nks
Nordic nuclear safety research

NKS-278
ISBN 978-87-7893-353-9

Safety culture in design

Luigi Macchi[1]
Elina Pietikäinen[1]
Marja Liinasuo[1]
Paula Savioja[1]
Teemu Reiman[1]
Mikael Wahlström[1]
Ulf Kahlbom[2]
Carl Rollenhagen[3]

[1] VTT Technical Research Centre of Finland
[2] RiskPilot, Sweden
[3] Vattenfall, Sweden

April 2013

nks
Nordic nuclear safety research

Abstract

In this report we approach design from a safety culture approach As this research area is new and understudied, we take a wide scope on the issue. Different theoretical perspectives that can be taken when improving safety of the design process are considered in this report. We suggest that in the design context the concept of safety culture should be expanded from an organizational level to the level of the network of organizations involved in the design activity. The implication of approaching the design process from a safety culture perspective are discussed and the results of the empirical part of the research are presented. In the interview study in Finland and Sweden we identified challenges and opportunities in the design process from safety culture perspective. Also, a small part of the interview study concentrated on state of the art human factors engineering (HFE) practices in Finland and the results relating to that are presented. This report provide a basis for future development of systematic good design practices and for providing guidelines that can lead to safe and robust technical solutions.

Key words

Safety culture, Design, Network safety culture, HFE

NKS-278
ISBN 978-87-7893-353-9

Electronic report, April 2013
NKS Secretariat
P.O. Box 49
DK - 4000 Roskilde, Denmark
Phone +45 4677 4041
www.nks.org
e-mail nks@nks.org

Safety culture in design

Final Report from the NKS-R SADE activity

(Contract: AFT/NKS-R(12)97/13)

Luigi Macchi[1]
Elina Pietikäinen[1]
Marja Liinasuo[1]
Paula Savioja[1]
Teemu Reiman[1]
Mikael Wahlström[1]
Ulf Kahlbom[2]
Carl Rollenhagen[3]

[1]VTT Technical Research Centre of Finland
[2]RiskPilot
[3]Vattenfall

Table of contents

Page intentionally left blank

1. Introduction

It has been long acknowledged that safety culture and human factors need to be taken into account and managed when operating and maintaining nuclear power plants. It has also been acknowledged that human factors that affect the people operating the plant need to be taken into account when designing equipment and technical interfaces. However, the fact that people taking part in designing the plants and their technological solutions are also affected by human and organizational factors and safety culture has not been given much emphasis. As design flaws have been identified as important contributors to serious nuclear power accidents, like the Fukushima nuclear accident in Japan in 2011, it is important to also start considering how human factors and safety culture affect the design activity and how the design work can be supported from this perspective.

In this report we take a safety culture approach on design in the nuclear industry. As this research area is new and understudied, we take a wide scope on the issue. We hope to provide a general basis for further research and practical development in this area. As a basis for all the other chapters we first describe the special characteristics of design in the nuclear industry. We then present and compare different theoretical perspectives that can be taken when improving safety of the design process. We then focus more on the safety culture perspective and discuss its application in the design context. We suggest that in the design context the concept of safety culture should be expanded from an organizational level to the level of the network of organizations involved in the design activity. After that we present the results of the empirical part of the research. In the interview study in Finland and Sweden we identified challenges and opportunities in the design process from safety culture perspective. Also, a small part of the interview study concentrated on state of the art human factors engineering (HFE) practices in Finland and the results relating to that are presented in the same section. After that we discuss the design aspects of the Fukushima nuclear power plant accident in the light of the network safety culture approach. We conclude in a synthesis, where we summarise the key points of the report and present directions for further research on safety culture in design. We hope the chapters in this report provide a basis for future development of systematic good design practices and for providing guidelines that can lead to safe and robust technical solutions.

2. Design in the nuclear industry

2.1 What is design?

Reviewing the literature on design indicates that there is no common agreement on the definition of the word ‘design’ (Trueman, 1998). In the nuclear power industry the term has been used to refer both to the process of designing and to the end product. For example the lay-out and construct of the whole power plant is often called design (e.g. IAEA, 2012) while e.g. Veland (2010) writes about design as specific type of activity. In the context of the present report, we adopt the latter view of design as an activity. We are interested in the whole variety of design processes in the industry – including the design of small technical components, sub systems, and systems that are part of or constitute a nuclear power plant (i.e. a safety critical large scale complex technical system) as well as the huge design processes of completely new power plants. We hope to provide a general view on design in the nuclear industry for the basis of more in-depth and contextual studies in the future.

What constitutes a design process then? What does design as an activity look like? Aspelund (2006) has described the design process as consisting of conceiving of ideas, planning and explaining, making decisions related to the development of the ideas and solving the problem. One can also consider even broader aspects of design as a process, also taking into account planning and management (Trueman, 1998). Mark et al. (2007) define design as the practice of inventing, creating, and implementing (technical) artifacts that depend upon, integrate, and transform heterogeneous and uncertain domains of knowledge Design is thus considered a complex practice taking place under uncertainty (cf. Norros, 2004).

A design process can aim at designing several different elements or components of a system, from training to human system interfaces, to procedures or structures etc. Design is an iterative process composed by a series of steps. The first thing to address is the **requirements** of the design (which, depending on the problem area, can be dealt with as an innovation process or as a “predefined” task/component). Now, given the iterative nature of the design process, the next phase consists of a rather broad **conceptual design** which consists of a rough “picture” of the design. This is especially needed when the designed component is supposed to interact with other loosely defined components and systems.

The next step, assuming that the conceptual design has been refined and adapted to the concept design of interdependent components/systems, is to develop the **detailed design** of the component or system. After developing the detailed design an **evaluation** of the detailed design (and its functions with the other interdependent components/systems) should be performed. After this, the actual **implementation** of the component/system can take place. Next the component has to be **tested**. The final phase of this tentative design process takes into consideration both maintenance and upgrade of the component or system. In a summary, design in an industrial context can be viewed as a process that has an objective of creating an artifact to solve an expressed problem or a need. This process is a combination of analytical problem solving and innovative creation of new features and combinations. The resulting artifact cannot be known in detail in advance but the function(s) that the artifact should fulfill can be known and should be specified early in the process.

2.2 Special requirements of design in the nuclear industry

Nuclear power plants consist of several complex systems whose design, operation and maintenance requires special expertise. The components designed for the power plants are usually tightly coupled i.e. they come with several interfaces to other designed products.

Design in the nuclear industry is highly regulated. Each step in the process has to be approved by the regulator. The components, systems and constructs have to withstand a certain range of identifiable conditions and events without exceeding pre-specified authorized limits. This certain range of conditions and events that the plant and its components and systems need to withstand is called the **design basis** (IAEA, 2007). Whether the designed product will hold out in predefined possible conditions well enough, is evaluated using both deterministic and probabilistic calculation methods. The results of these calculations are checked and approved by the regulator.

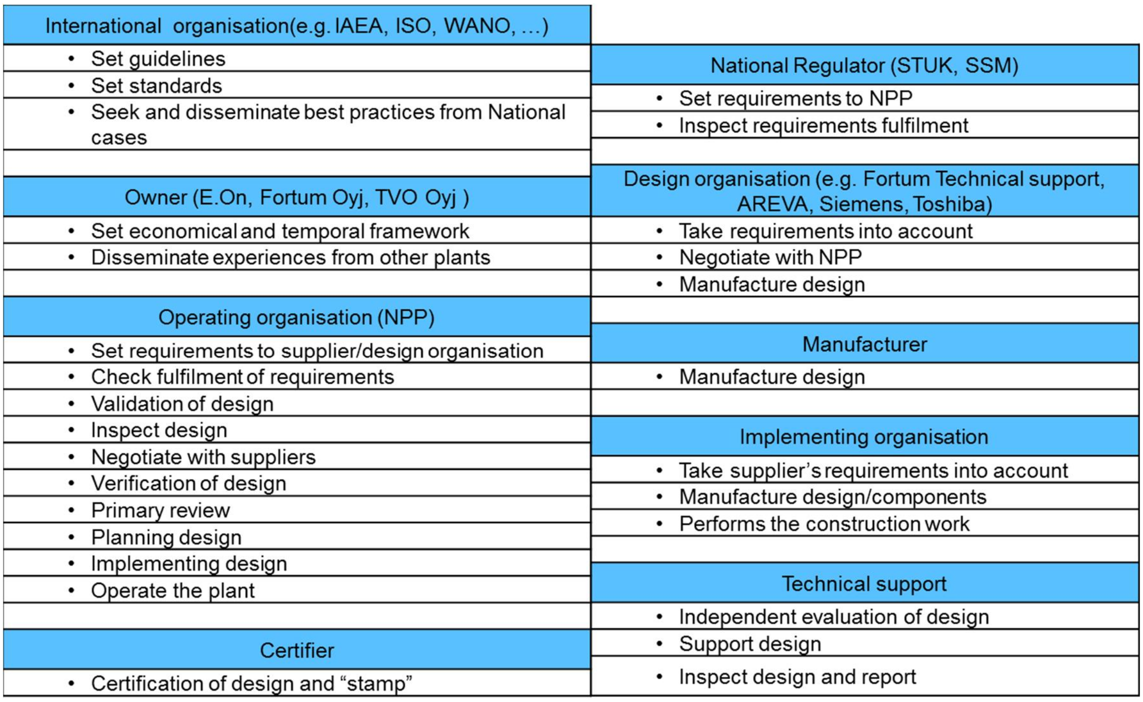
The principle of **defence in depth** has been a central safety principle for design in the nuclear industry since the dawn of the industry. The interpretation of this concept has evolved during the years, and in practice it is thus used with several but closely connected meanings. In the IAEA (2007) safety glossary the concept of defence in depth was defined as “a hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.” So basically the concept means that components and systems should be designed in a way that if one of them breaks down, another defence layer still remains, to protect the environment and population from radiation.

Other important safety principles in the nuclear industry are **redundancy**, **diversification** and physical **separation**. Redundancy means that there are several similar subsystems for carrying one function and either one of them alone is sufficient for carrying out that function. Diversification means that there are several systems or equipment that carry out the same function but whose functioning is based on different principles or mechanisms. Physical separation means that the parallel subsystems or equipment are situated in distinct physical locations and are not connected to each other.

2.3 Stakeholders in the design process in the nuclear industry

It follows from the above mentioned special characteristics of design in the nuclear industry that the design process is by nature a collective effort that involves several stakeholders. No one individual designer alone can ensure that the designed end product is functional and safe and complies with the strict regulatory requirements and design principles. Rather the design process can be understood as a complex interaction and negotiation process between different experts and organisations. In table 1 we have identified the key organisations involved in design processes in the nuclear industry and their main tasks.

