Safety and Reliability – Bedford & van Gelder (eds)
© 2003 Swets & Zeitlinger, Lisse, ISBN 90 5809 551 7

Causal modeling for integrated safety at airports

A.L.C. Roelen & R. Wever
National Aerospace Laboratory, NLR

A.R. Hale & L.H.J. Goossens
Delft University of Technology, Safety Science Group

R.M. Cooke & R. Lopuhaä
Delft University of Technology, Faculty of Information Technology and Systems

M. Simons & P.J.L. Valk
TNO Human Factors

ABSTRACT: A study funded by the Federal Aviation Administration via the Dutch Ministry of Transport has explored the possible structure of a causal model for aviation safety. The study is initiated by the regulator and the parties concerned at the airport to improve the modeling of risk, in order to be able to better understand the effects on the level of risk of different influencing factors. Existing modeling gives no insight into how the many factors under control of air traffic control, the airport or the airlines, play their part in the control of risk. The objective of the new modeling approach is to allow such assessment. This paper describes the overall approach proposed for the modeling and discusses the requirements and problems for full implementation. It is illustrated with two case studies considering the aspect of missed approach and the effect of flight-crew fatigue on performance.

1 THE IMPORTANCE OF CAUSAL MODELING

Despite the impressive level of safety of today's aviation system, it is generally acknowledged that the accident rate has to be decreased further. The main reason is the projected growth in the number of air traffic movements. If the accident rate does not decrease, the growth of air traffic will inevitably lead to an increase in the absolute number of accidents, which the industry believes would be unacceptable to the public and the regulator. This has led to attempts to increase the aviation safety level by introducing integral risk assessments into the design of the aviation system. In a design approach, the aviation safety level is considered an overall design requirement instead of an unavoidable result of aviation activities. Risk budgets (allowable independent contributions to the total risk level) can then be assigned to the various elements within the aviation system. Assigning risk budgets to aviation elements requires understanding how the risks of individual elements in the system influence the overall level of safety. This implies knowledge of causal sequences of accidents and incidents. The design approach requires a transparent causal structure in a risk model that explicitly relates changes in the design of individual elements to the overall level of safety. A causal model can be an important decision support tool, not only for the aviation authority, but also for other sector parties, in particular airports, airlines and ATC providers, in deciding where to invest money for maximum safety gain.

Like many other high-hazard, low-risk systems, the aviation system has developed such a high degree of technical and procedural protection that it is largely proof against single failures, either human or mechanical. The aviation system is more likely to suffer "organizational accidents" (Reason 1990). That is, a situation in which latent failures, arising mainly at the managerial and organizational level, combine adversely with local triggering events and with the active failures of individuals at the execution level (Reason 1997). These organizational failures can create common modes influencing several proximal factors (Hale et al. 1997). A causal model captures those failures and interactions qualitatively and quantitatively.

This research project aimed at developing a causal model of aviation safety which provides objective, quantified and unambiguous safety information for managerial decision making.

2 BASIC ARCHITECTURE OF A CAUSAL MODEL

A feasibility study on causal models for third party risk (Roelen et al. 2000) provided the basis for the development of the aviation model, based on accident and incident analysis. Event sequences of individual aviation accidents can be clustered into a smaller number of accident scenarios. The accident scenarios are initially modeled as trees with a logical and complete structure.

One of the characteristics of a tree structure is that safety influencing factors that occur much earlier in the sequence of events (sometimes referred to as latent factors and often management/organizational in nature) are located deep in the tree structure. In practice, this means that, in order to capture these factors, the tree must be expanded enormously. Beyond 5 to 6 levels, and sometimes earlier, events are generally influenced by common mode factors such as competence, procedures, maintenance, etc. This depth of modeling leads to a combinatorial explosion of the tree, which cannot be handled quantitatively. Hence the break-down of the tree must stop at the level where common mode influences begin. The elements at that level must be linked to the most important common modes through an interface to a Management Model, which is essentially a model of a different nature than a technical risk model. In searching for a modeling technique it is therefore important to assess how these problems can be resolved without losing essential influences and whilst keeping the tree manageable, but as complete as possible.

