSE operating window"

The possibility of safe maintenance approaches (with respect to legal requirements for Health, Safety and Environment, "HSE") that nevertheless pay too little attention to the economic risks should be tackled. Hence within the boundary values imposed by HSE measures, optimisation of the integral costs of maintenance and failure should take place.

## 2.5 Tagging of actual, agreed and optimal situation

In order to enable optimisation evaluations, maintenance intervals that have been determined by cost effective clustering with other activities, should be clearly discernible from those activities that have excessive maintenance demand or a shortage in maintenance. These triple states of every maintenance system should be clearly discernible in order to facilitate efficient evaluations.

## 3 APPROACH

The next straightforward approach with focus on maintenance interval assessment has been implemented in actual practise and has yielded effective results over approximately 4 years now.

## 3.1 Quantitative deterioration prediction

The deterioration mechanisms to be expected are to be evaluated by quantitative measures. The bottom line is a level I approach, which has the next characteristics.

It contains four predictability levels, 4 to 1, comparable with cost prediction levels (see Nowak A.S. 2002), that relate to an absolute effective deterioration rate. These levels have the next qualities: 4 =  $\pm 100\%$ , 3 =  $\pm 50\%$ , 2 =  $\pm 25\%$ , 1 =  $\pm 10\%$ . This can be described by predictability qualifications: 4 = "bad", 3 = "average", 2 = "good", 1 = "very good". One should be aware that this approach facilitates the description of situations with extreme behaviour between "no deterioration" and "extreme deterioration". These can be described by "bad prediction" and the "effective deterioration rate", represented by the centre value.

When this level I approach is too costly due to its inaccuracy, a more accurate prediction of the deterioration process needs to be filled in. This process is characterised by validated description of mechanisms such as the S-N curves for fatigue in specific cases.

## 3.2 Tagging deterioration mechanism

The deterioration mechanisms ought to be tagged by "pattern-tag". This tag is needed in order to prove that the underlying mechanisms are understood and accounted for. Therefore discrimination into the next mechanisms is needed in order to enable predictions: a) *time* of use dependant behaviour (typically gradual corrosion processes) b) *load* dependant behaviour (typically mechanisms as fatigue related deterioration processes) c) *case* type behaviour (typically incident mechanisms like collateral damage up to a specific impact level, that cannot be foreseen but can be predicted using statistics) and finally d) *non-trendable* mechanisms.

The difference between c) and d) is that the "non-trendable" mechanisms are labelled as mechanisms that can cause overrun for the reliability limits that are to be met while maintenance is well performed.

All mechanisms a) to c) can be described by means of "overall" terms, using effective values. When a more accurate prediction is needed, what may result when there is a need for assessing the possibility of delay of planned preventive measures, a fitness for purpose approach needs to be implemented by introducing FORM or SORM methods.

An implementation of a maintenance system by means of a level I approach provides a "quick scan" when compared with the actual maintenance situation, thus enabling in a second step a more thorough evaluation of the items that appear to provide risk.

### 3.3 Recognisable category sizes that last

Unambiguous effect determination can only be achieved by creating effect categories that are clearly discernible given the variations in the actual "situation of use". As an example: a common situation as "the amount of passengers that are subject in traffic to a certain type of incident" can increase over the years with up to 15% per year (or 100% in 5 yrs). Hence it will be clear that an increment in effect size with a factor 10 can provide both durability of data for a period of at least 5 yrs and prevail ineffective discussions. For example for maintenance purposes, for which the serviceability limit state (SLS) is of interest, a cost category listing in groups as Catastrophic, Critical, Large, Marginal, and Negligible (respective limits 1 M€; 0,1 M€; 10 k€; 1 k€, smaller than 1 k€), will provide guidance. Within the SLS area, effects on health and environment are to be integrated into these categories as well.

### 3.4 Optimisation in "HSE maintenance window"

Within the maintenance intervals provided by safety requirements, the remaining failure rates and failure effects can still be responsible for excessive financial losses. Therefore within the time limits imposed by the "HSE maintenance window", the cost optimal interval is to be determined by assessing the minimum of preventive and corrective costs as a function of the interval.

Clearly the resulting interval does not bear an "imperative" but a "preferable" status.

The approach to be used for the cost optimisation needs to be unambiguous and not sensitive for personal interpretation. Primary direct effects of failures and secondary effects of repair actions are to be taken into account. For example for traffic flow this secondary effect can be assessed by incorporating the effects of incident rate and delay (both for user and equipment) to total costs  $C$  (see Ehlen 1997).

$$C = N * A_{dt} * \left( \left( \frac{L}{S_r} - \frac{L}{S_n} \right) * R + L * C_a * (A_r - A_n) \right)$$

with the parameters:  $N$  = number of days of work, number of passing vehicles  $A_{dt}$ , length of affected road  $L$ , normal and reduced traffic speed  $S_n$  respectively  $S_r$  and  $R$  = average of hour costs car + hour costs transported people,  $C_a$  is average costs per car due to an accident,  $A_n$  respectively  $A_r$  is average incident day-rate per km during normal respectively during road repair activities.

### 3.5 "Ist", "Soll" and "Darf" approach

In order to facilitate clear assessment of the actual situation which in this case relates to intervals, the next

system states need to be defined and retrieved in any risk assessment system: the "Ist" interval, which is encountered in the actual operational situation. The "Soll" interval, which represents the result of obligatory and optimisation procedures (internal factors), and finally the "Darf" interval, which represents the ultimate value as resulting from legislative requirements (external factors). When evaluations takes place, it should be clear at all times which characteristic intervals need to be compared with each other.

## 4 STEP BY STEP METHOD

In order to implement a risk-based approach a clear sequence of steps is recommendable in order to structure the process. A number of these steps are elucidated in the case descriptions in section 6.

The steps A–E discussed here are shown in fig. 1.

- Determine work packages (for example inspection and repair of inspected unit) that can effectively be treated as one approach within an "integrity unit". Such a package includes tasks that need to be taken in account and yet may be skipped during the actual process.
- Determine criteria for status assessment on "unit level", incorporating the possibility for groups of defects.
- Determine deterioration mechanisms and accompanying acceptance limits for defects.
- Determine ultimate maintenance intervals based on Health, Environment and Safety precautions (HSE window).
- Determine maintenance intervals based on cost-effectivity criteria, including activity clustering.

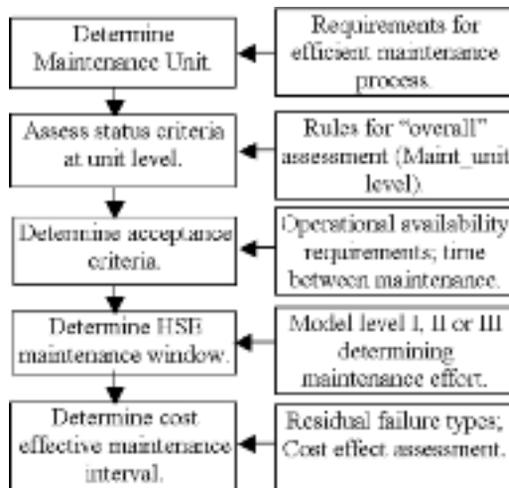


Figure 1. Steps for assessing unit level in RBM approach.

### 5 METHODOLOGY

In the methodology used, the assumption is made that the maintenance methods that have been selected comply with the specified performance and cost characteristics in that situation. This implies that evaluations

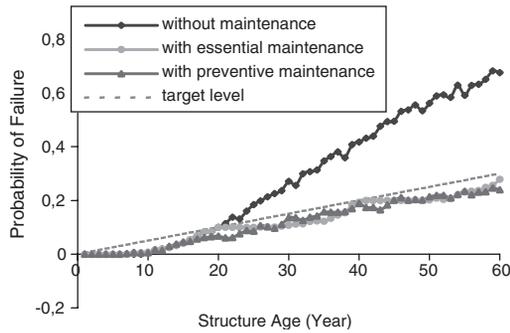


Figure 2. Probability of Failure for various maintenance approaches (Ying 2002).

have already taken place like the one shown in fig. 2, in which the effectivity of various maintenance concepts are evaluated, resulting in the selection of the appropriate approach.

So within the step by step method, only those maintenance processes are used that have proven to be effective.

So the problem definition is in this case: “given a specific set of effective maintenance procedures and a structure with specific deterioration characteristics, how often should specific tasks be applied”.

This question mainly focuses on determination of the rate of deterioration for a specific structure.

The methodology to tackle this question is depicted in the scheme shown below in fig. 3. One should note that in reality not all information is readily present in the format as displayed.

### 6 CASE DESCRIPTIONS

The next cases illustrate steps discussed in section 4. Accompanying models that are needed may differ

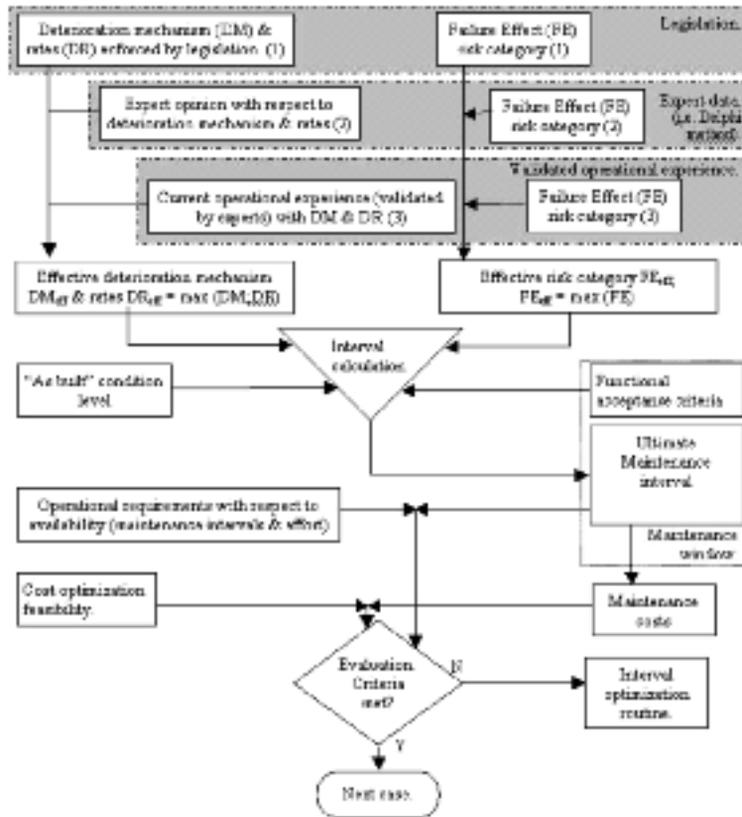


Figure 3. Integration scheme for deterioration mechanisms and failure effects.

widely and are therefore not discussed in this framework.

### 6.1 Painted steel bridges

In this case the definition of a cost effective work-package (steps A) and subsequent steps (-E) will be discussed.

In the case of painted steel bridges the deterioration mechanisms that ought to be addressed in the first step, is the deterioration of the steel itself due to lack of coverage, and the deterioration of paint due to the effects of shrinkage and cracking as influenced by weather circumstances.

A reliability approach based on the constructional failure is clearly linked to damage mechanisms in which relative large surfaces of the bridge will show corrosion (for a level III approach see Nowak 2002).

Without stepping to detail, it will be clear that the costs for repainting processes increase rapidly with the amount of corrosion. If this is not clear then this should strike the eye when viewing fig. 4.

Lets consider the perspective "under the circumstance that painting should be as cost-effectively planned as possible with the boundary condition that cost intensive corrective strengthening procedures are to be avoided". This approach clearly lies within the boundaries set by reliability requirements. A cost effective approach in this case, clearly provides a different view, especially when cost calculations incorporate secondary effects like traffic delay (see Purvis 1999).

The optimization that then takes place (step E) balances the costs that follow from interval reduction and job repetition against the increase in costs that arises due to the increasing intensity of paint and derusting activity in order to recuperate the layer.

In this case the definition of a cost-efficient work-package leads to restrictions that lie so clearly within reliability boundaries for the structure that exploration of the reliability details can be omitted.

### 6.2 Sewerage system

In this case of a buried sewerage system the maintenance typicals are defined as follows: periodic inspection by means of a preventive cleaning task followed by a camera inspection.

The acceptance limits that are needed in order to decide upon the optimal maintenance interval are determined by the next criteria: a) the groundwater level on a section of 1acre may not be changed with more than 0,1 m due to leaking into the sewerage system. This leads to an acceptance criterion based on effective performance criteria which are situation dependant. b) blocking occurring due to deformation

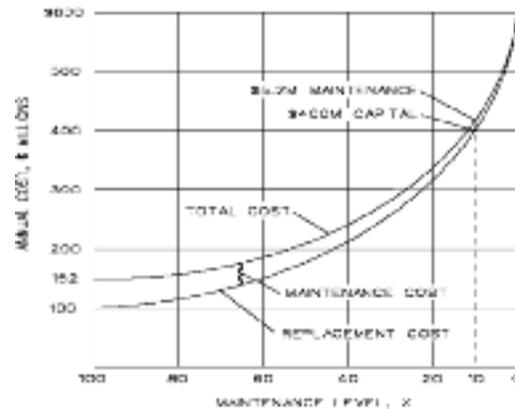


Figure 4. Costs increment as a function of maintenance level (100% = "well maintained") (Nowak 2000).

is allowable to the amount of excess capacity incorporated, which is typically 25%.

The failure mechanism that is dominant in this case, a concrete system, is leakage due to settling of the individual tubes. This mechanism (type a; gradual behaviour with time) has clearly predictable behaviour (overall rate: 0,01 m/yr.); corrective action will involve the system, not just parts.

Step A yields the "assessment unit level" in this case: from T-joint to other T-joint (multiple tubes; typical 16–160 cm Ø; inserts that are not able to "switch of" the infrastructure when being taken out of service are not being considered).

Using a level I assessment of the development of the failure rate for the system (step C; transferring settling rates to a prediction of misfit-aperture size and leakage rates) can lead to an assessment interval of 20 yr. (step D).

Using an repair decision criterion "functional acceptance criterion for new systems" (after inspection the system should be fit to for another 20 yr), step D results in a 20 yr, with a "functional level = 'as new'" acceptance criterion.

Within the timeframe of this HSE window, step E, the economic perception, yields the next perspectives: costs of inspection are smaller than 1% of an corrective measure (digging).

The time of initiation of leakage to exceeding the leakage level, can be determined to be 4 yr.

Incorporating step E within the HSE window, enables delay of corrective actions when adapting the acceptance limits. Since the costs involved are clearly smaller than the interest rate for a corrective costs, inspection is clearly a cost effective measure, complying with the functional requirements within the HSE window.

## 7 CONCLUSIONS

An approach has been presented in which a cost-effective implementation of timely maintenance tasks has been the starting point in order to implement a risk-based maintenance strategy.

The examples presented have shown that the next aspects need to be implemented in models in order to decide for cost-effective scenarios:

- the borders set by functional requirements yield a set of acceptance limits and maintenance intervals.
- within the borders set by functional requirements, cost optimisation with another set of both acceptance limits and maintenance intervals is possible.
- requirements applied should be clearly linked to limits and intervals determined in order to facilitate an unambiguous approach that meets the requirements set.
- the increase of labour effort with time (in terms of costs/m<sup>2</sup>) has to be modelled in order to yield an

adequate description of the actual situation, an effect that has been surpassed by previous approaches.

## REFERENCES

- Nowak A.S. and Thoft-Christensen P. 2002. In “International Contribution to the Highways Agency’s Bridge Related Research”, *Thomas Telford Publications, London*.
- Purvis R.L. 1999. “Integrating Preventive Maintenance Management into BMS”. *Proceedings international bridge management conference 1998*. Denver, Colorado. April 26–28, 1999.
- Li Y. and Vrouwenvelder T. 2002. “Probabilistic inspection and maintenance for concrete bridge structures”. *Proceedings of the First International Conference on Bridge Maintenance, Safety and Management IABMAS 2002*. Barcelona, 14–17 July 2002.
- Ehlen Mark A. 1997. “Life-Cycle Costs of New Construction Materials”. *Journal of Infrastructure systems*, Vol. 3, No. 4, 129–133, December 1997.

## Modelling a probabilistic safety management system for the Eastern-Scheldt storm-surge barrier, the basin and the surrounding dikes

A. Willems & P.B. Webbers

*Ministry of Transport, Public Works and Water Management. Department of Risk Analysis, Netherlands*

**ABSTRACT:** The Dutch government wants to have a computer model that calculates the annual probability of flooding the area around the Eastern-Scheldt. This model should also be able to determine the impact of maintenance and control management of the Eastern-Scheldt storm-surge barrier and dikes surrounding the basin. In this paper an approach is presented to obtain a model of this so-called safety management system using the design tool IDEF0. The model consists of a deterministic description of the system and will be translated into annual probabilities using Monte Carlo (MC) simulation.

### 1 INTRODUCTION

#### 1.1 Background

The Eastern-Scheldt storm-surge barrier was built from 1979 to 1986 to protect the south-west of the Netherlands against flooding. It consists of 62 moveable steel gates which only close in case of (expected) high water levels.

Together with the dike rings surrounding the Eastern-Scheldt, the second flood defence line, the Eastern-Scheldt storm-surge barrier forms the defence system that protects the hinterland against flooding. Of course, this flood defence system must be very reliable to guarantee an acceptable safety level of the hinterland. The Dutch government accepts a maximum annual probability of flooding of  $2.5 \cdot 10^{-5}$  for the storm-surge barrier and dikes surrounding the Eastern-Scheldt, and a maximum annual probability of flooding of  $2.5 \cdot 10^{-4}$  for the compartment dams. The reliability of the storm-surge barrier and dikes must be determined at least once every five years to see if they still meet these safety requirements.

In case of an oncoming storm the expected water levels on the Eastern-Scheldt are calculated by a water movement computer model. If the expected water level exceeds NAP<sup>1</sup> +3.0m the model will advise to close all 62 gates. For the Eastern-Scheldt storm-surge barrier the so-called “changing strategy” is in use on environmental considerations. This strategy implies specific moments of closing and opening

<sup>1</sup> Dutch reference plane.



Figure 1. The Eastern-Scheldt storm-surge barrier.

of the barrier. These moments lead to the adjustment of an average water level on the Eastern-Scheldt changing from NAP +1.0m to NAP +2.0m to NAP +1.0m et cetera.

It is important to emphasise that the moments of closing and opening of the barrier, given by the model, are only meant as an advise and should be evaluated and executed by humans. This is in contrast with the Dutch Maeslant storm-surge barrier near Rotterdam, which closes and opens fully automatically. There is one exception however: in case the water level near the Eastern-Scheldt storm-surge barrier *actually* reaches the level of NAP +3.0m all 62 gates close automatically. This is called the “emergency closure”.

Both the manual closure and the backup emergency closure are tested twice a year. Since 1986 the barrier has been closed twenty times for safety reasons.

Due to sea level rise, settlement of bottom level and deterioration of materials, the flood defence system must be maintained every year in order to keep up to the required reliability levels. Nowadays, the regular checks on reliability of the storm-surge barrier and the dikes are done separately. Good insight in the interactions between the reliability of both structure types in the total system is preferable. Since maintenance of both barrier and dikes is expensive, the economical benefit of such insight could be significant. For example, changing the closing strategy or maintenance of the storm-surge barrier could possibly allow no heightening of the dikes for many years.

### 1.2 Problem

From an economical point of view optimisation of maintenance for the whole flood defence system is more profitable than doing this for the individual parts separately. To make this optimisation possible we should be able to calculate the over-all reliability of the flood defence system and determine its impact on maintenance costs.

The Dutch government wants to have a computer model, which can automatically calculate the reliability of the flood defence system in probabilistic terms. This model must be compatible with both existing and future tests of dikes. Of course, it must be able to determine the effects of maintenance on the reliability of the flood defence system. An additional preferable feature is the determination of effects on the reliability due to changes in the closure strategy of the barrier. In other words, it would like to have a computerised safety management system (SMS).

One of the difficult matters is the time-dependency of the system in combination with the uncertainty of the water movements in the Eastern-Scheldt during a storm. For example, failure of the storm-surge barrier does not necessarily have to lead to flooding of the hinterland. This depends, among others, on the type of storm, the local water depths, the strength of the dikes and the capacity of the Eastern-Scheldt basin. Since this capacity is not exactly known, it is not only difficult to predict if flooding takes place, but also when this takes place.

Additional difficulty is the large amount of different storm types, together with the number of failure modes of the storm-surge barrier, for which the behaviour of water in the Eastern-Scheldt should be modelled. Furthermore, since only a very small number of these storms may lead to flooding of the hinterland, the SMS model should be able to deal with small probabilities.

It is therefore an interesting challenge to develop a computerised SMS which takes into account the interaction between the reliability of a storm-surge barrier and the reliability of the dikes lying behind the barrier.

Especially since the same principle could be used for other storm-surge barriers, e.g. the Dutch Maeslant storm-surge barrier.

### 1.3 Approach

The first step in developing a computerised SMS is describing the system that has to be modelled. Another important aspect is the outcome of the model. It should obviously be a probabilistic measure of safety against flooding of the hinterland (the "safety level" of the system), but which measure should be taken?

Secondly, an overview of the state-of-the-art is necessary: which studies have been made related to this subject and which useful methods and models already exist?

Third step is to describe a relationship between the suitable methods to determine the reliability of the storm-surge barrier and the reliability of the dikes. In fact, all relevant relationships within the system should be described. For this purpose the so-called IDEF0 method is used. Consequently, the system is described in a deterministic way. The necessary translation to a probabilistic outcome will be accomplished by using a Monte Carlo (MC) simulation technique.

To limit the amount of work some simplifications are carried out in modelling this complex system. The IDEF0 description will be used to see the effect of each simplification on the over-all model.

At this stage the impact of maintenance of the storm-surge barrier and dikes on the safety level is not yet taken into account.

## 2 SAFETY MANAGEMENT SYSTEM

### 2.1 System description

The system that needs to be modelled incorporates the North Sea, the Eastern-Scheldt storm-surge barrier, the Eastern-Scheldt basin, the surrounding dike rings 26–31 and four so-called compartment dams, i.e. Grevelingendam, Philipsdam, Oesterdam and Zandkreekdams. The system boundaries are shown in figure 2.

Basically the relevant sequence of actions within the system can be described as follows:

- A storm occurs, which causes a water level rise near the Dutch coast;
- If necessary, the storm-surge barrier has to close all 62 gates;
- If the barrier works properly the amount of water in the Eastern-Scheldt basin will only increase due to leak through the barrier;
- The dikes surrounding the basin have to prevent flooding of the hinterland.



Figure 2. Boundaries of the safety system.

However, if the barrier fails to close all 62 gates an extra amount of water will leak through the barrier. This will lead to higher water levels in the basin. Consequently, the loads on most of the dikes increase and flooding of the hinterland will become more likely.

## 2.2 Safety level

The safety level of the SMS can be determined using system reliability techniques. In this context the safety level of the system is the same as its reliability, so we can define a so-called undesirable top event. Occurrence of this event can be seen as failure of the system. In this way the safety level of the SMS is equivalent to the probability of occurrence of the undesirable top event.

Looking at the required safety levels of the system used since the design of the storm-surge barrier we see some significant differences.

For the design of the barrier a maximum probability of failure of the system has been used of  $10^{-7}$  per year (see Road and Hydraulic Engineering Division (1994)), while BARCON (1985) uses  $2.5 \cdot 10^{-5}$  per year. The first requirement however corresponds with the undesirable top event of exceeding the average water level on the Eastern-Scheldt of NAP +4.3 m, while the second one corresponds with exceeding NAP +3.5 m. More recently, in 2000, the occurrence

of a “flood disaster” has been used as an undesirable top event, and has been set to a maximum probability of  $10^{-7}$  per year by the Directorate Zeeland (2000).

In defining the undesirable top event of the SMS structural failure of the storm-surge barrier is left out of consideration. For, however it may be an undesirable event, the safety system does not always fail if the storm-surge barrier (partly) fails. Failure of the SMS takes place not before at least one of the dikes surrounding the Eastern-Scheldt fails.

Therefore we use the undesirable top event “failure of one or more of the dike rings surrounding the Eastern-Scheldt basin”. Since an important feature of the model will be the compatibility with both existing and future tests of dikes we mean by failure the occurrence of one of the failure modes summed up in Table 1.

## 2.3 Existing studies, methods and models

Since the design of the Eastern-Scheldt storm-surge barrier a long list of articles has been published. Studies have been made of the reliability of the storm-surge barrier (Van den Beukel & Kooman (1980), BARCON (1985)) and its control (Vereeke and Vroon 1999). Calculation methods to determine the reliability of the dikes are also known (TAW (1999), Vrouwenvelde et al. (1999)) To calculate the water levels on the Eastern-Scheldt several water

Table 1. Failure modes of a dike ring (Vrouwenvelder et al. 1999).

---

Overtopping
Wave overtopping
Slip circle inner slope
Slip circle outer slope
Erosion outer slope
Failure revetment en Erosion core
Macro instability outer slope
Macro instability inner slope
Micro instability inner slope
Burst of cover layer and Piping
Failure of constructions in the dike

---

movement models can be used, i.e. *Simplic* (used in *BARCON* (1985)) and *Implic*. The latter one has been used to determine the reliability of the dike revetments by calculating the water levels near the dikes for all possible storm types taking into account the probabilities of occurrence per storm (Stroeve F.M. 2000). Determination of the reliability of the dikes while taking into account a (partly or completely) failed storm-surge barrier is not common practice.

For practical reasons the focus is on using existing methods and models as much as possible during building of the SMS. This does not only reduce the amount of work; it will probably also reduce some of the “teething problems” that exist when developing a completely new model. On the other hand, the problem in using existing models and methods could be the lack of compatibility between them. To control this problem as much as possible we have made use of a design tool, called “*IDEF0*”.

#### 2.4 *IDEF0* method

*IDEF0* is a method designed to model the decisions, actions, and activities of an organisation or system. *IDEF0* was derived from a well-established graphical language, the Structured Analysis and Design Technique (SADT). The United States Air Force commissioned the developers of SADT to develop a function modelling method for analysing and communicating the functional perspective of a system. As a communication tool, *IDEF0* enhances domain expert involvement and consensus decision-making through simplified graphical devices. As an analysis tool, *IDEF0* assists the model designer in identifying what functions are performed, what is needed to perform those functions, what the current system does right, and what the current system does wrong.

With *IDEF0* we managed to combine the relevant aspects of the safety system into one integral model, such as the storm variables, the water movement, the failure of the storm-surge barrier and dikes and the occurrence of flooding.

### 3 SMS MODEL

#### 3.1 *Monte Carlo* simulation

The annual probability of occurrence of the top event is the applied measure for the safety level of the hinterland. However, due to the complexity of the system this annual probability is not easily determined analytically. Therefore MC simulation will be used. As mentioned in the introduction, the model should be able to deal with small probabilities of occurrence. At this stage it is not clear to what extent the “traditional” MC will be sufficient for reliable calculations, or that we will have to use directional sampling techniques in order to reduce the number of MC runs.

#### 3.2 *Monte Carlo* model

The over-all SMS model will be built as a MC model. The core of this MC model is a deterministic system describing a storm, the following water movements, the working of the storm surge barrier and whether or not the top event occurs.

The deterministic variables are drawn from probability density functions. By running the model a large number of times (for example 10,000 times) and checking every run whether or not the undesirable top event occurs, the percentage of runs in which this event does occur can be considered as the probability of occurrence of it. This can be done per year. The model will be set up in such a way that the impact of maintenance and management (for example the closing strategy) can easily be taken into account by changing the probability density functions of the state of the dikes, the state of the barrier or the moment of closing the barrier. Figure 3 shows the diagram of the SMS model.

#### 3.3 *Deterministic system* description

In figure 3 the inner block represents the deterministic description of the system. This description has been made using *IDEF0*.

*IDEF0* has the feature to describe the model on different levels of detail. Parts of the model can be zoomed in or zoomed out. The complete model has been described in *IDEF0* schemes. In this paper we will only show two levels of detail, named A-0 and A0; see figures 4 and 5.

Figure 4 shows the highest level of the model. One block that represents the action “determine whether or not the undesirable top event takes place”. The input consists of the water depths and capacity of the Eastern-Scheldt basin, together with the wind parameters and the astronomical tide. The output consists of not only the (non-) occurrence of the undesirable event, but also of the renewed water depths and

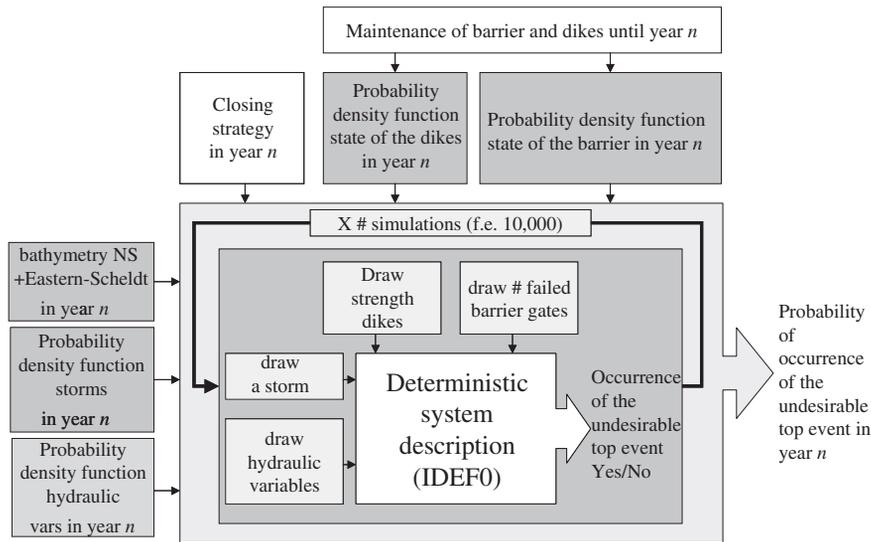


Figure 3. Diagram of the safety management model.

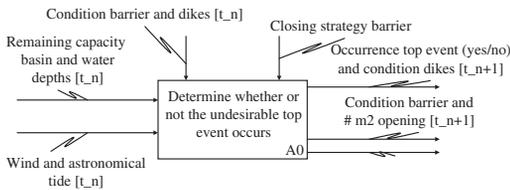


Figure 4. IDEFO A-0 scheme of the SMS.

remaining capacity of the basin. This is where the time-dependency should be taken into account. The model represents the working of the system for a time interval  $[t_n, t_{n+1}]$ . During this interval water comes in from the North sea to the Eastern-Scheldt basin. The amount of water depends on the number of square meters opening in the storm-surge barrier, which – in turn – depends on the number of steel gates that failed to close plus the leak of the barrier. So, after a period of time the water depths and remaining capacity of the basin have changed and should be renewed and used again for modelling the time interval  $[t_{n+1}, t_{n+2}]$ .

The same thing goes for the state of the storm-surge barrier (the number of failed gates or other parts of the barrier) and the number of square meters opening. As stated above, this information is necessary for determining the amount of water coming from the North sea into the Eastern-Scheldt basin and should also be used again for the next time interval. This iteration continues until the end of the storm, or until the undesirable top event takes place.

The determination of the relevant hydraulic variables, e.g.  $H_s$  and  $T_p$ , the state of the storm-surge barrier, the remaining capacity of the basin and the water depths is being described in figure 5.

### 3.4 Modelling water movements

As mentioned in paragraph 2.3, apart from whether or not the undesirable top events occurs, the steps in figures 4 and 5 have been done before by Stroeve (2000). Using the computer model Implic for modelling the water movements in the Eastern-Scheldt, water levels near the dikes have been determined for 3600 different storm types. These calculations were made based on a fully closed barrier. Closing the barrier manually according to the computer advise as well as the emergency closure has been taken into account.

We can use these results for the situation in which all 62 gates of the barrier work properly. In case one or more of the gates fail to close the impact on the water levels is unknown. New (computer) calculations should be made for each combination of the number of failing gates and the type of storm. This would result in  $3600 \cdot 62 = 223,200$  calculations. However, the moment of gate failure and the duration of failure are also important. The number of combinations will increase enormously if all these options are taken into account. Simplifications are necessary in order to reduce the amount of calculations.