Table 1- Stakeholders in the design process in the nuclear industry and their tasks



International organisation(e.g. IAEA, ISO, WANO, …)	
• Set guidelines	National Regulator (STUK, SSM)
• Set standards	• Set requirements to NPP
• Seek and disseminate best practices from National cases	• Inspect requirements fulfilment
Owner (E.On, Fortum Oyj, TVO Oyj)	Design organisation (e.g. Fortum Technical support, AREVA, Siemens, Toshiba)
• Set economical and temporal framework	• Take requirements into account
• Disseminate experiences from other plants	• Negotiate with NPP
	• Manufacture design
Operating organisation (NPP)	
• Set requirements to supplier/design organisation	Manufacturer
• Check fulfilment of requirements	• Manufacture design
• Validation of design	
• Inspect design	Implementing organisation
• Negotiate with suppliers	• Take supplier’s requirements into account
• Verification of design	• Manufacture design/components
• Primary review	• Performs the construction work
• Planning design	
• Implementing design	Technical support
• Operate the plant	• Independent evaluation of design
	• Support design
Certifier	• Inspect design and report
• Certification of design and “stamp”	

The people doing the actual hands-on design work can be in-house personnel of the power company but more often they work for a design organisation for which the power company has outsourced the design work. These design organisations may also provide services for other industries besides the nuclear power industry and they are not always that familiar with the nuclear industry context and its special requirements.

IAEA (2012, 9) safety standard on design states that prior to an application for authorization of a plant the responsibility for the design rests with the design organization (e.g. vendor). But once an application for authorization of a plant has been made, the prime responsibility for safety will lie with the applicant. However, detailed knowledge of the design will still rest with the responsible designers. IAEA points out that this balance will change as the plant is put into operation, since much of this detailed knowledge, such as the knowledge embodied in the safety analysis report, design manuals and other design documentation will be transferred to the operating organization.

The role of the regulator is more emphasised in the nuclear industry than what is typical to most other industries. The regulator sets requirements for design process and follows whether they are met. Thus the regulator can also be considered being part of the design process.

2.4 Expertise in design

As indicated above, design is a broad concept that is associated with many meanings and various contexts. To characterize design expertise in general terms seem therefore less appropriate. Rather each domain of design can be expected to manifest its own unique characteristics in terms of particular skills needed. However, some general psychological features can be identified. Design activities are often associated with open problem spaces rather than closed ones. That is, design is a dynamic cognitive act where several different solutions to a problem might be possible. Veland (2010) argues that design in the nuclear industry requires special kind of “design thinking” which is something else than just technical-rational problem solving. According to him, a core competence of a designer is a process skill. That is, the designer needs to “think on his feet” when immersed in active, flexible, reflective exploration of the problem space. This is presumably what makes design so challenging and interesting for many people.

But to navigate in an open and dynamic problem space involves uncertainty. New technological and organisational inventions are always associated with some uncertainty. Also, incremental changes in existing structures (hardware, software, organisational etc.) can be challenging from a safety point of view. These remarks might be seen as platitudes but a closer look reveals that there is an interesting dynamic between “conservatism” and “flexibility” when positioning design in a safety framework and in the specific context of the nuclear power industry. This dynamics is relevant for issues about safety culture in design: we would expect that many designers of risk sensitive systems are facing tensions between their roles as innovators on the one hand and the limitations set by rules and regulations and the nuclear power specific technical design principles.

In design of risk sensitive systems it is often a good practice to be as transparent as possible about the basis of the decisions made. If such information is documented and stored, it is much easier to later change the system. However, from a psychological perspective it could be challenging for a designer to continuously document what is happening in a design process and why one solution is preferred in favour of another. First, documentation takes time and may be perceived as unnecessary and disturbing. Secondly, there might be more uncertainty behind design decisions than a designer wants to reveal. Particularly in risk sensitive systems, both the public and the buyer of a system want to be sure that the designed end-product is safe and to be open about the uncertainties of the design process may therefore be a challenge for design organisations.

3. Theoretical approaches for analysing design

The purpose of this chapter is to provide an overview on different perspectives that take the human aspects of the design activity into account and that are, or could be, applied to improving design in the nuclear industry. From different points of view, they allow the identification of challenges hindering design processes and the quality and safety of their end-products, and they suggest ways to address them. Eventually, the chapter presents the theoretical background of this study, the model of safety culture that will be applied in design.

3.1 Improving design by engineering Human Factors

In order to enhance the quality and safety of the designed *products* one possible approach is to engineer human factor aspects into them. The approach called Human Factors Engineering (HFE) aims at affording reasonable assurance that the design of the plant systems, equipment, human tasks, and the work environment are compatible with the sensory, perceptual, cognitive, and physical attributes of the personnel who operate, maintain, and support the plant. (O'Hara et al 2012). In other words, HFE stands for the application of knowledge about human capabilities and limitations to design.

HFE may be interpreted to be related to safety culture in design, because the overall objective of HFE work is to improve the safety of the end products of design, from human factors point of view. To fulfill this aim, the HFE activities of a design organization comprise of applying different kinds of methods during the design which enable foreseeing the potential threats to safety in the forthcoming usage of the end result of the design already during the design. A comprehensive HFE process covers also the phases of implementation and operation in order to monitor the success of the design from the human factors perspective and if necessary, to define the required corrective actions. In this report, HFE process will be presented as defined by US Nuclear Regulatory Commission (NRC).

NRC has published an often-referred report that guides the conductance of HFE in design and operation organizations the NUREG-0711 (Human Factors Engineering Program Review Model). The report describes the regulatory guidance concerning what is considered to be an adequate *HFE program* of an applicant of one of the following: construction permit, operating license, standard design certification, or a combined license (O'Hara et al 2012). This means that the US regulator expects an applicant of any of those permits to follow a specified HFE program in order to make sure that the plant and its systems are developed in a manner which considers human factors adequately.

The scope of HFE according to NUREG-0711 is the design of plant, its systems, and equipment. This means that HFE process concerns a range of objects of design starting from the basic plant components.

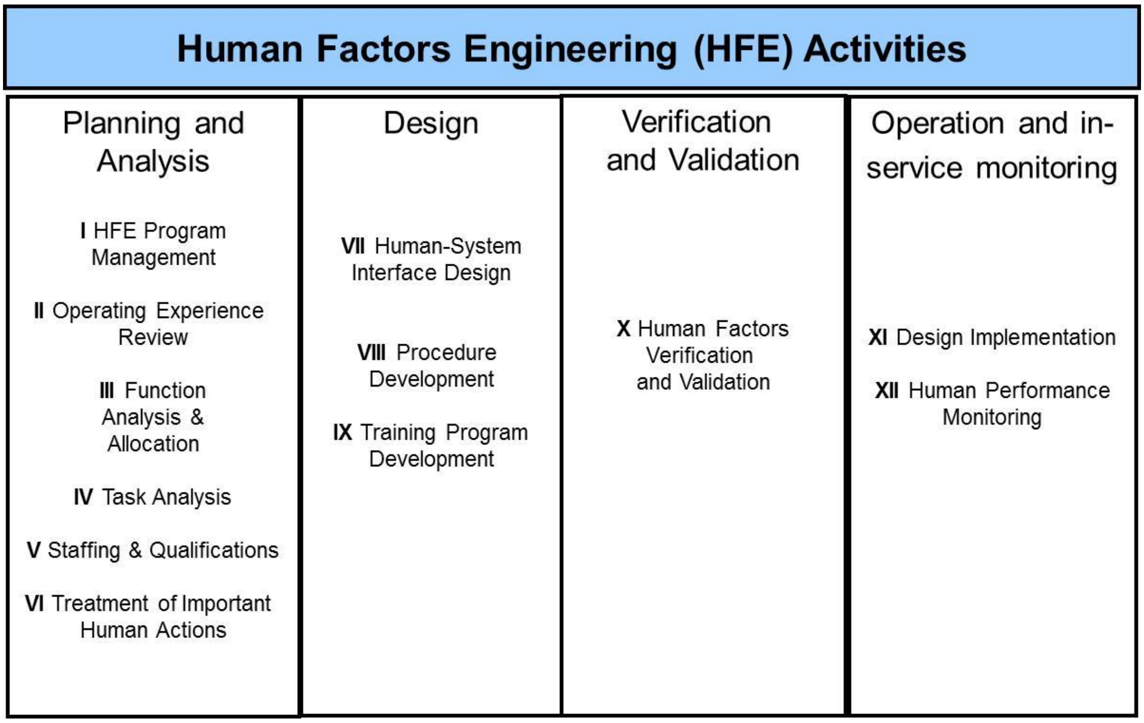
NUREG-0711 describes a HFE process which consists of four general activities: 1) Planning and Analysis, 2) Design, 3) Verification and Validation and 4) Implementation and Operation (Figure 1). The four activities are divided further into twelve review elements. In the following, the four general activities and the twelve review elements are introduced, together with a preliminary mapping with the different design steps above presented.

This general activity of **Planning and Analysis** consists of six review elements:

1. HFE Program Management,
2. Operating Review,
3. Functional Requirements Analysis and Function Allocation,
4. Task Analysis,
5. Staffing and Qualification,

6. Treatment of Important Human Actions.

The first element deals with the management of the HFE Program. The remaining five elements are concerned with establishing the requirements of the design.



Human Factors Engineering (HFE) Activities

Planning and Analysis	Design	Verification and Validation	Operation and in-service monitoring
I HFE Program Management **II** Operating Experience Review **III** Function Analysis & Allocation **IV** Task Analysis **V** Staffing & Qualifications **VI** Treatment of Important Human Actions	**VII** Human-System Interface Design **VIII** Procedure Development **IX** Training Program Development	**X** Human Factors Verification and Validation	**XI** Design Implementation **XII** Human Performance Monitoring

Figure 1. The HFE process described in NUREG-0711

The general activity of **Design** consists of three review elements:

1. Human-System Interface Design,
2. Procedure Development,
3. Training Program Development.

The first review element, Human-System Interface, consists of for example concept- and detailed design, which deals with the Conceptual design and Detailed design.

The third general activity, **Verification and Validation**, consists of one review element:

1. Human Factors Verification and Validation.

This element maps the Evaluation phase of the design process.

The fourth and final general activity, **Implementation and Operation**, consists of two review elements:

1. Design Implementation,
2. Human Performance Monitoring.

These elements roughly correspond to the Implementation and Testing steps of the design process.