3 RESEARCH APPROACH

In setting up a structure for a causal model of aviation safety, a top-down, system-wide, approach has been applied. The advantage of this approach is that the interconnections between the different actors in the aviation system are integrated from the outset. The disadvantage of the top-down approach is that it is more abstract than the bottom-up approach, especially early in the development stages. For this reason detailed interviews were held with practitioners at the operational level about the specific aspects of the management and technical factors which influence safety in each step of the processes modeled. This approach gave substance and detailed specification to the generic influences defined in the top-down approach.

4 STRUCTURE OF THE TECHNICAL MODEL

The technical model consists of generic accident scenarios. Historical evidence shows that aviation accidents are not random combinations of events. Analysis of accidents demonstrate typical accident patterns. Specific combinations of causal factors result in specific types of accidents. As an example, landing overrun accidents are often associated with landing long and fast on a wet or contaminated runway.

Generic accident scenarios have been built using a combination of retrospective and prospective analysis. The retrospective analysis consists of a detailed and structured analysis of aviation accidents. It requires high quality data, which is available from the NLR Air Safety Database. The prospective analysis is used to identify potentially hazardous combinations of causal factors that have not (yet) resulted in an accident. It requires a team of domain experts, such as those interviewed in this study.

The further the tree is developed in detail, the more the factors revealed penetrate into the organizational factors related to management and organization. They are related to issues such as training of competence, supervision and crew resource management, manpower planning to avoid fatigue and task overload, incident analysis for improvement of risk control, inspection and maintenance scheduling to optimize control of hardware failures, etc. At this point the detailing of the technical model interfaces with the management model.

5 MANAGEMENT MODEL

Safety management is a process of steering the organization, or group of organizations, its technology and its people so that they bring and hold the hazards in its activities under control. These hazards may be potentially harmful to its assets (e.g. damage to aircraft), its workforce, its customers (aircraft passengers) or third parties (e.g. those living around an airport). The process of steering the organization to avoid risks can be characterized as a control process which takes place at three interlocking levels of functioning: execution, plans & procedures, and structure & policy. This must occur in all phases of the life cycle of the technology and infrastructure: design, construction/manufacture, exploitation, maintenance and modification.

The primary task at the plans & procedures level of the safety management system is the delivery of the necessary resources and criteria, or controls for the execution level to operate safely. Resources are the means by which the tasks are carried out: the people and hardware, the information, money and time. The criteria are the methods, rules, means and goals which guide people on how to perform the task, to what standard and by what means. As the basis for describing the complete safety management system, the following generic categories of delivery systems for resources and controls are defined as follows:

- Competence of staff to perform and make safety critical tasks and decisions,
- Availability of the competent staff for all safety critical tasks,
- Commitment, alertness and motivation of individuals to achieve safety,
- Hardware, software and man-machine interface design, its appropriateness, reliability, robustness and user-friendliness,
- Spares and tools to keep the technology and infrastructure in its designed state,
- Communication and co-ordination for group and system safety tasks,
- Procedures rules and goals for safe performance,
- Plans for allocation of safety critical responsibilities and resources,
- Conflict resolution to resolve the inevitable choices between safety and other goals.

The safety management system is driven by a cycle of risk assessment, planning and organizational design, performance assessment and review, which incorporates the controlled management of change, both technical and organizational.

Modeling of safety management starts with a description of the processes which are carried out within the aviation system. In order to identify the risks in each of the aviation system's processes, they need to be broken down into discrete steps. The possible hazards and failures at each step can then be identified and linked to the major accident scenarios. Subsequently, the specific resources and controls from the generic delivery systems must be specified for each step. These provide the organizational factors which interface with the influences described in the technical model.