### 3.5 Simplifications

In order to model the system properly and keep the number of required calculations within bounds,

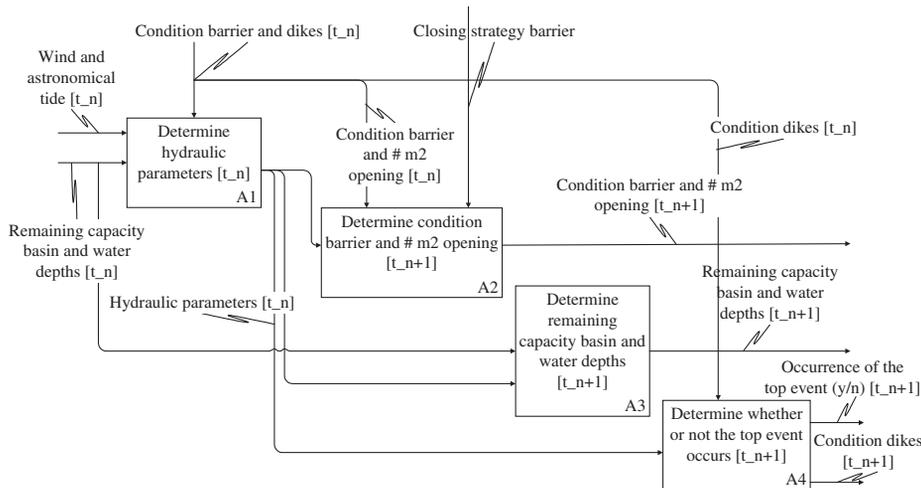


Figure 5. IDEF0 A0 scheme of the SMS.

simplifications have to be made. The most important ones are the following:

- Failure of the storm-surge barrier means failure of one or more of its gates. Other failure modes like structural failure will not be taken into account.
- Failure of the storm-surge barrier can only take place while closing or opening the barrier.
- The number of failing gates is categorised to 1, 2, 3, 4 and more than 4. The last one is set to all 62 gates.
- The duration of failing is categorised into less than 1 hour, 1 closing operation (about 12.5 hour) and longer than 1 day.
- The position of a failing gate is not relevant.

The moment of failure has not been simplified yet. First the idea was to consider each failure of a gate during a storm at the beginning of that storm, but that will probably be too conservative.

Another simplification was that failure to open the barrier would not be relevant for the flood risk. However, since the changing strategy uses the opportunity to sluice water out of the Eastern-Scheldt basin into the North sea during the “low tide-period” in a storm, opening the barrier could be relevant to reduce the risk of flooding.

In one of the further steps these simplifications will be checked and determined by making some calculations using Implic.

#### 4 PRELIMINARY RESULTS

At this stage the system description and model design have been made using IDEF0 schemes for all relevant

levels of detail. We managed to use existing methods and models in a consistent over-all concept of the safety management system.

The IDEF0 method proved to be a powerful modeling tool. It is helpful in getting a complete overview of the system, especially the relevant relationships through all levels of detail. The IDEF0 schemes appeared to be very useful in making a project breakdown in such a way that different aspects of the model could be assigned to different project team members to be worked out, without losing compatibility.

In modelling the system one of the most difficult aspects was the time-dependency of the relation between failure of the storm-surge barrier, the following water movements and the failure of the dikes surrounding the Eastern-Scheldt. Some significant simplifications had to be made in order to reduce the number of calculations. Again, IDEF0 proved to be helpful in assessing the effect of each simplification on the over-all model.

There is still a lot to be done though. Some of the most important further steps are mentioned in the next chapter.

#### 5 FURTHER STEPS

At this stage the system description and model design have been made. In building a computerised SMS, the following steps have to be made:

- Making test calculations to check simplifications.
- Choosing the proper MC simulation technique.
- Building a pilot model. This is a “quick prototype” of the model in which the most important relations

are defined. The input numbers, however, are not revised.

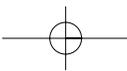
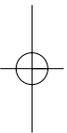
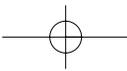
- Testing the pilot model.

After testing the pilot model, we can decide whether or not the pilot model should be upgraded to a fully operational SMS model. In case it should, some of the input information and simplifications should possibly be reconsidered. This implies that the probability of failure of the storm-surge barrier should be calculated with the most recent information. In the end, the SMS model should be linked with maintenance models of both the storm-surge barrier and dikes in order to optimise the maintenance strategy for the whole flood defence system.

With the results presented in this paper a first step has been made in reaching that objective.

## REFERENCES

- BARCON project. 1985. Part report: Safety aspects of management of the storm-surge barrier in the Oosterschelde (Concept). *Ministry of Transport, Public Works and Water Management, Directorate Zeeland*. Middelburg.
- Directorate Zeeland. 2000. 2nd generation Maintenance Plans Eastern-Scheldt storm-surge barrier. Starting-points document 1. Report no. E5897A152.OSK.
- Road and Hydraulic Engineering Division. 1994. Design Plan Oosterschelde Storm-surge Barrier, Overall Design and Design Philosophy, *Ministry of Transport, Public Works and Water Management*, Rotterdam: Balkema.
- Stroeve, F.M. 2000. Testing Framework for Block Revetments along the Eastern Scheldt (in Dutch). *Ministry of Transport, Public Works and Water Management, Civil Engineering Division*.
- TAW. 1999. PC-Toets. Pc-program Guidelines for Evaluating Safety (in Dutch). *Technical Advisory Committee for Water Defences*.
- U.S. Airforce. 1993. Integration Definition for Function Modelling (IDEF0). *Draft Federal Information Processing Standards Publication 183*.
- Van den Beukel, A. & Kooman, D. 1980. Failure Probability Analysis of the Eastern-Scheldt Storm Surge Barrier (In Dutch). *Institute TNO for Building Materials and Constructions*. Report no. B-80-62/62.3.2002. Delft.
- Vereeke, S. & Vroon, J. 1991. Safe Tide, Maintenance and use of Storm Surge Barrier Eastern Scheldt, experience and adjustment (in Dutch). *Ministry of Transport, Public Works and Water Management, Directorate Zeeland*. Middelburg.
- Vrouwenvelder, A.C.W.M., Steenbergen, H.M.G.M. & Slijkhuis, K. 1999. User's Manual PC-Ring (in Dutch). *TNO-Bouw*, Delft.



## Reliability of vibration predictions in civil engineering applications

M.S. de Wit & P.H. Waarts

*TNO Building and Construction Research, Delft, The Netherlands*

P. Holscher

*Geodelft, Delft, The Netherlands*

H.G. Stuit

*Holland Railconsult, Utrecht, The Netherlands*

**ABSTRACT:** The reliability of vibration predictions distinguishes itself from other reliability problems because of the highly non-linear behavior of the underlying models. Over the last two years, a combination of four institutes in the Netherlands has studied the reliability in this type of predictions. For the sake of comparison, besides sophisticated computational prediction models, also simple empirical models and expert judgment was analyzed. The paper describes the experimental set-up and the results of the project. Conclusions are drawn about the reliability of the predictions and the reduction that may be achieved from an increase in model sophistication.

### 1 INTRODUCTION

In densely populated areas, damage and discomfort from vibrations is an important issue. Vibrations are generated by e.g. road and rail traffic, by construction activities like pile driving and sheet piling, and by industrial production processes. They may result in discomfort for occupants of buildings in the neighborhood, damage to these buildings and/or disruption of sensitive equipment.

For the construction and exploitation of infrastructural works, vibrations often are an impediment. To avoid trouble, it is customary in The Netherlands to predict vibration levels on the basis of calculation models at the beginning of or prior to the construction phase. The predicted levels are compared to target values in codes or guidelines.

Predictions can be made at various levels of sophistication. At one end of spectrum are expert predictions without explicit models. At the other end are the multi-body and Finite-Element-models, which have a strong basis in first principles. Empirical models are somewhere in-between. At present, the reliability of vibration predictions in situations of practical interest is unknown. It is even uncertain whether a sophisticated model gives more accurate results than a simple approach.

To gain more insight in these issues, a Delft Cluster research project was initiated with participants from

four institutes in The Netherlands with an established reputation in the field of vibration prediction and measurement.

### 2 PREDICTION OF VIBRATION LEVELS

Just like sound, vibrations are a short disturbance of balance. Sound can be seen as a vibration of air. It is characterized by a power level in dB, a pitch and a frequency. The frequency reproduces the number of vibrations per second. This is expressed in Hertz (Hz). As for sound the vibration of solid objects (soil, buildings) are characterized with vibration level and vibration frequency in Hertz. Mostly the top value of the vibration velocity ( $v_{\max}$ ) is used for the assessment of damage to buildings due to vibrations. The effective value of the vibration velocity ( $v_{\text{eff}}$ ) is mostly used for the assessment of nuisance for people in buildings due to vibrations.

Prediction of vibration levels can be done at various levels of sophistication. Here we distinguish three levels:

- without explicit models (“expert judgment”)
- with an empirical model
- with a model derived from first principles

The first level concerns predictions, which are made on the basis of experience without the help of explicit

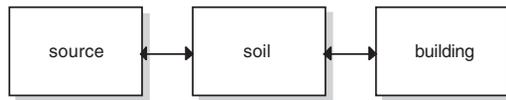


Figure 1. Subsystems in a model for the prediction of vibrations, and their connections.

models. Predictions at this level are often elicited from specialists in cases where a quick and cheap assessment has to be made, e.g. to determine whether a problem may potentially occur or not. We will refer to this type of predictions as “expert judgments”.

Empirical models are primarily constructed from experimentally obtained input/output data, with only limited or approximate recourse to laws concerning the fundamental nature and properties of the system under study. With this type of models predictions can be produced on the basis of concise and often coarse-grained input about the system.

At the highest level of sophistication are the predictions based on models, which are derived from first principles. Among this type of models are the Finite Element Models (FEM) and the multi-body models, which are regularly used in vibration modeling. These models require detailed input and are generally expensive to build and to run. They are typically applied in alleged problem situations and/or to evaluate mitigating measures.

Models for vibration predictions commonly consist of three submodels, which are connected as shown in Figure 1.

The figure expresses that vibrations are generated by a source on one place, propagate through the soil by some mechanism and subsequently result in vibrations in a construction or building at another location. It is common practice to model the three subsystems separately, and to connect them afterwards to make predictions.

### 3 UNCERTAINTY

The central question in this paper concerns the reliability of vibration predictions. To answer this question, the uncertainty in the predictions has to be analyzed. This uncertainty may result from essentially four sources:

1. incomplete information about the specification of the (sub)system under study.
2. incomplete information about the input and boundary conditions of the (sub)system.
3. simplifications and approximations in the physical modeling of the (sub)system.

4. discretizations and approximations in the numerical modeling of the (sub)system.

As an example we consider the soil subsystem. When modeling the behavior of the soil, uncertainty from the first source is always present. Indeed, only limited information about the soil structure and properties is available in practical contexts. The second source also contributes to the uncertainty. First, there is the uncertainty in the input data from source model. Second, the source model may not provide all required input/boundary conditions. Uncertainty from the third source is directly related to the modeling level discussed in the previous section. For practical situations, uncertainty from this source in case of a FEM modeling approach is expected to be small compared to an empirical modeling approach. Theoretically, the translation of the physical soil-model into a numerical model may introduce extra uncertainty in the FEM-approach, but we will assume here that this is a negligible contribution.

In the remainder of this paper we will refer to uncertainties from the first two sources as “parameter” uncertainty. Loosely stated, this is the uncertainty that arises from our limited knowledge about the state of the world: which system are we modeling and what exactly is driving it? Uncertainty from the third and fourth sources is addressed as “model” uncertainty. This uncertainty may be associated with our lack or neglect of knowledge about how the system works: given that we know the structure of the system, its properties and the forces driving it, what is the system’s response? In practice, the distinction between parameter and model uncertainty is not always clear, especially as the models become more empirical. We will not dwell on this subject here. A more elaborate discussion can be found in Wit (2001).

In practice, uncertainty is not explicitly accounted for. Vibration predictions are point-estimates (“best guesses” or “conservative” estimates), which have an unknown deviation from the actual values. We write:

$$v_{\text{obs}} = g * v_{\text{point}} \quad (1)$$

where:

$v_{\text{obs}}$  observed or actual vibration level  
 $v_{\text{point}}$  point estimate of vibration level  
 $g$  correction factor

and consider  $g$  a random variable. If we assign  $g$  a probability distribution, which, on the long run, matches the frequency distribution of  $v_{\text{obs}}/v_{\text{point}}$ , we may consider this probability distribution a measure of the (average) uncertainty in vibration predictions. Hence the approach in this paper will be to assess frequency distributions on the basis of recorded values for both  $v_{\text{point}}$  and  $v_{\text{obs}}$  in a large number of cases. Note that we assume here that the observed value  $v_{\text{obs}}$  equals the actual value without observation error.

## 4 EXPERIMENTS

### 4.1 Introduction

As mentioned in the previous paragraph, we estimated the prediction uncertainty on the basis of a statistical analysis of values for  $v_{\text{obs}}/v_{\text{point}}$  recorded in a large number of cases. In this process we distinguished between the three levels of sophistication mentioned in section 2. For each level we assessed the total uncertainty, i.e. the uncertainty in predictions:

- for the whole system including source, soil and building subsystem
- based on a level of information as commonly available in practice

For predictions on the basis of first principles models (level 3), a start was made to break down the total uncertainty into:

- contributions from the various subsystems
- contributions from the various sources of uncertainty (model versus parameter uncertainty)

In this paper only a partial breakdown was investigated as shown by Table 1.

All uncertainty assessments are based on statistical analyses of the ratio between measurements and predictions. Hence, predictions were collected for cases or situations, where reliable measurements were or could be made available. In all cases it was seen to that the predictions were done without any prior knowledge of the measured values.

The next sections describe the experimental set-up for the three different levels of prediction sophistication separately.

### 4.2 Expert judgment (level 1)

As shown in Table 1 only the total uncertainty was estimated at this level. As experts do not use explicit models, decomposition of the uncertainty not sensible.

Eight experts were selected as a representative sample of professional consultants active in the building and construction industry in the field of vibration modeling and/or measuring. The experts had to make 24 predictions of vibration levels in 7 different cases. These cases were selected from a large number of historical cases to form a representative section. All three subsystems were involved. The cases were described at a level of detail that is customary in practical situations. For a description of cases and measurements see Wit & Molenaar (2002).

To prepare themselves, the experts received global, qualitative information about the cases 2 days prior to the elicitation session.

The experts' assessments were obtained in an E(lectronic) B(oard) R(oom)-session. The experts

Table 1. Breakdown of the uncertainty in vibration predictions into modeling level, subsystem and type of uncertainty ("par": parameter, "mod": model, "tot": total). The crosses indicate which items are addressed in this paper.

level\ subsystem		1. expert	2. empirical	3. FEM
source	par			
	mod			
	tot			
Soil	par			X
	mod			X
	tot			X
building	par			
	mod			
	tot			
Total		X	X	X

were located in the same room, each seated behind a separate computer connected to a network. All experts received the same information and explanation, and made their assessments solely on the basis of their experience and background literature they brought along. They simultaneously and independently entered their assessments into their computer, without discussion with the other experts.

The assessments consisted of values for  $v_{\text{eff,max}}$  or  $v_{\text{max}}$  (see section 2). For each variable, two predictions were required, i.e. a median value or "best guess", and a value which in their opinion would not be exceeded with 95% probability.

The prediction uncertainty was calculated from comparisons between the predictions and the measurements (see section 3). A preliminary analysis was carried out immediately after the elicitation session. The results were presented to the experts in the same session as immediate feedback. For more information see Wit & Molenaar (2002).

### 4.3 Empirical model (level 2)

At this level, one single prediction tool was used, called D11 (CUR 1995). This tool is based on empirical models. As the user has hardly any influence on the results (limited number of choices to make in doing the predictions, choices quite obvious) all predictions were done by one single person, a TNO employee, behind his own desk. This person had no specific expertise in the field of vibration modeling.

Vibration predictions were made for the same cases and variables that were used in the expert judgment study (see previous section). The predictions were point estimates, i.e. the values produced by the prediction tool.

Again the uncertainty was calculated from a statistical analysis of the ratio between predictions and

measured values. Only the total uncertainty was assessed as the program does not give intermediate results. For more information about the predictions see Esposito (2002).

#### 4.4 *First-principles model (level 3)*

##### 4.4.1 *Total uncertainty*

For this level of prediction sophistication another set of cases was used. Indeed, to be able to break down the uncertainty, specific measurements were required. These measurements were done near the building pit of the “Tunnel Rotterdam Noordrand” in The Netherlands. Two grids of vibration sensors were installed in the soil, one at surface level and one at a depth of 14 m below surface level. Both horizontal and vertical vibration components were measured. Note that in these measurements the subsystem “building” was not involved. Moreover, all measurements were carried out in the same soil. Various vibration sources were used though: pile driving, sheet piling and heavy traffic over a speed ramp. The measurements were carried out by TNO.

Prior to the measurements, the vibration levels at the various sensor positions had been predicted ( $v_{\max}$ -values) by three different Dutch institutes, i.e. GeoDelft, Holland Railconsult and TNO. All three institutes regularly carry out Finite Element Model-vibration predictions in civil engineering projects.

From a comparison of the predicted and measured vibration levels, the total uncertainty has been estimated. Note that these uncertainty estimates concern a system that only consists of a source and soil subsystem, without the component “building”.

For more information about the predictions, see Koopman (2002a), Hölscher & Waarts (in prep.). More info about the measurements can be found in Koopman (2002b) and Wit (in prep.)

##### 4.4.2 *Uncertainty contribution from soil-subsystem*

To assess the contribution of the soil-subsystem to the total uncertainty, separate predictions and measurements were done. These predictions and measurements concerned the same subsystem “soil” (same grid of sensors), but a different source: a drop weight. During the measurements, also the impulse-like force that this weight exerts on the soil was measured. The force measurements were used as input of all prediction models for the soil system. In this way a source model could be avoided and hence the resulting uncertainty could be attributed to the subsystem “soil”. For details see Hölscher & Waarts (in prep.).

##### 4.4.3 *Parameter uncertainty and model uncertainty*

To discriminate between parameter uncertainty and model uncertainty, two sets of FEM-predictions were

carried out for the subsystem “soil”, excited by the drop weight. These predictions were produced in two subsequent phases, phase 1 and phase 2. For the purpose of the predictions in phase 1, information about the structure and properties of the soil was provided at a level, which resembles the level of information that is available in common practical situations. This was the same information that was also used for the assessment of the total uncertainty in FEM-based predictions. This information is limited and therefore gives rise to uncertainty in the model parameters: parameter uncertainty.

In phase 2, extra information about the soil had become available through extra sophisticated measurements (see Pruiksma et al. 2002, Hölscher 2002). This information implied a reduction of the parameter uncertainty. The reduction of the prediction uncertainty in phase 2 compared to phase 1 gives an indication of the relative contribution of the parameter uncertainty to the overall uncertainty for the subsystem “soil”.

## 5 RESULTS AND DISCUSSION

### 5.1 *Expert judgment (level 1)*

For each vibration velocity, the experts gave two assessments, i.e. a best guess (median value) and a 95-percentile. These assessments are subsequently discussed in the next subsections.

#### 5.1.1 *Best guesses*

In the expert judgment study, 8 experts gave their best estimates for 24 vibration velocities each, giving a total of 192 predictions. For each of the 24 velocities, a measured value was available. Realizations of the random factor  $g$  (see equation 1) were obtained by division of each prediction by the corresponding measured value. A frequency distribution of the resulting ratios is shown in Figure 2. More details about the measurements and the predicted values can be found in Wit & Molenaar (2002).

The values of  $g$  in the sample cover a range of almost 4 orders of magnitude, which is a considerable spread. This suggests that we consider the logarithm of  $g$  rather than  $g$  itself. This choice is also supported by the apparent goodness of fit between the frequency distribution of  $^{10}\log g$  and the normal distribution. We will interpret the observed frequency distribution as an estimate for the probability distribution of  $g$ . The underlying assumption is that the realizations of  $g$  are (sufficiently) independent. Estimates of the mean and standard deviation of  $^{10}\log g$  are shown in Table 2.

Both Figure 2 and the mean value of  $^{10}\log g$  in Table 2 show that on average the experts' estimates are hardly biased. This is consistent with the assignment

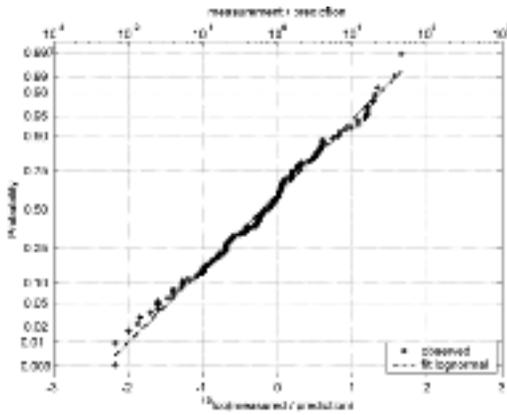


Figure 2. Frequency distribution of  $^{10}\log g$ , the logarithm of the ratio of measured values and the experts' best guesses. The frequency distribution is plotted on normal probability paper.

Table 2. Estimates for the mean and standard deviation of  $^{10}\log g$  for best guesses of all experts.

mean	-0.2
standard deviation	0.77

Table 3. Estimates for the mean and standard deviation of  $^{10}\log g$  for best guesses of the "best" expert.

mean	-0.2
standard deviation	0.6

to generate best guesses, so as a group the experts are well-calibrated in this respect.

The variation between the experts is not too large. If we select the best expert (median value close to 0 and small standard deviation) the statistics are shown in Table 3.

### 5.1.2 95% percentiles

The same procedure as described in the previous subsection can be repeated with the experts' 95-percentiles. We will refer to the ratios between measurement and 95-percentile as  $g_{95\%}$ . If the experts would be well-calibrated in their 95-percentile assessments, the frequency distribution of  $g_{95\%}$  would cross  $g_{95\%} = 0$  at a probability level of 95%. Only then the measured values would exceed the predicted values in only 5% of the cases.

Figure 3 shows, however, that the observed frequency distribution crosses  $g_{95\%} = 0$  at a probability level of 75%.

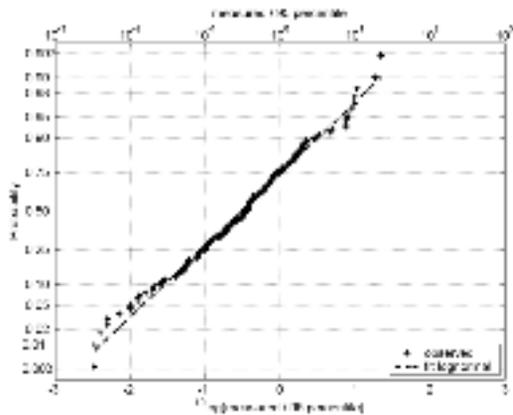


Figure 3. Frequency distribution of  $^{10}\log g_{95\%}$ , the logarithm of the ratio of measured values and the experts' 95-percentiles. The frequency distribution is plotted on normal probability paper.

This indicates that the experts as a group are overconfident: they choose their 95-percentile values too low, a factor 6 on average. Further analysis of the uncertainty in the experts' predictions is elaborated in Hölischer & Waarts (in prep.).

## 5.2 Empirical (level 2)

The predictions were made with prediction tool "D11" for the same cases as presented to the experts (see section 4). Few cases fell outside the scope of application of the tool and were skipped. A total of 18 predictions resulted. The predicted values were divided by the corresponding measured values to obtain realizations of  $g$ . Figure 4 shows the frequency distribution of  $g$ .

Figure 4 shows that the D11 predictions are somewhat conservative on average as the probability of finding a measurement exceeding the predicted value is only 25%. The figure also shows that the frequency distribution of the D11 results is very similar to the distribution of the experts' 95-percentiles. The D11-tool is apparently successful in the sense that with this tool a non-expert can produce "conservative" predictions, which are equally well (or poorly) calibrated as conservative predictions from an arbitrary expert. The degree of conservatism, although, is probably less than expected.

Table 4 summarizes the statistics of  $g$  for the D11 results.

## 5.3 First principles (level 3)

As the predictions at this level were made with the help of FEM-models, they are also referred to as FEM-level predictions.

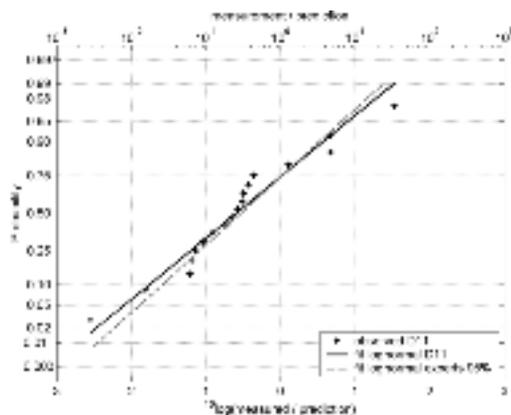


Figure 4. Frequency distribution of  $^{10}\log g$ , the logarithm of the ratio of measured values and the D11 predictions. The frequency distribution is plotted on normal probability paper. For reference the distribution fitted to the experts' 95-percentiles is also shown (dashed line).

Table 4. Estimates for the mean and standard deviation of  $^{10}\log g$  for D11 predictions.

mean	-0.6
standard deviation	0.8

### 5.3.1 Total uncertainty

A total of 560 predictions were produced by three institutes, which were compared with measured values as in the previous sections. The frequency distribution of the ratio between measured and predicted values is shown in Figure 5.

Again, the lognormal distribution appears to describe the frequency distribution well. The predictions are not significantly biased as the median value of  $^{10}\log g$  is close to 0. A summary of the total uncertainty statistics is given in Table 5.

These numbers are an indication for the uncertainty in the predictions of an arbitrary institute. When we extract the results for the best performing institute in the study (median value close to 0 and smallest standard deviation) we find the statistics in Table 6.

The limited reduction of the variance in  $^{10}\log g$  that is obtained when using FEM-based predictions in stead of instant expert judgment is striking. If we compare the predictions of all experts with the predictions of all institutes we find a factor of  $(0.6)^2 / (0.8)^2 \approx 0.6$ . Comparison of the best expert with the best institute gives a variance reduction of about 0.7. If we bear in mind that the FEM-predictions only concerned the subsystems source and soil, whereas the experts had to predict the behavior of source, soil and

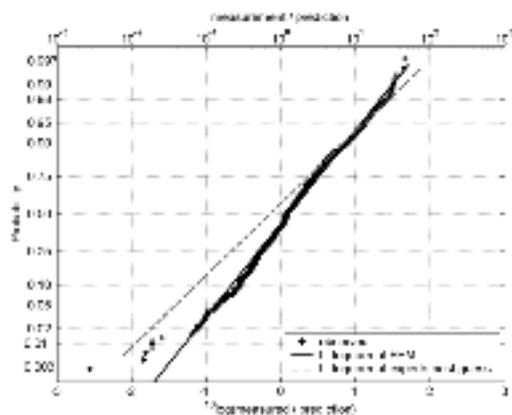


Figure 5. Frequency distribution of  $^{10}\log g$ , the logarithm of the ratio of measured values and the FEM-predictions. The frequency distribution is plotted on normal probability paper. For reference the distribution fitted to the experts' best guesses is also shown (dashed line).

Table 5. Estimates for the mean and standard deviation of  $^{10}\log g$  for all FEM-predictions.

mean	0.1
standard deviation	0.6

Table 6. Estimates for the mean and standard deviation of  $^{10}\log g$  for FEM-predictions of "best" performing institute.

mean	0.1
standard deviation	0.5

building in several cases, the reduction in practical cases might even be less.

### 5.3.2 Uncertainty in soil subsystem

To assess the uncertainty in predictions of the soil subsystem only, predictions for and measurements of the drop weight experiment were compared and statistically analyzed (see section 4.4.2). The predictions were carried out in phase 1, i.e. on the basis of the same soil data that were used for the analysis of the total uncertainty (section 5.3.1). The frequency distribution of the ratio between measured and predicted values is shown in Figure 6.

The most important observation is that the slope of the distribution for the soil system only is significantly steeper than the slope of the distribution associated with the system source + soil. This means that the uncertainty in the predictions increases once the input from the subsystem "source" is fixed without

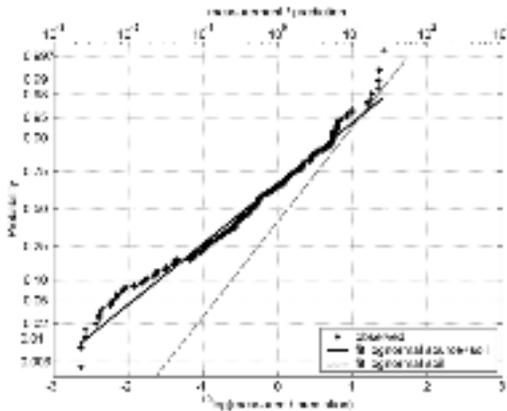


Figure 6. Frequency distribution of  $10^1 \log g$ , the logarithm of the ratio of measured values and the FEM-predictions for the soil only. The frequency distribution is plotted on normal probability paper. For reference the distribution fitted to the FEM-predictions for the system source + soil is also shown (dashed line).

uncertainty. This remarkable result implies that a dependency exists between the source model and the soil submodel (“negative correlation”). At first glance, this is awkward as the physical systems underlying these models are driven by separate and most probably statistically independent variables. However, the common factor in these two models is the user. This user is an expert, who, based on his experience in the field, has a certain expectation of the outcome of the prediction. Hence in choosing point estimates for the model parameters, he will avoid those values which give unrealistic results. As source models generally contain more parameters for which no direct empirical evidence is available, tuning of parameter estimates is most easily done in the source submodel. At the moment that this tuning opportunity disappears (source is fixed) and predictions have to be made for a rather unfamiliar vibration source (drop weight), the corrective opportunities of the user are ruled out and the real uncertainty in the submodel appears.

This mechanism would also explain why the uncertainties in FEM-predictions and expert judgments are similar. As the user strongly guides the FEM-prediction process, it is the expertise of the user, which determines the results in the end.

At this stage we consider the above explanation a plausible and promising hypothesis, but no verification steps have been taken yet.

### 5.3.3. Model uncertainty soil subsystem

To analyze the contribution of the soil parameters to the uncertainty, predictions for the soil system have

Table 7. Estimates for the mean and standard deviation of  $10^1 \log g$  for FEM-predictions of in phase 1 (standard parameter uncertainty) and phase 2 (reduced parameter uncertainty).

	phase 1	phase 2
mean	-0.4	-0.3
standard deviation	0.9	0.9

been made in phase 2, based on extra, measured data on the soil parameters. This reduces the uncertainty in the model parameters compared to phase 1. Table 7 shows the statistics of the frequency distributions of  $g$ , the ratio between measured and predicted values.

The table shows that the extra information about the soil parameters does not significantly improve the predictions. This indicates that either the reduction in parameter uncertainty obtained by the measurements was negligible or the model uncertainty is the dominant source of uncertainty in the predictions. At this point, only one single soil system was investigated, different results might be obtained for other soil systems.

## 6 CONCLUSIONS AND RECOMMENDATIONS

1. The uncertainty in vibration predictions in civil engineering applications is quite large, typically 1 order of magnitude.
2. The uncertainty in vibration predictions hardly reduces when in stead of expert judgment, empirical models or even sophisticated computational models are used. A possible explanation is that the modeling choices that have to be made are decisive for the uncertainty in the predictions. These choices are, in the end, based on expert judgment.
3. The experts in this study tend to choose their 95-percentile predictions too low: these predictions are exceeded by the measured values in about 25% of the cases.
4. Prediction uncertainty should not be attributed to a model or a modeling approach alone as it depends on the interaction between the model and its user.

## REFERENCES

- CUR 1995, Prediction model vibration discomfort (in Dutch), *Report 95-2*. Gouda: Civieltechnisch Centrum Uitvoering Research en Regelgeving (CUR).
- Esposito, G. 2002, Vibration predictions with the D11 model (in Dutch), *Report 01.05.02-006*. Delft: Delft Cluster.
- Hölscher, P. 2002, Reliability of global assessments of dynamic soil parameters (in Dutch), *Report 01.05.02-011*. Delft: Delft Cluster.

- Hölscher, P. & Waarts, P. in prep., Final report of DC project 01.05.02, *Report 01.05.02-020*. Delft: Delft Cluster.
- Koopman, A. 2002a, Description of predictions (in Dutch), *Report 01.05.02-007*. Delft: Delft Cluster.
- Koopman, A. 2002b, Measurements at the building pit Tunnel Rotterdam Noord (in Dutch), *Report 01.05.02-009*. Delft: Delft Cluster.
- Pruiksma, J., Hölscher, P., Stuit, H. Duin, F. van 2002, Reliability of vibration prognosis by FEM for extensive measurements at Rotterdam North building pit; part 4, input parameters phase 2, *Report 01.05.02-016*. Delft: Delft Cluster.
- Wit, M.S. de 2001, Reliability of vibration predictions – general philosophy (in Dutch), *Draft Report 01.05.02-001*. Delft: Delft Cluster.
- Wit, M.S. de & Molenaar, D.J. 2002, Expert judgment study on vibration predictions (in Dutch), *Report 01.05.02-002*. Delft: Delft Cluster.
- Wit, M.S. de, in prep. Post-processing of the measurements at the building pit Tunnel Rotterdam Noord, *Report 01.05.02-017*. Delft: Delft Cluster.

## The development of software tools for chemical process quantitative risk assessment over two decades

DRE Worthington & NJ Cavanagh

*DNV Software, Risk Management Solutions*

**ABSTRACT:** This paper reviews the advances in Chemical Process Quantitative Risk Assessment (CPQRA) techniques made over the last 20 years in the light of the widespread development of ICT technology. It examines the present situation and summarises the progress made in a number of areas. These include the steps taken to bring CPQRA up-to-date with 21st Century ICT, use of graphical user interfaces and other new technology such as databases, GIS systems and Internet technology, improvements in the underlying modeling technology, use of the risk analysis results to make decisions and communication of findings to stakeholders. A vision for the ideal CPQRA framework is postulated given the latest technology and a gap analysis is carried out between the vision and the present situation using the leading CPQRA tool SAFETI as a benchmark. The paper concludes that CPQRA techniques have exploited only a fraction of the available advancements in ICT and suggests how the methodology can be further improved.

