Chapter 0

Safety demonstration of novel solutions

0.1 Introduction

The course *PK6032 - Safety demonstration of novel solutions* presents theories, methods and models to demonstrate that sociotechnical systems are safe. In the first part of the course we mainly focus on classical methods to demonstrate that we have sufficient safety barriers in place and that these are sufficient reliable. This part is basically based on the the textbook of Marvin Rausand: *Reliability of Safety-Critical Systems - Theory and Applications*.

In the second part of the course more emphasis is placed on novel systems and challenges to identify, grasp and model aspect for which we do not have experience. In this part of the course we base the presentation on the textbook developed in the Safety 4.0 project: *Demonstrating safety of software-dependant systems*.

0.2 What is safety?

Various definitions of safety exist. One common definition is to state that safety is the state of being "safe" in the meaning of a condition protected from harm or other danger. This can be interpreted as being "untouchable". A challenge with such a definition is that we cannot claim safety if there is any chance of harm or danger we can not cope with.

Another common definition of safety is to state that safety is freedom from unacceptable risk. Safety is then used in a broad sense to cover all types of risk, including risk related to life, property, environment, production, reputation etc. IEC (2010). By this definition we realize that we can not protect ourselves from all harm and danger, but we can limit our exposure to harm and danger in terms of ensuring low risk, i.e., acceptable risk.

The term acceptable risk is also not easy to grasp and is discussed in the scientific risk community. It is beyond the scope of this course to elaborate on such a discussion, but we could still

proceed with the understanding that safety means that we are “sufficient protected” from harm and other danger.

0.3 What is safety demonstration?

With safety demonstration we mean that we use arguments to claim that our solution is safe. Argumentation theory, or argumentation, is the interdisciplinary study of how conclusions can be reached from premises through logical reasoning. It includes the arts and sciences of civil debate, dialogue, conversation, and persuasion. It studies rules of inference, logic, and procedural rules in both artificial and real-world settings (van der Meulen and Myhrvold, 2022).

0.4 The Safety 4.0 main steps to safety demonstration of novel technology

Figure 2 shows the main steps of demonstrating safety of novel technology.

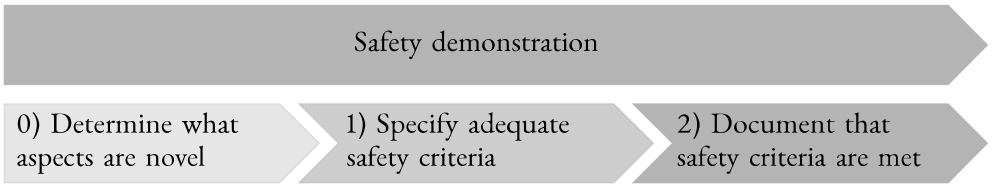

Figure 1: Safety 4.0—the main steps to safety demonstration of novel technology (van der Meulen and Myhrvold, 2022)

Safety 4.0 defines safety demonstration as: Documentation, based on evidence and structured reasoning, that adequate safety criteria are specified and met. From this definitions it follows that the safety demonstration process essentially consists of two main steps:

1. Specify adequate safety criteria
2. Provide arguments and evidence that the specified safety criteria are met

However, when demonstrating the safety of novel solutions, it is primarily the implications of the novel aspects that are of concern. An additional preliminary step is therefore included to determine what aspects of the solution are novel:

0. Determine what aspects of the solution are novel

The three steps shown in Figure 2 are not performed as one linear process. In practice, the safety demonstration process consists of several subprocesses that may be conducted by different parties with different focus and perspectives.To standardize the safety demonstration process, three main perspectives are defined van der Meulen and Myhrvold (2022):

- *Activity perspective (as part of risk assessment) - Is the activity safe?* Demonstrate that the overall risk of the activity (i.e., the consequences of the activity, with associated uncertainty) is tolerable and reduced as far as reasonably practicable. If the risk is not tolerable, determine the need for risk reduction.

- *Strategy perspective (as part of risk treatment) - Is the strategy safe?* Demonstrate that the chosen barrier strategy (including technical, operational, and organizational barrier elements) is able to provide sufficient risk reduction to ensure the activity is safe, and that the design and operation of systems are robust and prudent. The latter involves the strategy complying with specific requirements in the regulations, or that special conditions exist on which alternative strategies may be granted.

- *Technology perspective (as part of technology qualification) - Is the technology safe?* Demonstrate that the technology elements used fulfil the technical performance requirements and operational constraints needed for the activity and strategy to be safe.

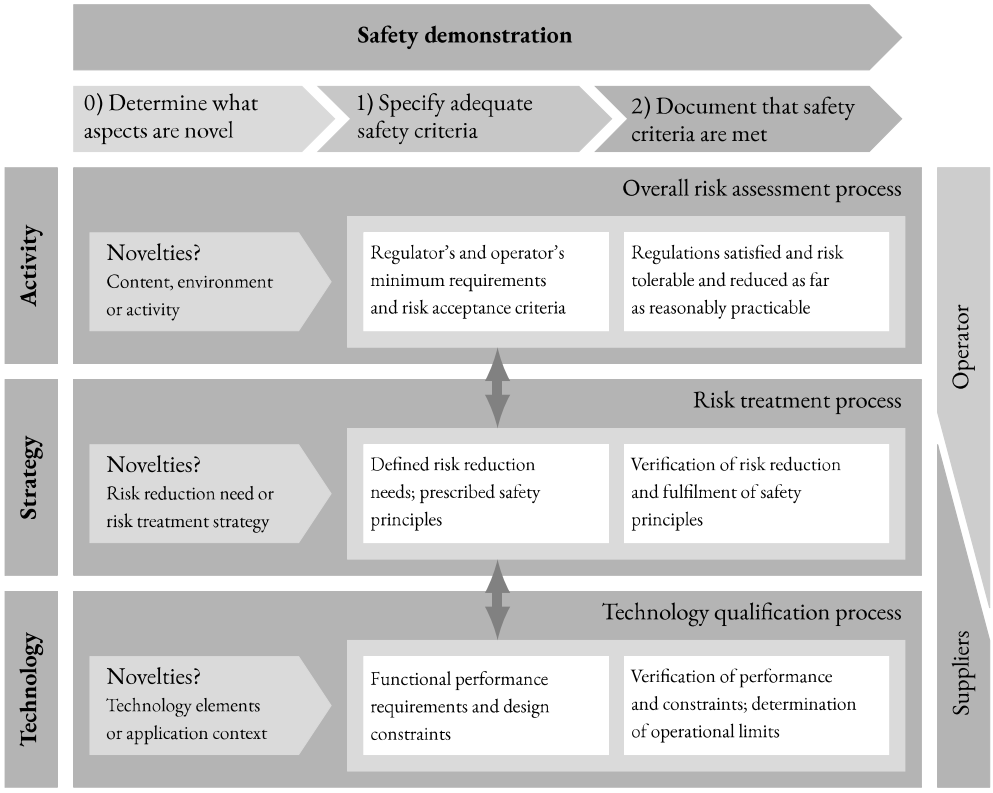

Figure 2: Overview of the safety demonstration process, consisting of three subprocesses with different perspectives and stakeholder involvement (van der Meulen and Myhrvold, 2022)

Bibliography

IEC (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems (e/e/pe, or e/e/pes). Standard, International Electrotechnical Commision, Geneva.

van der Meulen, M. and Myhrvold, T. (2022). *Demonstrating safety of software-dependant systems.* DNV AS.