6 LINKING THE MANAGEMENT MODEL TO THE ACCIDENT RISK MODEL, THE INTERFACE

It is important to realize here that the interface between a safety management model and quantitative risk analysis models requires a meeting point of two models which are philosophically different. The important difference is one of mechanism versus holism. A quantified risk analysis looks for causal chains, failure pathways, failure combinations. This mechanistic philosophy would be pure determinism if it was not for the necessary probabilistic and stochastic nature of failures and hence of risk analysis itself. Safety management audits, used for assessing the quality of safety management, however, are usually more holistic in nature.

Previous research efforts have attempted to address safety management within a quantitative risk analysis by linking directly from the top event of a number of scenarios (i.e. an accident) to the influences in the management system (e.g. PRIMA) (Bellamy et al. 1993). This, however, gave little insight into the way in which the management factors influenced the risk numbers. Later approaches tried to make the link at a more detailed level of the base events in a generic fault tree, or master logic diagram (Papazoglou & Aneziris 1999). This provided a richer insight into the causal links between management factors and technical failures. The I-Risk audit (IRMA) (Hale et al. 1999) was linked more explicitly to safety critical tasks and management functions (delivery systems). However, the interface was found to be at a level of detail too great to avoid the combinatorial explosions warned of above. The technical model in that study was too deterministic.

Our proposed solution to this interface problem is to develop an accident risk (technical) model that is more holistic in nature than a classical fault tree or event tree, but to retain the more mechanistic description of management by describing the mechanisms in safety management itself. This combines the best insights from PRIMA (its more generic accident risk model) and I-Risk (its audit focussed on management tasks).

One of the first exploratory studies on causal modeling of aviation safety already concluded that simple fault tree logic involving "and/or" relations cannot be used as the only technique for modeling the causal structure because of the existence of non-binary parameters, the dynamic behavior of systems and the existence of sequence dependencies (Roelen et al. 1996). Further analysis on causal modeling (Roelen et al. 1998, 1999) concluded that such models are not deterministic but probabilistic and that the modeling technique should be selected accordingly. Bayesian Belief Nets were proposed as the most suitable technique for further development of such a causal model, rather than a pure fault tree. Bayesian Belief Nets provide a representation which is closer to the viewpoint of management. They render causal relationships visible and allow the representation of management interventions as "decision nodes" in the belief nets, showing directly the causal relationships with technical and physical variables. See for further details Roelen et al. 2003, in this conference. The approach chosen also emphasizes the effects of introducing management changes to the system, rather than assessing the influence of management's absolute quality, an easier tasks for experts.

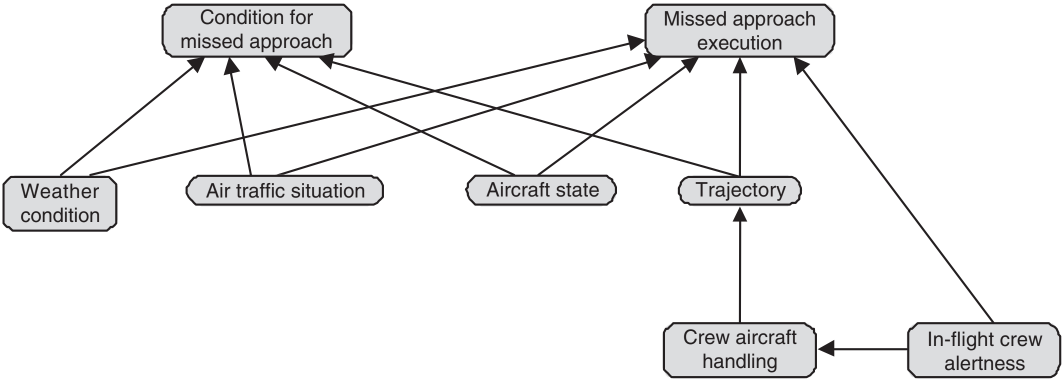

Figure 1. Missed approach model.