### 1 INTRODUCTION

Quantitative Risk Assessment (QRA) in the context of process plant safety provides a methodology for quantifying the risks associated with the activities involved in the production and processing of chemicals and petrochemicals. In order to quantify risks it is necessary to first identify all possible risk situations, quantify them in terms of event consequence and likelihood and compare them with acceptable criteria.

The main questions to be answered by a QRA are what can go wrong, what are the potential effects if it does go wrong, how often will it go wrong and is it important. Or, in QRA terms, identify the hazards, analyse the consequence, estimate the frequency, combine consequence and frequency to quantify the risks and put measures in place to mitigate and manage those risks. The key objectives of any QRA are to identify the major hazards, quantify the overall risk, optimise the risk reduction measures to be implemented and to help the decision making process with regard to acceptable risk criteria.

Typical outputs of a QRA study are individual risk contours as illustrated in Figure 1 and the F/N curve for representation of societal risk as illustrated in Figure 2. Individual risk can be defined as “the frequency at which an individual may be expected to

sustain a level of harm from the realisation of specified hazards” and is usually taken to be the risk of death expressed as a risk per year. Societal risk is defined as “the relationship between the frequency and the number of people suffering a given level of harm from the realisation of specified hazards”. It is normally taken to refer to the risk of death expressed as a risk per year and displayed as FN curves.

The first commercially available software tools for QRA in the chemical and process industries, commonly known as Chemical Process Quantitative Risk Assessment (CPQRA), were developed in the early 1980's. The terms QRA and CPQRA in the context of this work are interchangeable although in the generic sense QRA can refer to any type of quantitative risk methodology (financial, environmental, etc.).

This early work was as a direct result of recommendations made following the public enquiry into the safety of the many chemical installations operating in the Rijmond area of Holland in the late 1970's. In 1981 the Dutch Ministry of Health and Environment commissioned Technica, later to become part of DNV, to develop a software system for risk assessment of chemical plants using the simplified classical method. Christened “Software for the Assessment of Flammable Explosive and Toxic Impact” (SAFETI) in 1982, SAFETI (Cavanagh, 2001, Worthington & Witlox, 2002) was subsequently delivered to the Dutch Ministry

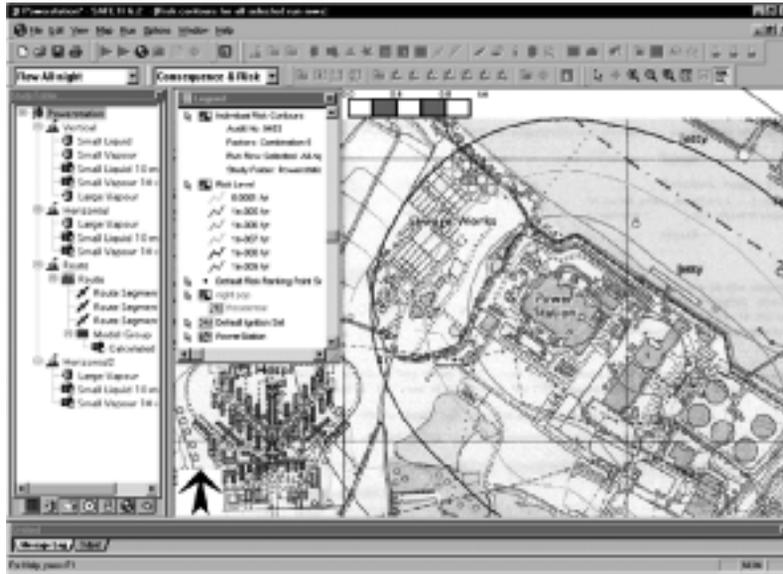


Figure 1. Typical individual risk contours displayed in SAFETI.

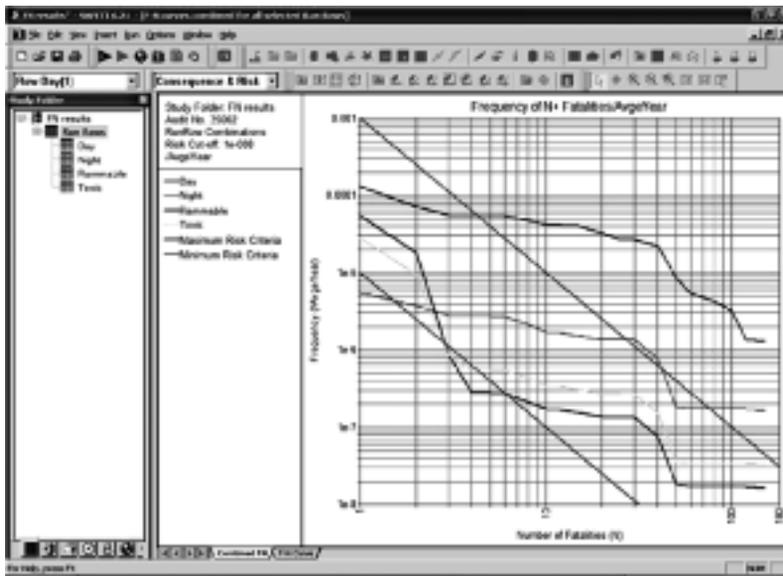


Figure 2. Typical F/N curves for societal risk displayed in SAFETI.

of Housing, Physical Planning and Environment in April 1983.

At that time, the techniques and methodologies developed to enable large scale QRA to be performed challenged the computing power generally available. This limited the development possible and meant that

the software architecture had to be carefully designed to enable the necessary calculations to be made within the IT limitations of that time.

Since then Information and Communication Technology (ICT) has developed rapidly and continuously. The so-called Moore's law shows that price/

performance ratio has doubled every 1.5 years. This suggests an improvement ratio in the last 20 years of over 10000. In addition, over the same period, there have been major advances in the development of Graphical User Interfaces (GUI), operating systems, databases, Geographical Information Systems (GIS) and Internet technology. At the same time there are those who challenge the value of the investment in this technology and point to the “productivity paradox” which suggests that there has been a failure of ICT to deliver improved corporate performance, at least in financial terms. The question we ask is what impact has there been in the area of CPQRA?

This paper reviews the advances in CPQRA techniques made over the last 20 years in the light of the widespread development of ICT technology. It examines the progress made in a number of these areas including the steps taken to bring CPQRA up-to-date with 21st Century ICT, use of graphical user interfaces and other new technology such as databases, GIS systems and Internet technology, improvements in the underlying modeling technology, use of the risk analysis results to make decisions and communication of findings to stakeholders. A vision for the “ideal” CPQRA framework is postulated and a gap analysis is performed to benchmark this against the SAFETI QRA software package.

## 2 CPQRA TECHNIQUES – THE CURRENT SITUATION

As mentioned earlier, the last 20 years has seen massive advances in ICT. However, the methodologies used in performing QRA have generally remained relatively static. Most QRA's still follow the Classical Risk Analysis Methodology as illustrated in Figure 3. Although individual components of the QRA have improved in-terms of both modeling accuracy and speed of operation, the underlying architecture still largely supports the methodology shown above. This is the case for a number of reasons, not least the fact that QRA studies in tools like SAFETI have been created over many years and have taken many man years of effort which their owners are loath to “throw-away”. Often the cost of recreating these studies from scratch is prohibitive given the current difficulty with data reusability from other sources.

But there are limitations to maintaining this structure. New EU legislation encapsulated within the Seveso II Directive (Council Directive 1996), implemented in the UK as COMAH (HSE 1999), includes additional requirements such as the inclusion of domino effects (Petrolekas & Andreou 1999, Balocco et al. 2001 for example). These are difficult to account for using the classic approach, which is largely a series of sequential calculations or summations and assumes that hazardous

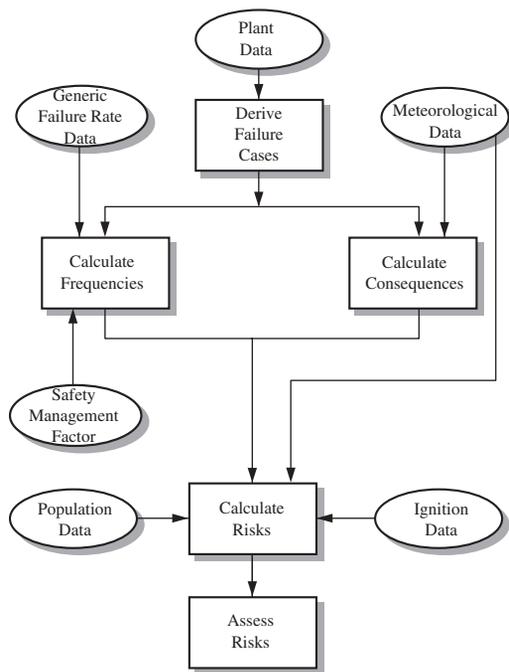


Figure 3. Classic risk analysis methodology.

events are independent of each other. Furthermore, restrictions associated with this sequential approach make it more difficult to take full advantage of ICT advances such as improved multi-tasking operating systems and client-server architecture as well as much more powerful client-server databases and network systems.

The data collection requirements when using tools like SAFETI for QRA are extremely labour intensive. The data used in QRA studies has historically been collected manually and is often stored in product specific databases which are essentially standalone. Although technologies like Computer Aided Design (CAD), Enterprise Asset Management (EAM) and Computerised Maintenance Management Systems (CMMS) contain much of the data required for a QRA study, links, where they exist, are rudimentary and largely unintelligent. Because of this data re-use has been poor and similar data may have been acquired in a number of separate places for process design, process simulation, maintenance management, inspection planning and QRA. Maintenance of data is a burden and yet neglect leads to degradation of its value. Seveso II also has additional requirements over its predecessor in respect of change management when performing risk assessment (Malmén 2001). This has repercussions for data management and version control of existing QRA studies which is very difficult within existing systems. However, if this data were available within a

	← Constraints	Drivers →
<b>Social</b>	Herd Behaviour	Public Perception of Risk
	Periods without Incident	Value of Life
	Demand for Products	Company Reputation
<b>Technical</b>	Lack of Validation of Risk Models	New ICT Technology
	Infeasibility of Realistic Experiments	Feasibility of Model Formulation
	Computing Limitations	Increasing Computer Power
	Uncertainty of results	New Experimental Data
<b>Environmental</b>	Periods without Incident	Accidents
		Near misses
<b>Economic</b>	Satisficing	Cost of Accidents
	Cost of Experimental Work	Value of Life
	Commercial Competition	Insurance Requirements
	Shareholder Expectations	Company Reputation
	Cost Benefit Justification	Understanding of Financial Risks
<b>Political</b>	Periods without Incident	Accidents
	General History of Industry	Near Misses
		Legislation/Regulations
		Value of Life
	← Constraints	Drivers →

Figure 4. Constraints and drivers for change in QRA technology.

CMMS or EAM system or even a data warehouse like Intergraph's SmartPlant Foundation (Intergraph, 2002), then providing facilities and procedures for change management could be comparatively straight forward.

### 3 DRIVERS FOR CHANGE

To put the ICT developments into context with respect to CPQRA Figure 4 explores the range of drivers and constraints on the development of this technology. Technical advances in ICT have been dramatic over the last 20 years and there are many other forces that have influence.

Relevant areas of ICT development are

- Computing "Power"
  - Processor speed
  - Computer memory
  - Storage capacity
- Distributed computing (PCs)
- Graphical User Interfaces
- Databases
- Networks
- Internet

These areas are considered in the following sections.

### 4 INCREASES IN COMPUTING POWER

At the time when the CPQRA techniques were developed (TNO 1980) computer limitations were a major constraint. As an example the dispersion models developed at that time simplified the problem to enable an integral approach to be taken. The resulting models could be executed in a practical time frame but took a simplistic view of the time varying nature of real clouds and neglected any local obstacles. Computation Fluid Dynamics (CFD) modeling was

available at that time and overcomes the limitation of the integral model approach. However, it is a far more computationally intensive technology and could not be conceived in the context of a QRA where many dispersion simulations are required.

With computing power increasing by more than 5 orders of magnitude over the last 20 years, it might seem logical that the simpler modeling techniques would have been displaced by the more complete models. However, CFD dispersion models are used in practice very rarely in the context of a QRA and the application of integral models remains the most normal approach. Furthermore, the conclusions of the EU model evaluation project SMEDIS (Cambridge Environmental Research Consultants, 2002) support the continued use of such models. These models continue to be developed to deal with obstacles (Cooper 2001) and terrain (Dutrieux and Van Mulder 1999) without resorting to CFD modeling.

Other areas of modeling employed in CPQRA may be visited to assess changes in this period in the light of the increase in computing power. Reviewing the changes in the Dutch "Yellow Book" between versions published in 1980 (TNO, 1980) and 1997 (Committee for the Prevention of Disasters, 1997) is one way to view the changes. Typically the changes are incremental rather than radical suggesting that computing power has had little influence.

It could be argued that explosion modeling methods have advanced more significantly over the last 20 years than the other techniques. Confined zone modeling is now a mainstream approach with the emergence of the Multi Energy and the Baker Strehlow Models (Baker et al., 1983). These techniques may now be used in QRA studies on a routine basis (Woodward J.L. & Crossthaite P.J., 1995). These techniques are more computationally intensive in the context of QRA than the simple TNT equivalence models (Technica, 1988, Lees 1980); mainly due to the calculation of the intersection of the cloud and the confinement zones for a range of times and wind directions. However, again this increase in computing requirement is relatively small compared to the available increase in power. Furthermore these methods do not apply the full modeling capabilities of the most advanced class of model, again CFD based. In contrast, in the offshore safety context, CFD has become an established method for analysing explosions and this remains a method that demands the maximum possible computing power.

Considering the SAFETI model, the changes with respect to modeling technique have also been incremental, rather than radical. When the first version was developed, numerous devices were required to enable the volume of data to be handled in terms of computation time, computer memory capacity and disk storage. As an example, flammable effect zones

were represented as a single elliptical zone because this information could be represented by just 3 numbers. Of course in reality the effect zone could have any shape depending on the radiation modeling but the approximate method was an acceptable approach at the time. Within the zone a single vulnerability factor was applied to any population present. A more rigorous approach is to use the calculated boundary of the effect zone directly. This requires the storage of more data which, with today's hard disk capacity, is no longer a constraint. As a further extension the concept of flammable probits can now be applied in a QRA (Ale & de Haag, 1999) because, whilst this approach is more computationally intensive, the demand is relatively small compared with the available increase in computing power.

Overall, while there have been some specific advances in modeling techniques in the last 20 years these changes are far less significant than the advances in computing power. We now look at the impact of advances in other areas of ICT.

## 5 DISTRIBUTED COMPUTING AND GRAPHICAL USER INTERFACES

The advent of the PC in this period has revolutionized the way users work with computers. When SAFETI was first developed it was installed on a central computer but now it is most commonly installed and run on local PCs. Calculations that might have taken days to run on a mainframe 20 years ago can now be run quickly on a PC. This is an area that has changed significantly within this time frame and has consequently had far more effect than advances in the modeling techniques themselves.

The software itself now employs graphical user interfaces as a significant advance from the teletype or menu driven interfaces of the past. The input data and results can be manipulated and presented in a far more visual way as illustrated in Figures 1 and 2. These are areas where ICT has had a major impact on the software tools.

## 6 DATABASES, NETWORKS AND INTERNET

Handling data using ICT has developed substantially over the last 20 years. State-of-art approaches to managing data within an organization now involve enterprise-wide systems with integrated financial, personnel and production software applications. They either handle the data within an application from one vendor or more commonly employ a number of applications that are interfaced so that they can share data. These developments have had a dramatic effect on the way data is used and shared. The data itself has a value to the organization in proportion to the extent it can be

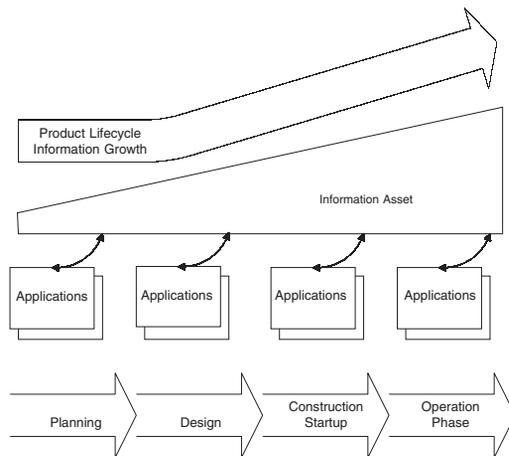


Figure 5. Information asset growth over the plant lifecycle.

distributed and shared. The synergy with network and internet technology developments makes enterprise-wide data sharing possible, adding enormous value to knowledge based organizations.

The concept of the “information asset” is illustrated in Figure 5 in the context of the process industry. As the plant progresses through its lifecycle the information asset grows as information is contributed and shared throughout the organization.

A case has been made for such integration in the Nuclear Industry (McPhater, 2002). Typically, the different types of input data required for a QRA will exist in datasets belonging to different departments. The software applications used to manage the data may come from different vendors and it is likely to be structured in different ways. This necessitates a common data modeling system so that the applications can communicate. Such systems are now emerging, like Intergraph's SmartPlant Foundation for example.

A QRA needs data from many sources as input to the calculations. Often this data will already exist in other applications within the organization but the entry and manipulation of this data for QRA remains a largely manual process.

Undertaking a QRA without software tools is labour intensive and this was a major motivation for the computerisation of the process and the development of SAFETI in the first place. In spite of such tools, QRA remains a time consuming and therefore costly task. Whether the analysis is performed using spreadsheets or a specific software tool designed for the purpose, like SAFETI, it is the preparation of the input data and the presentation of results that takes up most of the time and cost.

The latest version of SAFETI has taken a first step towards enabling integration by incorporating

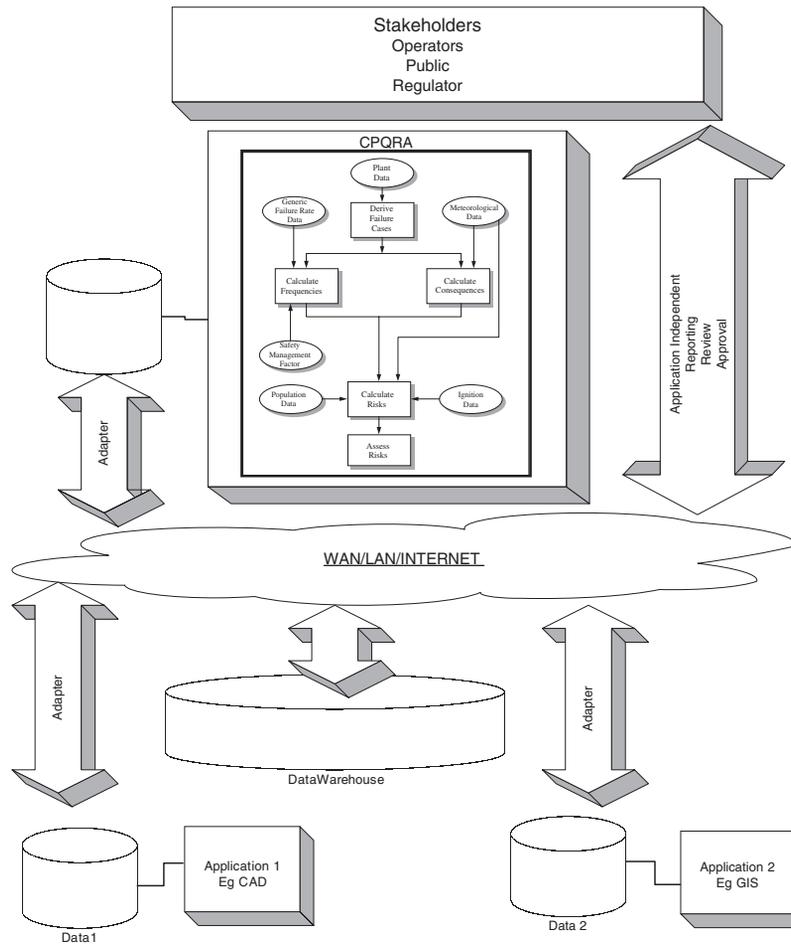


Figure 6. Integration of applications over the network/web.

Intergraph’s GeoMedia GIS system and this also permits publication of the results using the built-in integration capabilities. However, this addresses only a part of the input data requirements and the potential for better results communication.

7 THE FUTURE POTENTIAL

If the software applications used for the QRA were part of the organisation’s integrated system then it would have two direct benefits. One would be the reduced time to conduct the QRA as a direct saving of data input costs. Another would be the publication of the results. This concept of an integrated approach to QRA is something of a “vision” because of the lack of progress in this direction so far. Such a vision has the

potential to transform the QRA exercise from being a static analysis to providing live operational management information.

Currently, presentation of QRA results involves volumes of information normally presented in paper-based reports. These will often sit passively on the Safety Manager’s bookshelf, never providing all the potentially useful feedback possible. Web technology transforms the accessibility of all the information. If the input data were also live and the QRA results updated constantly then the risk information provided takes on a direct relevance not previously possible.

Figure 6 illustrates the potential with the QRA system linked to all other relevant applications via a shared data system. The QRA information would be available to all those with authorization via a Web browser. Version control of the data is facilitated through the data

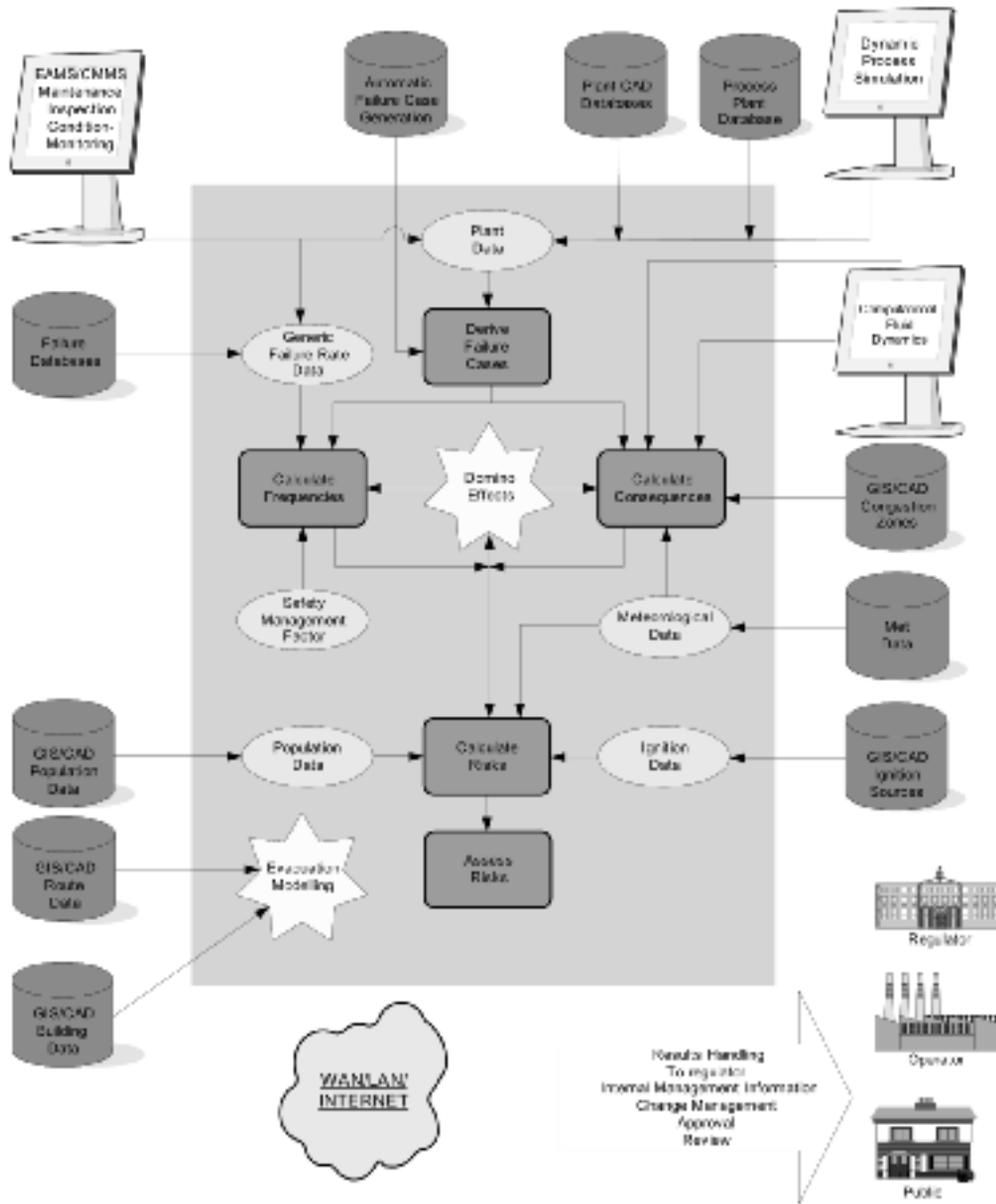


Figure 7. Integration potential for CPQRA.

management system and change management can be demonstrated as required by SEVESO II.

Synergy between the QRA analysis and other analytical views such as Environmental risks and Risk Based Inspection means such a live data connection has multiple uses. An integrated approach to viewing safety, environmental and financial risks becomes

possible and has multiple benefits. A business information “Dashboard” approach could make the results of such an integrated analysis live and online.

We speculate further that if such integration were implemented then there would be synergy between being able to take advantage of the more intensive computational methods. Figure 7 also illustrates the

potential for the use of applications during the QRA process that are currently regarded as too costly.

Dynamic process simulators for instance could be used to help improve the source term modeling. CFD models could be used routinely if the geometry could be input directly from CAD or GIS systems. The same information could be used directly for the consideration of domino effects. GIS systems are the natural place for population information, route information and objects relevant for ignition source identification. This information can be used directly in the QRA analysis and the analysis could be extended to take into account people's behaviour in buildings and along evacuation escape routes.

The enabling step for these developments is the integration of the QRA tools with the mainstream information systems. Currently, investments in the mainstream systems are primarily business information driven and QRA is not really a consideration.

## 8 CONCLUSIONS

We conclude that CPQRA techniques have exploited only a fraction of the potential advances offered by ICT developments. In the last 20 years the position has reversed regarding CPQRA and ICT with the advancement of the former now apparently lagging significantly behind the latter. No longer can it be claimed that the ICT environment limits CPQRA techniques. Moreover, CPQRA tools and techniques have not taken full advantage of all the possibilities made available by the technological revolution of the last 20 years.

The reasons can be assessed by viewing the drivers and constraints on CPQRA techniques. Factors other than ICT have varying influences and we conclude that these are the reasons for the exploitation of some but not all ICT developments in the period.

Looking forward we review the potential for further development and conclude that only by embracing integration possibilities, already proven in other application areas, will QRA step forward in utilizing ICT technology.

## REFERENCES

- Ale, B.J.M. and Uijt de Haag., 1999. Guidelines for Quantitative Risk Analysis, (CPR18) RIVM (Purple Book).
- Baker, W.E., Cox, P.A., Westine, P.S., Kulesz, J.J. and Strehlow, R.A., 1983. Explosion hazards and evaluation. *Fundamental Studies in Engineering*, Vol. 5, Elsevier, Amsterdam.
- Balocco, G., Carpignano, A., Di Figlia, G., Nordvik, J.P. and Rizzuti, L., 2001. Development of new tools for the consequence assessment of major accidents. *ESREL 2001, Towards a Safer World, Turin, September 2001*.
- Cavanagh, N., 2001. Calculating Risks, *Hydrocarbon Engineering, Volume 6, Number 6, June 2001*, Palladian Publications, London.
- Committee for the Prevention of Disasters. Methods for the calculation of physical effects, 1997. The Hague: SDU (Yellow Book).
- Cooper, G., 2001. A model for jet dispersion in a congested environment. *Research Report 396/2001, The Health and Safety Executive*.
- Council Directive 96/82/EC, 1996. On the control of major-accident hazards involving dangerous substances, *Official Journal of the European Communities, No L10, 14.1.1997*
- Dutrieux, A. and Van Mulder, G., 1999. The Seveso expert system "SEVEX"; an integrated approach for off-site effects analysis and effective emergency planning. In Seveso 2000, Editor G.A Papadakis, *European Conference on Risk Management in the European Union of 2000: The Challenge of Implementing Council Directive 96/82/EC "SEVESO II"*, Athens, November 1999.
- HSE (Health and Safety Executive), Environment Agency and Scottish Environmental Protection Agency, 1999. A guide to the Control of Major Accident Hazards Regulations.
- Intergraph, The Engineering Framework, Integrating the Plant Information Asset throughout the Plant Lifecycle, Intergraph Process, Power and Offshore, 2002.
- Lees, F.P., Loss Prevention in the Process Industries, 1980. Butterworths, London.
- McPhater, N., 2002. IT software in the nuclear industry. *The Chemical Engineer, December, Institute of Chemical Engineers, UK*.
- Malmén, Y., 2001. Is EU's Seveso II Directive leading to a more systematic use of risk assessment methods? – A Finnish case-study. *ESREL 2001, Towards a Safer World, Turin, September 2001*.
- Petrolekas, P.D. and Andreou, I., 1999. Domino effects analysis for LPG storage installation of Hellenic Petroleum Aspropyrgos refinery. In Seveso 2000, Editor G.A Papadakis, *European Conference on Risk Management in the European Union of 2000: The Challenge of Implementing Council Directive 96/82/EC "SEVESO II"*, Athens, November 1999.
- Salzano, E., Marra, F.S. and Russo, G., 2001. Gas explosion consequences in industrial environment. *ESREL 2001, Towards a Safer World, Turin, September 2001*.
- TNO, 1980. Methods for the calculation of the physical effects of the escape of dangerous materials (liquids and gases). *Netherlands Organisation for Applied Scientific Research, Directorate General of Labour*.
- Worthington, D.R.E. and Witlox, H., 2002. SAFETI Risk Modelling Documentation – Impact of Toxic and Flammable Effects, *DNV Software Risk Management Solutions, October 2002*.
- Cambridge Environmental Research Consultants Ltd., 2002. SMEDIS Model Evaluation Report on UDM Version 6.0, SMEDIS/00/9/E.
- Technica, 1988. Techniques for assessing industrial hazards – manual. World Bank technical paper no. 55a.
- Woodward J.L. and Crossthwaite P.J., 1995. How to set explosion protection standards. *Hydrocarbon Processing, vol. 74, no. 12*.

## Introduction of an easy-to-use risk assessment tool for natural gas transmission pipelines

Jeroen Zanting, Johan Duinkerken & Robert Kuik

*Gasunie Research, The Netherlands*

Rein Bolt & Eric Jager

*Gastransport Services, The Netherlands*

**ABSTRACT:** A new pipeline safety program has been developed by Gasunie Research to carry out a quick risk survey of (part of) a pipeline. The survey results in appropriate proximity distances, individual risk contours, societal risk and gas dispersion levels. This program is meant to fill the gap between applying rules of thumb and an extensive risk analysis. All the results are graphically presented on a topographical map of the area. The program uses data from validated and internationally acknowledged models, which are approved by the Dutch Government. Although the program is developed to carry out risk assessments according to Dutch standards, it can be easily adapted to comply with other standards. The amount of input parameters is limited to a few network and surroundings parameters, which makes it very suitable to carry out a preliminary study of the risk in the design phase of the pipeline. It can also be used for existing pipelines in changing surroundings. Some of the major characteristics of the program are: It saves money and time on risk assessments of new and existing pipelines and is to be used by non-specialists. The graphical interface enables quick and easy use.

### 1 INTRODUCTION

Gastransport Services owns and operates most of the natural gas transmission network in the Netherlands. The pipeline system consists of about 11600 kilometres of steel pipe. Most of it has been in use for over 30 years. The system is divided into a 66 bar high-pressure part (about 5100 km) with diameters ranging from 18" to 48" (HTL) and a 40 bar regional system (about 6500 km) with diameters ranging from 4" to 16" (RTL).

A lot of effort is invested to maintain the excellent safety record of the gas transmission network. During different stages in the life cycle of pipelines, the safety performance is subject to study. In the planning and construction phase, the safety aspect is a very important factor to establish the most suitable route. When the pipeline is in operation, the surroundings of the natural gas pipelines are subject to change: due to expansion of residential, commercial or industrial areas more and more people are likely to live or work relatively close to the pipeline. In some cases destination plans alter. The rural surroundings of the pipeline can change into heavily populated recreational facilities or other valuable infrastructure facilities are built in the vicinity of the pipeline.

### 2 THE PROBABILISTIC APPROACH

The risk-based approach has been used in the Netherlands for several centuries. In the long struggle of the Netherlands against the flooding seawater and rivers, risk assessment appeared to be very useful to assess the risk of flooding. To avoid flooding, dikes (and other infrastructure) were built. A higher level of protection required an enormous increase in costs. Therefore, risk assessments were used to estimate the heights of the dikes to achieve an acceptable risk level. This saved a considerable amount of money. After a major flooding occurred in the province of Zeeland (Netherlands) in the fifties of the last century, a major delta plan was developed to reduce the flooding risk. For this risk reduction a quantitative risk approach was used.

