PhD Course Safe by Design

Teachers: Pieter v Gelder, Genserik Reiniers, Behnam Taebi, Ibo van de Poel, Pieter Vermaas, Fernando Kuipers (tbc), Wolter Pieters (tbc)

The hallmark of Safe by Design at TU Delft is the identification of commonalities and differences at different engineering faculties our university. During this course we will have several lecturers representing these different angles giving an excellent overview of the extensiveness and importance of the integral approach of Safe by Design. The team of lecturers together represent the broad approach at TU Delft about Safe by Design.

In recent years, we have been witnessing an increased attention in research and innovation for society's grand challenges. Think of the Sustainable Development Goals, and the large national and European mission-oriented research and innovation programs.

An associated shift can be seen in the recognition that outcomes of today's research and innovation should not only help resolve such grand societal problems (think of climate, energy, mobility, ageing or urbanization) but should simultaneously be designed in such a way as to ensure that they do not bring forth their own, new problems.

Under labels such as Responsible Research and Innovation, Corporate Social Responsibility, or Science With & For Society, efforts are undertaken to engage in research and innovation in reflective, anticipative, forward-looking and simultaneously responsive ways and incorporate this way work working into grand societal needs.

This approach serves the purpose, amongst other things, of proactively addressing potential risks and addressing ethical, legal and societal issues early on in research and innovation. In several fields of emerging technologies, much of such thinking and doing has been undertaken under the tag of '**Safe-by-Design' (SbD)**.

Safe-by-Design is a design approach that makes safety a core value, based on the consideration that preventing harm is better than curing it. The approach connects the two fields of Safety and Security Science on the one hand and Design for Values on the other. In both fields, TU Delft is considered to be world leading. SbD acknowledges the importance of safety in all phases of research and innovation trajectories and potentially looks at safety as integral to the entire chain of any research or innovation trajectory. What this precisely entails in terms of risk assessment, risk management, chain coordination and so on, will vary from one field to the next.

SbD aims to mitigate risks as much as possible during the design process rather than during manufacturing or customer use. This approach frontloads thinking about safety at an early stage of development. And of course, this preventive rationale gains all the more force in light of the transition towards circularity. Think of the circular economy in which products and materials are intended to escape the linear produce – consume – dispose pathway and are foreseen to remain here to stay.

This course will address two facets:

I) Discussion of theory and practice of Safety Science, focusing on interdisciplinary perspectives on the notion of risk, the design models and tools of value sensitive design as well as methods of identifying and including values in design, as for instance promoted by Responsible Research and Innovations (RRI).

II) Designing for Safety: how can this approach be addressed at all phases of the life cycle of the system, i.e. plan, design, test, implement/build, operate, maintain and dispose / reuse. SbD by definition, concentrates on the plan and design phase of the system. SbD aims for the inclusion of safety as a design requirement at the earliest stages of product and process development. This implies addressing questions such as: What could go wrong with this design; which components and

structures are potentially dangerous; how can the design be adapted to prevent the occurrence of risks, for instance by replacing, changing or reducing components; and if things do go wrong, how do we prevent or control adverse effects.

Keywords:

Safe by design, secure by design, fail safe design, fail secure design, inherent safe design, active safety, passive safety, fault tolerant design, graceful degradation design, fool proof design, redundant design, probabilistic design, risk-based design, safety chain, life cycle, quantitative risk analysis, risk management, safety management systems, probabilistic safety analysis.

Course Objectives:

1. Introduce you to state of the art of *safety science*
2. Introduce you to the *Safe by Design approach*
3. Consider design for safety in the *broader societal context* of security, privacy, autonomy, …
4. Give *tools to design* for safety in a way that complies with other values

It will be a highly interactive workshop consisting of three days. The workshop does not require any prior reading. There will be a final paper to conclude the course. The course material will be made available by the organizers.