7 DETAILED MODELING

In order to properly demonstrate the feasibility of the causal model, two parts of it were developed in detail. In order to be a proper demonstrator, the selected part must be fully representative of the possibilities and limitations of the model's use as well as the potential problems associated with its development. A set of focussed risk elements had to be developed in detail to represent both the multidisciplinary character of the aviation system, and consequently the multidisciplinary team of experts needed for the development of the model, as well as to provide a proper balance of technical and management-related factors. To allow proper calibration and validation of the demonstration model within the timeframe of the study, sufficient high quality data had to be already available about these elements. Finally, it was believed that it would be wise to make the selection such that the results of the demonstration model are relatively simple to comprehend and are already useful to the sector parties. For these reasons, it was decided to develop the demonstration model in two directions:

- Missed approach, to illustrate the modeling of a complete and crucial aviation activity.
- Flight crew alertness, to illustrate the modeling of an influence common to several scenarios.

8 MISSED APPROACH

When during the approach to the landing runway any situation exists or arises, which would make the continuation of the approach and consecutive landing "unsafe", the flight crew should initiate a missed approach and go around or divert to another airfield. The purpose of the missed approach procedure is to reject flying into unsafe conditions or under unsafe circumstances and to enable the crew to carry out a new approach and landing under safe circumstances. A missed approach is ultimately initiated by the flight-crew, based on their mental representation of the current situation. A potentially unsafe situation exists when there is a mismatch between the flight-crew's mental representation of the situation and the "actual" situation. Based upon ICAO and JAR documentation, operator documentation (Basic Operating Manual and Aircraft Operating Manuals) and interviews with a current Boeing 747-400 Captain, the main factors that are important in the missed approach decision making are considered to be the following:

- Weather
- Air traffic situation
- Aircraft systems
- Aircraft trajectory
- Flight crew.

This leads to the model of missed approach, expressed in the form of a Bayesian Belief Net in Figure 1.

In this "model" each of the nodes has two possible states. Missed approach initiating nodes are either "OK" or "NOT OK", and the two top nodes can be either "YES" or "NO". The situation which is considered most unsafe occurs when the state of the node "condition for missed approach" is "YES", while the node "missed approach initiation and execution" remains "NO". In other words the conditions require a missed approach to be initiated, but for whatever reason the approach is continued.

9 FLIGHT CREW ALERTNESS

Commissioned by the Netherlands Civil Aviation Authority, the Aviation Medicine Group of TNO Human Factors has conducted a number of field and

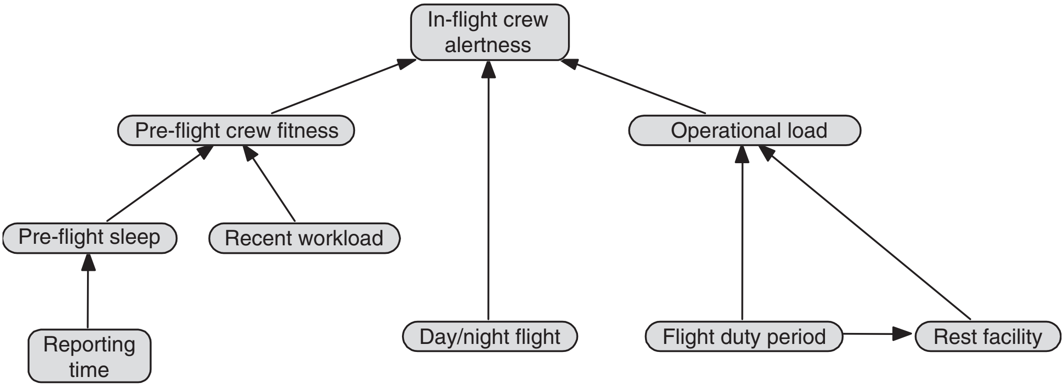

Figure 2. Flight crew alertness model.

laboratory studies (Simons et al. 1994, 1997, 1998; Valk et al. 1996, 1998, 1999) on the different determinants of flight-crew fatigue and their effects on alertness and performance. The studies, employing subjective and objective measures of in-flight performance and alertness, concerned quality and duration of sleep, effects of early reporting times, effects of night flying, effects of alcohol and medication, and the effects of countermeasures, such as onboard sleep (augmented crew) and pre-planned napping in the cockpit seat. The results of these studies provide an extensive database on factors causing flight-crew fatigue and impaired performance and alertness in flight. This database is further complemented with data collected by fellow participants in the European Committee on Aircrew Scheduling and Safety.