#### 2.1 Individual risk

The Netherlands have developed two risk criteria for the industry. The first deals with the risk of an individual who lives near a potentially hazardous location. This is called individual risk. The criterion is that the individual risk should be lower than  $10^{-6}$  year<sup>-1</sup>. It is defined as the fatality rate at a point if someone

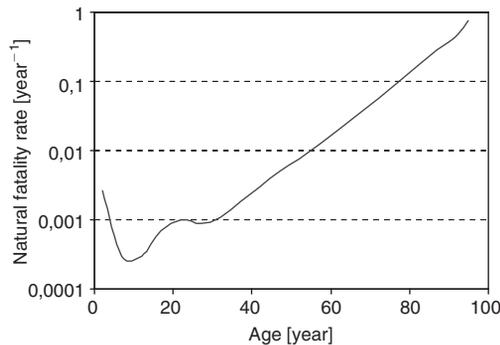


Figure 1. Natural fatality rate for people in 2000 (source: CBS, 2002).

would be present at that point 100% of the time unprotected by clothes or buildings. Also the individual is not allowed to escape if the incident takes place, but on the other hand the scenario takes into account only 20 seconds of the incident. So in case of a fire the individual will dose up radiation for 20 seconds.

The origin of the risk level of  $10^{-6} \text{ year}^{-1}$  is based on the natural fatality rate for people. Statistical data lead to the distribution of the natural fatality rate presented in figure 1.

The approach chosen by the Dutch government is that the risk on people caused by industrial activities should be lower than a factor 100 compared to that period in a human life with the lowest natural fatality rate. This lowest fatality rate is  $10^{-4} \text{ year}^{-1}$  at the age of 15. Therefore the risk due to industrial activity should be at maximum  $10^{-6} \text{ year}^{-1}$ . Therefore the maximum allowed risk due to pipelines is set at  $10^{-6} \text{ km}^{-1} \cdot \text{year}^{-1}$ .

## 2.2 Societal risk

The second criterion deals with societal risk. It is defined as an F-N curve: The maximum frequency F for N or more people that would suffer loss of life in one incident. For point sources like compressor stations or chemical plants (anything with a fence around it) the criterion is  $F \cdot N^2 < 10^{-3} \text{ year}^{-1}$ . For transportation type locations like motorways, railroads, canals and pipelines the criterion is  $F \cdot N^2 < 10^{-2} \text{ km}^{-1} \text{ year}^{-1}$ . In the societal risk calculation again 20 seconds exposure and no escape is assumed, but the fraction of the persons that are inside a building which is located outside the house burning distance will survive. Also for societal risk people outside will be protected by clothes.

The criteria for the individual risk and the societal risk are described in detail in "purple book" [1]. For

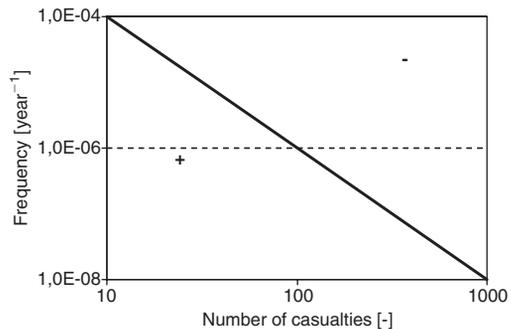


Figure 2. Societal risk.

pipeline fires the dose effect calculation is based on the "green book" [2].

The F-N curve for transportation facilities is displayed in figure 2.

If the societal risk in figure 2 is in the area marked with a plus sign (+) the risk is acceptable, if the societal risk value crosses the black diagonal and reaches the area marked with a minus sign (-), the societal risk is unacceptable.

## 3 NECESSITY OF RISK ASSESSMENT FOR TRANSMISSION PIPELINES

For transmission pipelines it is not necessary to make risk assessments for all locations. There is a list of proximity distances for different diameters and pressures. These are in the pipeline code [3] and in a ministerial circular letter [4]. It is assumed that if people would build houses outside the proximity distance the individual risk would be low enough. Because of the fact that understanding of risk has developed in the last two decades, these distances are now recalculated with PIPESAFE [5]. To accommodate for the societal risk tables are developed to allow a maximum number of people per hectare outside the proximity distance. It is assumed that these tables will be published by the regulator in 2003, most likely as an order in council. Only in special cases (proximity distance infringements, population concentrations which can not be assumed to be evenly distributed) risk assessments have to be carried out.

The gap between applying the numbers from the above mentioned table and a full size risk analysis is considerable. Therefore, within Gasunie Research a new tool has been developed to carry out a simplified risk assessment to fill this gap. With minimal effort, individual and societal risk are (graphically) compared with the appropriate criteria. If, according to the new tool, the criteria are exceeded, a full risk assessment is still necessary, due to the conservative approach in

the tool. When this tool indicates that the criteria are not exceeded, the costs of a detailed risk assessment can be saved. This may lead to a significant cost reduction.

#### 4 FULL RISK ASSESSMENT

When a full risk assessment is carried out, Gasunie Research uses the PIPESAFE package. PIPESAFE is a package that consists of various modules, for instance: failure frequency analysis models, gas outflow models, heat radiation models and lethality models resulting in the individual and societal risk. These models have been developed by a group of international gas transport companies and have been approved by the Dutch government for use in risk assessments of high-pressure natural gas pipelines. In these models about a hundred parameters are used, categorized in: pipeline (or network) data, gas properties, environmental/atmospheric data (including wind distribution), specific data for failure frequency analysis, model parameters for gas outflow calculations, crater formation parameters, ignition probability, heat radiation parameters, exposure and escape options and site properties.

Gathering the data for these parameters is very time consuming. Very often, with a few well-chosen parameters, a conservative estimate of the situation can be made with the new tool. If the calculated risks do not fulfil the criteria for individual risk and societal risk, a full size risk calculation has to be made.

#### 5 NEW APPROACH

The approach that has been chosen in the simplified risk assessment model is that with five essential parameters of a gas transportation network the risk can be calculated. These calculations are carried out in the following steps: failure rate assessment of the pipelines, determination of the gas outflow, calculation of the heat radiation and the corresponding lethality for people. The five parameters are: Pipeline diameter (D), wall thickness (w), internal pressure (P), depth of cover (z) and steel type (S). Besides these parameters, coordinates of the pipeline and coordinates of buildings are needed.

##### 5.1 Model description

In this paragraph is explained how the existing modules in PIPESAFE have been used to generate the required results for the simplified model.

###### 5.1.1 Failure frequency

The failure rate is calculated with historical pipeline failure data, resulting from over 30 years incident

registration. In these incident databases the different types of incident causes, like external interference, corrosion, material defects et cetera are distinguished. Also the incident type is registered, for instance: a dent, a hole, or a full bore rupture. From all these incidents the pipeline parameters like diameter, wall thickness, steel type and depth of cover are entered in the table as well. This enables statistical analysis of the incidents. With fracture mechanics the probability that a hit pipeline will fail is calculated. With the incident registration and fracture mechanics, the influence of extra wall thickness, extra depth of cover, and the steel grade is quantified. This leads to a very reliable number for the failure frequency. In this model, only the frequency of a full bore rupture of a pipeline is used, since this dominates the risk for the surroundings.

Apart from the corresponding failure frequency, also the failure frequency when mitigation measures have been taken to protect the pipeline from third party interference (i.e. buried warning ribbon above the pipeline, buried concrete slabs or a combination of both) can be used in the risk assessment. The failure frequency is corrected for the depth of cover with a formula derived by Gasunie Research. This formula is based on incident data analysis [6].

###### 5.1.2 Gas outflow

For pipeline ruptures the gas outflow can be calculated by BRAM [7], developed by Gasunie Research. In this model the physical phenomena that occur when a pipeline depletes through a hole or a full bore rupture are mathematically solved. Also, the outcome of BRAM has been tested against field tests. These field tests proved that BRAM provides reliable results.

To be able to use this model, a parameter fit has been carried out for all relevant RTL and HTL pipelines. This resulted in a simple parametric function with only pressure and diameter dependency that yields the gas outflow as a function of elapsed time. With the current directions in the Netherlands, the average outflow of the first twenty seconds is used to calculate the subsequent heat radiation.

###### 5.1.3 Heat radiation

In the simplified risk assessment model the risk calculations are carried out assuming that once a pipeline is ruptured, the gas will always ignite (the ignition probability is one). Incident reports show that in real life only a certain part of the incidents has lead to ignition of the released gas. In order to be conservative on the heat radiation, the decision was made to calculate the heat radiation downwind from the outflow, assuming an average wind velocity. For several RTL and HTL configurations the heat radiation field have been calculated, by the PIPESAFE module

CRISTAL. The resulting values have been incorporated in a database that is used as a look-up table. With the diameter, the pressure, the elapsed time and the distance to the ruptured pipeline, the corresponding heat radiation can be read. When non-standard pipelines are to be assessed, the radiation is interpolated between pipelines with lower and higher diameters.

#### 5.1.4 Lethality

The calculation of the lethality is carried out with the so-called dosage that is the input for the Probit equation. The dosage is calculated by equation 1

$$\text{dosage} = Q^3 \cdot t \quad (1)$$

where:

$$Q = \text{heat radiation (kW/m}^2\text{)}$$

$$t = \text{exposure time (s)}$$

The Dutch guidelines on risk assessment states that people are exposed to the heat radiation for twenty seconds, without the possibility to escape from the heat source. To calculate the lethality, the dosage is entered in a Probit function, equation 2.

$$\text{Probit} = A + B \ln(\text{dosage}) \quad (2)$$

where:

A and B are constants

Consequently the Probit is inputted in the cumulative standard deviation distribution, which leads to a mortality, equation 3.

$$p = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\text{probit}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} dx \quad (3)$$

where:

$$p = \text{mortality (-)}$$

$$\sigma = \text{standard deviation (=1)}$$

$$\mu = \text{mean (=5)}$$

For use in the societal risk calculation, the lethality for persons is subsequently corrected. Within the 35 kW/m<sup>2</sup> heat radiation level, it is assumed that houses will burn and all persons present, inside or outside, will become fatalities. The number of inhabitants is corrected by the fraction of absence during the day and night. Outside the 35 kW/m<sup>2</sup> heat radiation level the assumption is people indoor will survive the heat radiation and that people outside will have a probability of suffer loss of life that is calculated by the lethality. Furthermore, people are supposed to be partly shielded by their clothes, this lowers the mortality rate significantly.

#### 5.1.5 Coordinates

To be able to study the consequence of pipeline failure to the surroundings, the position of the pipeline to the neighbouring buildings is necessary. Therefore, a coordinate system had to be chosen. For the Dutch version, the coordinates used are from the national coordinates system. This coordinate system has its origin Amersfoort (a city centrally situated in the Netherlands, such chosen that no negative values for the coordinates exist within the boundaries of the country). For each pipeline segment that is to be examined, the appropriate coordinates from these segments are entered. These are the basics for the graphical presentation of the results. The locations of buildings are entered in the computer program as well. The coordinates of each house, residential block, hospital, office building, workplace or recreational facility are entered with the corresponding population.

#### 5.1.6 Individual risk

The calculation is carried out in a grid with a grid size of one metre. For each grid cell, the failure rate of the pipeline is multiplied with the lethality at this location. This results in the individual risk value at this cell. The cells that approximate one of the 10<sup>-5</sup>, 10<sup>-6</sup> or 10<sup>-8</sup> year<sup>-1</sup> risk number best, are connected and form the desired risk contour.

#### 5.1.7 Societal risk

With the distribution of the buildings around the pipeline, the societal risk is calculated. Again the failure frequency and the lethality field are used. In this calculation, the lethality regimes (within and outside the 35 kW/m<sup>2</sup> distance) are needed as well. This calculation divides the pipeline in small segments and counts the number of victims if an incident occurs at that segment.

With the distribution of casualties along the stationing, a subroutine checks if a kilometre of pipeline can be identified where the societal risk criterion is exceeded. If the criterion ( $F \cdot N^2 < 10^{-2} \text{ km}^{-1} \cdot \text{year}^{-1}$ ) is indeed exceeded, the section of pipeline of one kilometre that is used to calculate the F-N-curve is chosen such that the worst case F-N-curve is identified. The F-N-curve displays the frequency that N (N is any whole number starting by ten) or more casualties are expected.

So, the F-N-curve is constructed from a cumulative table. For example: there are n1 sections with failure frequency F1 that can lead to N casualties (with N is the maximum number of casualties) and there are n2 sections with failure frequency F2 that can lead to N-1 casualties. In the F-N-curve, the corresponding failure frequency of N casualties is n1F1 [year<sup>-1</sup>], the failure frequency of N-1 casualties will be n1F1 + n2F2 [year<sup>-1</sup>]. This procedure is repeated until N = 10.

## 6 GAS DISPERSION

If a full bore rupture of the pipeline occurs, there is a high probability that the resulting gas outflow does not ignite at all. In this case, a gas cloud is the result of the pipeline failure. The size of the gas cloud can cover a large area and is of course dependent of the pressure and the diameter of the pipeline. Also the atmospheric conditions have a major influence on this size. In case of a pipeline rupture, the size of the gas cloud is important information. To prevent the gas cloud from igniting after some time, all buildings within a certain fraction of the lower flammability level are evacuated by the emergency services. Therefore the size of a possible gas cloud should be used in a risk assessment.

In this tool, for every pipeline diameter and pressure combination, gas cloud calculations have been made, again assuming an above average heavy wind speed. Since no information on wind directions is available on forehand, the approach is to calculate the downwind cloud size and project this in a circular contour around the ruptured pipeline. Due to the initial momentum of the gas outflow and the buoyancy the released gas will rise quickly. Therefore, the indicated cloud size (presented at 50% of the lower flammability limit) is calculated at a height of ten metres. It is assumed that at this height no ignition sources are present (in situation where facts do not agree with this assumption, a detailed calculation is advised).

## 7 USER INTERFACE

One of the key features of the new easy to handle risk assessment tool is that it enables the users to do a quick survey of the risk that the pipeline in question pose on the surroundings. This is guaranteed by two aspects: restricting the number of input parameters and maintaining a clearly structured user interface. Therefore, all inputs and outputs are on one screen. On one side the pipeline and the inhabitants parameters. On the other side of the screen a large overview of the site is displayed, which is directly updated upon input of one of the input parameters. Some other buttons are necessary to select the desired criteria for individual and societal risk. When selecting the criteria, the program directly calculates the risks and draws the appropriate individual risk contours on the site map. The pipeline (section) is marked if it exceeds the societal risk criterion. Finally, a report is generated with the conclusions regarding the safety of the site: is this site acceptable in risk terms, or is an advanced risk assessment necessary in this case. In this short report the input parameters and the graphical lay out of the site with the selected risk results are presented.

## 8 OUTPUT

To demonstrate how the outputs of a risk survey with the risk assessment tool can be carried out, in this section some example are shown. From part of a pipeline of Gastransport Services the coordinates and properties are inputted in the program. These coordinates and properties lead to the individual risk as plotted as the red outer lines in figure 6. In the next step the nearby houses and other buildings are identified. The buildings appear as blue-circled objects. The result is presented also in figure 3.

The societal risk criterion is met in this situation. This leads to the F-N-curve in figure 4.

The gas dispersion cloud in case of a pipeline rupture on this individual is displayed in figure 5. The circular shape indicates where the gas concentration reaches 50% of the lower flammability limit.



Figure 3. Screen output of  $10^{-6}$  year<sup>-1</sup> individual risk contour.

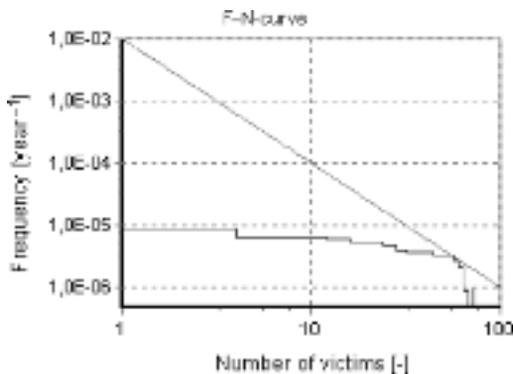


Figure 4. F-N-curve.

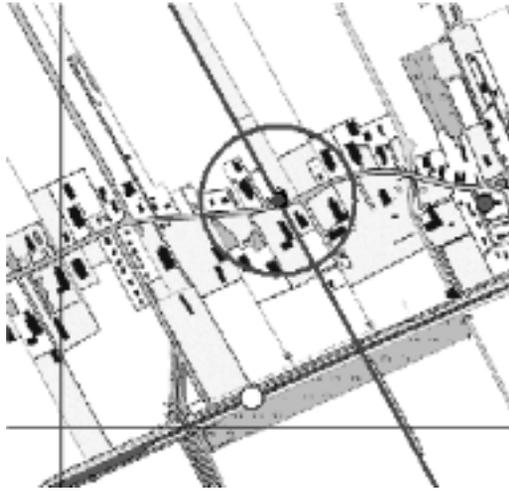


Figure 5. Gas dispersion cloud size.

## 9 CONCLUSIONS

The developed easy-to-use pipeline safety program works very intuitively and enables users to make a quick survey whether a pipeline fulfils the risk criteria. This can be used in the design phase of a pipeline when an optimal pipeline route needs to be found. By altering the pipeline properties (increasing the wall thickness or depth of cover) the minimum configuration of the pipeline for the studied route can be found. For existing pipelines when improved failure rate data of the transmission system becomes available, checks can be made whether the safety situation is still up to standards or mitigating measures have to be taken. In case of proposed changing of the surroundings of the pipeline it is possible to check whether the changes comply with the risk regulations. Recommendations to destination plans can be made with the results of the risk study. Especially in a densely populated country

as the Netherlands and indeed a lot of other countries, this type of calculations is often needed. With the simple but efficient approach of this program a significant amount of valuable time can be saved.

Due to the very advanced failure rate and failure consequence models that are used, a highly reliable though conservative answer can be expected. If the easy-to-use pipeline safety program indicates that the pipeline meets the criteria, than no further risk studies are needed. If the criteria are exceeded, a further risk investigation is recommended. With the PIPESAFE package a full risk assessment can be carried out to determine whether the approach in the easy-to-use tool might be too conservative in that case.

With this approach, this new tool is very useful to fill in the gap between simply applying the rules of thumb and carrying out a complete risk assessment.

## LITERATURE

- [1] Committee for the Prevention of Disasters, Guidelines for Quantitative Risk Assessment CPR18E, 1999.
- [2] Committee for the Prevention of Disasters, Methods for the determination of possible damage CPR 16E, 1992.
- [3] Nederlands Normalisatie Instituut, NEN 3650 Eisen voor stalen transportleidingen (requirements for steel pipeline transportation systems), 1992.
- [4] VROM (Ministry of Housing, Spatial Planning and the Environment), Zonerings langs hogedrukleidingen (zoning along high pressure pipelines), 1984.
- [5] Acton, M.R., Baldwin, P.J., Baldwin, T.R., and Jager, E.E.R., The development of the PIPESAFE Risk Assessment Package for Gas Transmission Pipelines, Proceedings of the International Pipeline Conference, ASME International, Book No. G1075A-1998.
- [6] Eric Jager, Robert Kuik, Jeroen Zanting, Gerard Stallenberg: The Influence of Land Use and Depth of Cover on the Failure Rate of Gas Transmission Pipelines, Proceedings of the International Pipeline Conference IPC02-27158, ASME International, 2002.
- [7] Internal Report.

## Towards a qualitative predictive model of violation in transportation industry

Z. Zhang, P. Polet, & F. Vanderhaegen

*Laboratoire d'Automatique, de Mécanique et d'Informatique industrielles et Humaines (LAMIH),  
 University of Valenciennes, Valenciennes Cedex, France*

**ABSTRACT:** This paper focuses on the prospective analysis of potential violation, called Barrier Removal (BR) with emphasis on the transportation applications. Based on BR indicator data in terms of different performance criteria and the corresponding statistics, probabilistic prediction of the removal of a changed/new barrier is implemented. This is called the removal prediction based on a Neural Network model. Moreover, a concept of Erroneous Barrier Removal (EBR) is discussed. EBR can be identified in terms of different performances criteria. The feasibility study on a research simulator is finally illustrated.

### 1 BARRIER CONCEPT

The risk analysis of a Human-machine system (HMS) contributes to identify combinations of technical failures and human errors that lead to unwanted events. In order to avoid the occurrence of these events the designers provide the system with means. These means aim at decreasing the event occurrence probability (prevention means) and/or at reducing the event impact (protection means). These means of prevention/protection constitute a set of defence-in-depth (Reason, 90). They are called barriers. A barrier is defined as an obstacle, an obstruction or a hindrance that may either (Hollnagel, 99a):

- Prevent an action from being carried out or a situation to occur,
- Prevent or lessen the severity of negative consequences.

Four classes of barriers are distinguished:

- Material barriers: barriers that physically prevent an action or limit the negative consequences of a situation,
- Functional barriers: barriers that logically or temporally link actions and situations,
- Symbolic barriers: barriers that require interpretation,
- Immaterial barriers: barriers that are not physically in the work situation.

The barrier concept is common in the field of nuclear safety, but also in other areas (Lars Harms-Ringdahl,

1998). Based on barrier classification, several retrospective accident analyses have been conducted. It is noted that the barrier concept also plays an essential role in system design. Barriers are placed by the designers in order to guarantee a safe space of use. The study of the barriers placed in a HMS can be used to identify the normal functioning mode accepted and prescribed by the designers (Cf. Fig.1).

Three reasons can explain in exploitation phase the observation of non-tolerated, regarding designer point of view, functioning mode:

- Lack of barrier: some situations are not considered by the designers and there is no barrier to prevent

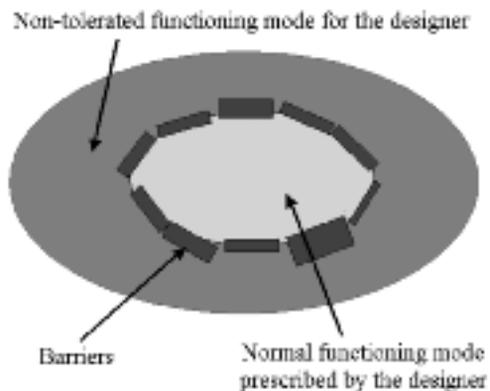


Figure 1. Delineation by the designer of accepted functioning modes, regarding barriers.

- or protect human operators from particular event leading to non-tolerated space.
- Failure of barrier: a barrier is a component of the system that can fail and become non-operational to ensure its function.
- Inhibition of barrier: a material or a functional barrier can be deactivated by users, and symbolic or immaterial barriers can be not respected by users.

This third reason is our subject of study. It refers to the notion of human error.

## 2 HUMAN BEHAVIOUR FACING BARRIERS

The human error is defined as the result of “actions that exceed some limit of acceptability” (Swain, 83). Reason /90/ distinguishes errors such as slips, lapses or mistakes and violations. The consequence or the occurrence of a slip/lapse/mistake is unintentional whereas the occurrence or the consequence of a violation is intentional.

Regarding designer viewpoint, the inhibition of a barrier can be an error or a violation of users: it is either a non-intentional inhibition (slip, lapse or mistake) or an intentional deviated behaviour (violation). In the first case “traditional” human reliability assessment methods may be used to predict this kind of errors. In the second case Polet et al. (2002) propose a model of these violations so-called barrier crossing<sup>1</sup>. A barrier removal is an intentional misuse or disobeying of a barrier provided that adequate conditions are present. The causes of a barrier removal may be:

- A motivation to improve the performance by means of improving the working conditions, or
- A motivation to realise a triumph over the automation (based on operational experience).

The operational risk of a barrier removal is a combination of a cost of the removal, of an immediate benefit after a removal and a possible deficit due to the removal:

- The immediate cost of removal: in order to remove a barrier the human controller has to modify sometimes the material structure (essentially for material and functional barrier), and/or the operational mode of use (essentially for symbolic and immaterial barriers). It usually leads to an increase of workload, but can have negative consequences on productivity or quality.
- A barrier removal is goal driven. Removing a barrier is immediately beneficial. The benefits outweigh the costs.

<sup>1</sup>In the transportation domain, “Barrier Removal” is used.

- A barrier that is removed introduces a potentially dangerous situation. So, the removal of a barrier has also a possible deficit.

## 3 REMOVAL PREDICTION OF A CHANGED/NEW BARRIER

To identify the BR during the analysis of a new barrier or of a new risk for the designer during the earlier design phase or in the re-design, a method integrating three different neural network algorithms have been developed (Zhang et al., 2002a):

- In the Unsupervised SOM<sup>2</sup> (Kohonen, 1990, 2001; Héroult et al., 1994), the input data are the subjective evaluations of benefit, cost and possible deficit in terms of different performance criteria;
- In the Supervised SOM, the input data are as same as the ones of Unsupervised SOM, but with a removal label of the corresponding barrier (Zhang et al., 2002c);
- In the Hierarchical SOM (Zhang et al., 2002a), the input data are as same as the ones of Supervised SOM, the network can be realized by classifying into certain parallel subset according to the characteristics of human controller, e.g. experimental BR data may be grouped into several subset in terms of controllers’ nationalities.

However, the subjective evaluation was made class by class without considering the differences between the barriers of a same class. The removal prediction is therefore performed for a class of barrier, not for a single barrier. The judgment of whether a barrier will be removed or not is subjective and concerns the traffic controllers’ opinion.

In order to study the human (un)reliability in the safety and conformity assessment on the transportation system, a systemic analysis approach for human factor impact on Functional Requirements Specification (FRS) is being studied. This approach finally provides designers tools to support the prediction of removal of a changed/new barrier. It should be able to deal with not only the subjective judgment according to the BR indicators, but also the objective data on the performance criteria.

### 3.1 Reconfiguration of BR indicator data

During the identification of the final removal result, a barrier has been judged “removed” so long as one barrier of a same class is removed. Some controllers removed a few number of signals, and the others removed all signals of the same class, both of cases have been identified “removed” before. E.g. it was

<sup>2</sup>SOM: Self-Organizing Maps.



Figure 2. Structure of input data of BR.

observed that arrival signals at the depots are always removed whereas the ones for departure movement were sometimes respected. Both of them have been considered as same barriers. In a same barrier class, different controllers can remove different number of barriers.

In order to make the prediction of the removal of a changed/new barrier as close as possible to its objective result, the subjective evaluation in terms of different performance criteria are made barrier by barrier. Fig. 2 shows the structure of input data during the SOM learning and removal prediction.

In the figure, the horizontal axe is represented by the different BR indicators in terms of different performance criteria. In case of mono-performance mode (Zhang et al., 2002b) the horizontal direction can be, for instance, criterion 1: workload-benefit, criterion 2: workload-cost, criterion 3: workload-deficit<sup>3</sup>; at the vertical axe, all scenarios are listed. Each controller can remove several classes of barriers, (s)he can remove different barriers in the same class as well.

### 3.2 Discovering & memorising the similarities between all BR scenarios

The similarities between all BR scenarios can be discovered and memorised by training relative neural networks. The SOM networks are used in this paper.

The SOM consists of two layers: the input layer and competitive layer (output layer), which is usually a two-dimensional grid. Both of these layers are fully interconnected. The input layer has as many neurons as it has indicator data (e.g. workload-based criteria: workload-benefit, workload-cost, workload-possible deficit). Let  $m$  be the number of neurons in the input layer, and let  $n$  the number of neurons in the output layer that are arranged in a hexagonal pattern (see Fig. 3). Each neuron in the input layer is connected to each neuron in the output layer. Thus, each neuron in

<sup>3</sup>If it concerns Supervised SOM, there will be the criterion 4: result of removal.

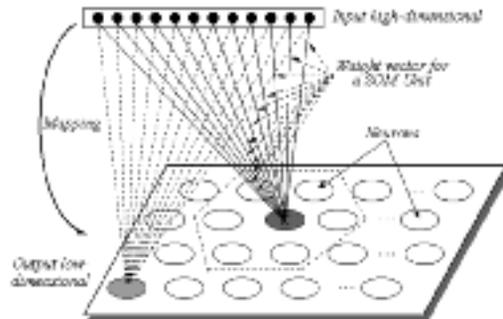


Figure 3. Graphical illustration of a SOM architecture.

the output layer has  $m$  connections to the input layer. Each one of these connections has a synaptic weight associated with it. Let  $W_j$  the weight vector associated with the connection between  $m$  input neurons  $i = 1, \dots, m$  and one output  $j = 1, \dots, n$ . The neurons of the maps are connected to adjacent neurons by a neighborhood relation. Each neuron  $k$  is represented by a  $m$ -dimensional prototype vector  $W_k = [W_{k1}, \dots, W_{km}]$ , where  $k = j = 1, \dots, n$ . On each learning step, a data sample  $\xi$  is selected and the nearest unit, best matching unit (BMU)<sup>4</sup> is found from the map. The prototype vectors of the BMU and its neighbors on the grid are moved towards the sample vector.

Based on learning in terms of indicator data, removal predictions can be made prospectively for a changed/new barrier (for more detail, please see Zhang et al., 2002c).

In Fig. 4, a structural illustration of statistics on the BR indicator data is shown. The removal probability/frequency of a barrier corresponding to a combination of different indicators parameters can be obtained.

Based on the data about the different BR indicators and the corresponding removal probabilities/frequencies, the probabilistic similarities between all input scenarios can be found out and memorised through training neural network with input data matrix. Based on the statistical data and perception data on removal of barriers, removal predictions can be made for the changed/new barriers. The removal prediction result will be removal state (removal or not removal), as well as relative probability.

Note that the data sources for learning of the connectionist network may belong to either of two categories: Human-machine system, and system simulators (Hollnagel, 1981). Within each of these categories one may distinguish several different types. For instance,

<sup>4</sup>BMU: the output layer neuron whose weight vector is closest to the input vector  $\xi$  is called Best-Matching Unit (BMU).

	Benefit	Cost	Deficit	Result of Removal	Probability	
Removal of barrier	Very high	Low	Low	Yes	10%	
		Very Low	Very Low	Yes		
	High	Normal	Normal	Yes	Non.	
		Low	High	Yes		
		Very Low	Normal	Very Low	Yes	Non.
			High	High	Yes	Non.
	Normal	Normal	Normal	Yes	Non.	
		Low	Low	Yes		
		Very Low	Very Low	Very Low	Yes	Non.
			Low	Very Low	Yes	Non.
	Low	Low	Low	Yes	Non.	
		Very Low	Very Low	Very Low	Yes	Non.
			Low	Very Low	Yes	Non.
		Very Low	High	High	Yes	Non.
	Normal		Low	Yes		
			Normal	Normal	Yes	
	Low		Very Low	Very Low	Yes	
			Very Low	Very Low	Yes	
	Very Low		Very High	Yes	Non.	

Figure 4. Illustration of statistics on the BR indicator data.

the following distinct sources of data could be considered,

- Routine event reports, it includes near-miss report, incident/accident report, etc.
- Audit, inspection reports, interview.
- Training simulator data (if exist).
- Research simulators
- Etc.

Research simulators data (Data on TRANSPAL) are used in the paper. Based on the learning phase, removal predictions can be made for the changed/new barriers.

#### 4 ILLUSTRATION ON TRANSPAL

##### 4.1 Research simulator

TRANSPAL (Vanderhaegen et al., 2002) is an experimental platform developed in order to study barrier removal (Cf. Fig. 5). The platform aims at simulating pallets movements on railway system from depots to several workstations. Several barriers were defined:

- Depot, station and switching device signals. There are signals that are red to stop a pallet or green to authorize it to move. When a pallet has removed the signal, the signal fire has to be put back on red.

- Minimum distance control. It is prohibited to authorize a pallet movement if the separation between this pallet and another one is under a defined distance.
- Switching control. It is prohibited to operate on a switching device if there is a train moving on the corresponding route.

Two experiments are planned:

- One with all the designed barriers,
- One with the barriers selected by the human controller who controlled the traffic.

Several performances will be considered:

- The respect of scheduled time,
- The synchronisation of the announcement before arriving into and leaving from a workstation,
- The traffic safety,
- The human workload in term of number of action.

After each experiment, a questionnaire focuses on the evaluation of the interest of all barriers in terms of benefit, cost, potential deficit.