NUREG-0711 also gives guidance of the composition and expertise areas of a HFE team which carries out the HFE activities in the design and operative organizations. It is not assumed that HFE should comprise a separate organizational unit. Also, HFE design team may change over time, for example, in transitioning the design from vendor's ownership to that of the operational unit.

The competence areas that are identified to be needed in an adequate HFE process are:

- Project management
- Systems engineering
- Nuclear engineering
- I&C engineering
- Architect engineering
- Human factors engineering
- Plant operations
- Computer system engineering
- Plant procedure development
- Personnel training
- Systems safety engineering
- Maintainability/Inspectability engineering
- Reliability engineering

3.2 Improving design by managing the design process – focus on hazards

An alternative way for improving design consists in trying to manage the design process. Two approaches are possible there. The first approach focuses on pinpointing and evaluating hazards and applies models and techniques, such as the STAMP model and the associated STPA technique (Leveson, 2004, 2011), to try and control as rigorously as possible the process by performing hazard analysis and risk reduction. STAMP focuses on (1) the early part of the design process, i.e., how to hinder hazardous conditions to emerge, (2) the process for how the system will develop, and (3) control components that are outside the information flow. Based on the STAMP causality model (Leveson, 2011) the STPA technique (System-Theoretic Process Analysis) is used to analyze possible hazards proactively before a design has been created, not only for evaluating it afterwards (Ibid, p. 212). According to Leveson (2011) "STPA can be used in a proactive way to help guide the design and system development". One of the most important features of STPA is the continuously iterative process of performing hazard analysis of design decisions, (see Figure 2). The general idea is to design, evaluate the hazards related to the design, and if necessary re-design, then evaluate the hazards again and so on.

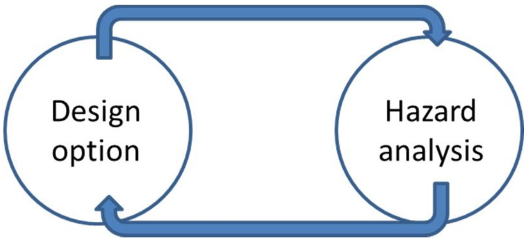


Figure 2. The iterative process of design and hazard analysis (adapted from Leveson, 2011)

STAMP and STPA identify specifications, safety information systems and communication as the key issues for safe engineering or design (Leveson, 2011). Specifications and safety information systems are considered the glue that integrates the activities of design and the operation of complex systems. Communication is considered critical in handling any emergent property in a complex system. Leveson points out that our systems today are designed and built by hundreds and thousands of engineers and then operated by thousand and even tens of thousands more people. Thus enforcing safety constraints on system behavior requires that the information needed for decision making is available to the right people, at the right time, whether during system development, operations, maintenance, or reengineering (Ibid, p. 307). Leveson also states that good documentation is the most important thing in complex systems where nobody is able to keep all the information necessary to make safe decisions in their head (Ibid, pp. 308-309").

Even though widely accepted and used, the approach of controlling the design process by hazard analysis and risk reduction also has some shortcomings. The complexity of nuclear power plants makes it challenging for designers, and for the entire nuclear industry, to identify possible hazards. Perrow (1999) comments on nuclear power plants as the product of a design process, arguing that errors in the system cannot be identified or understood since the error depends on unexpected "links" between at least two components. In tightly coupled systems a change in one part of the system heavily affects other parts of the system. Thus, it is very hard to identify potential accident scenarios beforehand.

3.3 Improving design by managing the design process – focus on organizational capability

The acknowledgment of the complexities inherent in nuclear power production and the difficulty of identifying each possible risk have led to the development of another kind of approach for managing safety in complex systems. This approach is called Resilience Engineering (Hollnagel et al., 2006, 2011). The basic assumption behind Resilience Engineering is that due to the complexity of the designed products (including their use and interaction with the other artefacts as well as actors in the system), and to the complexity of the design process itself and to the inherent uncertainties in both of them it is in practice impossible to ensure that all unacceptable risks are identified and eliminated. Thus it is important to increase the actors' (e.g. individual designers', regulators', power companies') ability to succeed under varying conditions instead of trying to identify and remove each individual source of risk.

While the Resilience Engineering approach has developed in the safety science arena, the concept of resilience has gotten increased attention also in other research areas that are relevant for the design process, e.g., the supply chain management. Based on their review on supply chain literature Ponis and Koronis (2012) define supply chain resilience as "the ability to proactively plan and design the supply chain network for anticipating unexpected disruptive (negative) event, respond adaptively to disruptions while maintaining control over structure and function and transcending to a post-event robust state of operations, if possible, more favourable than the one prior to the event, thus gaining competitive advantage". This definition comes close to the idea of resilience used in the safety science literature.

According to Resilience Engineering (see Hollnagel et al., 2006, 2011) there are no special 'error producing' processes that begin to work when an accident is going to happen. There is no fundamental difference between performance that leads to failures and performance that leads to success. Thus the focus on safety work should be on trying to understand and steer performance in general, whether on individual, collective or organisational level.

Resilience Engineering also acknowledges that because of the complexity of the activities organisations face many conflicts and contradictions. One of them is the constant struggle between safety and being "better, faster, cheaper" (Hollnagel, 2004). In a nuclear power plant there is also an inherent contradiction between decentralization and centralization solutions (Perrow, 1999; Woods and Branlat, 2011; Reiman and Rollenhagen, 2012). The justification for having centralized control in a nuclear power plant organization is the need to understand, or see, what is occurring in different parts of the system – the whole system might be difficult to perceive from the vantage point of different sub-systems. On the other hand, the justification for having decentralized control is that a single centralized unit might not understand or identify the cause of a disturbance if it relates to interactions within or between sub-systems; they could be best dealt by implementing fast and creative solution by personnel working directly in that sub-system. Another typical conflict an organisation has to solve is the need to deal with and find a balance between acute and chronic goals and problems. Nuclear power plants have also to balance between investing on and developing specialist and/or generalist roles and competences (Hoffman and Woods, 2011)

These tensions will most likely apply to the design process as well, even though they have not been explicitly studied in this context. These kinds of tensions are not easily solved. Rather they are issues that need to be constantly taken into consideration and balanced between in the design process.

All in all the approach of Resilience Engineering for managing the design process thus consists in investigating how organizations can increase their ability to create processes that are both robust and flexible, to deal with the uncertainties of the design work and on how to deal with inherent and induced tensions and pressures. How to do this in practice in the best possible way (for example what kind of methods to use for supporting resilience), is not clear, but some practical ways forward have been suggested (see Hollnagel et al., 2011).

3.4 Improving design by managing safety culture

The concept of safety culture reached a rather broad audience when related to discussions of causes for the Chernobyl accident (IAEA, 1986). The concept was later defined by IAEA (1991, p.4) as follows:

> *"Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance."*

The research concerning safety culture took off in the 90's, and a number of perspectives and definitions arose. Reiman, et al. (2010) claim that despite two decades of research there is no common agreement of the definition of safety culture. According to Reiman et.al., (2010, p. 2) there are two main reasons for this:

> *First, the definitions of safety culture emphasize to varying degrees the attitudes, behavior, or knowledge of the personnel, with some definitions placing emphasis on the structural features of the organization. This leads to very different ideas about the best means of developing safety culture. Second, the definitions of safety culture are often generic in nature. Thus, they do not take into account the varying demands of different functions operating at the power plants or the life-cycle of the given unit.*

Another interesting discussion regarding different perspectives on safety culture is presented by Guldemund (2010, p. 227):

> *Going through these different approaches attentively, it is evident that none of them is completely off the mark, or sheer nonsense. On the contrary, together they provide a rather comprehensive image of what safety culture might stand for or symbolizes. Nevertheless, there are also various differences of opinion, which makes a full resolution near impossible.*

Despite the different approaches and definitions, the concept of safety culture has brought with it a number of positive contributions to safety. It does for example facilitate the possibilities to address different "soft" aspects of safety management, such as norms, attitudes, behavior, and overt and covert expectations. All of these are areas which then could be discussed, evaluated, and to some extent, managed.

One of the strongest driving forces for research and practices departing from the concept of safety culture has been the observation that neither technical factors nor “human errors” are by themselves sufficient to explain major accidents (Pidgeon, 1997). To understand safety and risk, one has to understand the larger cultural and organisational context in which an industry operates. The external environment including technological, institutional, and socioeconomic factors influences individual organisation’s policies through management decisions which, in turn, have influences on systems for risk control, plans and policies, individual behaviour etc (Rasmussen, 1997). The concept of safety culture has sometimes been used as a holistic term aiming for this larger system centred perspective. On the other hand we also find a more narrow conception of safety culture as a basically human centred concept but without necessarily incorporating the whole “system” that might be relevant for risk and safety. In such a view safety culture represent just one aspect among others.

The concept of safety culture has not been applied that much in the context of design activities. However, the people taking part in the design process are human too and cultural phenomena affect them just as the people in operation and maintenance. Thus it is important to consider how the safety culture perspective could be applied in the design activities as well.

3.5 Improving design by managing the design network

As described already in chapter 2.3 the design process of a large scale complex technical system typically involves a number of actors, all affecting the process, and thus potentially the outcome, to various degrees. There are a number of different approaches to networks, i.e. telecommunication, computer, biological, cognitive and semantic networks, and social. The network perspective in general aims to take into account a rather broad number of different relations relevant for the network, which can be exemplified with the rather loose broad definition by Thompson (2003):

> *“A specific set of relations making up an interconnected chain or system for a defined set of entities that forms a structure.”*

The most relevant network perspective in terms of our current topic is the social network perspective. In a broad sense, the social network perspective focuses on relations among social entities, for example communication between actors of the relevant groups, economic transactions between corporations etc. (Wasserman and Faust, 1994). The fundamental difference between a social network explanation of a process and a non-network explanation of a process is thus the inclusion of concepts and information on relationships among the units in a study (Ibid).

One well known approach of the social network perspective is Social Network Analysis (SNA), and according to Wasserman and Faust, SNA can be used when analyzing a broad range of applications such as for example the world and political system, community elite decision making, coalition formation, markets and group problem solving. SNA further claims, above else to be concerned with relationships between interacting units or entities such as for example individuals, parts of organizations, separate organizations etc. Five important characteristics for SNA are (Ibid):

- SNA is based upon an assumption of the importance of relationships among interacting units, and the social network perspective encompasses theories, models, and applications that are expressed in terms of relational concepts or processes.
- Actors and their actions are viewed as interdependent
- Linkages between actors are channels for transfer of resources
- Network models focusing on individuals view the network structural environment as providing opportunities for or constraints on individual action

- Network models conceptualize structure as lasting patterns of relations among actors.