Based on the results of these studies, a model for flight crew fatigue/alertness has been developed that is presented in Figure 2. Flight crew fatigue is determined by the fitness of the crew before the flight (pre-flight fitness), whether it is a day or a night flight, and in-flight operational factors (operational loads). Factors that influence pre-flight fitness are recent workload and the quality of pre-flight sleep. Operational factors are the flight duty period, and the quality of in-flight rest facilities. In-flight rest facilities are only used on long haul flights. There is a conditional dependence between flight duty period and rest facility, hence the arrow linking the two nodes.

10 MANAGERIAL INFLUENCES ON MISSED APPROACH AND FLIGHT CREW ALERTNESS

The generic delivery and learning systems that are used to model safety management were specified for each of the main actors (airline, airport, ATM organization and regulator) for the missed approach phase and for flight crew alertness. Although theoretically each of the safety critical tasks is influenced by all of the ten delivery and learning systems, the influences of some management delivery systems on some tasks is considered so marginal relative to others that they are considered to be not applicable.

Based on interviews that were conducted with KLM and ATC the Netherlands, a list of possible management changes with respect to the missed approach phase and flight crew alertness was developed. The two lists were combined into a single list of management influences on missed approach and flight crew alertness of which 26 were retained for use in the quantification process. Each management influence was linked to one or more elements of the technical model of missed approach.

11 QUANTIFICATION

To quantify the model, the conditional probabilities that are represented as arrows in the model must be determined. A combination of techniques is needed for this quantification. The use of historical data is often preferred because this represents real world observations. Historical date are, however, not always available and do not represent future situations that may be the subject of interest. Expert judgement is used in these cases. To ensure objectivity and transparency, it is essential that expert judgement be quantified via a traceable, structured process (Cooke & Goossens 2000). The quantification process is described in Roelen et al. (2003).

12 APPLICATION OF THE MODEL

A causal model can be used as a decision tool because it allows the calculation of the effect of specific changes in the aviation system on the overall risk. As such it can help to take decisions that require, for instance, a choice to be made between alternatives. It can also help in proactive decision policy development by providing insight into the effect on risk of anticipated changes to the system.

For instance, an airline may want to reduce flight crew fatigue. They consider several options for doing so:

1. Improving the quality of the hotel that is used by the flight crew during layovers.
2. Changing the layover policy from one local night before the next flight to two local nights before the next flight.
3. Reducing the flight duty period to less than 8 hours.

Application of the causal model in our study (op cit) demonstrates that changing the layover policy will lead to an insignificant improvement in flight crew. Improving the quality of the hotel and reducing the flight duty period has significantly more effect, both options provide similar increase in alertness.

13 CONCLUSIONS

A demonstration causal model of aviation safety has been successfully developed. This demonstration model is generic, with two elements developed in full detail. The model combines technical and managerial elements.

The construction of the model requires a number of distinct steps to be carried out and information to be available:

1. An accident scenario model based on detailed analysis of accidents and incidents and which is continuously updated;
2. A process description of all safety system processes in which the scenarios can occur, worked out to a level of detail at which safety critical tasks can be defined;
3. A description of the relevant generic management influences on these safety critical tasks;
4. Derivation of realistic management decisions which would improve the safety effect of these influences (or which would allow them to deteriorate);
5. Appropriate data to quantify the model based on the appropriate system boundaries for the question being posed (e.g. specific airport, world-wide operation, specific type of traffic, etc.);
6. Explicitation of the assumed default conditions against which the experts assess the effect of the proposed management decision and change.

A Bayesian Belief Net is a proper way to express a causal model. It provides a comprehensive model which is maximally data driven, yet which includes expert assessments of potential impact of contemplated decisions.

REFERENCES

Bellamy, L.J., Wright, M.S. & Hurst, N.W. 1993. History and Development of a Safety Management System Audit for Incorporating into Quantitative Risk Assessment, *International Process Safety Management Workshop*, San Francisco, USA.