##### 4.2 Removal prediction of the probabilistic similarities for a changed/new barriers

In order to verify the feasibility of the proposed model, Depot signals, Shunting signals and Stop

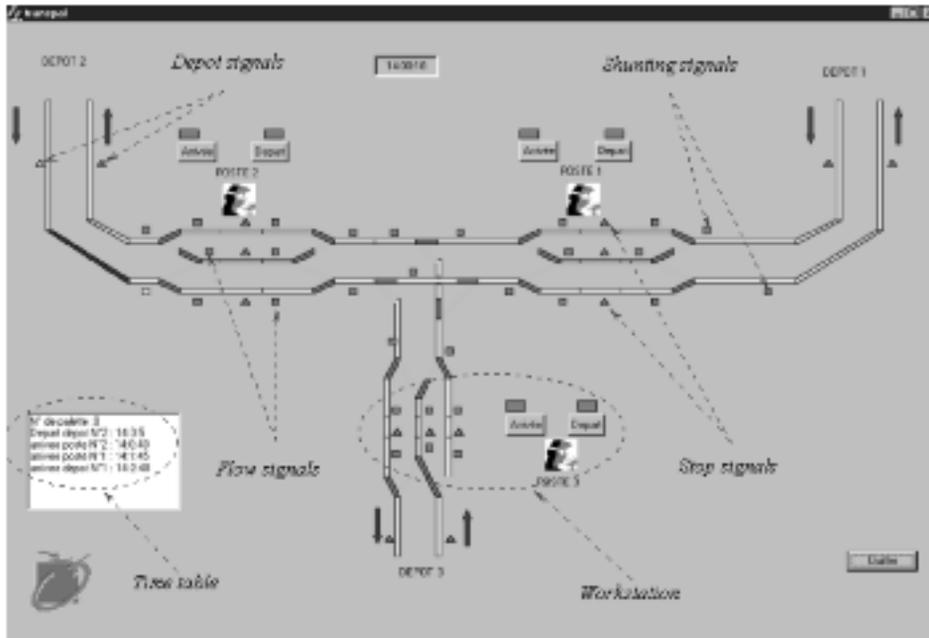


Figure 5. The TRANSPAL platform.

signals at transformation area (see Fig. 5) are considered as the existing barriers, and the fourth barrier – Flow signals is supposed as a barrier which needs to be changed or a new barrier for this system.

Along the experiment schedule, the data from 22 controllers who have performed the experiment on TRANSPAL have been studied. Their data for previous three barriers and respective removal probabilities are gathered to implement the learning of constraint based similarity.

In this application, as connectionist network, the Supervised SOM is used in discovering and memorising the similarities between all BR scenarios. Before, the subjective evaluation were made class by class, the prediction is therefore performed for a class of barrier, not for a single barrier. However, there is difference between the barriers in a same class. It can be found in Table 1, the removal probabilities are different between the arrival signals of pallets (No. 2, No. 72, No. 93) and the departure ones (No. 1, No. 71, No. 94). So the learning of the supervised SOM is performed in terms of different performance criteria by inputting the BR indicator data considering each barrier.

Once the learning phase is completed, the data in terms of removal indicators for the new barrier – each flow signal at transformation area – are input into the network, the removal probability for this barrier is given one by one for each controller.

Table 2 illustrates an example of removal prediction results of the removal probability for a new barrier and actual results in terms of the respect of scheduled time. The column of “observation” is the observed result during the experiment. In the column of “removal probability”, e.g. the controller No. 5 (Cf. Table 2), 83.3% means the evaluation is same as the observed result in terms different BR indicators, its removal probability is predicted as 83.3%.

The removal prediction accuracy is defined as:

$$\text{Accuracy} = \frac{\sum_{s=1}^m N(s)}{\sum_{i=1}^m N(\xi_i)} \quad (1)$$

where  $N(s)$  is number of scenarios which have same predictive removal status as ones from the observations,  $N(\xi_i)$ ,  $i = 1, \dots, m$  means the total number of scenarios whose removal results have been anticipated.

Prediction accuracy of the example in Table 2 is 59.1%. It is noted that there are not only the predictive removal state for a changed/new can be made, but also its relative removal probability. In Table 2, there are some removal probabilities whose values are marked “–”, since there were no such cases in the statistics for the former three barriers during the learning of SOM network.

Table 1. The removal probabilities of all 45 barriers studied.

Classes	Barrier	Total removed	Removal probability (%)
Depot signals	No. 2	18	81,8
	No. 72	19	86,4
	No. 93	19	86,4
	No. 1	13	59,1
	No. 71	11	50,0
Flow signals	No. 94	9	40,9
	No. 13	10	45,5
	No. 14	3	13,6
	No. 15	3	13,6
	No. 19	4	18,2
	No. 20	3	13,6
	No. 21	8	36,4
	No. 52	9	40,9
	No. 53	4	18,2
	No. 54	3	13,6
	No. 58	3	13,6
	No. 59	3	13,6
	No. 60	9	40,9
	No. 79	3	13,6
	No. 80	4	18,2
	No. 81	8	36,4
	No. 91	9	40,9
No. 92	3	13,6	
No. 95	1	4,5	
Shunting signals	No. 11	6	27,3
	No. 12	11	50,0
	No. 28	6	27,3
	No. 29	6	27,3
	No. 30	12	54,5
	No. 33	7	31,8
	No. 42	6	27,3
	No. 43	5	22,7
	No. 44	6	27,3
	No. 45	6	27,3
	No. 67	6	27,3
	No. 68	15	68,2
	Stop signals	No. 16	1
No. 17		0	0,0
No. 18		0	0,0
No. 55		0	0,0
No. 56		0	0,0
No. 57		0	0,0
No. 82		0	0,0
No. 83		0	0,0
No. 84	0	0,0	

## 5 TOWARDS A PREDICTION OF “ERROR OF VIOLATION”

Similarities between different barrier classes have been studied (Zhang et al., 2002b). The prediction of removal and removal probabilities for a changed/new barrier is further implemented in above subsection. There are two sets of barriers during the prediction: a

Table 2. Example of removal prediction results of the removal probability for a new barrier.

Controller No.	Observation	Removal state prediction	Removal probability prediction (%)
No. 1	Not removed	Removed	83.3
No. 2	Not removed	Removed	–
No. 3	Not removed	Removed	54.2
No. 4	Not removed	Not removed	44.4
No. 5	Removed	Removed	83.3
No. 6	Removed	Not removed	–
No. 7	Removed	Removed	83.3
No. 8	Not removed	Removed	83.3
No. 9	Removed	Removed	83.3
No. 10	Not removed	Not removed	50.0
No. 11	Removed	Removed	44.4
No. 12	Not removed	Removed	54.2
No. 13	Not removed	Removed	–
No. 14	Removed	Removed	–
No. 15	Not removed	Not removed	50.0
No. 16	Not removed	Removed	–
No. 17	Not removed	Not removed	–
No. 18	Removed	Removed	16.7
No. 19	Removed	Removed	–
No. 20	Removed	Removed	50.0
No. 21	Not removed	Removed	8.3
No. 22	Removed	Removed	50.0

set of barrier non-removed, and another one of barriers removed. If we focus on the latter one, i.e. the removal set, the correct and erroneous removal of barrier will be met.

The motivation to remove a barrier, i.e. to make a violation, can be erroneous, e.g. difference between the perception of the benefit, cost and potential deficit and the real benefit, cost and potential deficit. Therefore, there is an “error of violation” or difference between the viewpoint of several references such as designers and users.

### 5.1 Correct & erroneous barrier removal

In order to statute about error, it is essential to define a referential. Two referential are commonly used:

- The prescribed task,
- The result of the activity.

For the first referential, a human operator commits an error when (s)he does not respect the prescriptions (usually procedures). For the second referential, the operator commits an error when (s)he does not obtain the expected result.

Moreover the status of error depends on the “judge”. For instance an action may be considered as an error for the designer but as a correct action for the user.

Following the definition of barrier removal, it is an error and more precisely a violation regarding the designer viewpoint. Regarding user viewpoint the barrier removal is not necessary a negative violation. The barrier removal model proposed by Polet et al. (2001) defines it as a behaviour motivated by an improvement of the performance. The performance can be evaluated considering several criteria such as the workload of the human operator, the safety, the quality, the productivity, etc. The barrier removal can be seen as a gamble. If it is a success, the human operator does not consider it as an error. The barrier removal is an error regarding the user viewpoint when it leads to the unexpected result. So two kinds of barrier removal can be distinguished:

- Correct barrier removals: regarding designer viewpoint they are violations, but regarding user viewpoint they correspond to correct barrier removal because they lead to the expected result;
- Erroneous barrier removal: they are also, violations regarding designer viewpoint and regarding user's viewpoint they are intended behaviours with intended actions, and lead to the negative and unexpected consequences.

It is important to note that an erroneous barrier removal is not necessarily considered as an error for the user. For instance, a Barrier Removal (BR) can lead objectively to decreasing of the performance. So it is an Erroneous Barrier Removal (EBR). But the user may subjectively estimate that the result of this barrier removal contribute to an improvement. In this case it is an error of perception or an error of assessment from the user.

## 5.2 Towards a predictive model of EBR

Violations do not solely lead to undesired events. They are actions that intentionally break procedures (Parker et al., 1995; Reason, 1987), e.g. aiming at easing the execution of a given task. When they are coupled with a valid mental model, they can ensure or even increase the safety level of a system (Besnard, 2002). They can be seen as the two facets of the same coin. Keeping in mind this paradox, the probability of erroneous removal of barrier can be given as following,

$$Prob.(EBR/BR) = 1 - Prob.(CBR/BR) \quad (2)$$

where CBR means Correct BR.

During the identification of the EBR, the removal evaluation of barrier should be implemented with not only subjective data (subjective evaluation of Benefit Cost and possible Deficit on BR), but also the objective data on the controller's performance (e.g. productivity, quality, safety and workload).

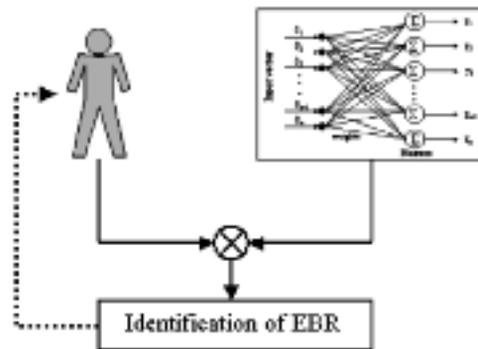


Figure 6. The predictive model of EBR.

By comparing the subjective removal evaluation with the objective performance variation, the statistics on EBR can be implemented in terms of different performance criteria.

The similarity of BR can be found out and then memorised in a connectionist network for a given HMS system in terms of mono-performance mode and multi-performance mode (Zhang et al., 2002b). Furthermore, the probabilistic similarities can be provided by adding in the connectionist network the relative statistical data (see section 3). By same way, the statistical similarities between all input scenarios can be found out and memorised through learning of a connectionist network with the data about the different BR indicators and the corresponding EBR statistics (as a supplementary criterion in the Fig. 2).

The learning by the connectionist network is related to the right part in Fig. 6. Based on the statistical similarities learning, predictions of EBR can be made for the changed/new barriers.

The identification of the EBR can be helpful for,

- The designer as a predictive analysis support tool for the (re)design of the changed/new barriers.
- The human controller as a decision-making support facing removal of a barrier.
- The regulatory authorities as verification means.

The ultimate goal is, in each period of defence-in-depth, to reduce the probability of EBR by,

- Reducing the benefit of removal of a barrier, by increasing the cost and the possible deficit.
- Making the human controller's perception of the benefit low, the cost high and the possible deficit high, e.g. improving the human-machine interface, reducing the perception error.
- Surveillance or monitoring of states of the barriers in terms of benefit, cost and possible deficit.
- Protection and mitigation measures for erroneous BR.

Table 3. Illustration of identification of EBR ( $\uparrow$  improvement,  $\downarrow$  degradation).

Performance criteria	Subjective judgment	Objective sources	Variation	Identification of EBR
Respect of scheduled time	$\downarrow$	$\downarrow$	None	–
Percentage of product treated	$\uparrow$	$\downarrow$	Yes	EBR
Traffic safety	$\downarrow$	$\uparrow$	Yes	Additional
Number of action	$\uparrow$	$\uparrow$	None	–

Table 4. EBR statistics in terms of different performance criteria.

Performance criteria	Total variation		EBR		Additional	
Quality	11	55%	4	20%	7	35%
Productivity	17	85%	5	25%	12	60%
Safety	12	60%	4	20%	8	40%
Workload	8	40%	0	0%	8	40%

### 5.3 Identification of EBR

The EBR could be distinguished from the correct BR through comparing the performance variation (between prior-removal and posterior-removal) of human controller. Table 3 gives an example of Identification of EBR based on variation between the subjective judgment and the objective sources.

Secondly, there is improvement according to subjective judgment, the controller removes barrier. But there is degradation regarding the objective sources, so it is considered as an EBR.

There is the third case (see “traffic safety” in Table 3), controller removes the barrier even if (s)he assesses there will be a degradation, in fact, there is improvement regarding the objective sources. It is marked as “additional” in the table.

From the overall viewpoint of the experiment, the number of EBR may be identified with the above assessment. Table 4 provides EBR statistics in terms of different performance criteria. In the future, as a supplementary criterion (Cf. Fig. 2), EBR statistics can be integrated into the learning of the connectionist network. The prediction of EBR can be ultimately realized.

## 6 CONCLUSIONS

The paper presents a prospective approach aiming at predicting the removal of a changed/new barrier. The

approach is based on a Neural Network model that integrates data on the removal of barrier into a learning phase. The predictive results include the removal state, as well as its removal probability. It indicates if a changed/new barrier will be removed, and the certainty level on this removal is given by a probability. The feasibility study on a research simulator TRANSPAL is illustrated.

Then erroneous & correct barrier removal are discussed and distinguished regarding the viewpoints of designers and users in this paper. The concept of EBR is then established. Moreover an example of identification of EBR is provided.

It should be noted that EBR should be identified in terms of different performance. As a supplementary criterion in Fig. 2, EBR statistics can be integrated into the learning of the connectionist network. The prediction of EBR can be finally implemented. The ultimate goal is to try to reach an “EBR-free” system.

As applications in transportation industry, there are two stages: the study on a research simulator TRANSPAL in the paper is the first stage; the second stage is the application of proposed model to the general safety conceptual approach and guidelines for FRS in UGTMS project.

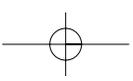
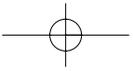
## ACKNOWLEDGEMENT

This work is a part of European framework project of *Urban Guided Transport Management System (UGTMS)* founded by the European Commission under the transport R&D Programme of the 5th framework Programme (*contract n° GRD2-2000-30090*).

## REFERENCES

- Besnard, D. & Greathead, D. 2002. A cognitive approach to safe violations. *Cognition, Technology and Work*, in review.  
 European Commission, 2002. Deliverable D1, First report for a preliminary definition of UGTMS, GROUT GRD2-2000-30090-UGTMS.

- Free, R. 1994. The role of procedural violations in railway accidents. Ph.D. Thesis, University of Manchester.
- Harms-Ringdahl, L. 1998. Proc. of Society for Risk Analysis – Europe. The 1998 annual conference: *Risk analysis: Opening the process*. Paris.
- Hérault, J. et al. 1994. *Réseaux neuronaux et traitement du signal*, Hermès, Chapitre VII, p. 173–204.
- Hollnagel, E. 1999a. Accident and barriers. In: Proc. of the 7th European Conference on Cognitive Science Approaches to Process Control, Villeneuve d'Ascq, France, p. 175–180.
- Hollnagel, E. 1999b. Accident analysis and barrier functions. Report of the project TRAIN, Version 1.0, Sweden.
- Hollnagel, E., Pedersen, O. M. & Rasmussen, J. 1981. Notes on Human Performance Analysis, RISO-M-2285, DK-4000, Riso National Laboratories, Roskilde, Denmark.
- Kohonen, T. 2001. *Self-Organizing Maps*. Springer-Verlag, Third edition, Berlin, Heidelberg, Germany.
- Kohonen, T. 1990. The self-organizing map. In: Proc. of the IEEE 78(9):1464–1480.
- Parker, D., Reason, J., Manstead, S. R. & Stradling, S.G. 1995. Driving errors, driving violations and accident involvement. *Ergonomics*, 38, 1036–1048.
- Polet, P. 2002. Modélisation des Franchissements de Barrières pour l'Analyse des Risques des Systèmes Homme-Machine, Thèse de l'Université de Valenciennes, France.
- Polet, P., Vanderhaegen, F. & Wieringa, P.A. 2002a. Theory of safety-related violations of system barriers. *Cognition, Technology and Work*, (2002) 4:171–179.
- Polet, P., Vanderhaegen, F., Millot, P. & Wieringa, P. 2001. Barriers and risk analysis. In: Proc. of the 8th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design and Evaluation of Man-Machine Systems, Kassel, Germany.
- Polet, P., Vanderhaegen, F., Amalberti, R. 2003. Modeling border-line tolerated conditions of use (BTCUs) and associated risks. *Safety Science*. Vol 41, Issues 2–3, March 2003, pp. 111–136.
- Reason, J. 1990. Human error. Cambridge University Press, New York.
- Reason, J. 1987. Chernobyl errors. *Bulletin of the British Psychological Society*, 40, 201–206.
- Swain, A.D. & Guttmann, H.E. 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278.
- Valancogne, J. & Nicolet, J.L. 2002. Defence-in-depth: a new systematic and global approach in socio-technical system design to guarantee better the timelessness safety in operation. In: Proc. of Im13/Esrel2002, Lyon, France. p. 298–305.
- Vanderhaegen, F., Polet, P., Zhang, Z. & Wieringa, P.A. 2002. Barrier removal study in railway simulation, *PSAM 6*, Puerto Rico, USA.
- Vanderhaegen, F. 2001. A non-probabilistic prospective and retrospective human reliability analysis method – application to railway system. *Reliability Engineering and System Safety* 71(1):1–13.
- Zhang, Z. & Vanderhaegen, F. 2002a. A method integrating Self-Organizing Maps to predict the probability of Barrier Removal. C. Warren Neel Conference on the New Frontiers of Statistical Data Mining and Knowledge Discovery, Knoxville, Tennessee, USA, June 22–25, 2002. In press by the Chapman & Hall/CRC.
- Zhang, Z., Polet, P., Vanderhaegen, F. & Millot, P. 2002b. Towards a method to analyze the problematic level of Barrier Crossing. In: Proc. of Im13/Esrel2002, Lyon, France. p. 71–80.
- Zhang, Z., Polet, P., Vanderhaegen, F. & Millot, P. 2002c. Artificial Neural Network for Violation Analysis. *Reliability Engineering and System Safety*. In review.



## Measuring the reliability importance of components in multi-state systems

E. Zio & L. Podofillini

*Department of Nuclear Engineering, Polytechnic of Milan, Italy*

**ABSTRACT:** Several concepts of importance measures have been proposed and used in system engineering, based on different views of the influence of the components on the system performance. The standard definitions of importance measures hold for binary components in binary systems (i.e., the components, as well as the whole system can only stay in two states: working or failed). However, a multi-state modelling of components and systems is often required in practice.

In this paper, the most frequently used importance measures are generalized to the case of multi-state systems made of multi-state components. The introduced extensions characterize the importance of a component achieving its different possible levels of performance with respect to the overall mean multi-state unavailability.

The work is methodological in nature. An illustrative example is provided with regards to a simple multi-state system.

### 1 INTRODUCTION

Importance measures (IMs) are widely used in system engineering to identify the components that mostly influence the system behaviour with respect to reliability as well as to safety. The information provided by importance measures gives useful insights for the safe and efficient operation of the system, allowing the analyst to trace system bottlenecks and providing guidelines for effective system improvement.

Different definitions of IMs exist in the literature, based on different views of the influence that components may have on the system performance. The Birnbaum measure, the Fussell-Vesely measure, the risk achievement worth and the risk reduction worth are some of the most frequently used [Birnbaum 1969, Fussell 1975, Cheok et al. 1998, Vasseur & Llory 1999, van der Borst & Shoonakker 1999, Borgonovo & Apostolakis 2001].

Importance measures have been typically applied to systems made up of binary components (i.e., components which can be in two states: working and failed). This hypothesis does not fit with the real functioning of many systems, such as those, for example, employed in production and transportation engineering. For such systems, an overall performance measure is defined, and depending on the operative conditions of the multi-state components, the system may work at, say, 100%, 80%, 50% of the nominal performance capacity.

Systems characterized by different levels of performance are referred to as Multi-State Systems (MSS) [Levitin & Lisnianski 1999].

It is worth pointing out, as a limit situation, that in practice there are systems whose performances may be characterized in terms of an infinite set of continuous states. This, for example, is the case of the passive systems whose utilization is growingly advocated in the new generation of nuclear power plants and whose physical behaviour dictates the system performance, much in a continuous fashion.

Recently, then, efforts are being made to evaluate the importance of components of multi-state systems. For example, in [Levitin & Lisnianski 1999], the Birnbaum measure is extended to the case of multi-state systems composed by binary components; in [Armstrong 1997] the case of components with dual failures-modes is considered.

In this paper, the most frequently used IMs are generalized to multi-state systems made of multi-state components. The introduced extensions characterize the importance that a component achieves a given level of performance with respect to the overall mean multi-state unavailability. It is noteworthy that the introduced measures are directly extendable to continuous-state systems and components.

The paper is organized as follows. In the following Section 2, we introduce the concepts of availability and performance of multi-states systems. In Section 3, the

classical importance measures are briefly summarized. Then, in Section 4, we propose the extension of these IMs to multi-state systems made up of multi-state components. A numerical example is provided in Section 5 to illustrate the informative content borne by the proposed extended measures. As for the system modelling tool, we resort to the Monte Carlo (MC) method which, in principle, allows handling many realistic issues of the multi-state system dynamics [Marseguerra & Zio 2002]. We close the paper with some remarks and suggestions for future work.

## 2 MULTI-STATE SYSTEM AVAILABILITY

When applied to MSS, the concept of availability is related to the capacity of the system to meet a required demand. In the following, the formal definition of MSS availability is given [Levitin et al. 1998].

Consider a system made up of  $N_C$  components. Each component  $i$  may stay in one of  $N_S(i)$  states,  $i = 1, 2, \dots, N_C$ . The system is characterized by a set  $S$  of  $N_{\text{sys}}$  states:

$$N_{\text{sys}} = \prod_{i=1}^{N_C} N_s(i) \quad (1)$$

Concerning the generic  $i$ -th component, each state is characterized by a different level of performance. We number the states of component  $i$  according to decreasing performance levels, from state 1 (100%) to state  $N_S(i)$  (0%) and denote by  $w_{ji}^i$  the performance of component  $i$  when operating in state  $j_i$ ,  $j_i = 1, 2, \dots, N_S(i)$ . Concerning the whole system, let  $W_j$  denote its performance level when in state  $j = (j_1, j_2, \dots, j_{N_C})$ .

In practice, some systems are requested to operate at different performance levels at different times. For example, the production of electrical and thermal power plants follows the daily and seasonal load demands. Assume that at time  $t$  a minimum level of system performance  $W^*(t)$  is required to meet the current demand. The system availability, usually defined in terms of the system safe state, is generalized according to whether its performance is larger or smaller than  $W^*$  (for ease of notation, in the writing we shall often neglect the dependence on  $t$ ). Then, the MSS availability  $A^{MSS}(W^*, t)$  of the system at time  $t$  is the probability that at that time the system is in any state  $j$  with performance  $W_j \geq W^*$ . If the probability that at time  $t$  the system is in state  $j$  is denoted by  $P_j(t)$ , the availability is:

$$A^{MSS}(W^*, t) = \sum_{W_j \geq W^*(t)} P_j(t) \quad (2)$$

Obviously, the MSS unavailability  $U^{MSS}(W^*, t)$  is:

$$U^{MSS}(W^*, t) = \sum_{W_j < W^*(t)} P_j(t) = 1 - A^{MSS}(W^*, t) \quad (3)$$

## 3 IMPORTANCE MEASURES

With reference to a given risk metric  $R$  (e.g. the unavailability), the standard definition of importance measures holds for binary systems constituted by binary components. In our notations this implies  $N_S(i) = 2$  and  $j_i = 1, 2$ ,  $i = 1, 2, \dots, N_C$ . Coherently with our ordering of component states, we assume that for each component  $i$ , state  $j_i = 1$  is the working state (100% of performance) and  $j_i = 2$  is the failed state (0% of performance).

For the definition of the IMs, it is useful to introduce the following quantities:

$R_i^+(t) = R[t|j_i = 2 \text{ in } (0, t)]$ : value of the risk metric  $R$  when component  $i$  has been in its failed state  $j_i = 2$  throughout the time interval  $(0, t)$ . It represents the maximum risk achievement if component  $i$  is considered failed with certainty and permanently, or, which is equivalent, removed from the system.

$R_i^-(t) = R[t|j_i = 1 \text{ in } (0, t)]$ : value of the risk metric  $R$  when component  $i$  remained in the working state  $j_i = 1$  throughout the time interval  $(0, t)$ . It represents the maximum reduction in risk if component  $i$  is considered perfect, i.e. always in the working state.

The definition of four of the most frequently used IMs is here recalled with reference to the generic  $i$ -th component [Cheok et al. 1998]:

– Risk achievement worth

$$a_i(t) = \frac{R_i^+(t)}{R(t)} \quad (4)$$

The risk achievement worth is the ratio of the risk when component  $i$  is considered always failed in  $(0, t)$  (i.e. in state 2) to the actual value of the risk.

– Risk reduction worth

$$r_i(t) = \frac{R(t)}{R_i^-(t)} \quad (5)$$

The risk reduction worth is the ratio of the nominal value of the risk to the risk when component  $i$  is always available (i.e. in state 1). It measures the potential of component  $i$  in reducing the risk, by

considering the maximum decrease in risk achievable when optimising the component to perfection.  
– Fussell-Vesely measure

$$FV_i(t) = \frac{R(t) - R_i^-(t)}{R(t)} = 1 - \frac{1}{r_i(t)} \quad (6)$$

The Fussell-Vesely measure represents the maximum fractional decrement in risk achievable when component  $i$  is always available.  
– Birnbaum measure

$$B_i(t) = R_i^+(t) - R_i^-(t) \quad (7)$$

The Birnbaum measure is the maximum variation of the risk when component  $i$  switches from the condition of perfect functioning to the condition of certain failure. It is a differential measure of the importance of component  $i$ .

#### 4 MSS UNAVAILABILITY IMPORTANCE MEASURES

Considering a multi-state system and a given required performance function over the mission time  $T_m$ ,  $W^*(t)$ ,  $t \in (0, T_m)$ , we introduce the mean multi-state unavailability,  $\bar{U}^{MSS}(W^*)$ :

$$\bar{U}^{MSS}(W^*) = \frac{1}{T_m} \int_0^{T_m} [1 - A^{MSS}(W^*, t)] dt \quad (8)$$

Furthermore, with reference to the generic  $i$ -th component of the system,  $i = 1, 2, \dots, N_C$ , we introduce:

$\Gamma_i^\alpha$ : the set of those states of component  $i$  characterized by a performance level below or equal to  $\alpha$

$\bar{\Gamma}_i^\alpha$ : the set of those states of component  $i$  characterized by a performance level above  $\alpha$  (complement set of  $\Gamma_i^\alpha$ )

$\bar{U}_i^{MSS, \leq \alpha}(W^*) = \bar{U}^{MSS}(W^* | j_i \in \Gamma_i^\alpha \text{ in } (0, T_m))$ : mean MSS-unavailability when the performance of the  $i$ -th component is restricted to be below or equal to  $\alpha$  (i.e.,  $j_i \in \Gamma_i^\alpha$  in  $(0, T_m)$ ).

$\bar{U}_i^{MSS, > \alpha}(W^*) = \bar{U}^{MSS}(W^* | j_i \in \bar{\Gamma}_i^\alpha \text{ in } (0, T_m))$ : mean MSS-unavailability when the performance of the  $i$ -th component is restricted to be above  $\alpha$  (i.e.,  $j_i \in \bar{\Gamma}_i^\alpha$  in  $(0, T_m)$ ).

Note that the values of the above mean MSS-unavailabilities are within the closed interval  $[0, 1]$  and that the above definitions hold also for continuous-states components and systems. In the latter case of continuous states, the  $\alpha$ -level can continuously assume any intermediate value within its range (e.g.  $\alpha \in [0\%,$

100%]) and the state indicator variable  $j_i$  can vary continuously within the continuous sets  $\Gamma_i^\alpha$ ,  $\bar{\Gamma}_i^\alpha$  and  $\Gamma_i = \Gamma_i^\alpha \cup \bar{\Gamma}_i^\alpha$

Given the above definitions, we extend the standard IMs for binary systems to the case of multi-state systems (for simplicity of notations, the inherent dependence on  $W^*$  of  $\bar{U}_i^{MSS}(W^*)$ ,  $\bar{U}_i^{MSS, \leq \alpha}(W^*)$  and  $\bar{U}_i^{MSS, > \alpha}(W^*)$  is omitted):

– Unavailability Achievement Worth of  $\alpha$ -level

$$ua_i^{MSS, \alpha} = \frac{\bar{U}_i^{MSS, \leq \alpha}}{\bar{U}^{MSS}} \quad (9)$$

The numerator represents the mean MSS-unavailability of the system over the mission time  $T_m$  when component  $i$  evolves only through states with performance below, or at most equal to  $\alpha$ , i.e.  $j_i \in \Gamma_i^\alpha$  in  $(0, T_m)$ ; the denominator represents the mean MSS-unavailability with all components freely evolving through all their possible states (i.e. the real system mean unavailability).

The  $ua_i^{MSS, \alpha}$  depends on the mean unavailability achieved by the system when component  $i$  is obliged to operate with a performance at most equal to  $\alpha$  in  $(0, T_m)$ . Thus,  $ua_i^{MSS, \alpha}$  is a measure of the importance, with respect to system performance unavailability, of the fact that component  $i$  assures at least a level  $\alpha$  of performance.

– Unavailability reduction worth of  $\alpha$ -level

$$ur_i^{MSS, \alpha} = \frac{\bar{U}^{MSS}}{\bar{U}_i^{MSS, > \alpha}} \quad (10)$$

The numerator is the MSS mean unavailability over  $T_m$  when all states can be reached by the components; the denominator represents the MSS mean unavailability when component  $i$  evolves only through states with performance above  $\alpha$ , i.e.  $j_i \in \bar{\Gamma}_i^\alpha$  in  $(0, T_m)$ . Hence,  $ur_i^{MSS, \alpha}$  represents the reduction in MSS mean unavailability (i.e. the improvement in MSS mean availability) which can be achieved when the output performance of component  $i$  is maintained above level  $\alpha$ .

– Fussell-Vesely unavailability measure of  $\alpha$ -level

$$uFV_i^{MSS, \alpha} = \frac{\bar{U}^{MSS} - \bar{U}_i^{MSS, > \alpha}}{\bar{U}^{MSS}} \quad (11)$$

The Fussell-Vesely measure is the ratio of the decrement in the mean multi-state system unavailability due to the component  $i$  operating with a level of performance above  $\alpha$  in  $(0, T_m)$  to the nominal value of the mean unavailability. Also in the case of multi-state systems,  $uFV_i^{MSS, \alpha}$  and  $ur_i^{MSS, \alpha}$  produce the same ranking of component importance.

– Birnbaum unavailability measure of  $\alpha$ -level

$$uB_i^{MSS,\alpha} = \bar{U}_i^{MSS,\leq\alpha} - \bar{U}_i^{MSS,>\alpha} \quad (12)$$

The Birnbaum measure is the maximum change in system mean unavailability over  $T_m$  when the performance of component  $i$  is changed from always below or equal to the  $\alpha$ -level to always above the  $\alpha$ -level of performance.

When continuous-states components and systems are considered, the above definitions are still applicable: in such case, the importance measures  $ua_i^{MSS,\alpha}$ ,  $w_i^{MSS,\alpha}$ ,  $uFV_i^{MSS,\alpha}$  and  $uB_i^{MSS,\alpha}$  are continuous functions of the  $\alpha$  level.

### 5 NUMERICAL EXAMPLE

#### 5.1 System description

Let us consider a system made up of a series of  $N_n = 2$  macro-components (nodes), each one performing a given function (Figure 1). Node 1 is constituted by  $N_p(1) = 2$  components in parallel logic, whereas node 2 is constituted by a single component ( $N_p(2) = 1$ ) so that the overall number of components in the system is  $N_c = 3$ . The mission time  $T_m$  is 1000 hours.

For each component  $i = 1, 2, 3$  there are  $N_S(i) = 5$  possible states, each one corresponding to a different hypothetical level of performance  $w_{j_i}^i, j_i = 1, 2, \dots, 5$ .

Table 1 gives the values of the performances  $w_{j_i}^i$  (in arbitrary units) of the three components in correspondence of all the possible states  $j_i = 1, 2, \dots, 5$ . Note that state 5 corresponds to zero-performance, i.e. component failure.

Each component is assumed to move stochastically from one state  $j_i$  to another state  $k_i$ , according to

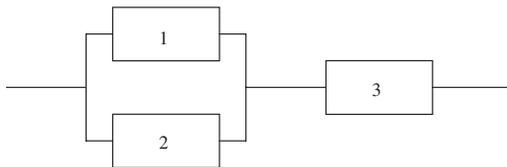


Figure 1. System sketch.

Table 1. Components' performance data.