Of critical importance for the development of methods for social network analysis is the fact that the unit of analysis is not the individual, but an entity consisting of a collection of individuals and the linkages among them.

SNA has for several years been applied when analyzing large project relationships. Given that some of the challenges that are related to design in the nuclear industry are related to project issues, there might be lessons learned from the existing literature (Pryke, 2012).

3.6 Summing up the different perspectives on design

All the perspectives described in chapters 3.1 – 3.5 can be considered applicable to improving design in the nuclear industry. All of them deal with the human aspects of design work. And even though all of them emphasize somewhat different things, they also resemble each other in certain specific ways. For example, the HFE perspective, the safety culture perspective as well as the Resilience Engineering perspective all represent a proactive and positive approach to managing the work carried out in the nuclear industry. All of them aim to evaluate and develop the ability of the organization carrying out the work to succeed in the future. The Resilience Engineering approach, the safety culture approach and the network approach also point out that it is not only up to individual people to ensure safety in the design process. Rather, safety is created in the interactions between people and between organisations.

The following chapters are founded on the safety culture perspective. However, we enrich the safety culture perspective with considering the inherent tensions and trade-offs in the design work. We also utilize the network perspective and expand the safety culture concept to a network level because the design process in the nuclear industry typically takes place in a network of actors.

4. Safety culture and design

In the present section of this report we go a bit deeper into the concept of safety culture and discuss its application in a design context. This discussion will provide a basis for the interview study we present in chapter 5 and the discussion of the Fukushima nuclear power accident (chapter 6).

The concept of safety culture has since its introduction after the Chernobyl accident become increasingly applied in research and practice: numerous articles have been published that use the concept of safety culture as a point of departure. However, the main body of research and practical applications associated with safety culture is much focused on “sharp end” activities in the operational context rather than technological design. It is thus often assumed that the properties characterising a good/strong safety culture are basically the same regardless of application area (nuclear, transportation, etc.) and type of safety (system safety, personal safety, etc.). Our focus here is on safety culture in the design context specified as technological design in the nuclear industry. More specifically we like to better understand which cultural properties (including human and organisational factors) that best can support technological design so that the product becomes safe and reliable.

A first step for such an inquiry is to elaborate on the following general questions; (1) What can be understood by the concept of safety culture? 2) What properties of a good safety culture have been identified in previous research? (3) To what extent are these general properties applicable in the domain of technical design?

4.1 The concept of safety culture

As already noted, many articles about safety culture start by reminding the reader that the concept of safety culture has several interpretations and no clear definition (Guldenmund 2000). Common to most definitions of safety culture, however, is that they speak about culture as a *collective* attribute – culture is something that people *share* in terms of beliefs, values, perceptions, attitudes and behaviour. Nonetheless, the analytical unit in use when characterising a culture is a tricky question – cultures exists at many levels both inside and outside an organisation. For example, Thompson et al. (1998) argue that there might be differences among management levels with respect to safety culture characteristics, which, in turn, influence how management acts toward subordinates in safety related matters. The existence of various subcultures in organisations is easily observed and a question then arises if it makes sense to speak about an overriding organisational culture containing attributes shared by all different subcultures. To speak about safety cultures it is generally wise to first attempt to understand what an organisational culture is about and then to position safety culture in that context.

Many generic models of organisational culture have been proposed. One of the more influential is by Schein (1992) who differentiates among several layers of organisational culture. At the most deepest level, an organisational culture is assumed to be characterised by a set of basic assumptions (for example, the nature of human beings). These assumptions, Schein argues, then will influence what is called “espoused values” e.g. values and norms that could be represented by policies, strategies and goals (the second level). Artifacts (the third level) are the most salient and visible aspects of an organisational culture and can be seen in dress codes, architecture, work processes, organisational structures etc. For Schein, it is rather difficult to understand a culture’s deepest roots since some of its antecedents might have been forgotten. On the other hand, Schein also warns about the difficulties of interpreting whether an observed behaviour is an artefact of the culture or rather caused by situational and individual factors. Applying Schein´s generic model to safety culture one could use observations and questionnaires to grasp the surface oriented climate aspects. However, in order to develop a deeper understanding of safety culture, more qualitative approaches are needed.

In the context of design, Schein´s general approach opens for interesting questions. What are the basic assumptions that drive design organisations towards a particular design solution? For example, what are designer's assumptions about the "operators" that should manage a nuclear power plant? To simplify, are the designers striving to *design for the operators*, or to design *operator-proof* solutions – that is, do the designers see operators as a threat to safety or as people who create safety with the solutions provided by the designers? Further, how do the designers understand the plant's functioning and the meaning of the safety principles? Or what kind of hazards the designers assume to be relevant in a nuclear power plant context? Answers to such questions could eventually clarify certain issues sometimes perceived as design flaws in the interface between man and machine. Moreover, the design of instructions, work processes etc. sometimes reveals a too idealistic view on what people can accomplish in a certain context – a focus on basic assumptions may reveal distorted world views which makes a design less optimal for operation,

4.2 What characterizes a good safety culture?

Today a common conceptualisation of safety culture is that it represents an *aspect* of a more general organisational culture. A problem then emerges considering what other aspects than safety should be considered as (sub)cultures in their own right – examples of such other suggested cultures in organisations are innovation cultures, ethical cultures, and production cultures. But how should we perceive such subcultures in interaction with one and another? To what extent, and in which situations, do these "x-cultures" support or oppose each other? Research attempting to explore this issue has begun to emerge but in this research the concept of "safety climate" is often used in favour of safety culture. Organisational climate is usually perceived as a more surface oriented aspect of organisational culture, representing individuals' perceptions of procedures and practices related to safety, innovation, production etc. Application of cultural questionnaires has been the most common research method in the context of safety climate research (Zohar, 2010).

In a recent study by Colley et al. (2013), the role of different organisational values as an antecedent of perceived safety climate was explored. The authors refer to previous research by Zohar and Luria (2004) which argued that safety climate depends on the relative importance people place on safety relative production. However, Colley et al. also recognizes that several values are in focus in most organisations, and not only safety and production. To explore how a broad set of values might interact with safety climate, Colley at al. used The Competing Values Framework (CVF) which was developed by Quinn and Rohrbaugh (1983). In this framework the most discussed dimensions consist of flexibility vs. control and internal vs. external focus. Combining these dimension, four quadrants are generated which are assumed to be correlated with four models of organisational effectiveness.

One of these models is characterised by high flexibility and high internal orientation and is associated with a *Human Relation* orientation. Cohesion and morale are desired outcomes and the means for their realisation are training and development, open communication and participative decision making. Another model derived from the CVF is named *Internal Process* and is characterised by internal orientation and control and the desired outcomes are stability and control. The means to realize this state are, for example; information management, formalization, rule enforcement and data based decision making. The *open system model* of CVF focuses on innovation and development and is characterized by flexibility and external orientation. The means are assumed to be, for example; adaptability, visionary communication, adaptable decision making, and risk taking. Finally, *the Rational Goal Model* is characterised by focus on efficiency and productivity and the means are goal setting, planning, centralized decision making, production orientation, pursuit of goals and objectives.

A reasonable hypothesis is that depending on the profile of values (e.g. their relative strength), different climate characteristics would emerge in an organisation. For example, Quinn and Spreitzer (1991) argue that, in general, companies with a *balanced value profile* perform better than organisations with an unbalanced profile, that is, none of none of the four goal models – flexibility, control or internal vs. external orientation – should dominate. Colley et al. (2013, p. 71) takes these observations as a basis for a hypothesis that "individuals who perceive that their organisation has a balanced value profile also will perceive that their organisation has a more positive safety climate, and report fewer incidents in comparison with individuals that perceive that their organisation has an imbalanced value profile". They justify this by arguing that a "balanced profile suggests that people are valued, trained and supported (human relation focus), there are adequate and useful rules and procedures (internal focus), production goals and targets are appropriate and achievable (rational goal focus) and the system is adaptable, innovative and has up-to date technologies and equipment (open system focus)" (Ibid, p. 71).

A second hypothesis put forward by Colley et al. is that individuals who perceive their organisation as focusing either on human relations or open system models will perceive a better safety climate than those focusing on either internal processes or rational goal models. The rationale behind this idea is that previous research has found that if there is an overemphasis on production (rational goal model) people may feel that achieving production targets are more important than care for people (Wright, 1986) and if people believe that managers are overly focused on formal rules and procedures, they might be seen as more interested in compliance in itself that caring about people (Morgan, 1986). These assumptions and associated research can of course be questioned and interpreted in several ways but there appears to be face validity behind these assertions at least judging from common observations in many organisations. For example, as researchers and consultants in the nuclear industry we have often heard critical voices regarding the influence of production pressures and the burdens of bureaucracy.

In order to test their hypothesis, Colley et al. worked with a sample of 368 individuals working in various high risk industries in Australia. The best safety performance was found in cultures that were characterized by a Human Relation-Rational Goal Model and the worst performance in profiles that were biased towards the Internal Process-Rational Goal Model. The data did not allow for supporting the first hypothesis (e.g. that a balanced profile is best for safety) since none of the data profiles had that balanced characteristics. Interestingly, the data showed that those profiles showing a weak safety performance all were characterised by emphasise on the Internal Process Model. The profiles with better safety performance all shared an emphasis on human relations. Colley et al. interpret those findings in the context of previous research which have found that overly focusing on control by rules and restrictions tend to limit motivation and learning and to create a passive orientation toward safety with a less proactive orientation (Parker et al. 2003; Turner et al, 2005). One of the most interesting finding from this research is that focusing on production (Rational Goal Model) in itself is not negative for safety given that production focus is balanced with a human relation focus (supportive and flexible orientation). On the other hand when the Rational Goal Model was strongly combined with focus on rules and procedures (Internal Process Model) this profile was found to be negative for safety. Applied to the nuclear domain it seems, then, that a strong focus on human relations should always balance the common focus on rules and regulations.