Cooke, R.M. & Goossens, L.H.J. 2000. *Procedures guide for structured expert judgement*, EURATOM document EUR 18820EN, European Commission, Directorate General for Research.

Hale, A.R., Bellamy, L.J., Guldenmund, F., Heming, B.H.J. & Kirwan, B. 1997. Dynamic modelling of safety management. In Guedes Soares (ed.*) Advance in Safety & Reliability*. pp. 63–70. Pergamon. Oxford.

Hale, A.R., Guldenmund, F., Bellamy, L. & Wilson, C. 1999. IRMA: Integrated Risk Management Audit for major hazard sites. In Schueller G.I. & Kafka, P. (Eds.*) Safety & Reliability*. Balkema. Rotterdam. 1315–1320.

Papazoglou, L.A. & Aneziris, O.N. 1999. On the quantification of the effects of organisational and management factors in chemical installations. *Reliability Engineering and System Safety* 63, 33–45.

Reason, J. 1990. *Human Error*, New York: Cambridge University Press.

Reason, J. 1997. Maintenance related errors: The biggest threat to aviation safety after gravity?, In "*Aviation Safety"*, H. Soekkha (ed.), VSP, Utrecht, The Netherlands.

Roelen, A.L.C. et al. 1996. *Systematic Safety, study on the feasibility of a structured approach using a quantified causal tree*, NLR CR 96206 L, NLR Amsterdam.

Roelen, A.L.C. & Keer, J. 1998. The development of a causal model for aviation safety, an exploratory study, NLR-CR-98182, NLR Amsterdam.

Roelen, A.L.C, van der Nat, G.W.F.M., Keer, J. & de Ruijter, I.V. 1999. *The development of a causal model for aviation safety, Step 1 – Specification phase and preliminary analysis phase*, NLR-CR-99203, NLR Amsterdam.

Roelen, A.L.C., Bellamy, L.J., Hale, A.R., Molemaker, R.J. & van Paassen, M.M. 2000. *Feasibility of the development of a causal model for the assessment of third party risk around airports, Part 1: Main report*, NLR-CR-2000-189-PT-1, NLR Amsterdam.

Roelen, A.L.C., Wever, R., Cooke, R.M., Lopuhaä, R., Hale, A.R. & Goossens, L.H.J. 2003. Aviation Causal Model using Bayesian Belief Nets to quantify Management Influence (*this conference*).

Simons, M., Valk, P.J.L., de Ree, J.J.D., Veldhuijzen van Zanten, O.B.A. & D'Huyvetter, K. 1994. *Quantity and quality of onboard and layover sleep: effects on crew performance and alertness*. Report RD-31–94. Netherlands Aerospace Medical Centre, Soesterberg.

Simons, M. & Valk, P.J.L. 1997. *Effects of a Controlled Rest on the Flight Deck on Crew Performance and Alertness*. Report: NLRGC 1997-B3. Netherlands Aerospace Medical Centre, Soesterberg.

Simons, M. & Valk, P.J.L. 1998. *Early starts: effects on sleep, alertness and vigilance*. AGARD-CP-599; NATO-AGARD, Neuilly-sur-Seine, France. p. 6/1–6/5.

Valk, P.J.L. & Simons, M. 1999. *Effects of early reporting times and irregular work schedules on sleep, alertness, and performance of pilots engaged in short-haul operations* Report: NLRGC 1996-B2. Netherlands Aerospace Medical Centre, Soesterberg.

Valk, P.J.L. & Simons, M. 1998. *Pros and cons of strategic napping on long haul flights*. AGARD-CP-599; NATO-AGARD, Neuilly-sur-Seine, France (pp. 5/1–5/5).

Valk, P.J.L., van Roon, D.B. & Simons, M. 1999. *Effects of an alcohol hangover on performance and alertne*ss. Report 1999-B2. Netherlands Aeromedical Institute, Soesterberg, The Netherlands.