Component ( $i$ )	Performance ( $w_{j_i}^i$ )				
	$j_i = 1$	$j_i = 2$	$j_i = 3$	$j_i = 4$	$j_i = 5$
1	80	60	40	20	0
2	80	60	40	20	0
3	100	75	50	25	0

exponential time distributions with rate  $\lambda_{j_i \rightarrow k_i}^i$  ( $h^{-1}$ ). For each component  $i = 1, 2, 3$ , we then have a transition matrix  $\Lambda^i$  of the values of the transition rates:

$$\Lambda^1 = \begin{bmatrix} - & 5 \cdot 10^{-3} & 0 & 0 & 5 \cdot 10^{-4} \\ 5 \cdot 10^{-3} & - & 5 \cdot 10^{-3} & 0 & 6 \cdot 10^{-3} \\ 0 & 5 \cdot 10^{-3} & - & 5 \cdot 10^{-3} & 8 \cdot 10^{-3} \\ 0 & 0 & 5 \cdot 10^{-3} & - & 8 \cdot 10^{-3} \\ 1 \cdot 10^{-2} & 5 \cdot 10^{-3} & 5 \cdot 10^{-3} & 5 \cdot 10^{-3} & - \end{bmatrix}$$

$$\Lambda^2 = \begin{bmatrix} - & 5 \cdot 10^{-3} & 0 & 0 & 1.5 \cdot 10^{-3} \\ 5 \cdot 10^{-3} & - & 5 \cdot 10^{-3} & 0 & 2 \cdot 10^{-3} \\ 0 & 5 \cdot 10^{-3} & - & 5 \cdot 10^{-3} & 3 \cdot 10^{-3} \\ 0 & 0 & 5 \cdot 10^{-3} & - & 4 \cdot 10^{-2} \\ 1 \cdot 10^{-2} & 5 \cdot 10^{-3} & 5 \cdot 10^{-3} & 5 \cdot 10^{-3} & - \end{bmatrix}$$

$$\Lambda^3 = \begin{bmatrix} - & 5 \cdot 10^{-4} & 0 & 0 & 5 \cdot 10^{-5} \\ 5 \cdot 10^{-3} & - & 5 \cdot 10^{-4} & 0 & 6 \cdot 10^{-5} \\ 0 & 5 \cdot 10^{-3} & - & 5 \cdot 10^{-4} & 7 \cdot 10^{-5} \\ 0 & 0 & 5 \cdot 10^{-3} & - & 8 \cdot 10^{-5} \\ 1 \cdot 10^{-1} & 5 \cdot 10^{-2} & 5 \cdot 10^{-2} & 5 \cdot 10^{-2} & - \end{bmatrix} \quad (13)$$

The output performance  $W_{j_i}^i$  associated to the system state  $\underline{j} = (j_1, j_2, \dots, j_{N_c})$  is obtained on the basis of the performances  $w_{j_i}^i$  of the components constituting the system. More precisely, we assume as in [Levitin & Lisnianski 1998] that the performance of each node  $l$ , constituted by  $N_p(l)$  elements in parallel logic, is the sum of the individual performances of the components and that the performance of the two-nodes series system is that of the node with the lowest performance, which constitutes the “bottleneck” of the system. For example, with reference to the system configuration  $\underline{j}^* = (1, 3, 2)$ , the first node is characterized by a value of the performance equal to  $w_1^1 + w_3^2 = 120$ , while the second node has performance  $w_3^3 = 75$ . This latter node determines the value of the system performance  $W_{j_i}^i = 75$ .

To catch the complex dynamics of multi-state systems, a Monte Carlo simulation code has been developed in Fortran. The simplifying assumption of exponentially distributed transition times is not a limitation of the approach but simply allows us to obtain analytical solutions in a simplified case of binary components, for verification of the code.

#### 5.2 Standard importance measures

In this Section we compute the risk achievement worth  $a_i, i = 1, 2, 3$ , (Section 3) for the components of the system of Figure 1. Results obtained both analytically and by Monte Carlo simulations are provided for

code verification purposes. The other IMs of Section 3, with the corresponding extended ones in the multi-state system case ( $IM_S^{MSS}$ ), have been investigated too but for brevity the results are not presented here (the interested reader should consult [Zio & Podofillini 2002]).

Given that the standard IMs of Section 3 are defined for binary components, we consider a system equivalent to that of Figure 1 in which the three components, 1', 2', 3', have only two states, the first one (1) gathering the four operative states 1-4 of the multi-state case and the second (2) corresponding to the failed state 5. To do so, we have proceeded as follows: the transition rates of the binary components,  $\lambda_{1 \rightarrow 2}^{i'}$  and  $\lambda_{2 \rightarrow 1}^{i'}$ ,  $i' = 1, 2, 3'$  are established such as to give an average probability over the mission time  $T_m$  of being in the failed state (2),  $\bar{p}_2^{i'}(T_m)$ , equal to the average probability of the original multi-state components of being in the zero-performance state 5 over the mission time,  $\bar{p}_5^{i'}(T_m)$ ,  $i = 1, 2, 3$ . Table 2 reports the values of  $\bar{p}_2^{i'}(T_m)$ ,  $\lambda_{1 \rightarrow 2}^{i'}$  and  $\lambda_{2 \rightarrow 1}^{i'}$  for the three components. Note how component 3', in series, is significantly more reliable than the other two in parallel logic.

For the calculation of the measures  $a_i$ , the risk metric considered,  $R$  (Section 3), is the average unavailability  $\bar{U}$  over the mission time  $T_m$ . The results, reported in Table 3, show the agreement of the analytical values with the MC estimates, within one standard deviation.

As for the ranking produced, component 3' is ranked first. Indeed, component 3' is in series to the others two so that obviously its removal, as specified in the definition of the risk achievement worth, implies the system complete unavailability throughout  $T_m$ , so that  $R_{3'}^+ = 1$ . In this sense, component 3' is the major contributor to the overall system unavailability. As for the

relative ranking among components 1' and 2', component 2' is ranked highest. Indeed, in a parallel logic block, the risk achievement measure  $a$  ranks highest the more reliable component (from Table 2, component 2' is more "available" than component 1', i.e.  $\bar{p}_2^{2'}(T_m) < \bar{p}_2^{1'}(T_m)$ ).

### 5.3 MSS-unavailability importance measures

With reference to the multi-state system described in Section 5.1, we now apply the MSS importance measure  $ua_i^{MSS,\alpha}$  presented in Section 4,  $i = 1, 2, 3$ . In the case of MSS the analytical solution becomes impractical and thus only the Monte Carlo results are reported.

From Section 2, we know that the required performance level,  $W^*(t)$ , affects the MSS mean unavailability  $\bar{U}^{MSS}(W^*)$ . In turn, the importance measures depend on  $W^*(t)$ , too: indeed, the performance of a component may turn out to be more important for the achievement of a given system performance level and less important for another. The effects related to different required performance levels,  $W^*$ , have also been studied but are not reported here, for brevity's sake. For a discussion of such effects the reader should refer to [Zio & Podofillini 2002]. Here, in order to underline the improvement in informative content provided by calculating the  $IM_S^{MSS}$  with respect to different levels  $\alpha$  of components' performance, the case of a system required performance function  $W^* = 50$  (in arbitrary units), constant in  $(0, T_m)$ , is considered.

For the assigned level of required minimum system performance  $W^* = 50$ , Figure 2 reports, in logarithmic scale, the values of  $ua_i^{MSS,\alpha}$  for each of the three components as a function of their  $\alpha$ -level (i.e. for different components' reference states  $j_i$  with corresponding performances  $w_{j_i}^i = \alpha$ ,  $j_i = 2, 3, 4, 5$ ,  $i = 1, 2, 3$ ). The numerical values are reported in Table 4. Note that, for state  $j_i = 1$ ,  $i = 1, 2, 3$  (corresponding to  $\alpha = w_1^i = 80$  for  $i = 1, 2$  and  $\alpha = w_1^3 = 100$  for the third component) the sets  $\Gamma_i^\alpha$  and  $\Gamma_i^\alpha$  reduce to the whole set of components' states and to the empty set, respectively, and the corresponding importance measures loose meaning, so that such anomalous case ( $j_i = 1$ ) is not considered.

Let us examine first how the risk achievement worth of component 3 changes with the different  $\alpha$ -levels. Consider the values of the  $IM_S^{MSS}$  calculated in correspondence of the  $\alpha$ -level identified by the last state  $j_i = 5$ , i.e. that corresponding to zero performance (Table 1,  $\alpha = w_5^i = 0$ ,  $i = 1, 2, 3$ ). According to the measure  $ua_i^{MSS,\alpha}(50)$ , component 3 is the most important one. Such ranking is in agreement with that obtained with the corresponding standard IMs applied to the binary system of Section 5.2 and this is true also for  $j_i = 4$ ,  $i = 1, 2, 3$ . Indeed, due to the system series-parallel logic, the whole system performance

Table 2. Average probabilities  $\bar{p}_2^{i'}(T_m)$  and corresponding transition rates,  $\lambda_{1 \rightarrow 2}^{i'}$  and  $\lambda_{2 \rightarrow 1}^{i'}$  for the equivalent system of binary components 1', 2', 3'.

Component ( $i'$ )	$\bar{p}_2^{i'}(T_m)$	$\lambda_{1 \rightarrow 2}^{i'}$	$\lambda_{2 \rightarrow 1}^{i'}$
1'	0.113	$5.000 \times 10^{-4}$	$2.560 \times 10^{-3}$
2'	0.103	$1.000 \times 10^{-3}$	$7.510 \times 10^{-3}$
3'	$2.031 \times 10^{-4}$	$5.000 \times 10^{-5}$	$2.450 \times 10^{-1}$

Table 3. Values of the  $a$  importance measure for the components 1', 2', 3' of the equivalent system.

Component ( $i'$ )	$a_i$	
	Analytical	Monte Carlo
1	8.097	$8.092 \pm 0.106$
2	8.786	$8.775 \pm 0.114$
3	77.922	$77.836 \pm 0.965$

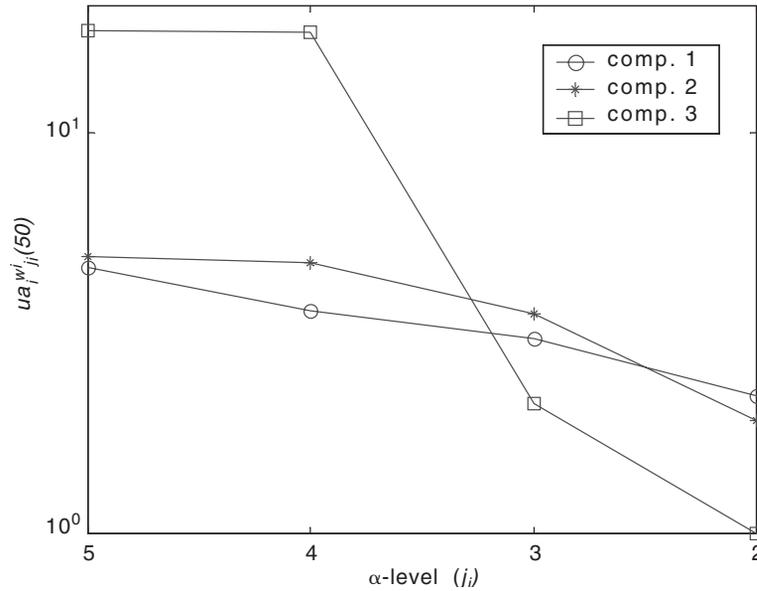


Figure 2. Values of  $ua_i^{MSS,\alpha}(50)$  as a function of the reference  $\alpha$ -level state for each component.

Table 4. Values of  $ua^{MSS,\alpha}(50)$ .

$\alpha$ -level for $i = 1,2/$ $i = 3$ (state $j_i$ )	Component ( $i$ )		
	1	2	3
0/0(5)	4.768 ± 0.066	5.088 ± 0.070	17.415 ± 0.223
20/25(4)	3.760 ± 0.053	4.903 ± 0.067	17.372 ± 0.222
40/50(3)	3.247 ± 0.047	3.713 ± 0.053	2.271 ± 0.035
60/75(2)	2.372 ± 0.036	2.072 ± 0.032	1.113 ± 0.020

$W$  cannot exceed the performance  $w_{j_3}^3$  of the “bottleneck” series-component 3 operating in its state  $j_3$ , i.e.  $W \leq w_{j_3}^3$ . Thus, when component 3 is forced to evolve through states  $j_3$  with corresponding performance  $\alpha = w_{j_3}^3$  below the required  $W^* = 50$  (i.e. states  $j_3 = 4$ , corresponding to  $w_4^3 = 25$ , and  $j_3 = 5$ , corresponding to  $w_5^3 = 0$ ), it fully impacts the system mean performance and unavailability ( $\bar{U}^{MSS,\leq\alpha}(50) = 1$ ). ( $\bar{U}_3^{MSS,\leq\alpha}(50) = 1$ ). Indeed, states  $j_3 = 4$  and  $j_3 = 5$  are very critical since, due to the system series-parallel logic which implies  $W \leq w_{j_3}^3$ , when component 3 transfers in any one of these two states, there is no chance for the system of providing the required performance  $W^* = 50$ : hence, the high values of the measures  $ua_3^{MSS,\alpha}(50)$  when component 3 is restricted by the  $\alpha$ -level to live in states  $j_3 = 4, 5$ . On the contrary, when considering, still in Figure 2, the highest two values of components’  $\alpha$ -levels, corresponding to states  $j_i = 2$  and  $j_i = 3$ , component 3 becomes the least important component.

Hence, the significance of a multi-state importance analysis which accounts for the different performance levels of the components. The ranking inversion, at high  $\alpha$ -levels, between component 3 and the other two can be explained as follows. Due to the high “availability” of component 3 (i.e. low values of “failure” rates  $\lambda_{2 \rightarrow 5}^3, \lambda_{3 \rightarrow 5}^3, \lambda_{4 \rightarrow 5}^3$  and high values of “recovery” rates  $\lambda_{5 \rightarrow 2}^3, \lambda_{5 \rightarrow 3}^3, \lambda_{5 \rightarrow 4}^3$ , or equivalently low values of  $\bar{p}_2^3(T_m)$  in Table 2), the criticality of component 3 is softened at  $\alpha$ -levels allowing the visit of states 3, 4, 5 or 2, 3, 4, 5, which are such to provide the system with a chance of achieving a performance  $W \geq W^*$ : hence, the low values of  $ua_3^{MSS,\alpha}(50)$  when component 3 is restricted to live in states  $j_3 = 2-5$  or  $3-5$  by the  $\alpha$  level.

Examining components 1 and 2, we note in the same Figure 2 that the ranking provided in correspondence of  $\alpha = 0$  ( $j_i = 5, i = 1, 2$ ), indicates that component 2 is slightly more important than component 1. Indeed, the relevant numerical values of Table 4 are:

$$ua_1^{MSS,0}(50) = 4.77 \pm 0.07 < ua_2^{MSS,0}(50) = 5.09 \pm 0.07$$

The same ranking is confirmed also for  $N_{sys} = \Pi^{NC} N_s(i)$  ( $j_i = 4, i = 1, 2$ ) and  $\alpha = 40$  ( $j_i = 3, i = 1, 2$ ) and agrees with the findings of the binary system of Section 5.2. Instead, for the highest  $\alpha$ -level of 60 units corresponding to  $j_i = 2, i = 1, 2$ , the ranking is inverted, the corresponding values in Table 4 being:

$$ua_1^{MSS,60}(50) = 2.37 \pm 0.04 > ua_2^{MSS,60}(50) = 2.07 \pm 0.03$$

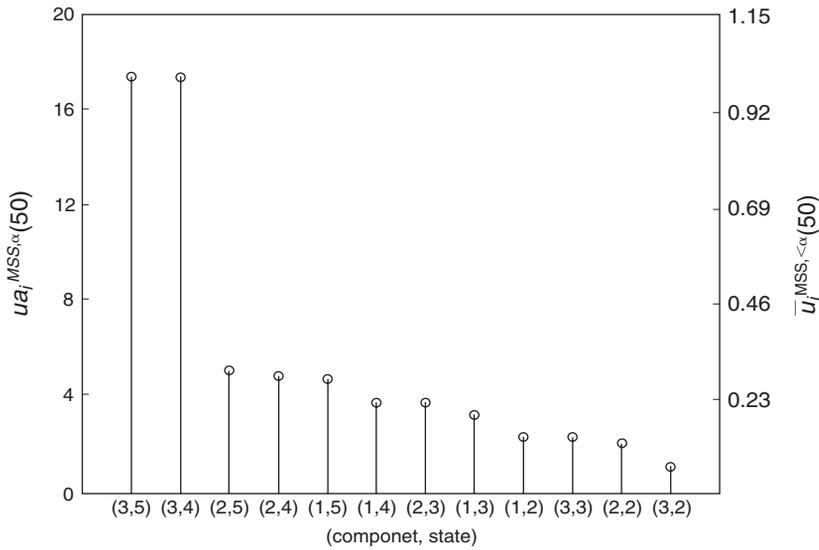


Figure 3. Values of  $ua_i^{MSS,\alpha}(50)$  ( $\alpha = w_2^i, w_3^i, w_4^i, w_5^i, i = 1, 2, 3$ ) in decreasing order (Table 5).

This behaviour is mainly due to the fact that the contribution of component 2 to the MSS-mean unavailability,  $\bar{U}_2^{MSS,\leq\alpha}(50)$ , is higher than that of component 1,  $\bar{U}_1^{MSS,\leq\alpha}(50)$ , when the considered  $\alpha$ -level is such that the components evolve only through the lowest-performance states 3, 4 and 5: in this case, component 2 is on average “more unavailable” than component 1 due to the higher value of the rate of transition to the failed state 5 when in state 4 ( $\lambda_{4 \rightarrow 5}^2 = 4 \cdot 10^{-2} h^{-1}$  and  $\lambda_{4 \rightarrow 5}^1 = 8 \cdot 10^{-3} h^{-1}$ , in the last column of the first two matrices of eq. (13)). On the contrary, the contribution of component 1 to the MSS-mean unavailability,  $\bar{U}_1^{MSS,\leq\alpha}(50)$ , is higher than that of component 2 when the performance threshold  $\alpha$  is such to allow the components transferring among states 2, 3, 4, 5 since the transition rates to failure  $\lambda_{2 \rightarrow 5}^1, \lambda_{3 \rightarrow 5}^1$  of component 1 are higher than the corresponding  $\lambda_{2 \rightarrow 5}^2, \lambda_{3 \rightarrow 5}^2$  of component 2.

5.4 Design retrofit

The information content provided by the introduced importance measures can be exploited for decision making at the design or operation level to identify the most important components within the system, tacking into account their performances. In this multi-state framework, the decision maker holds information relevant for driving design and operative actions to address the most critical components’ performance states. Again, we refer to our example in which the system is requested to provide a performance  $W^* = 50$  throughout the mission time  $T_m$ : the decision maker is interested in tracing which components’ performance

Table 5. Values of  $ua_i^{MSS,\alpha}(50)$  ( $\alpha = w_2^i, w_3^i, w_4^i, w_5^i, i = 1, 2, 3$ ) in decreasing order.

Component $i$	$j_i$ ( $\alpha$ -level)	$ua_i^{MSS,\alpha}(50)$	$\bar{U}_i^{MSS,\leq\alpha}(50)$
3	5 (0)	17.400	1.000
3	4 (25)	17.372	0.998
2	5 (0)	5.090	0.292
2	4 (20)	4.903	0.282
1	5 (0)	4.770	0.274
1	4 (20)	3.760	0.216
2	3 (40)	3.710	0.213
1	3 (40)	3.250	0.187
1	2 (60)	2.370	0.136
3	3 (50)	2.270	0.130
2	2 (60)	2.070	0.119
3	2 (75)	1.110	0.063

levels are to be guaranteed for the system to be available at the required performance threshold  $W^*$ . The ranking provided by the unavailability achievement worth,  $ua_i^{MSS,\alpha}(50)$ , can be exploited to the purpose. The twelve values of  $ua_i^{MSS,\alpha}(50)$  ( $\alpha = w_2^i, w_3^i, w_4^i, w_5^i, i = 1, 2, 3$ ) are ranked in decreasing order and reported in Figure 3 and Table 5. The corresponding values of  $\bar{U}_i^{MSS,\alpha}(50) = ua_i^{MSS,\alpha}(50) \bar{U}_i^{MSS}(50) \cdot i = 1, 2, 3$ , are also reported in the Table and in the right-hand vertical axis of Figure 3. These latter values represent the mean unavailability achieved by the MSS when component  $i$  never reaches a level of performance above  $\alpha$ . The largest values of  $ua_i^{MSS,\alpha}(50)$  in the Table are those of component 3 in correspondence of the lowest performance  $\alpha$ -levels ( $j_3 = 5$  and  $j_3 = 4$ ,

corresponding to  $\alpha = w_3^3 = 0$  and  $\alpha = w_4^3 = 25$ ). As above stated, these are obviously the most critical states of the system which remains always unavailable ( $\bar{U}_3^{MSS, \leq 0}(50) = \bar{U}_3^{MSS, \leq 25}(50) = 1$ ), due to the “bottleneck” component 3 having performance  $w_3^3$  below the required threshold  $W^*$ . Then, as expected, it is important to invest efforts in preventing also the other components 1 and 2 from transferring to their lower performance states 4 and 5. Hence, in general, actions aimed at reducing the transition rates  $\lambda_{ji \rightarrow ki}^i$ ,  $i = 1, 2, 3$  from any state  $j_i$  to state  $k_i = 5$  and 4 should be prioritarily performed. Following these most effective actions, possible further efforts should be devoted to ensure the other intermediate levels of performance  $\alpha > 0$ . As expected, the least effective actions are those aiming at improvements of performances already above high  $\alpha$ -levels, in particular those pertaining to component 3.

## 6 CONCLUSIONS

Importance measures associated to the components of a system are extensively employed both in the design phase and in operation to trace the system weaknesses and guide actions for effective system improvement. They have been commonly used for systems made up of binary components (i.e. only two possible conditions of the components are considered: working and failed). Actually, in many systems, e.g. the production and transportation ones, the components can operate at different conditions, characterized by different performance levels. Consequently, the system itself provides different performances. In the limit, continuous-state systems exist whose performance can range continuously from perfect functioning to failure. This is the case, for example, of the passive safety systems foreseen for use in the nuclear power plants of the future generations: in this case, the physical state of the system affects, in a continuous fashion, the system performance. For such systems, the criticality of the components must be measured with reference to their performance level with respect to the overall system performance.

In this paper, we have extended the definitions of the most frequently used importance measures to the cases of multi-state systems made up of multi-state components. The extensions are intended to quantify the relevance, with respect to the mean system unavailability, of a component achieving a given level of performance. For this purpose, we have introduced an extension to multi-state systems of the concept of unavailability, which is related to the capability of the system of meeting a required performance demand.

The defined measures have been applied to a simple multi-state system defined in such a way to highlight the dependence of the obtained rankings on different levels of components' performance. The comparison with an “equivalent” binary system has shown that a

given multi-state component may have performance states that are “more critical” than others for the system availability and performance. Furthermore, although not shown here, a component performance level can turn out to be more important for the achievement of a given system performance and less important for another.

The work presented is methodological in nature and its application to practical systems is yet to be tested. Particularly worthwhile seems a future extension of the concepts here presented to continuous-state systems such as the passive systems employed in the current nuclear engineering design practice.

## ACKNOWLEDGEMENTS

The authors are indebted to Professor Marzio Marseguerra for his precious suggestions and comments.

## REFERENCES

- Birnbaum L. W. 1969. *On the importance of different components in a multi-component system. Multivariate analysis 2*. New York: Academic Press.
- Fussell J. B. 1975. How to calculate system reliability and safety characteristics. *IEEE Trans. on Reliab.* R-24(3): 169–174.
- Cheok, M. C., Parry G. W., Sherry R. R. 1998. Use of importance measures in risk informed applications. *Reliab. Eng. Sys. Safety* 60: 213–226.
- Vasseur D., Llory M. 1999. International survey on PSA figures of merit. *Reliab. Eng. Sys. Safety* 66: 261–274.
- van der Borst M, Shoonakker H. 1999. An overview of PSA importance measures. *Reliab. Eng. Sys* 72(3): 241–245.
- Borgonovo E., Apostolakis G. E. 2001. A new importance measure for risk-informed decision making. *Reliab. Eng. Sys* 72: 193–212.
- Levitin G., Lisnianski A. 1999. Importance and sensitivity analysis of multi-state systems using the universal generating function method. *Reliab. Eng. Sys*; 65: 271–282.
- Armstrong M. J. 1997. Reliability-importance and dual failure-mode components. *IEEE Trans. on Reliab.* 46(2): 212–221.
- Levitin G., Lisnianski A., Beh-Haim H., Elmakis 1998. Redundancy optimization of for series parallel multi-state systems. *IEEE Trans. on Reliab.* 47(2): 165–172
- Lisnianski A. 2002. Continuous-state system reliability models as an extension of multi-state systems. *Proceedings of MMR, Mathematical Methods in Reliability, June, 17–20, Thronheim, Norway*: 401–404. Thronheim: H. Langseth and B. Lindqvist.
- Zio E., Podofillini L. 2002. Importance measures of multi-state components in multi-state systems. *Invited paper for “special issue on multi-state systems” of the International Journal of Reliability, Quality and Safety Engineering.*
- Marseguerra M., Zio E. 2002. *Basics of the Monte Carlo Method with Application to System Reliability*. Hagen: LiLoLe-Verlag GmbH (Publ. Co. Ltd.).

## Probabilistic aspects of maritime transport of tunnel elements

T.J. Zitman

*Delft University of Technology, the Netherlands*

**ABSTRACT:** After being prefabricated in a dry dock, elements of the Wijker tunnel (the Netherlands) have been transported over the North Sea to the location of the tunnel where they have been submerged. For transport operations an upper limit had been defined with respect to the probability of an element not being able to withstand the wave loads to be expected offshore. Implementation of this safety criterion necessitated an assessment of two sources of uncertainties. One of them is that only a forecast of wave conditions is available at the moment of deciding upon initiating or postponing a transport operation. The other is that this forecast concerns general characteristics of wave conditions, whereas wave loads on the element depend on the properties of individual waves. To deal with these uncertainties, a probabilistic tool has been developed that relates a wave forecast to the probability of meeting the safety criterion for transport.

### 1 INTRODUCTION

In the second half of the 18th century the North Sea Channel was constructed to connect the port of Amsterdam (the Netherlands) to the North Sea. To facilitate road traffic across this channel ferries were installed at various locations. About half a century after its completion, socio-economic developments necessitated widening of the channel and it became clear that in due time the capacity of the ferries would become insufficient to satisfy the envisaged increasing demand for road transport. As an alternative for the ferry at Velsen, the Velsler tunnel was constructed. It was opened for traffic in 1957. In response to the ongoing increase of road traffic, it was decided in the early 1990's to construct a second tunnel close to the existing one: the Wijker tunnel. Since its opening in 1996, the Wijker tunnel is used for through traffic, whereas the local traffic is concentrated in the old Velsler tunnel.

Like most Dutch tunnels for rail and road traffic, the Wijker tunnel consists of a series of prefabricated concrete elements. They are transported in floating condition from their construction site to the location of the tunnel where they are submerged in a trench dredged between the banks of the channel.

Commonly, tunnel elements are prefabricated in a dry dock fairly close to the actual location of the tunnel. That contributes to the efficiency of the building process for instance, and it limits adverse effects on shipping along the transport route. For mainly economical reasons it was considered not feasible to install a

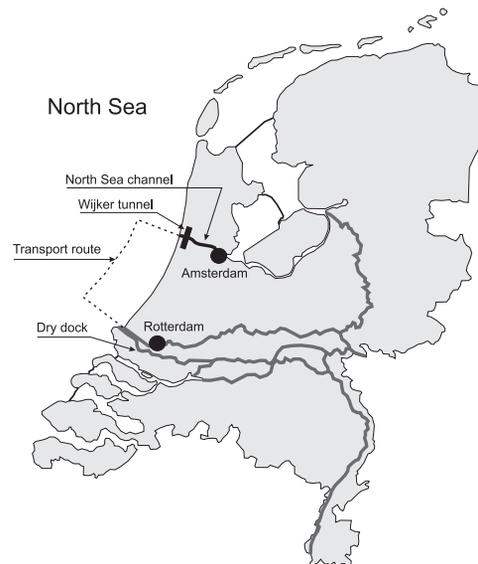


Figure 1. Schematic map of the Netherlands, indicating the transport route from the dry dock to the tunnel.

dry dock near the location of the Wijker tunnel. In stead, it was chosen to construct its six elements in an already existing and available dry dock along the river Meusse near the port of Rotterdam (see figure 1). Measured in a straight line this dock is about 70 km away from

the location of the tunnel. At the time, this was by Dutch standards unusually large a distance. In addition, transportation of tunnel elements over inland waterways that connect the river Meuse and the North Sea Channel was practically impossible. Maritime transport was considered a feasible alternative, although it had never been done before in the Netherlands.

The main challenge of maritime transport lies in the inevitable exposure of a tunnel element to waves. That is attained with loads on the structure that have a dynamic nature not encountered during transport over inland waterways, to which experience was limited at that time. In particular, there are two sources of uncertainties associated with these dynamics that play a crucial role in transport planning. One of them is that when deciding upon initiating the transportation of an element, only a forecast is available of the wave conditions that will be encountered. The reliability of such a forecast is limited. The other uncertainty is that the wave forecast concerns the general characteristics of an entire wave field, whereas momentary wave loads on the structure depend on the properties of individual waves.

To deal with these uncertainties a tool has been developed that shows for any (physically) realistic wave forecast whether the probability of overloading an element during transportation exceeds some predefined safety level. The details of this tool are presented hereafter.

## 2 SAFETY LEVEL

As the design of the elements of the Wijker tunnel was not focused on achieving a high degree of seaworthiness, transportation could take place only during periods of fairly moderate hydrodynamic conditions. Actually, in an early stage of the design it was decided to concentrate transportation in late spring and summer. Laboratory tests carried out on a scale model have provided the design criteria necessary to ensure that tunnel elements would be able to withstand wave conditions that are not exceeded during major part of this period of the year. This does not mean however that transportation of an individual element could be initiated at any arbitrary moment. As also during summer wave conditions may show considerable temporal fluctuations, it had to be ensured prior to the transportation of each element that the wave loads to be expected during transport would not exceed the strength of the element.

How to go about this became an issue only a few months before the first element was ready for transport. Evidently, the design of the elements was beyond discussion at that time. In other words, a fully probabilistic design including all relevant aspects of maritime transport was not an option. In stead, the structural

characteristics of the tunnel elements turned into boundary conditions for transport planning.

A safety level for transporting the six elements of the Wijker tunnel was formulated against this background. It is focused on preventing flooding of an element. This is considered a highly unfavourable event, as it will lead almost inevitably to uncontrolled immersion of the element, most likely well away from its actual destination.

For a proper understanding of the safety level chosen for the transportation of the tunnel elements, we will briefly consider how they are constructed. The immersed part of the Wijker tunnel consists of a series of 24 segments. The connection of two adjacent segments is flexible in the sense that they may rotate slightly relative to one another. This way, the segments form a look-alike of a chain, hung up between the two (spatially fixed) approaches of the tunnel. To combine this flexibility with the necessary watertightness, rubber profiles are placed in the joints between adjacent segments.

The segments are transported from the dry dock along the river Meuse to their destination in the North Sea Channel in sets of four. Such a set is called an element. During transportation and immersion, the segments in an element are kept together by prestressed cables in the roof and the floor (see figure 2). This prestressing is intended to have an element behave like a coherent, more or less stiff object. Simultaneously it is meant to prevent leakage in the joints, which is assumed the most likely cause of flooding.

When wave-induced bending moments become so large that this latter effect of prestressing perishes, leakage may occur anyway. Hence, the applied prestressing determines the maximum bending moment an element may be exposed to without endangering the essential watertightness of the joints. This sets an upper limit to the wave conditions that can be accepted during transportation.

For transportation of tunnel elements over inland waterways, it was common to demand that the pressure in the joints must be at least  $0.2 \text{ N/mm}^2$  at all times.

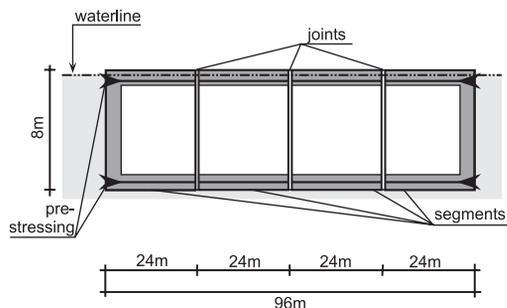


Figure 2. Schematic cross-section of an element.

As the conditions at sea are considerably more dynamic than those on inland waterways, this demand has been sharpened rather arbitrarily to  $0.3 \text{ N/mm}^2$ . This however, is not a guarantee against leakage, in particular as wave loads on the structure have a random character. In view of this, the party responsible for the maritime transport reasoned that in conventional design methods this demand would be associated with 1.8 times the expected load. Assuming that loads on the structure are normally distributed, it then follows that the probability of the pressure in the joints becoming less than the prescribed  $0.3 \text{ N/mm}^2$  must not exceed 3.5%.

With this reasoning the demand regarding the minimum pressure in the joints was transformed into a requirement appropriate for a probabilistic approach. In addition, it has been chosen to focus elaboration of this requirement on wave loads on the structure. This is not entirely correct, as wave loads do not determine the actual pressure in the joints only. Random deviations of structural characteristics from design specifications may also affect the actual pressure in the joints, but they are assumed negligible compared to the random fluctuations in wave loads.