Somewhat disappointingly for our purpose, the above research did not focus on design organisations. Thus even though the reported research has general relevance for many issues that relate to safety culture and safety climate, we are still lacking specific understanding on what a design organisation should concentrate on in order to develop its safety culture. However, some hints could nevertheless be derived from the research by Colley et al. First, we can assume that design organisations (and also other design activities made internally at a nuclear power plant) are in need of a balanced value profile. The nuclear industry is highly regulated, which means that the values characterizing the Internal Process Model (formalisation, rules etc.) must be salient. But design is also associated with innovation and new solutions so there is an intriguing balance between "proven design" and the possibilities offered by new technology (we could call these "unproven designs"). The Open System Model supports adaption, new thinking, and new possibilities and this motivates many engineers. At the same time, focus on a Rational Goal Model is of course also necessary – a system design project is restricted by budget, plans, goals and a centralized decision making is often assumed as being necessary to achieve the goals. Finally, the Human Relation model and its associated focus on competence development, participatory decision making etc. is often perceived as important in system design. As a tentative suggestion, then, we assume that design organisations, perhaps even more than operating organisations, are in need of a balanced safety culture in order to reach its goals and contribute to the safety of the end product.

Reason (1998) argues that a safe organisation is characterized by a culture which continuously collects and shares information about hazards – it is an *informed culture*. In concrete terms this means both to collect information about own and others events as well as performing risk analytical activities. Both these processes constitute a cornerstone in safety management systems. For external design organisations, these features of safety culture are not always easy to manage because information about events resides in the operating organisations. Consequently, providers of nuclear designs must develop a network of contacts with operators in order to be an informed culture.

To be an informed culture, many dimensions of safety must of course be considered. In engineering organisations, including design organisations, a traditional way to think about safety has often departed from technology. It is therefore a risk that experience feedback system, risk analysis methods etc. become biased towards technology only. This presents a challenge for engineering organisations since they may feel that they do not have the proper methods and background knowledge in order to collect and analyse risk contributions arising from human and organisational factors. An important safety culture issue, then, is to develop a broader understanding in design organisations about the interaction between people, technology and organisational factors. Issues about human and organisational factors must thus have a salient role in safety management system but not only as policies and procedures, but also in terms of real integration with technical factors in terms of knowledge, management and behaviour (Kennedy and Kirwin, 1998).

Pidgeon and O'Leary (1994) argue that the following factors are particularly important for developing a strong safety culture. First, a strong senior management commitment to safety. This general management commitment factors show up in a majority of safety climate studies as being one of the most important drivers for safety culture and climate. Secondly, a genuine care for people should be a salient feature. In the nuclear industry this can also be interpreted, we believe, as a *moral stance* which involves not only people at site but also everyone outside that might be affected by the risks associated with nuclear power production. Here there is a difference between types of safety cultures which predominantly focus on internal processes and those industries associated with high risks which also involve people outside the organisational boundary. For design organisations, the artefacts produced usually contain risks that evoke a moral responsibility (but not necessarily a legal responsibility). A third factor is associated with norm and rules. This topic constitutes a research domain in itself and has been in focus for a long time. In a recent review by Hale and Borys (2012) it is argued that two different models have been salient in research about rule management. The first model is characterized as being a classical top-down approach with a main emphasis on limiting the freedom of choice and where rule breaching is always perceived as negative behaviour. The second approach is more dynamic and bottom-up; rules are perceived in a dynamic context in which adaption to various situational characteristics often becomes necessary. Operators are in this model seen as expert resources that should participate in the design of instructions, rules and procedures. Both these models have their pros- and cons and Hale and Borys argue for a middle ground between these two models. Of course, a nuclear design organisation is restricted by rules and regulation of many types and the room for being flexible in interpretation of rules is limited. On the other hand, if engineering (design) is conducted at the nuclear stations, for example when retrofitting technology, this may be associated with so much paper work, even for small changes, that the processes impose such a heavy burden on nuclear organisations that discussion sometimes emerges about the rationality of “too much rules”. These situations represent difficult trade-offs for nuclear organisations; rules are necessary but when do they become detrimental for safety? No definite answers to this question can be given but it still is a salient feature connected to safety culture and design. A fourth factor discussed by (Pidgeon and O’Leary 2000) is associated with reflection and learning. To be a “learning culture” is usually seen as an important feature of safety cultures and there are good reasons for this. This general property often associated with good safety cultures is obviously connected to what Reason (1998) calls an informed culture. The concept of “learning” is however associated with a multitude of different aspects which makes the concept vulnerable to all kinds of sweeping and idealistic generalisations. However, one useful distinction is between single-loop learning in contrast with double loop learning (Argrys and Schön, 1978, 1996). Single loop learning concerns correcting deviation in existing processes whereas double loop learning is associated with learning entirely new things (and thus not only correcting deviations from an existing process).

Researchers at VTT Technical Research Centre of Finland (Reiman and Oedewald, 2009; Oedewald, et al., 2011; Reiman, et al., 2012) have stated the following six criteria for good organisational safety culture:

1. safety is a genuine value in the organisation which reflects to decision making and daily activities
2. safety is understood as a complex and systemic phenomenon
3. hazards and core task requirements are understood thoroughly
4. organization is mindful in its practices
5. responsibility for the safe functioning of the entire system is taken
6. activities are organised in a manageable way.

These criteria have been further summarised into three easily communicable cornerstones of safe activities: mindset, understanding and organisational systems and structures (Figure 4).

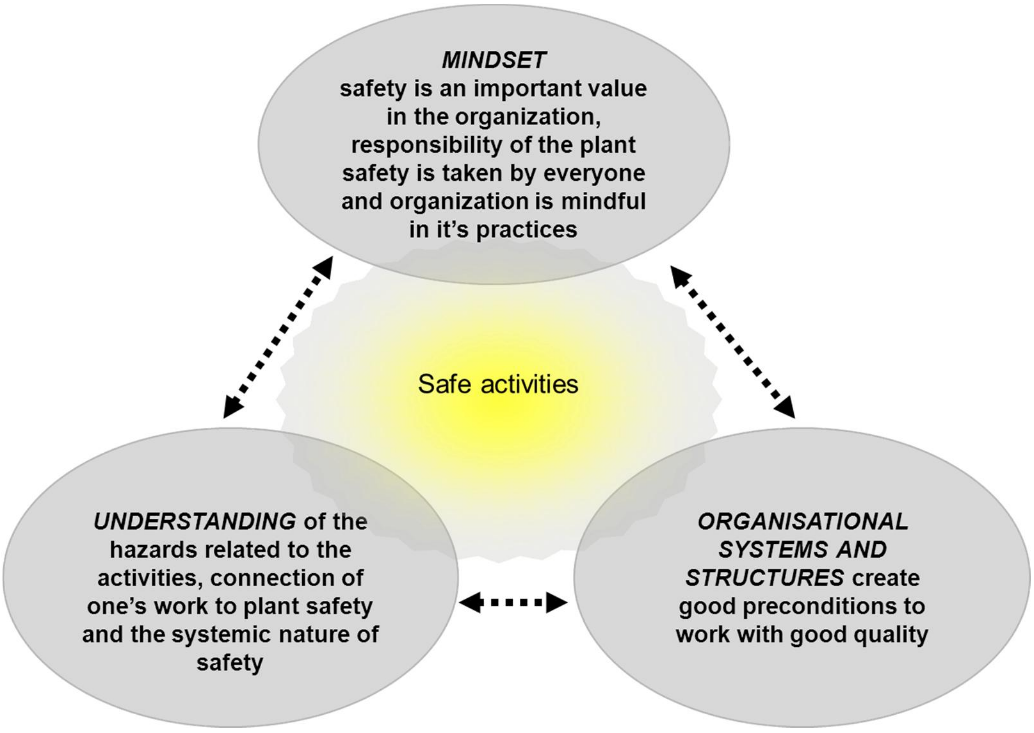

MINDSET
safety is an important value in the organization, responsibility of the plant safety is taken by everyone and organization is mindful in it's practices
Safe activities
UNDERSTANDING of the hazards related to the activities, connection of one's work to plant safety and the systemic nature of safety
ORGANISATIONAL SYSTEMS AND STRUCTURES create good preconditions to work with good quality

Figure 4. Cornerstones of safe activities (Oedewald, Pietikäinen & Reiman, 2011)

These criteria have been used as a foundation for evaluating safety culture at Nordic nuclear power plants (e.g. see Oedewald, et al., 2011). These criteria could also be utilised in understanding what good design safety culture is like. For example it can be argued that design organisations – whether in-house units or contractor companies – should have a certain shared mindset where safety is valued, where responsibility for the safety of the whole plant that will be utilising the designed object is taken and where constant vigilance or mindfulness is maintained.

4.3 Safety culture and maturity scales

One of the few studies about safety culture that explicitly addresses safety climate and culture in design organisations was conducted by Gordon and Kirwan, (2004). This study also represents a view on safety culture that makes use of maturity scales, that is scales that attempt to classify a given safety culture on a dimension from being less mature towards more advanced (Fleming, 1999). The authors developed a scale to measure the current safety culture in an air traffic navigation R&D organisation. The scale consist of subsections under four main headings (1) Management demonstration of safety, (2) Planning and organisation of safety, (3) Communication, Trust and Responsibility for safety, (4) Measuring, Auditing and Reviewing. In this particular setting the results showed that the main improvement areas were found in the safety management system, team integration and responsibility for safety.

Scales of the sort developed above usually extend from a state of "pathological" or "emerging" toward a state of "continuously improving" with a constant striving for being better. In the particular scale developed by Gordon and Kirwan (2004), the scales were named as follow:

Level 1: **emerging;** safety is defined as a technical and procedural solution in compliance with regulations and safety is not seen as a business risk.

Level 2; **managing;** safety is perceived as a business risk but is mainly defined in terms of adherence to rules and procedures.

Level 3: i**nvolving:** at this level employees are involved in the development of safety and safety is actively monitored

Level 4: **proactive**: safety is considered in a broad scope of factors and preventive measures are taken.

Level 5: **continually improving**; constantly striving to find effective measures for hazard control.

Since organisational cultures contain many subcultures one could question the ambition to classify a whole organisation as belonging to a certain safety climate level. However, it generally seems sound to collect information so that a given state of a climate/culture can be compared to a standard of excellence. Particularly, if one likes to consider a complex network organisation with many stakeholders (which is the case in design) there would be a great benefit to be able to compare different stakeholders with each other with respect to a criteria – such a strategy could function as a benchmark for different stakeholders and put pressure on their safety culture development.

Another option besides categorising a specific safety culture into one category in terms of its maturity is to look at the safety culture profile. For example, Oedewald et al. (2011) evaluated the fulfilment of six safety culture criteria in a Nordic nuclear power plant on a four-point evaluation scale: very good, quite good, quite poor and unacceptable. Instead of giving one single estimate of the safety culture maturity level the evaluation produced a safety culture profile of the case organisation. This profile showed that in terms of some safety criteria the organisation was mature. For example, safety was a clear value for the organisation. However, in terms of some of the other criteria more development was clearly needed.

4.4. Network safety culture

Design processes can be perceived as distributed decision making where a number of different stakeholder has to cooperate in order to reach a safe a reliable design. Decision making has however often been perceived as isolated decisions made by one person. In reality, decision making is a continuous process involving many stakeholders – the decisions are thus distributed rather than being controlled by a single actor. Each stakeholder (individuals and groups) always have a limited view of the whole system (a bounded rationality). Cooperation, coordination and trade-offs are thus necessary to reach the goals. How a system involving many stakeholders succeeds in fulfilling its task is a difficult organisational problem which has no clear answer. Usually some kind on self-organisation emerges representing an informal organisation and not necessarily the same as can be seen in the organisational charts. Particularly in situations where large uncertainties exist, the organisation must adaptively and dynamically use all its resources. Regarding this problem Brehmer (1991) states:

> *"An organisation that cannot foresee all the problems that it will encounter, nor all the resources that it will command, must rely upon self-organisation to solve its task. How the capability for self-organisation is to be built into an organisation is something of a mystery, if not an outright contradiction"* (p. 9).

A central and most important factor to reach goals in a distributed network of actors is of course communication (such as face-to-face, intranets, e-mails etc.). Thanks to the convenient digital communication technologies of today, the problem does not lie in the practical issue of achieving contact. Instead, however, in a distributed network of several stakeholders, constructing coherent and shared plans can be challenging because different participants have their limited view of situations. One suggested way to solve this problem has been the *multi-agent planning approach* (Durfee et al. 1989). Adopting such a strategy, all the stakeholders (or nodes in the network) construct a multiagent-plan specifying future actions, resources, etc.

This rather common approach has however its limitations because each stakeholder usually need timely and correct information about the others as well as means to resolve conflicts. An alternative approach to coordination is to use *partial global planning* (Durfee and Lesser, 1988). This approach builds on the idea that in dynamic and complex environments information must be continuously updated and plans reformulated in view of new information. Local actors are given freedom to build their own plans and these are shared with others in the network to improve coordination. Other coordination mechanism is described by Brehmer (1991) and will not be covered here. Suffice to say, that this whole research area is of interest for the quest of finding what may constitute what we refer to as a *network safety culture.* By this we mean that the system boundary is drawn widely to include a number of different stakeholders of relevance for the success of a project involving safety concerns. Considering the topic for the present research we define nuclear design activities as a class of activities in the nuclear domain which involve a set of stakeholders (e.g. power plants, regulators, vendors, consultants etc., see chapter 2 in this report). We thus expand the concept of safety, which is usually applied to individual organisations, into a network where each stakeholder constitutes a culture of its own (containing subcultures). As was mentioned previously, the traditional perception of the concepts of safety culture (and safety climate) has, with some exception, not been particularly focused on design activities and their relation to safety culture. Nor has the domain of safety culture have had much attention to a whole network of safety cultures and their interactions.

Building on the idea that we can define a network of safety cultures and a set of activities (in this case nuclear design and redesign), we should then attempt to identify some of the most crucial safety culture related factors for such a network. Based on the literature on distributed decision making, it could be suggested that one of the most important factors for understanding network safety culture would be cooperation and communication in the network. Durfee et al. 1989 (quoted in Brehmer, 1991), suggest that three important factors in communication influence coherence in a network, (1) relevance, (2) timeliness and, (3) **completeness.** With respect to relevance, it is important that the actors in the network agree upon what particular issues are of relevance and thus get prioritised. If some actors in the network give priority to issues that the others will find less relevant, then it is less likely that focus and coherence in the network will generate the desired outcomes. A problem with implications for design is that some issues which are represented and focused by some actors in a network are relevant for safety but other actors fail to perceive this relevance. Timeliness is usually very important in the sense that the right information must be presented timely to have effect. To be complete, *it is desirable that the actors in a network share at least some general model that is common to all the actors in the system.* What implications does this have for the concept of a network safety culture? With the risk of being overly abstract and general it still appears that what Reason (1989) names an "informed culture" comprising knowledge about events and risks, others tasks etc. should be a very important factor for a network safety culture. This, in turn, evokes all the issues associated with communication among the stakeholders in the network - including some strategy for setting up an efficient communication structure. This feature of a network safety culture also evokes a need to develop a *systemic model of nuclear safety* including a broad set of factors important for safety management.

Secondly, there is an ethical aspect which should be of strong relevance for a network safety culture: all the stakeholders should agree, we suggest, about an ethical code that could be referred to when trade-offs and negotiations are made in the network.

One of the rare efforts to define the basics of network safety culture in the nuclear domain has been done by Gotcheva, et al., (2012). Drawing on the work of Reiman and Oedewald (2009) and Oedewald et al. (2011) they have suggested that it is not enough to view the safety culture on an individual organisation’s level. As described earlier in figure 4, each organisation can be characterised in terms of the different cornerstones of safety culture, that is: understanding, mind set and organisational structures and systems. But because in the nuclear industry several organisations usually work in close co-operation, it is also important to look at how the different organisational safety cultures interact. Safety emerges from these interactions. Thus it is important to assess for example, whether the understanding concerning the hazards and core task demands is the same in the different organisations and whether the organisations have compatible organisational systems and structures in place. In section 5 we describe how we have utilised this categorisation to analyse the challenges in the network that carries out design activities in the nuclear industry.

5. Empirical study on the challenges and opportunities of design

In this section we describe an empirical interview study we carried out in the Nordic nuclear power community in 2011-2012. The purpose of the interviews was to get an understanding of the challenges and opportunities of the design process from safety culture perspective. We used the classification of the cornerstones of good safety culture (see Figure 4 and Oedewald, Pietikäinen & Reiman, 2011) as a framework in the analysis. The interview study also dealt with the conceptions of and practices utilised or planned to conduct HFE as systematic conductance of HFE activities could be interpreted to be part of good safety culture in design because it aims to foresee the potential consequences of the products already during the design phase.

5.1 Data collection

We conducted 21 semi-structured interviews within the Nordic nuclear power community (Finland and Sweden) during 2011-2012. The interviews lasted from 45 minutes to 2 hours. In most of the interviews there were two interviewers present. Main themes of the semi-structured interviews were: professional background and work role of the interviewee and conceptions/practises in relation to

- design activities
- safety culture
- human factors engineering.

The outline of the interview is presented in appendix A. These interview questions were however modified according to the organisation and the role of the interviewee. For example, questions concerning the history of design were only asked from the people who had been involved in nuclear power plant design for a long time.

Some of the interviews were used as background material for the researchers in understanding the challenges and strengths in design, while 14 of the Finnish interviews were audio recorded, transcribed, translated into English when needed and analysed in more detail. These 14 interviewees represented different perspectives to design. A summary of these 14 interviewees and their occupational background is given in table 2. The interviewees were all somehow involved in the design process. They represented different design disciplines from automation design to the design of whole new power plants. In the following subsections we describe the analysis of these 14 interviews and its results.

Table 2 - Interviews in Finland

Organisation	Number of interviews	Occupations of the interviewees
Fennovoima (power company)	4	specialist, manager
STUK (regulator)	4	inspector, manager
TVO (power company)	2	engineer
VTT (research organisation)	1	scientist
Fortum (power company + design organisation)	3	specialist, manager

5.2 Data analysis

5.2.1 Analysis of challenges

The interview analysis process we carried out in order to understand the challenges of design is described in figure 6. The transcribed and, when needed, translated, interview raw data was first roughly analysed for the extraction of challenges. Any expression that referred to a possible challenge for design from safety point of view was extracted from the interviews. These extracts were transformed into more general level statements in order to make comparison and the formation of an overall picture possible. The identified challenge statements were then categorized into groups using a bottom-up approach. This grouping helped us to get acquainted with the data and form an overall understanding of the large data set. However, it did not provide a meaningful overall structure as such. Thus the analysis was continued with a top-down analysis approach, where the statements were grouped into three groups based on the safety culture model depicted in figure 4: mindset, understanding, organisational processes and structures. This grouping was done by one of the authors and cross-checked by another author. The results of this analysis were presented and discussed together with two groups of nuclear power specialists (in two of the steering group meetings of the Finnish SAFIR nuclear safety research programme). Based on this the challenges were condensed further into the final key challenges that are presented in section 7.3. These final results were presented in the SADE project final seminar in January 2012.

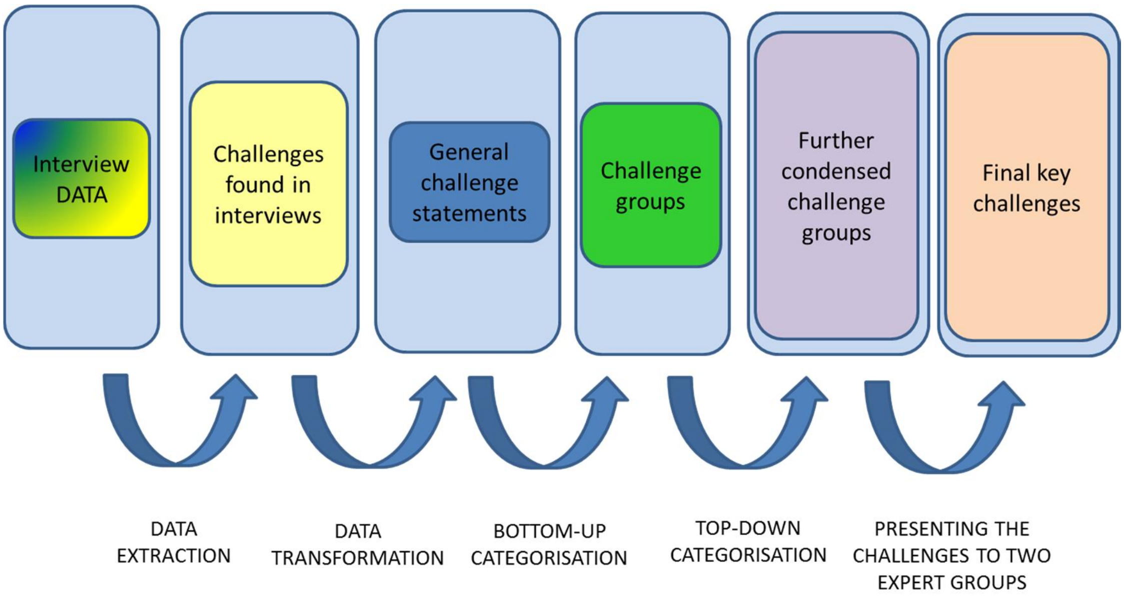

Interview DATA
Challenges found in interviews
General challenge statements
Challenge groups
Further condensed challenge groups
Final key challenges
DATA EXTRACTION
DATA TRANSFORMATION
BOTTOM-UP CATEGORISATION
TOP-DOWN CATEGORISATION
PRESENTING THE CHALLENGES TO TWO EXPERT GROUPS

Figure 5. The analysis process of the challenges

During the analysis process we proceeded gradually from a large and rich data set to a compact set of key challenges. We also preceded from concrete and situated challenge descriptions towards more abstract and general challenges that are applicable to different types of design processes in the nuclear industry. Only the challenges that were interpreted to refer to challenges in mindset, understanding or organisational structures and systems *between the different organisations* involved in the design process were included in the analyses of the challenges. Thus with the analysis, we hoped to provide understanding on what kind of specific safety culture challenges there are in the design process on the organisational network level.