With the above, a safety level has been defined for the maritime transport of elements of the Wijker tunnel. It is focused on preventing leakage in the joints between adjacent tunnel segments. It is not clear beforehand however, what this safety level means in terms of the probability of complete structural failure. In view of this, a second safety level has been defined. It sets an upper limit of 0.01% to this latter probability. This value is meant to express aversion against potential failure; it is not the result of for instance a risk optimisation.

The method we have applied to elaborate a safety level into maximum wave conditions that can be accepted during transportation is explained hereafter. As it is identical for both mentioned safety levels, it is sufficient to focus this explanation on one of the two. In this respect, we have chosen the one meant to prevent leakage.

### 3 ANALYSIS

#### 3.1 Describing wave conditions

In general, an individual wave can be characterised by its height, its period (to which the wavelength is directly related) and its direction of propagation. In a natural wave field, these properties may vary from one wave to another. Yet a clear coherence exists that allows description of the entire wave field in terms of generalised versions of the mentioned three parameters. Wave heights for instance, are by fair approximation Rayleigh distributed. The parameter of this distribution is a measure for the diversity of wave heights that occur in the wave field at hand. It is commonly associated to

the so-called significant wave height  $H_s$ , defined as the average of the 1/3 highest waves.

The distribution of wave energy over periods (the wave energy density spectrum, in short “wave spectrum”) is commonly used to characterise the diversity of wave periods. As wave fields show noticeable similarity with respect to the shape of this distribution, it forms a natural basis for deriving a characteristic wave period. One example often used in engineering applications is the so-called peak period  $T_p$ . It coincides with the maximum of the energy distribution. Due to interaction between waves, there is a continuous transfer of energy to waves with ever-larger periods. As a result, the peak period increases with the age of the wave field.

As the scale of the energy distribution over periods is directly related to the significant wave height, the combination of wave peak period and significant wave height yields a fairly complete description of a wave field. To include information on the direction of wave propagation, this combination is commonly complemented with the average wave direction.

#### 3.2 Forecasting wave conditions

Offshore wave conditions are almost without exception a combination of locally generated waves (called sea) and waves generated previously by a different wind field and at some distant location (this is called swell).

The numerical wave model deployed for transport planning, produced forecasts of wave peak period and significant wave height for sea ( $T_p$  and  $H_s$ ), as well as a significant wave height for swell (henceforth denoted by  $D$ ). A characteristic period for swell was not part of the model output. However, from experience we know that along the transport route swell can be associated on average with a wave period of 10 s or more. We have used this wave period throughout our probabilistic computations to characterise swell. This is a conservative approach as waves with a period of 10 s yield the most adverse loads on the elements (this is explained in the next section on wave loads).

Although the wave forecasts are quite reliable, they are not exact. A part of the deviation between predicted and actual wave properties will have a random character, whereas the other part is bias. To gain quantitative insight into both parts, we have evaluated over 400 previous model predictions against corresponding field observations. All these predictions concerned the period from May up to September as transportation of tunnel elements was scheduled for this part of the year. Experience has learned that it is more difficult to predict the comparatively moderate conditions in this period than the “bad weather” encountered during autumn and winter. Focusing the analysis on the entire year might therefore lead to an estimate of the model performance not entirely

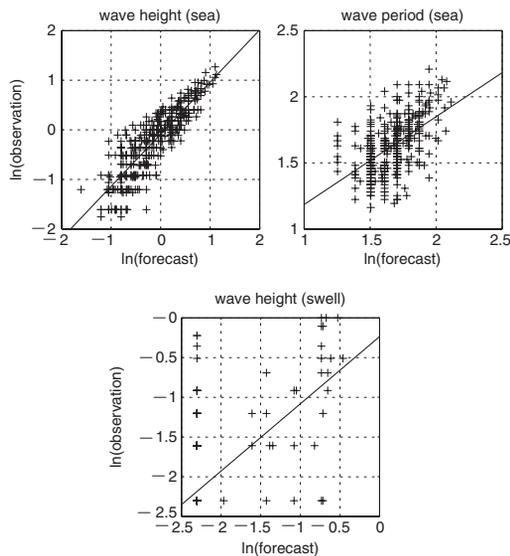


Figure 3. Estimating bias and random error in forecasts of wave parameters. As wave heights for swell are rounded to multiples of 0.1 m, each + in the graph may concern more than one occurrence.

representative for predictions concerning late spring and summer.

For all three wave properties predicted by the model, we have assumed that the bias can be described as

$$\ln \xi = \alpha_{\xi} \ln \hat{\xi} + \beta_{\xi} \tag{1}$$

in which  $\xi$  stands for either  $T_p$ ,  $H_s$  or  $D$  and the  $\hat{\xi}$  indicates that it concerns a model prediction. The only reason for choosing a relation of this form is that it agrees reasonably well with the data.

Application of linear regression to the mentioned selected sets of predictions and corresponding observations has provided estimates of the coefficients  $\alpha$  and  $\beta$  (see figure 3). For simplicity, we have henceforth disregarded the inherent limited reliability of these estimates and we have interpreted any disagreement between (1) and individual sets of observed and predicted  $\xi$  as random error. Hence, for the  $i$ -th set, it can be written that

$$\ln \xi^{(i)} = \alpha_{\xi} \ln \hat{\xi}^{(i)} + \beta_{\xi} + \psi_{\xi}^{(i)} \tag{2}$$

in which  $\psi$  is the random error. In our analysis, we have approximated the joint probability distribution of the three  $\psi$  by a multi-normal distribution. The corresponding (co-)variances have been estimated from the results of the applied linear regression.

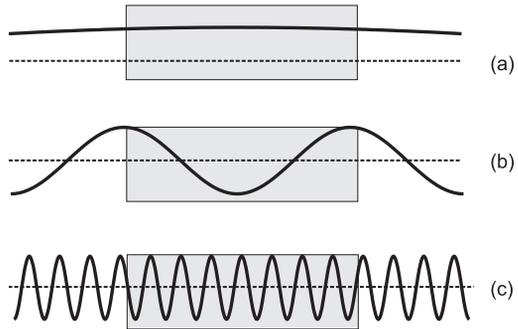


Figure 4. Wavelength and characteristic length of an element.

### 3.3 Wave loads

The actual pressure in the joints between adjacent segments in an element is primarily the combined result of prestressing and wave-induced bending moments. To obtain an impression of the relation between these bending moments and wave properties, we consider an element exposed to unidirectional, monochromatic waves propagating along the longitudinal axis of an element.

If the length of the waves is large compared to the size of the element, the spatial variations in wave loads will be comparatively small. Seen at the length-scale of the element, a passing wave has the character of a gradually changing surface level elevation (see figure 4a). It will force the element into a mild oscillating motion, not attended with substantial bending moments.

In the case of relatively short waves on the other hand, wave forces will show variations at such small spatial intervals that they closely resemble an equally spread load on the element (see figure 4c). Consequential bending moment will be small.

Comparatively large bending moments can be expected if the wave length is close to or equal to the length of the element (i.e. 96 m, corresponding to a wave period of about 10 s, at least along major part of the transport route). In the sketch given in the figure 4b for instance, the element more or less spans the wave trough between two consecutive crests. In situations like this, the length-scale of spatial variations of wave loads is comparable to that of the size of the element. That may lead to bending moments that are substantially larger than those induced by shorter or longer waves.

With the above sketch we have obtained a fair impression of how bending moments vary with wavelength. This relation applies also to pressure in the joints. However, neither bending moments nor pressure depend on the length of the waves only. Their height plays a role as well and so does the angle of wave incidence relative to the element. In addition, the pressure

may differ from one joint to another. Actually, the relation between pressure in the joints on the one hand and wave properties on the other hand is far too complicated to be quantified sufficiently accurate on the basis of a purely theoretical assessment of the physics involved. As an alternative, we have revisited the results of the aforementioned laboratory tests that have been conducted in support of designing the tunnel elements.

These laboratory were meant to arrive at a relation between the general characteristics of a wave field (sea only) on the one hand and the probability distribution of the minimum pressure that may occur during transportation on the other hand. The test results have shown that temporal variations of the pressure resemble a Gaussian process. Momentary values are by good approximation normally distributed and peaks in the pressure are roughly Weibull distributed. As the safety level defined for the transportation of tunnel elements concerns the minimum pressure encountered during a transport operation, the evaluation of test results was focused on these peaks (ic. minima).

Temporal fluctuations in pressure vary from one joint to another and so do the properties of the corresponding Weibull distribution. They depend on the general characteristics of the wave field (wave peak period and significant wave height) as well as on the direction of wave propagation relative to the element. In the laboratory tests the pressure in the joints has been monitored for various combinations of wave period, height and direction. Subsequently, the test results have been elaborated into estimates of Weibull parameters for all considered combinations of wave properties and joint. In addition, for each combination of considered period and direction, the significant wave height has been determined that corresponds to a probability of 1% of the minimum pressure that occurs during transportation, nonexceeding the prescribed  $0.3 \text{ N/mm}^2$ . These wave heights are indicated in figure 5.

Only the latter significant wave heights were available for the present analysis. Unfortunately these wave heights provide insufficient information to reproduce the parameters of the underlying Weibull distributions: it is not possible to determine the two Weibull parameters from a single quantile. To deal with this we have reasoned that the safety level concerns the entire element, not one joint in particular. Hence we may focus on the joint where the lowest pressures occur as that one determines the wave conditions that can be accepted during transportation of the elements. In addition, we have chosen to disregard the influence of the direction of wave propagation on the pressure in the joints. In stead, we have assumed that during transportation waves continuously propagate in the most adverse direction (ic. parallel to the element). In other words, we conservatively focus our analysis on the lower envelope of the significant wave heights shown in figure 5.

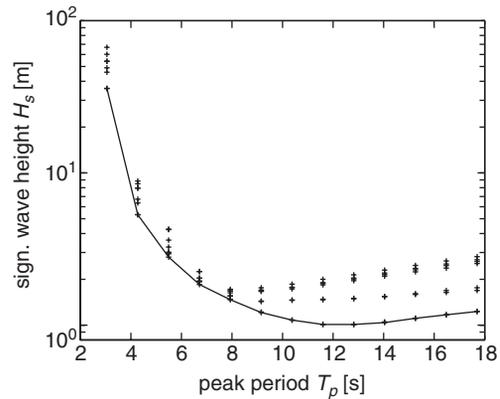


Figure 5. Combinations of wave height and period for which the non-exceedance probability of the prescribed minimum pressure equals 1%. Each + refers to a different direction of wave propagation and joint in the element.

Furthermore, we have approximated the Weibull distribution for the minimum pressure in the joint by a single parameter exponential distribution. The corresponding probability density function is given by

$$p(m) = \frac{e^{-m/\mu_m}}{\mu_m} ; \quad m = \frac{\Delta\tau}{\Delta\tau_{\max}} \quad (3)$$

in which  $\Delta\tau$  is the wave-induced (random) reduction of the pressure in the joints relative to the one that results from the applied prestressing and  $\Delta\tau_{\max}$  is the maximum allowed reduction, equal to the difference between the pressure due to prestressing and the safety limit (ic.  $0.3 \text{ N/mm}^2$ ). As wave-induced bending moments will be attained always with an increase of the pressure on one side of the structure and a simultaneous pressure decrease on the other side,  $\Delta\tau \geq 0$  and hence,  $m \geq 0$ . Furthermore, the encountered minimum pressure is larger than the safety limit when  $m < 1$ .

The parameter  $\mu_m$  of the exponential distribution is a function of wave peak period  $T_p$  and significant wave height  $H_s$ . We have assumed that  $\mu_m$  is proportional to  $H_s$ . The corresponding proportionality constant depends on  $T_p$  such that for combinations  $(T_p, H_s)$  on the lower envelope of the test results, the probability of  $\Delta\tau \geq \Delta\tau_{\max}$  (or, identically,  $m \geq 1$ ) equals 1%. This yields

$$\mu_m(T_p, H_s) = -\frac{H_s}{H_s^*(T_p) \ln 0.01} \quad (4)$$

in which  $H_s^*(T_p)$  refers to the lower envelope of the test results.

This concludes our approximation of the relation between the statistical properties of the minimum pressure in the joints between adjacent segments in an element on the one hand and the general characteristics of a natural wave field on the other hand. It is important to note however, that it applies to sea only. The reason for this is that the laboratory tests used to arrive at this relation were focused on sea and did not include swell.

#### 4 DECISION SUPPORT TOOL

Maritime transport of elements of the Wijker tunnel is subjected to a demand with respect to the pressure in the joints between adjacent segments in an element. It sets a maximum of 3.5% to the probability of the minimum pressure encountered during transport non-exceeding a prescribed lower limit (ic. 0.3 N/mm<sup>2</sup>). Prior to the transportation of each element it must be judged on the basis of a forecast of wave conditions, whether this demand will be met. The relations derived in the previous sections between forecasted and actual wave conditions and between actual wave conditions and loads on tunnel elements during transportation are used for this purpose. They are combined into a tool that shows for any wave forecast whether the non-exceedance probability of the minimum allowed pressure in the joints is larger or less than 3.5%. If it is larger, transportation of the element at hand needs to be postponed.

A complicating factor in this respect is that the conditions offshore are determined by a combination of sea and swell. This has been taken into account in forecasting wave conditions, but the relation we have derived in the previous section between actual wave conditions and loads on the element, applies to sea only. To deal with this, we have assumed that swell can be treated as a deterministic quantity. A first step in this direction has been made already when we fixed the wave period for swell to 10 s.

With these two assumptions we have simplified the effect of swell to a continuously present reduction of the pressure in the joints. Assuming in addition that the effects of sea and swell may be superimposed, we may write the wave-induced pressure reduction  $\Delta\tau$  introduced in (3) as the sum of a deterministic swell-related part ( $\Delta\tau_{\text{swell}}$ ) and a random part resulting from sea ( $\Delta\tau_{\text{sea}}$ ). This way,

$$m = \frac{\Delta\tau_{\text{sea}}}{\Delta\tau_{\text{max}}} + \frac{\Delta\tau_{\text{swell}}}{\Delta\tau_{\text{max}}} = m_{\text{sea}} + m_{\text{swell}} \quad (5)$$

and the probability of the actual minimum pressure encountered during transport being less than the safety limit becomes

$$\begin{aligned} P(m \geq 1) &= P(m_{\text{sea}} \geq 1 - m_{\text{swell}}) \\ &= 1 - \int_0^{1-m_{\text{swell}}} \frac{e^{-m_{\text{sea}}/\mu_m}}{\mu_m} dm_{\text{sea}} \end{aligned} \quad (6)$$

To the analogy of the test results obtained for sea, we have defined

$$m_{\text{swell}} = \frac{D}{H_s^*(10)} \quad (7)$$

With this definition, we cannot accept any sea when  $D = H_s^*(10)$ . In such a situation,  $P(m \geq 1) = 100\%$  for any  $H_s > 0$ . On the other hand, if we consider sea with  $H_s = H_s^*$ , then in the absence of swell,  $P(m \geq 1) = 1\%$  (this holds by definition: it is the basis for the definition of  $\mu_m$ , see (4)). This difference suggests that definition (7) leads to conservative estimates of acceptable combinations of sea and swell.

With expressions (6) and (7) the probability of meeting the safety level can be estimated for any combination of sea, characterised by  $(T_p, H_s)$  and swell described by  $D$ . Prior to the transportation of an element however, only forecasts of the wave parameters  $T_p, H_s$  and  $D$  are available and they may deviate from the ones reflecting the actual wave conditions encountered during transport. Combining this with (6)–(7) yields

$$\begin{aligned} P(m \geq 1 | \hat{T}_p, \hat{H}_s, \hat{D}) &= \\ 1 - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} N_{\psi} \int_0^{1-m_{\text{swell}}} \frac{e^{-m_{\text{sea}}/\mu_m}}{\mu_m} dm_{\text{sea}} d\psi_T d\psi_H d\psi_D \end{aligned} \quad (8)$$

in which  $N_{\psi} = N_{\psi}(\psi_T, \psi_H, \psi_D)$  is the probability density function of the multi-normal distribution assumed for the random errors  $\psi$  in the wave forecast. The corresponding bias as given in (1) is used in combination with (4) and (7) to relate  $\mu_m$  and  $m_{\text{swell}}$  to predictions of the wave parameters  $T_p, H_s$  and  $D$ .

The above expression yields for any wave forecast (prediction of  $T_p, H_s$  and  $D$ ) the probability of the minimum pressure in the joints of the elements encountered during transport, being less than the safety limit of 0.3 N/mm<sup>2</sup>. If this probability does not exceed 3.5%, the wave forecast gives no reason to believe that wave conditions will lead to undesired low pressure in the joints of the element to be transported.

In essence, expression (8) is the intended decision support tool. However, in this form it is not very suitable for use in the field. To cope with this, we have used the expression to obtain sets of predicted  $T_p, H_s$  and  $D$  for which  $P = 3.5\%$ . The result is presented in

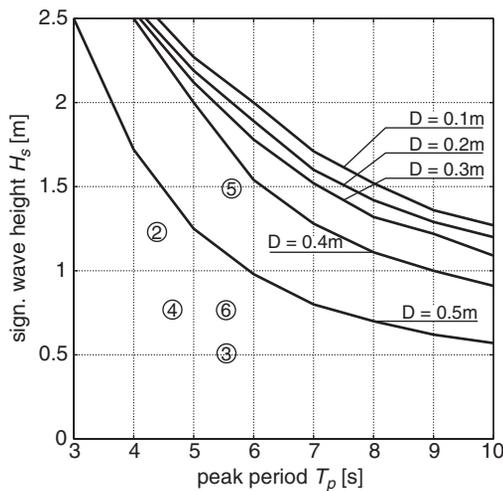


Figure 6. Curves reflecting the wave forecasts for which the safety level is only just satisfied. Actual forecasts (sea) for the transportation of elements 2–5 are indicated by encircled numbers.

figure 6. Each curve in this graph reflects an upper limit. They show for a specific prediction of  $D$  the relation between predicted  $T_p$  and  $H_s$  for which the safety level is only just satisfied. In deciding upon initiation of a transport operation, the point reflecting the predicted ( $T_p$ ,  $H_s$ ) is plotted in this graph. When this point is below the curve corresponding to the predicted  $D$ , the safety level is not exceeded so that transportation may commence.

The angular character of the curves in figure 6 can be explained to a large extent from the computational methods that have been applied to evaluate expression (8). In addition, figure 6 also includes the results of an assessment similar to the one presented above but with respect to safety against structural failure of an element. Which of the two is determinative differs from one wave forecast to another.

## 5 EVALUATION

With the graph in figure 6 an easily manageable, probabilistic tool has been obtained to evaluate on the basis of a forecast of wave conditions whether the safety

level set for transporting elements of the Wijker tunnel will be satisfied. This tool has played a central role in the decision making process with respect to the transportation of those elements. Its principles are widely applicable in offshore operations planning.

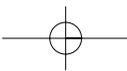
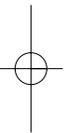
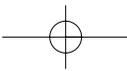
The first element was transported over a very calm sea ( $T_p = 1.0$  s,  $H_s = 0.1$  m and negligible swell). In the case of element number 2 adverse wave conditions had been forecasted and transportation had to be postponed (the encircled 2 in figure 6 corresponds to the second attempt to transport element 2). The wave forecast made prior to the transportation of the fifth element read  $T_p = 5.5$  s,  $H_s = 1.5$  m and  $D = 0.4$  m (see the encircled 5 in figure 6). This only just satisfies the safety level. After the element had reached its destination, the wave forecast was compared to field data gathered during transport. It appeared that the forecast was slightly optimistic in the sense that the maximum  $H_s$  observed during the transport operation was almost 1.9 m. If the forecast had been fully accurate, transportation of element 5 would have been postponed as well. Some people have concluded from this observation that more risk had been taken than intended. Evidently, this conclusion is incorrect.

## ACKNOWLEDGEMENT

The probabilistic exercise described in the present paper has been carried out within the framework of the advisory services rendered by Tunnel Engineering Consultants (the Netherlands) in support of the maritime transport of the six elements of the Wijker tunnel. The co-operation of this firm in realising this paper is appreciated.

## LITERATURE

- Glerum, A. 1998. Developments in immersed tunnelling in Holland. *Tunnelling and underground space technology* 10 (4): 455–462
- Hakkaart, C.J.A. 1996. Transport of tunnel elements from Baltimore to Boston, over the Atlantic Ocean. *Tunnelling and underground space technology* 11 (4): 479–483
- Stikma, K. 1988. *Tunnels in the Netherlands, underground transport connections*. Rotterdam: Illustra
- Zitman, T.J. 2002. Zeetransport elementen Wijkertunnel. In: *Kansen in de Civiele techniek, part 2* (in Dutch). CUR publication 209: 80–105



## Foundations of the UPM common cause method

Athena Zitrou & Tim Bedford

*University of Strathclyde, Glasgow, UK*

**ABSTRACT:** Common cause failures (CCF) have a significant impact on the risk of complex engineering systems, such as nuclear plants. Consequently, modelling this class of events is an important part of risk assessments, and the authorities that are responsible for the safe and efficient functioning of the aforementioned systems have taken this issue on board. The current approach in the UK towards CCF modelling is the Unified Partial Method (UPM), which is based on the Partial Beta Factor Model and the Cut-Off Methodology. The UPM scoring system itself is based on an additive weighting factors approach. This is closely allied to the additive value function approach of Multiattribute Value Theory. However, within MAVT there are many other possible models. We explore whether the preferential independence axiom, required for an additive value function, is conceptually appropriate. In addition we discuss the impact of new data availability, in particular from the ICDE project. The research discussed here is part of an on-going research project, funded by the Health and Safety Executive.

### 1 INTRODUCTION

High reliability and safe design play an important role in complex technological systems like nuclear power plants, since their inefficient or irregular operation would have enormous environmental, social and political impacts. Nuclear power plants are designed in accordance with the Defence-In-Depth philosophy, which employs redundant systems to serve as multiple defence layers. Given the assumption that the components fail independently, multiple systems/components offer a major level of defence: in case one component fails, others can perform its designed function. However, operating experience and collected data revealed that the risk posed to these systems is higher than estimated. This is due to the fact that events are often dependent. Probabilistic Risk Analyses (PRAs) have long recognised the contribution of dependent failures to accidents and system unavailability and modelled this in principle through the use of common cause failure models. This paper looks at some of the assumptions implicit in the UPM method, which is the current approach of the UK.

Common Cause Failures (CCFs) are “simultaneous” failures of a number of components due to some common event. They pose a major threat to redundant systems, as they can defeat the defence design. Within a PRA scope some events leading to CCFs may be explicitly modelled while there are a host of other which are not. For this second category numerous approaches

have been proposed to quantify their impact on the system of interest: these are mostly parametric models. A few examples of such models are the Multiple Greek Letter Model (Apostolakis & Moieini, 1987), the Binomial failure Rate Model (Atwood, 1996), the Alpha Factor Model (Siu & Mosleh, 1998) and the Unified Partial Method (UPM) (Brand, 1996). The primary objective of parametric models is to quantify the frequency of multiple component failures through the assessment of model parameters.

### 2 UNIFIED PARTIAL METHOD

There are various levels of complexity among the parametric models, starting from very simple models in terms of assumptions and data input, like the Beta Factor model, and shifting to more complex ones, like the Marshall-Olkin model. The simplest approaches have often been criticised for embracing over-simplifying assumptions. On the other hand, the more complex ones can lose predictive accuracy due to lack of sufficient data.

Nuclear industries in many countries use parametric models of intermediate complexity level. However, UK has developed its own approach towards CCF modelling, the Unified Partial Method (UPM) (Brand, 1996). UPM is a methodology that introduces a single systematic structure based on the Beta-Factor model and the Cut-Off method. Once the analyst has decided the

physical boundaries of the system of interest, a Pre-Analysis table is filled, which aims to identify the data available and the time to be spent in the analysis. At this point the level of the analysis is being decided (system/component). In both cases similar steps are followed.

Within the UPM framework, the system is calibrated across a number of subfactors/areas such as redundancy or operator interaction. This is done through a number of tables, each of which is related to a different system design or operation, and scores are given depending on the categories assigned to the system.<sup>1</sup> Finally, a Beta factor (component level) or a Cut-Off (system level) is obtained, which represents the common cause failure rate of the system of interest.

UPM offers a step-by-step, auditable methodology. The framework proposed is easy to implement, even by an analyst who does not have in-depth knowledge of analytical procedures. During the application of UPM, the analyst is encouraged to study the system of interest, in order to classify it across the generic categories, thus gaining insight into the potential for CCF events (the insight gained may also indicate possible modifications that would increase the reliability of the system).

Despite all the above advantages of UPM, there are aspects which are ready for further research. First of all, changes in the design and age of the system raise the issue of whether a recalibration of the UPM scoring system is needed. The recent availability of data through the ICDE database, which represents many reactor years and includes information from various sources across a number of countries, gives an opportunity for further development. In addition, both the Beta-Factor and Cut-Off approach used in UPM make use of an additive weighting system. Throughout the rest of the present paper, the recalibration issue will be explored and the implications of this additive system will be highlighted. Some conceptual inconsistencies will be identified, which give directions to further improvement by using theoretical tools such as Multiattribute Value Theory (MAVT). We highlight those similarities of the UPM structure with MAVT that give grounds for alternative approaches.

### 3 INTERNATIONAL COMMON CAUSE FAILURE DATA EXCHANGE (ICDE) PROJECT

#### 3.1 Introduction

The availability of reliability data is of vital importance, not only because data is used for the quantification of

<sup>1</sup>These scores have been deduced from surveys conducted on historical data and engineering judgment and characterise the vulnerability of the system towards CCF events.

parameters in the models, but also because it may be used in a qualitative way for identifying and understanding the various failure mechanisms. However, a number of pitfalls arise in data collection procedures. Firstly, CCF events are rare events and consequently it is difficult to gather enough plant-specific data in order to perform robust parameter estimations and credible reliability analyses. Secondly, due to the complex nature of CCF failures, a considerable amount of ambiguity exists in their classification.<sup>2</sup> Certainly data may be gathered from well-run tests, but it has been recognised that this type of data fails to capture the particularities and complexity of CCF events in the way that operational data can (Walls, 1989, Atwood, 1996).

In order to overcome these drawbacks and produce credible analyses, efforts have been made to collect information and failure data from multiple sources and to create a generic database. One important effort in this direction is the International Common-Cause Failure Data Exchange (ICDE) Project. The philosophy behind this initiative is to encourage multilateral co-operation in the collection and analysis of data relating to CCF events (ICDE project, 2001). Once pitfalls such as data heterogeneity<sup>3</sup> have been overcome, the ICDE database will be a valuable source of information, which could be used in both qualitative and quantitative ways.

#### 3.2 ICDE and UPM

The ICDE database contains a large amount of information concerning CCF events; nonetheless it is not currently used for quantification purposes in the UK. The current approach is to use it for the identification of CCF events, and it is mainly used as a means for gaining insight into the relevant failure mechanisms. Since ICDE is a generic database, the data that it contains comes from various sources; this fact leads to problems regarding the interpretation of the information when it is intended to be used for specific quantification purposes. Nevertheless, the observations in ICDE are relatively homogeneous because a systematic data-collection-procedure is shared. In addition, we expect in the future there will be further moves to common data collection procedures.

As has been already mentioned, UPM is used exclusively by the UK. The other national members of the ICDE project have adopted different approaches towards the issue of CCF quantification. Therefore, the failure reports included in the ICDE database do not

<sup>2</sup>There is no fixed rule for distinguishing a multiple dependent failure from coincident multiple independent failures; or a single failure from a CCF event that happened to cause the failure of only one component.

<sup>3</sup>System-to-system and plant-to-plant variation impact on the analyses' results and this issue should be taken into consideration when using generic reliability data.

Table 1. Data available for quantification purposes.

System	Total common cause events	Total number of times a component fails	Scores at Subfactors			
			$S_1$	$S_2$	...	$S_8$
$i$	$m_i$	$n_i$	$x_{i1}$	$x_{i2}$		$x_{i8}$

incorporate information regarding the subfactors of UPM. If that were the case, statistical techniques such as regression might be applied to assess the impact of subfactors.

Assuming the ideal case, every failure report in the ICDE database incorporates information regarding the different UPM subfactors. Then, for every failure event the categories characterising the system would be available in the event reports. Moreover, for every system the partial beta factor ( $\beta$ ) can be estimated, based on the data gathered during the operational years contained in the database. Therefore, the data available for quantification purposes would be of the form given in Table 1.

The beta factor of a system describes the probability of a component failing due to a common cause, given that the component fails. It is estimated as a fraction of the total common cause events over the total number of times that a component belonging in the redundant group of the system failed. In other words,

$$\hat{\beta}_i = \frac{m_i}{n_i}$$

The model that the UPM methodology proposes for estimating the beta factor of the system of interest is of the form:

$$\hat{\beta}_i = w_1 x_{i1} + w_2 x_{i2} + \dots + w_8 x_{i8} \quad (1)$$

where

$x_{ij}$  ( $j = 1, \dots, 8$ ) are the scores of the categories assigned to system  $i$  across the eight subfactors

and

$w_j$  ( $j = 1, \dots, 8$ ) are the weights determining the impact that each subfactor has to the determination of the overall failure rate.

Given that the proposed model is linear, then by applying the method of multiple linear regression to the data available, the weights of each subfactor are estimated, and the dependencies of the failure rate on the several subfactors are determined based on actual failure data.

This is one potential way to address the issue of recalibration of UPM in the light of the new information contained in the UPM database. Nonetheless, two

pitfalls exist: firstly, it is doubtful whether the amount of available data is sufficient to produce statistically significant results, even if the UPM scores had been collected in previous data collecting exercises; secondly, a linear relationship between the failure rates and the subfactors is an a priori assumption of the methodology just described. Hence, the readjustment of the weights of the different subfactors, an issue of major importance, can in principle be tackled; yet, the issue of the existence of a linear relationship remains unsettled and constitutes an area of further research. We shall now consider this latter issue further.

#### 4 CONNECTION BETWEEN MULTIATTRIBUTE VALUE THEORY AND UPM

##### 4.1 *Multiatribute Value Theory*

Multiatribute Value Theory (MAVT) is a modelling tool that supports the decision-making process. Given a decision problem and in the general case, the decision-maker is free to choose among a number of alternatives/actions. For each course of action there is an effect, which has implications across multiple criteria. In the scope of MAVT, it is assumed that the effects/outcomes of each action are well defined, known to the decision-maker with certainty, prior to the choice of action. MAVT is concerned with the definition of a trade-off structure among the different outcomes that reflects the preferences of the decision-maker. A value function is defined, that assigns a value to each set of outcomes consistent with the preference statements of the decision maker. The definition of the preference relation and the value functions should comply with the axioms and conditions of MAVT. In the rest of the paper the similarities of UPM and MAVT are going to be highlighted and to assess what implications this has for the UPM model structures.

##### 4.2 *UPM structure*

Within the framework of MAVT, in order to completely describe the outcomes of a specific course of action, each objective is broken down in a number of measurable qualities (attributes) and a hierarchy is

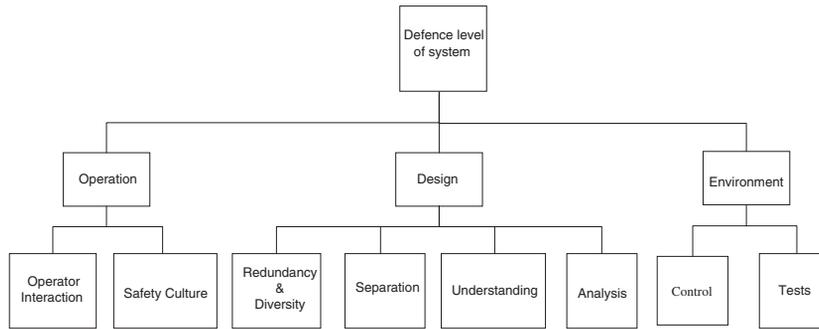


Figure 1. UPM hierarchy.

formed. Similarly, within the UPM context multiple performance measures are used; the initial objective is the determination of the system's defence level, which is broken down to eight different measurable qualities, the different subfactors. The hierarchy formed is illustrated at Figure 1.

The level of defence of a system against dependent failures is estimated across eight different areas (subfactors), each of which corresponds to five different categories (having letters A, B, C, D and E). The system of interest is assigned to one of these categories across all areas. Scores are given accordingly and the overall failure rate of the system of interest is estimated as the sum of all the scores.

For the purposes of this paper, let:

$A_1, A_2, \dots, A_8$  denote the different subfactors

$x_j^i (j = 1, 2, \dots, 8, i \in Z^+)$  denote the category assigned to subfactor  $A_j$  in assessment  $i$

$v_j(x_j^i) (j = 1, 2, \dots, 8, i \in Z^+)$  denote the score corresponding to each category in assessment  $i$ .