5.2.2 Analysis of opportunities

The transcribed and, when needed, translated, interview material for opportunity analysis was first roughly analysed for the extraction of opportunities. Any expression that included a possibility or benefit for design from the safety point of view, for example, good practise or mindset that enhances or supports safety in design, was extracted from the interview material. Then, the extracts were transformed into the so called statements to present more clearly the opportunity in question. For instance, an interviewee, working at the national regulator, stated: "If we have a cross-technological problem, we will have discussions afoot in no time-from the coffee table to more official discussions. That is one of our strengths." This was transformed into a more general statement of “The cross-technical interfaces at the regulator are not as challenging as at the power companies”. All analyses are based on statements.

Actual classification

The main analysis was performed according to the cornerstones for safety potential, based on the DISC (Design for Integrated Safety Culture) framework (see e.g. Reiman, et al., 2012). The statements were classified according to their belonging to the three cornerstones of (i) Mindset, (ii) Understanding or (iii) Organisational structures and practises. Additionally, some supporting classification was made in order to clarify the nature of opportunities.

Clarity of statement

If the opportunities are not clearly understandable, there is a possibility for misunderstanding. Clarity classification is a tool for studying the validity of the possibilities found. Thus, the statements were categorised depending on whether the interviewee had expressed the opportunity clearly and directly or whether the opportunity was concluded by the analyser (VTT). In the latter case, the interviewee had not expressed or apprehended the opportunity clearly. Clarity of statement has two categories, expressed (by the interviewee) and concluded (by the analyser).

Locus of realising organisation

The realising organisation is the one that could realise or realises the opportunity. The realising organisation is not necessarily the one in which the interviewee is working. The locus of the realising organisation, whether it is own or another, depicts how the opportunities in the field are perceived – whether own organisation is powerful in creating possibilities or another organisation is wished for doing that. The categories are data based but the main options are own organisation, another organisation or own and another organisation.

Origin of opportunity

This classification tells in what level of the whole system or network the opportunity originates. Thus, this reflects the network nature of opportunities. It also shows what the primary location is for modifying or enhancing the opportunity. Categories are data based, the basic possibilities being the level of individual, the level of own organisation, and the level beyond that.

State of actualisation

The statements were also categorised depending on whether they presented an actual, existing opportunity or an idea, that is, something that does not exist at the moment, or something that is planned to take place in the future or just envisioned as something desirable.

The whole process of analysis is depicted in the Figure 7 below.

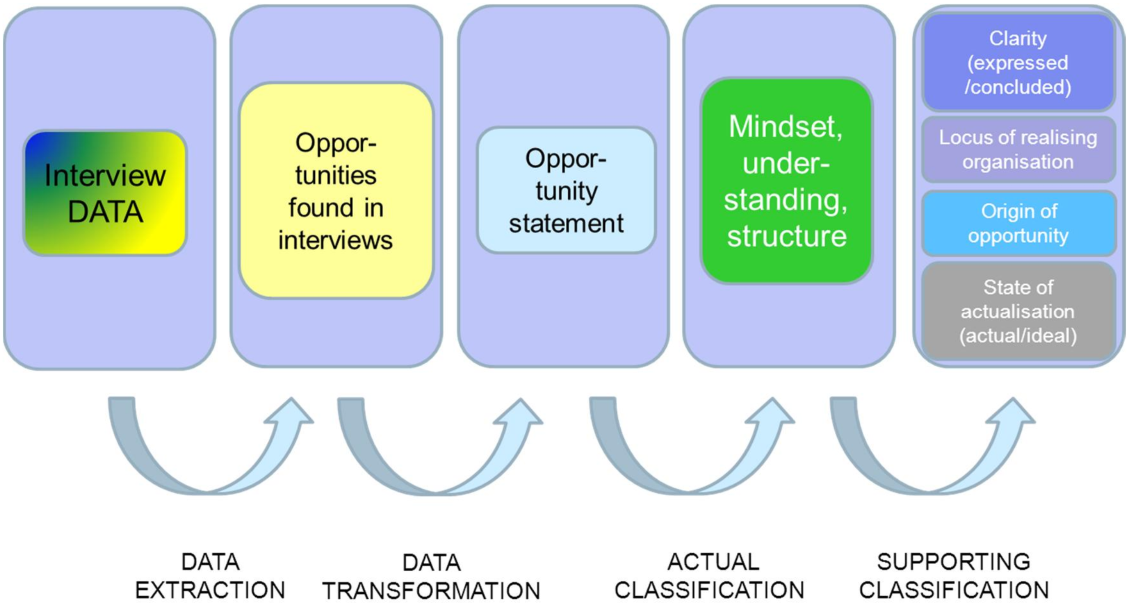

Interview DATA
Oppor-tunities found in interviews
Oppor-tunity statement
Mindset, under-standing, structure
Clarity (expressed /concluded)
Locus of realising organisation
Origin of opportunity
State of actualisation (actual/ideal)
DATA EXTRACTION
DATA TRANSFORMATION
ACTUAL CLASSIFICATION
SUPPORTING CLASSIFICATION

Figure 7. The proceeding of data analysis for opportunities

5.2.3 *Analysis of HFE*

The data collected concerning HFE consisted of answers to one or two specific questions concerning conceptions and practices utilised or planned to conduct HFE. The amount of data was quite small as the concept of HFE was not familiar to all of the interviewees.

In the analyses of the data all the remarks concerning HFE were identified in the interview data. The data consisted of conceptions concerning what constitutes HFE and what is its significance in the design process. The HFE practices which were mentioned in the interviews were mapped to the NUREG HFE process in order to formulate results concerning scope and coverage of HFE in Finland currently. The practices were either utilised or planned to be utilised within the participating organizations.

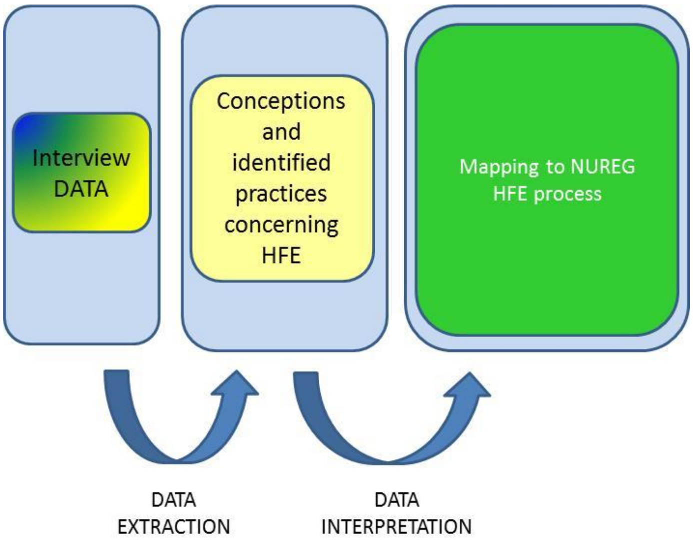

Interview DATA
Conceptions and identified practices concerning HFE
Mapping to NUREG HFE process
DATA EXTRACTION
DATA INTERPRETATION

Figure 8. The proceeding of data analysis for HFE

5.3 Results: challenges in the design process in the nuclear industry

In the following we discuss the safety related challenges that came up in the interviews that related to the fact that design is a complex process involving several different organizations.

5.3.1 Challenges relating to shared mindset

Many of the challenge statements related to valuing safety. It came up in the interviews that **safety is not always the first and most important guiding value in the design process**. Rather the different actors involved in the design process – including the regulators – are constantly balancing between safety and economics in their work. For example, when making contracts with design organisations, the power companies strive to make a good bargain, as any private company would do. There is quite understandably a temptation not to start the bargaining with explaining all the possible risks and complexities that relate to the design work. However, if this is not done already in the contract phase, it may be difficult to make demands later in the design process. This is how the issue was discussed in one of the interviews:

> *"There are commercial constraints between the supplier and the power company that sometimes are close to the limits of good safety culture […] you are trying to arrive at the cheapest possible price. You won't say there are all these special things. You try to buy the bulk of it and add to that later. This has happened, and it is not proper practice. It would be fair to explain to the subcontractor which special requirements are included, that it will be included in a nuclear power plant et cetera"*

Also the regulators discussed in the interviewees how they were sometimes struggling to take their time to carry out detailed inspections and making demands while realising the strong commercial pressures the companies were struggling with. Also, the tension between safety and productivity was said to hinder the shared learning between companies. One power company representative expressed it like this:

> *"With [company X] we don't have those open discussions as we are kind of competitors so it comes mainly from individual people from there who have transferred to us. In international forums, in my opinion it is quite superficial the discussion with no-one really willing to open up, necessarily."*

5.3.2 Challenges relating to understanding

As mentioned earlier in this report, it is typical in the nuclear industry that the design work is purchased from design organisations outside the actual nuclear power industry. Thus it was brought up strongly in the interviews that **understanding the context where the designed end-product will be utilized may be difficult for the designers and this may lead to dysfunctional designs.** It was mentioned by the interviewees that, for example some of the I&C designers have never been to an operating power plant and might thus not think of some relevant issues in their design work. One of the power company representatives talked about the importance of understanding the operational context like this:

> *"…the same part can function one way in a certain operational situation, and another way in a different operational situation. And there's this risk involved, that you can't picture every situation. But you need to strive for that, that the designer knows, what they are doing. Whether it's our own designer or an outside designer. …You can encounter these situations, that some, for example a testing situation, or a revision, can be different from what you expected. And then the device will no longer function, in the expected manner. For example.. the temperature might change, or something like that."*

Also, the interviewees pointed out that in some countries, the nuclear domain has been developed and in others recessed, so the level of designers' nuclear power specific expertise may vary depending on the country. Thus it was considered important that power company's personnel who guide the design work have solid understanding on functioning of the plant and can communicate this understanding to the designers.