If  $\lambda$  denotes the failure rate of the system of interest, then the UPM model assumes that:

$$\lambda = \sum_{j=1}^8 v_j(x_j^i) \tag{2}$$

Within UPM we might identify a particular set of scores as an "action", namely the act of accepting a system with these specific scores. Therefore, a set of actions  $\{B_1, B_2, \dots\}$  is defined, where each action leads to a specific outcome (the categories that are assigned to the system of interest). The configuration of the system is being done across eight subfactors, which can be considered as attributes. The eight-dimensional set of assigned categories can be considered as the set of outcomes. Thus, each act  $b_i \in \{B_1, B_2, \dots\}$  corresponds an 8-attribute outcome vector. In other words,

$$\underline{x}^i = (A_1(b_i), A_2(b_i), \dots, A_8(b_i)) = (x_1^i, \dots, x_8^i) \in V = X_1 \times X_2 \times \dots \times X_8$$

where  $X_j$  is the domain of attribute  $A_j$ .

Table 2. Acts and attributes in UPM.

		Attributes				
Acts		$A_1$	$A_2$	$A_3$	...	$A_8$
$B_1$		$x_1^1$	$x_2^1$	$x_3^1$		$x_8^1$
$B_2$		$x_1^2$	$x_2^2$	$x_3^2$		$x_8^2$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

The actions and the attributes in UPM form a matrix in which each row corresponds to an action and each row to an attribute (different performance measures). See Table 2.

### 4.3 Definition of the preference structure

UPM implies the existence of a preference structure as follows:

"The smaller the failure rate obtained, the bigger the defence level of the assessed system, and, therefore, the more preferable the action yielding this outcome is."

This preference structure can be expressed as a binary relationship  $\succsim$  defined over the outcomes space  $V = X_1 \times X_2 \times \dots \times X_8$ . Note that  $\succsim$  is a negatively oriented relationship, since the lower scores are preferred.

Definition: If  $\underline{x}, \underline{y} \in V$ ,

$$\underline{x} \succsim \underline{y} \Leftrightarrow -\lambda(\underline{x}) \geq -\lambda(\underline{y}) \Leftrightarrow \rho(\underline{x}) \geq \rho(\underline{y}) \tag{3}$$

where

$$\begin{aligned} \rho(\underline{x}^i) &= -\lambda(\underline{x}^i) \\ \rho(\underline{x}^i) &= -\sum_{j=1}^8 v_j(x_j^i) = \sum_{j=1}^8 u_j(x_j^i), \quad i \in Z^+ \end{aligned} \tag{4}$$

$$u_j(x_j^i) = -v_j(x_j^i), \quad i \in Z^+, \quad j = 1, \dots, 8$$

The relationship  $\succsim$  represents a preference structure, as it obeys the axioms of comparability, transitivity, consistency of indifference and weak preference, and consistency of strict preference and weak preference.

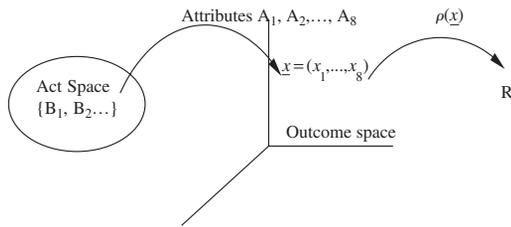


Figure 2. The mapping of acts.

A relationship defined on a set for which the above axioms hold is known as a *weak order*; consequently, set  $V$  is a weakly ordered set (French, 1993).

Every element of the act space is mapped to an 8-dimensional outcome space, as equation (4) is a function  $\rho: V = X_1 \times X_2 \times \dots \times X_8 \rightarrow R$ , where  $X_j$  is the domain of attribute  $A_j$  and  $u_j: X_j \rightarrow R, j = 1, 2, \dots, 8$ . See Figure 2.

So far, UPM's preferences are expressed through a weak order  $\succcurlyeq$  and a real-value function  $\rho$  is defined such that (3) holds. Then, we say that  $\rho$  is an ordinal value function representing  $\succcurlyeq$ .

The properties below stem from the definitions and assumptions made so far:

1. The smaller the failure rate of an action, the more "preferable" for a decision maker this action is:

For  $\underline{x}, \underline{y} \in V$ ,

$$\underline{x} \succcurlyeq \underline{y} \Leftrightarrow -r(\underline{x}) \geq -r(\underline{y}) \Leftrightarrow \rho(\underline{x}) \geq \rho(\underline{y})$$

2. (Marginal Orders over sets  $X_j, l = 1, 2, \dots, 8$ ). The smaller the score of a category, the more "preferable" to the decision maker this category is, since it results to a smaller failure rate:

For  $x, y \in X_j$

$$x \succcurlyeq y \Leftrightarrow v_j(x) \leq v_j(y) \Leftrightarrow u_j(x) \geq u_j(y) \quad (j = 1, 2, \dots, 8)$$

These properties imply that functions  $\rho$  and  $u_j, j = 1, 2, \dots, 8$  are monotonic functions.<sup>4</sup> Therefore,  $\rho$  is a value function that represents  $\succcurlyeq$  and  $u_j, j = 1, 2, \dots, 8$  are marginal value functions (single attribute functions) (French, 1993).

#### 4.4 Additive form and mutual preferential independence

Equation (4) implies that  $\rho$  is a value function for the preference relation defined in (3). This is clearly an

<sup>4</sup>If  $\phi: X \rightarrow Y$  is monotonic, then  $\forall x_1, x_2 \in X, x_1 < x_2 \Leftrightarrow \phi(x_1) < \phi(x_2)$

additive value function. However, in MAVT the existence of an additive value function over the set  $V$  requires that the attributes are *mutually preferentially independent*.<sup>5</sup> This statement says that every subset of attributes  $Y \subset V$  is preferentially independent of its complementary set  $Z = V - Y$  [7]. Or, in other words, the conditional preference structure of the subset  $Y$  does not depend on the level of the subset  $Z$ ; therefore, the trade-offs between the attributes belonging to subset  $Y$  do not depend on the level of the attributes belonging to set  $Z$  (Keeney, 1976). Mathematically expressed,

If  $\underline{y}', \underline{y}'' \in Y$ ,

$$[(\underline{y}', \underline{z}') \succcurlyeq (\underline{y}'', \underline{z}')] \Rightarrow [(\underline{y}', \underline{z}) \succcurlyeq (\underline{y}'', \underline{z})] \quad (5)$$

for all  $\underline{z}, \underline{z}' \in Z$

#### 4.5 Preferential independence within the context of UPM

The form of the Multiattribute Value Function (4) used within the UPM framework makes the assumption of mutual preferential independence. Transferring this notion in the UPM framework implies that a given set of attributes influences the overall failure rate in a fixed way, regardless of the level of the rest of the attributes. However, this may not be consistent with our own judgement about how the model should behave. This inconsistency will be illustrated by considering three hypothetical cases:

Case 1: In order to demonstrate this argument, we assume an assessment of a particular system. We choose typical categories  $x_4, x_5, \dots, x_7$  for all the attributes except Safety Culture ( $A_1$ ), Redundancy ( $A_2$ ) and Analysis ( $A_3$ ) and we keep them fixed. We are going to examine the preference structure in the subspace  $Y = X_1 \times X_2 \times X_3$ . More precisely, we are going to examine the trade-offs between the subfactors of Redundancy and Safety Culture, when modifying the level of Analysis.

First we assume that the system of interest has been classified as category A at the subfactor of Analysis ( $x_3 = x_3^1 = A$ ),<sup>6</sup> as category A at the subfactor of

<sup>5</sup>Apart from the conditions of weak ordering and mutual preferential independence, there are other necessary conditions for the existence of an additive value. These are restricted solvability, the Archimedean and essentiality conditions (see Reference i). Even though the random variable  $x_j^i, j = 1, 2, \dots, 8, i \in Z^+$  can take only five values (there are only five categories), we assume that it could be conceptually extended to a continuous random variable with the above conditions met.

<sup>6</sup>Category A in the attribute of Analysis means that no formal safety assessment has taken place and that there is no design knowledge of dependent failure issues.

Redundancy ( $x_2 = x_2^l = A$ )<sup>7</sup> and as category D at the subfactor of Safety Culture ( $x_1 = x_1^l = D$ ).<sup>8</sup> Redundancy is considered to impact significantly on the defence level of the system; therefore, if the Safety Culture level drops ( $x_1 = x_1^l = B$ ),<sup>9</sup> redundancy should significantly increase ( $x_2 = x_2^h = D$ )<sup>10</sup> for the failure rate of the system to stay at the same level. Expressing that mathematically, we have just argued that

$$(x_1^h, x_2^l, x_3^l) \sim (x_1^l, x_2^h, x_3^l) \quad (5)$$

We now assume that the configuration of the system in terms of Analysis is high, meaning that previous analyses have taken place ( $x_3 = x_3^h = E$ ).<sup>11</sup> In this case we can presume that the aspect of redundancy or diversity has been taken into consideration during the previous assessments, and the present design has been recognised as the one that functions better in case of a Common Cause event. Therefore, the impact of Redundancy on the determination of the overall failure rate should be smaller. Then, having low redundancy (A) and high safety culture (D) would yield a higher defence level (lower failure rate) than high redundancy and low safety culture. In other words,

$$(x_1^h, x_2^l, x_3^h) \succ (x_1^l, x_2^h, x_3^h) \quad (6)$$

However, the UPM structure implies that the preference structure stays the same, regardless of the level of analysis. Consequently it should hold

$$(x_1^h, x_2^l, x_3^h) \sim (x_1^l, x_2^h, x_3^h) \quad (7)$$

which contradicts our expectation about the behaviour of the model.

Moreover, an additive value function implies from (5) and (6) that the range  $u_2(x_2^h) - u_2(x_2^l)$  is constant;

<sup>7</sup>Category A in the attribute of Redundancy means that there is simple redundancy (1oo2).

<sup>8</sup>Category D in the attribute of Safety Culture means that there is simulator training of normal operation AND there is dedicated staff and evidence of good safety culture including systematic training of emergency conditions.

<sup>9</sup>Category B in the attribute of Safety Culture means that there is systematic regular training covering general and emergency operations.

<sup>10</sup>Category D in the attribute of Redundancy means that there is unusually high redundancy 1oo8 or higher in a passive system with engineering diversity.

<sup>11</sup>Category E in the attribute of Analysis means that previous reliability assessment has taken place with clear evidence of results feedback and management support AND there is evidence of designer knowledge of dependent failure issues.

consequently, the weight of the subfactor of Redundancy does not depend on the level of Analysis. This means that the trade-offs between a subset of subfactors do not depend on the categories that the rest of the subfactors have received, fact that is not coherent with what we intuitively expect.

Case 2: In the same view, if the level of Analysis were high, someone would expect that the issue of Diversity would have been considered. Therefore, the configuration of the system in terms of diversity is not expected to have the same impact on the overall level of defence, as it would have if previous analyses had not taken place and defence measures had not been adopted. In the second case, non-diversity would impact much more on the overall failure rate, compared to the first case.

Case 3: If we consider the subspace comprised by the attributes of Redundancy, Safety Culture and Operator Interaction, the preference structure is disturbed again. Let it be that, at a specific assessment, the attribute of Operator Interaction receives category A (it is being fixed at a low level). That would suggest that there are no written procedures regarding the functioning of the system, whereas operator interaction is at a normal level. In this case the impact of Safety Culture (how expert the operator is) on the overall failure rate should be stronger, compared to the one that it would have if Operator Interaction was fixed in a higher level, suggesting that there is minimal operator interaction with the system and written procedures available.

## 5 CONCLUSION

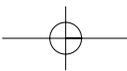
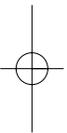
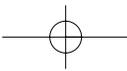
CCFs are major contributors to system unavailability. This has been recognised in Probabilistic Risk Analyses and many models have been proposed so far for their efficient and robust modelling. The UK has adopted its own CCF quantification approach: UPM.

UPM makes use of an additive value function, which assumes the condition of mutual preferential independence between the subfactors. This fact leads to conceptual inconsistencies. The similarities that the UPM structure shares with MAVT, a decision tool, are of great importance. This may give directions towards the incorporation of MAVT value functions that weaken the condition of preferential independent subfactors. In any case the above arguments suggest that in further enhancing UPM, a non-linear model should be considered.

The establishment of the ICDE Project offers means for further development of the UPM framework: the information accumulated in the database offer opportunities for reassessing the UPM structure. However, pitfalls exist in the collection of failure data, even though efforts are made towards the establishment of a more coherent collection method across the different countries.

## REFERENCES

- Apostolakis, George & Moieini, Parviz, 1987. The foundations of models of dependence in Probabilistic Safety Assessment. *Reliability Engineering*. Vol. 18. p. 177–95.
- Atwood, Corwin L. 1996. The binomial failure rate common cause model. *Technometrics*. Vol. 28. No. 2. p. 139–148.
- Brand, P.V. 1996. UPM3.1: A pragmatic approach to dependent failures assessment for standard systems, AEA Technology plc.
- French, Simon, 1993. *Decision Theory: An Introduction to the Mathematics of Rationality*, Chichester: Ellis Horwood Limited.
- ICDE Project, Terms and Conditions for Project Operation 25/10/01.
- Ralph L. Keeney & Howard Raiffa, *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*, New York: John Willey & Sons Inc, 1976.
- Siu, Nathan & Mosleh, Ali, 1998. Treating data uncertainties in common-cause failure analysis. *Nuclear Technology*. Vol. 84. p. 265–81.
- Walls L.A & Bendell, 1989. Exploring field reliability data for potential dependent failures, UK Reliability Symposium, Reliability 89. Paper 4Ab/3.



## Author index

- Absil, L.H.J. 537, 543, 1679  
 Achalakul, T. 1047  
 Åkerlund, O. 237  
 Albeanu, G. 19  
 Albrechtsen, E. 25  
 Ale, B.J.M. 1, 993  
 Altavilla, F. 1227  
 Andersen, H.B. 575  
 Aneziris, O.N. 1205  
 Anoop, M.B. 73  
 Ansell, J. 33  
 Antão, P. 37  
 Appa Rao, T.V.S.R. 73  
 Aprili, P. 305  
 Aprili, P.G. 45  
 Arbaretier, E. 53  
 Archibald, T. 33  
 Ardon, J. 53  
 Arends, B. 863  
 Argiento, R. 1345  
 Arild, Ø. 1375  
 Arjas, E. 151  
 Asche, F. 59  
 Aubry, J.F. 1401  
 Aven, T. 59, 807, 821, 969,  
 1375, 1607, 1615
- Băjenescu, T.I. 67  
 Baker, R.L. 635  
 Balaji Rao, K. 73  
 Balderstone, M. 813  
 Balfanz, H.-P. 1409  
 Ballesio, J.E. 447  
 Ballocco, G. 81  
 Baraldi, P. 1069  
 Barón, J.H. 91, 1189  
 Barros, A. 99  
 Baskoro, G. 107  
 Basso, B. 113  
 Bâzu, M.I. 67  
 Becker, G. 119, 127, 321, 331  
 Bedford, T. 133, 1113, 1575  
 Behr, A. 127, 141  
 Bellucci, A. 1567  
 Benedikt, S. 147  
 Bérenguer, C. 99  
 Berg, H.P. 1409
- Bertsche, B. 1255  
 Beugin, J. 1301  
 Bhattacharjee, M. 151  
 Bianchi, M. 1085  
 Bieber, P. 237  
 Billy, F. 195  
 Blanco, H. 165  
 Blanco, J.A. 171  
 Bocquet, J.C. 195  
 Böde, E. 237  
 Boersma, J. 191, 1041  
 Bolt, R. 1737  
 Bonanos, G. 1205  
 Boonstra, H. 1437  
 Bot, Y. 201  
 Bottelberghs, P.H. 1383  
 Botterhuis, A.A.J. 213  
 Bougnol, C. 237  
 Boulanger, J.L. 221  
 Bouwman, E.C.J. 661  
 Bouzaïène, L. 195  
 Bovalini, R. 229  
 Bozzano, M. 237, 247  
 Braband, J. 1307  
 Brandowski, A. 255  
 Bretschneider, M. 237  
 Brinkhuis, M. 1053  
 Brinkhuis-Jak, M. 261  
 Briombacher, A.C. 1041  
 Briš, R. 271  
 Brombacher, A.C. 107, 191  
 Bubbico, R. 279, 287, 1543  
 Bucciarelli, G. 297, 305  
 Buchlin, J.-M. 741  
 Buijs, F.A. 311  
 Bunea, C. 321, 331, 1105  
 Burgazzi, L. 339  
 Bye, R. 157
- Cagno, E. 347  
 Caires, S. 353  
 Callies, U. 363  
 Camarinopoulos, L. 119  
 Candeloro, L. 439  
 Canepa, G. 1575  
 Cappelli, I. 1567  
 Carlos, S. 1093, 1099
- Caron, F. 347  
 Carpignano, A. 81  
 Carta, R. 1543  
 Caruana, S.A. 695  
 Casal Fabrega, J. 479  
 Casal, J. 1247  
 Castel, C. 237  
 Cauffriez, L. 1301  
 Cavallero, D. 373  
 Cavallo, A. 237  
 Cavanagh, N.J. 1729  
 Cepin, M. 381  
 Chaddock, P. 171  
 Chantelaue, G. 387  
 Charitos, T. 321  
 Châtelet, E. 271  
 Chbab, E.H. 1179  
 Chelakara, S. 1233  
 Chen (Frank) H.-K. 397  
 Chery, O. 591  
 Christou, M. 479  
 Cifaldi, M. 237  
 Cimatti, A. 237  
 Circelli, I. 287  
 Cizelj, R.J. 1645  
 Coit, D.W. 1295, 1671  
 Commandeur, A.J. 403, 411  
 Constantinescu, A.C. 1581  
 Cooke, R.M. 321, 331, 363,  
 1315, 1321  
 Coolen, F.P.A. 417  
 Cope, A. 1233  
 Corneliussen, K. 423  
 Coroiu, N. 623  
 Cozzani, V. 1365  
 Cremonini, M.G. 439  
 Cross, R.B. 447  
 Csenki, A. 457  
 Curbach, M. 1263  
 Curry, R. 411
- da Silva, L.F.M. 1497  
 Daghigh, M. 465, 1433  
 Dandrieux, A. 741, 1543  
 Davies, P.A. 471, 475, 695  
 de Boer, A. 179  
 de Boer, J. 185, 523

- de Bruyn, P.C.A.M. 1679  
 De Franchi, G.B. 439  
 de Lange, G. 999  
 de Marcellis-Warin, N. 1061  
 De Souza Jr. D.I. 1487  
 De Varti, A. 229  
 de Weger, D. 1699  
 de Wit, M.S. 1721  
 Debernardi, M.L. 373  
 Debray, B. 575  
 Delvosalle, C. 479, 1247  
 den Heijer, F. 495  
 den Heijer-Aerts, M. 689  
 Denning, R. 489  
 Di Cave, S. 279, 287, 1543  
 Di Giulio, A. 503, 513  
 Dibitonto, C. 113  
 Diermanse, F.L.M. 495  
 Dijkerman, E.M. 185, 523  
 Diniz, S. 1233  
 Djordjevic, I. 643  
 Donders, J. 531  
 Drab, A. 567  
 Drewett, L. 1497  
 Duijm, N.J. 575  
 Duinkerken, J. 1737  
 Duriez, S. 591  
 Dusserre, G. 741, 1543
- Edigarov, A. 1357  
 Eid, M. 599  
 Eisinger, S. 599, 735  
 Elrada, H.A. 801  
 Erdos, G. 769, 775  
 Evandt, O. 1289
- Fabbrocino, G. 615  
 Fadier, E. 591  
 Felea, I. 623  
 Fiévez, C. 479, 1247  
 Finkelstein, M.S. 629  
 Fontana, R. 1153  
 Franciotti, D. 45, 297, 305  
 Frank, M.V. 635  
 Fredriksen, R. 643, 701
- Gaido, G. 113  
 Galle, L.F. 605  
 Gargiulo, M. 81  
 Gaston, D. 1543  
 Gaver, D.P. 649  
 Geerse, C.P.M. 495  
 Gerboni, R. 653  
 Geri, F. 287  
 Ghalandarzadeh, A. 667  
 Ghodrati Amiri, G. 667
- Giagnoni, L. 1567  
 Giannone, B. 339  
 Ginestar, D. 1093, 1099  
 Giovinnazzi, S. 671  
 Girish, T. 681  
 Göb, R. 1289  
 Goldstein, M. 417  
 Goossens, L. 575  
 Goossens, L.H.J. 689, 1315, 1321  
 Gopalakrishnan, S. 73  
 Gould, J.H. 471, 475, 695  
 Grabski, F. 255  
 Grall, A. 99  
 Gran, B.A. 643, 701  
 Griffault, A. 237  
 Groeneweg, J. 707  
 Gucma, L. 713  
 Guedes Soares, C. 37, 719  
 Guida, M. 727  
 Guilhem, E. 1401  
 Guillon, B. 53  
 Gurley, K. 1233  
 Gustavsson, F. 735  
 Guttormsen, G. 1197
- Hagen, O. 719  
 Haïk, Ph. 195  
 Hald, K. 741  
 Hale, A. 575  
 Hale, A.R. 431, 747, 783, 853, 1315, 1321  
 Hall, J.W. 311  
 Hamid, S. 1233  
 Han, S.H. 901  
 Hansson, L. 157, 755  
 Harms-Ringdahl, L. 763  
 Harvey, J. 769, 775  
 Hauge, S. 1197  
 Haugen, S. 1469  
 Heijer, T. 783, 853  
 Held, M. 791  
 Henderson, E.M. 801  
 Herfjord, K. 1015  
 Hjorteland, A. 807  
 Hodge, R. 813  
 Hofer, E. 907  
 Hokstad, P. 25, 821  
 Holmås, T. 1015  
 Holscher, P. 1721  
 Holterman, S.R. 261  
 Holub, R. 1623  
 Hourtolou, D. 431, 829  
 Hubert, E. 1543  
 Hukki, K. 837  
 Hundseid, H. 1607
- Hussels, U. 127  
 Hutinet, T. 1401  
 Hwang, M.J. 897
- Iervolino, I. 615  
 Imhof, D. 843  
 Inoue, K. 915, 923  
 Ionescu, D.C. 1581
- Jacobs, P.A. 649  
 Jager, E. 1737  
 Jagtman, H.M. 853  
 Jang, S.C. 901  
 Jayaram, J.S.R. 681  
 Jenkins, I. 1575  
 Jo, Y.R. 1211  
 Jonkman, S.N. 261, 863
- Kabranis, D. 119  
 Kalk, H.J. 1179  
 Kallen, M.J. 873  
 Kang, D.I. 897  
 Kanis, H. 583  
 Karelse, J.W. 1679  
 Kari, O. 977  
 Kehren, C. 237  
 Kenett, R.S. 881  
 Kermisch, C. 889  
 Kim, K. 897  
 Kim, K.Y. 901  
 Kim, S.H. 901  
 Kloos, M. 907  
 Kohda, T. 915, 923  
 Kok, M. 261, 927, 1653  
 Kolowrocki, K. 937  
 Kongsvik, T. 157  
 Konovessis, D. 1587  
 Konstantinidou, M. 1167  
 Koornneef, F. 783  
 Kootstra, F. 947  
 Korving, H. 959  
 Kouniali, S. 1145  
 Kraggerud, A.G. 735  
 Kragh, E. 719  
 Krijnen, F.J. 1383  
 Kristensen, V. 969  
 Kruidhof, W. 185, 523  
 Krzykacz-Hausmann, B. 907  
 Kuik, R. 1737  
 Kumar, D. 977  
 Kun, I. 147  
 Kurowicka, D. 363  
 Kwon, J.G. 1211
- Labeau, P.E. 889  
 Lagomarsino, S. 671

- Laheij, G.M.H. 993  
 Lam, S.W. 681  
 Lancioni, G.E. 707  
 Lannoy, A. 195  
 Lassing, B.L. 1005  
 Lauridsen, K. 719  
 Lawrence, B. 237  
 Le Coze, J-C. 431  
 Lecomte, O. 53  
 Leira, B.J. 1015  
 Lenic, J. 1575  
 Li, J.-P. 1025  
 Linsenmaier, B. 1409  
 Lisi, R. 1031  
 Lodder, G.H. 537  
 Loh, H.T. 191, 1041  
 Loke, G. 191, 1041  
 Lombardo, P. 439  
 Londiche, H. 575  
 Lopuhaä, R. 1315, 1321  
 Lu, Y. 191, 1041  
 Luansritsakul, Y. 1047  
 Luccone, L.G. 1543  
 Lüdtke, A. 237  
 Lombard, D. 813  
 Lyridis, D.V. 1271
- Madsen, H.G. 1113  
 Madsen, M.D. 575  
 Maggio, G. 801  
 Mancini, M. 347  
 Mariano, G. 221  
 Marmo, L. 373, 1153  
 Marseguerra, M. 297, 1069, 1077, 1085  
 Marshall, J. 813  
 Martorell, S. 1093, 1099  
 Maschio, G. 1031  
 Maskuniitty, M. 1389  
 Mathisen, S. 701  
 Mazzarotta, B. 279, 287, 1543  
 Mazzini, M. 229  
 Mazzuchi, T.A. 331, 559  
 McCaffrey, A. 213  
 McCollin, C. 1105  
 McDonald, G.J. 1113  
 Medonos, S. 1121, 1129, 1137  
 Merad, M.M. 1145  
 Metaal, N. 707  
 Metge, S. 237  
 Middleton, C.R. 843  
 Mikuličić, V. 1447  
 Milanolo, S. 1153  
 Milazzo, F.M. 1031  
 Miyabayashi, A. 977  
 Monsen, J. 1197
- Morelli, G. 1575  
 Motamed, R. 667  
 Mravak, I. 1503  
 Mushtaq, F. 479  
 Muzi, F. 297
- Neerincx, M.A. 1351  
 Nellen, Ph.M. 791  
 Neu, H.R. 1629  
 Nikolovski, S. 1503  
 Nilsen, E.F. 1161  
 Nivolianitou, Z.S. 1167  
 Norstrøm, J.G. 1113  
 Núñez Mc Leod, J.E. 91, 1189
- Odisharia, G. 1357  
 Øien, K. 1197, 1607, 1615  
 Ouwerkerk, S.J. 1653  
 Ovtcharov, S. 1357  
 Øygarden, B. 1469
- Pabst, I. 1281  
 Paci, P. 439  
 Papadopoulos, C. 237  
 Papageorgiou, L.G. 1241  
 Papazoglou, I.A. 1205  
 Pardi, L. 719  
 Park, S.D. 1211  
 Park, S.J. 1211  
 Parkhi, R.S. 959  
 Parozzi, F. 1153  
 Passarello, R. 237  
 Passenier, P.O. 1351  
 Pearce, J.J. 1215  
 Pearson, P. 1575  
 Pecvarac, D. 1219  
 Pedrali, M. 503, 513  
 Peikenkamp, T. 237  
 Pelliccioni, A. 1227  
 Pérès, F. 195  
 Persson, P. 237  
 Pertusio, R. 1553  
 Peschke, J. 907  
 Petersen, E.S. 1271  
 Piccini, M. 81  
 Pietersen, C.M. 689  
 Pievatolo, A. 347, 1289, 1345  
 Pinelli, J.-P. 1233  
 Pipart, A. 479, 1247  
 Pixopoulou, N. 1241  
 Planas, E. 479, 1247  
 Plot, E. 431  
 Podofillini, L. 1753  
 Polet, P. 1743  
 Ponte, E. 653  
 Popentiu-Vladicescu, Fl. 19, 623
- Post, J.G. 993, 1383  
 Pozsgai, P. 1255  
 Preyssl, C. 1575  
 Prinsen, G.F. 495  
 Proske, D. 1263  
 Psaraftis, H.N. 1271  
 Pulcini, G. 727  
 Pulkkinen, U. 837
- Quigley, J. 133, 813
- Radford, N. 107  
 Raffetti, A. 1271  
 Rakowsky, U.K. 1281  
 Ramalhoto, M. 1105  
 Ramalhoto, M.F. 881, 1289, 1497  
 Ramirez-Marquez, J. 1295  
 Randazzo, G. 513  
 Rapicetta, C. 439  
 Renaux, D. 1301  
 René van Dorp, J. 551, 559  
 Renpenning, F. 1307  
 Reunanen, M. 1389  
 Rivera, S.S. 91  
 Robotto, A. 113  
 Rodrigues, N. 1543  
 Roelen, A.L.C. 1315, 1321  
 Romano, D. 1329  
 Rosmuller, N. 1337  
 Rouvroye, J.L. 107  
 Roy, B. 1145  
 Ruggeri, F. 347, 1345  
 Rypkema, J.A. 1351
- Safonov, V. 1357  
 Salina, E. 1153  
 Salmikuukka, J. 1289  
 Salmon, R. 1145  
 Salvi, O. 829, 1543  
 Salzano, E. 615, 1365  
 Sánchez, A. 1093, 1099  
 Sandøy, M. 1375  
 Sarsama, J. 1389  
 Satish, B. 73  
 Sayers, P.B. 311  
 Schäbe, H. 1395  
 Schoenig, R. 1401  
 Schott, H. 1409  
 Schouten, S.P.F. 1415  
 Schubert, B. 119  
 Schueremans, L. 1425  
 Seglie, E.A. 649  
 Seguin, C. 237  
 Serbanescu, L. 19  
 Shabakhty, N. 465, 1433, 1437

- Shade, J. 881  
 Sheberstov, E. 1357  
 Shetty, N.K. 719  
 Silva, W. 927  
 Silveti, B. 1543  
 Šimić, Z. 1447  
 Simiu, E. 1233  
 Simons, M. 1321  
 Skjong, R. 1453, 1461  
 Sklet, S. 423, 1197  
 Soma, H. 1469  
 Soma, T. 1477  
 Sonnenkalb, M. 907  
 Sørum, M. 821, 1615  
 Steiro, T. 1197  
 Sterl, A. 353  
 Stewardson, D.J. 1497  
 Stijnen, J.W. 927  
 Stojkov, M. 1503  
 Stølen, K. 643  
 Strong, A. 775  
 Stuit, H.G. 1721  
 Suddle, S.I. 1511, 1519, 1527  
 Suleimanov, V. 1357  
 Szász, G. 147
- Teixeira, A.P. 719  
 Terrinoni 439  
 Thomas, L. 33  
 Thompson, G. 1025  
 Tiemeyer, B. 1535  
 Tixier, J. 1543  
 Tommasini, R. 1553  
 Tomter, A. 1561  
 Trotta, L. 237  
 Trucco, P. 503, 513  
 Tucci, M. 1567  
 Tuominen, R. 1575
- Uittenbogaard, M. 185, 523  
 Ulmeanu, A.P. 1581
- Valacca, L. 237  
 Valk, P.J.L. 1321  
 van 't Sant, J.P. 1383  
 van den Berg, A.C. 1691  
 van den Boogaard, H.F.P. 495  
 van der Graaf, H.J. 1415  
 van der Hoeven, B. 185, 523  
 van Dongen Ph. 537  
 van Doormaal, J.C.A.M. 543  
 van Duijne, F.H. 583  
 van Erkel, A. 605  
 Van Gelder, P. 1437  
 van Gelder, P.H.A.J.M. 311,  
 863, 959, 1337, 1415  
 Van Gemert, D. 1425  
 Van Gestel, P.J. 661  
 van Manen, S.E. 1053  
 van Noortwijk, J.M. 873, 959,  
 1179  
 van Vuren, S. 1653  
 van Wees, R.M.M. 1679  
 Vanderhaegen, F. 1743  
 Vassalos, D. 1587  
 Vassmyr, K-A. 1607  
 Vatn, J. 821  
 Vaurio, J.K. 1595, 1601  
 Veldkamp, J.G. 999  
 Ventikos, N.P. 1271  
 Ventulini, M. 297  
 Venturino, C. 1271  
 Verdel, T. 1145  
 Vermey, P. 531  
 Versloot, N.H.A. 1691  
 Vicario, G. 1329  
 Villafiorita, A. 237, 247  
 Vinnem, J.E. 1607, 1615  
 Vintr, Z. 1623  
 Voets, H.J.L. 747  
 Vogt, M. 1629  
 Vollen, F. 1607  
 Voortman, H.G. 1637
- Vrbanić, I. 1645  
 Vrijling, J.K. 311, 863, 1637  
 Vrouwenvelder, A. 719  
 Vrouwenvelder, A.C.W.M. 11,  
 311, 1005  
 Vuković, I. 1447
- Waarts, P.H. 179, 1005, 1511,  
 1663, 1721  
 Walls, L. 813  
 Wassing, B.B.T. 999  
 Wattanapongsakorn, N. 1047,  
 1295, 1671  
 Weaver, M.A. 635  
 Webbers, P.B. 1713  
 Weerheijm, J. 1679, 1691  
 Wehrung, M.J. 311  
 Wery, S. 1307  
 Wever, R. 1315, 1321  
 Wijnants, G.H. 1707  
 Willems, A. 1713  
 Winther, R. 701  
 Wooff, D.A. 417  
 Worthington, D.R.E. 1729  
 Wosinska, L. 791
- Yalaoui, F. 271  
 Yazdpour, S.J. 801
- Zacco, G. 237  
 Zambardi, F. 339  
 Zanting, J. 1737  
 Zhang, L. 1233  
 Zhang, Z. 1743  
 Zio, E. 297, 1069, 1077, 1085,  
 1753  
 Zitman, T.J. 1761  
 Zonato, C. 113