Another challenge relating to understanding that came up strongly in the interviews was that **organisations do not always share the same safety philosophies and understand safety requirements in the same way**. This is especially the case, if the organisations involved in the design process represent different national cultures - as is often the case in the nuclear industry. For example, it was mentioned in the interviews that the Finnish regulator emphasises the principle of continuous improvement much more than regulators in some other countries. If the designers don't understand this principle, they may not design enough buffers for the designed components. This is how one of the power company representatives described this issue:

> *"In some countries it is that when once approved for the operation, you don't have to do almost anything for that plant, unless very drastic and dramatic happens in a generic way, generic for that design. But in Finland (…) you really do have to have this spare capacity or otherwise you will end up with a trouble."*

Also safety philosophies and understandings of the safety requirements may differ between operating organisations and design organisations. Partly this may be due to their inherently different core tasks. For example, while operational personnel may emphasises conservative decision making, designers may focus more on quality issues of their work. The interviewees brought up that not only designers and operating personnel should understand the safety requirements, but the people doing the commercial contracts concerning the design process at the power companies as well.

5.3.3 Challenges relating to structures and processes

In terms of structures and processes it was found in the interviews that **coordinating activities may be difficult between organizations that work according to different logics and understandings.** For example, it was difficult to match the creative and iterative design process with the strict regulatory process. These two sub processes of the wider design process seemed to follow a different kind of time logics. It was brought up that there are constant discussions and negotiations between the power companies and the regulator on this issue. Also, the differences in national cultures came up in this respect. One of the power company representatives described the challenge of coordinating time-tables with the designers of a foreign company as follows:

> *"I must admit personally that the culture, working culture and how they negotiate and so on, it has been quite unclear, sometimes even confusing for me and that is also the learning experience, how to deal with those people. Because unless you don't understand how they feel, how they work, how they act, it will be quite difficult to cooperate with them in time schedule."*

Another challenge relating to structures and processes that was found in the interviews related to **distributing responsibilities and balancing roles between different stakeholders**. Especially the following questions were discussed in the interviews:

- If the design activities are purchased from several subcontractors, who manages the interfaces?
- Should the regulator inspect subcontractors that carry out the design work or only the power company who is the licensee and who purchases the design work from the design organisations?
- How should regulators balance between inspection and giving improvement suggestions in the design process? On the other hand it is important for the regulators to stay in an independent evaluator role, which is their core task. However, how can they not interfere and suggest some directions for the companies when they evaluate

the step-by-step design process in all its stages and see the situation with outsiders' eyes?

5.3.4 Summary of the challenges and discussion

The challenges found in the interviews can be summarised into five main points that connect to three different cornerstones of good safety culture:

1) Safety is not always the first and most important guiding value in the design process and commercial pressures may hinder safety
2) Understanding the context where the design will be utilized may be difficult for the designers and this may lead to dysfunctional designs
3) Safety philosophies may differ between different organizations
4) Coordinating activities may be difficult between organizations that work according to different logics and understandings
5) Distributing responsibilities and balancing roles between different stakeholders needs careful consideration

Many of these challenges are rather general. Similar challenges might be found for example in nuclear power maintenance activities, since both design activities and maintenance activities often involve several organisations (e.g. power company's own personnel and contactor companies) working together in a tight network. For example, commercial pressures between the different organisations is something most people working in the nuclear industry face in in their work in some form. However, some of the challenges, we believe, reflect or are strengthened by the inherent requirements of the design work - the fact that the work is strongly future oriented and deals with an open problem space. For example, what comes to challenge number one, there may be an especially strong need to emphasise the financial aspects in the design process in order to avoid losing control over the budget exactly because the design process can sometimes be so unpredictable. Also, it may be both more important and more challenging for the designers to deeply understand the context for which they are doing their work than e.g. for welders or painters that carry out regular maintenance activities at the power plants. While maintenance is more about fixing or checking some specific parts of the plant and solving delimited problems, designers often need to understand the context in a more multidimensional way in order to develop totally new and functional solutions. Also, the competence required in the design work may be more specialised and uncommon than in maintenance work. Thus the design organisations and the designers working for them may generally be more detached from the overall nuclear power plant context than maintenance workers. Also, as came up in relation to the structures and processes, it may be that the conception of time is somewhat different in design activities when compared to for example regulating activities or maintenance work. The iterative, future oriented creative thinking needed in order to design safe end-products might not easily follow the logics of other highly regulated nuclear power activities and this may cause problems. All in all, as suggested in chapter 4.2 it may be that in supporting safe design it is important to develop a balanced culture that not only provides structures and rules for the work, but also supports creativity, rational decision making and participation in the work community.

5.4 Results: opportunities in the design process in the nuclear industry

A total of 64 opportunities for safety in design were found in the interviews. The cornerstones for enhancing safety in design were represented as follows:

- Mindset and other more mental representations related to opportunities in design: 7 statements

- Understanding of own work and its relation to safety and the complex (systemic) nature of safety in design: 31 statements
- Organisational structures and processes related to opportunities in design: 26 statements

The opportunities related to mindset were underestimated relative to the other ones. This may reflect that mindset, values and norms do not emerge easily in a discussion unless especially sought for and they may also be hard to trace in any case. Another type of interpretation is that the mindset-related opportunities are not represented in the same degree as the other cornerstones for safety. As the interviews were not requiring specifically opportunities in design in general, nor the mindset-type of opportunities in specific, the former interpretation seems to be the more probable one.

On the other hand, the results don't mean that the other factors (understanding and organisational system) would be of ideal state either, as the study was not designed to find answers to such questions. The results should be treated as findings of possibilities that have emerged in the discussion without any emphasise in asking them or discussing about them specifically after they have been expressed.

Most of the opportunities were clearly stated by the interviewee; only four statements were concluded by the analyser. As there are no problems in direct expressions, only the concluded ones are presented in Appendix B to validate the analysis.

Among the 64 opportunities found, 6 were not actual but in the level of an idea. This can be interpreted as a good result as new ideas were not directly asked for in the interviews; the manifestation of new ideas is due to the interview method, theme interview, which made it possible to enlarge the focus of interview questions. It must be remembered, however, that not all such statements are really new but are also plans to be realised in the future.

It was not always possible to evaluate whether the idea was a plan or just ´wishful thinking. Only three statements that could be clearly classified as plans emerged. The rest three statements were expressed in the way it did not become evident that they would be realised in the future. The list of the statements that are ideal (not existing/is planned/ is envisioned) is presented Appendix C.

The analysis performed about the locus in which the opportunity could be or is actualised revealed that most statements were about opportunities that could be realised within the organisation in question. Only 10 statements were about opportunities for safety in design that involved another organisation (5 statements) or both own and other organisation (5 statements), that is, that were inter-organisational opportunities. This can be interpreted as showing at least good mindset for these people from the viewpoint of enhancing safety in design: the opportunity to improve safety in design is perceived to be "in our hands". The result may also reflect the fact that own organisation is known the best. The locus of realising organisation for all statements can be found in Appendix D.

The categories for the origin of opportunity are data based. When classification is raised to a higher level, the categories of personal level, organisational level and national and international level are found. The organisational level as the source or opportunity is clearly standing out.

This reflects probably the fact that own organisation is known the best. On the other hand, it could be assumed that own competence is known better than organisational practises so that the personal level should be emphasised. One possibility is that people are not eager to emphasise their own expertise, the strive for modesty is perhaps still regarded as a virtue in Finland. Additionally, as the interviews were conducted within the context of work, interviewees may have borne the big picture of the work context in mind, according to which the input of one person does not become the most relevant when considering all possibilities the practises, structures and processes the organisation makes possible. The detailed results of the origin of the expressed opportunity can be found in Appendix E.

5.4.1 Opportunities relating to shared mindset

For the sake of clarity, the expressed opportunities are classified further so that they can be discussed more easily. Mindset-related statements are here further categorised into the following classes:

- Person expresses safety-enhancing attitude
- Openness and discussions are executed among parties
- Safety-enhancing support is given also when not required
- New people enter the industry

The mindset-related opportunities, even if small in numbers, represent quite a lot variety in their content. One set of safety-enhancing mindset is related to communication – expressing safety-enhancing attitudes or having discussions. An example of this is this quotation:

> *"If we have a cross-technological problem, we will have discussions afoot in no time-from the coffee table to more official discussions. That is one of our strengths*".

Another type is a practise of offering support also when it is not required. Finally, it was stated that new people entering the industry – it represents an opportunity as new people can have a fresh and safety-supporting mindset which affects, in turn, in the safety culture of surrounding people and organisation.

5.4.2 Opportunities relating to understanding

Statements related to understanding are here further categorised into the following classes:

- Personal and organisational competence is acquired by experience
- Personal competence is acquired by the perspectives relevant to own task
- Understanding has grown due to widening of the human-factors perspectives in the domain
- Limitations (own and others') are understood and acted upon
- Limitations in guides is overcome by personal/organisational competence
- Cooperation with another type of company widens understanding
- Cooperation among different professionals (users and designers) benefits understanding
- The effect of people's safety orientation in spreading safety orientation is understood
- New tasks in the area of human factors widen safety perspective
- Safety is understood due to safety-specific work role
- Safety is "sold" to another party in practises in an anticipatory manner
- Safe working principles in error correction are assumed
- Safety orientation is not lost with retiring personnel but is transferred to younger professionals

Opportunities related to understanding own work and its relation to safety is a subject that was often met in interviews. Such opportunities relate to personal, organisational or domain-related competence that originates from the development or that domain or from experience as a whole or a safety—relevant task. Limitations are understood and handled appropriately; cooperation is exercised; the value of individual attitudes are understood as affecting safety in general; and finally, specific activities are performed, showing that safety is understood, such as safety is "sold" to another party in situations where it has been proved difficult, error correction is performed in a safe manner; and the safety orientation is transferred from retiring to younger professionals.

As an example of expressed opportunities related to understanding, one interviewee stated how a wider perspective in safety issues can be obtained by learning these things from other context:

> *"But, I think, perhaps I could use some information that I, some, something I learned in these other projects that I can use when I, in these nuclear related projects and, you.."*

5.4.3 Opportunities relating to structures and processes

Statements related to structures and processes are here further categorised into the following classes:

- Finnish requirements for safety are strict and include also human-factors
- Finland has a principle and practise of continuous development
- Safety-promoting departments and other structures can be established in a NPP
- Safety-promoting processes and practises for learning are/can be established
- Good practises are used in recruiting people
- Good practises in design projects (traceability and planning) are developed
- Multifaceted safety monitoring and evaluation practises are/can be used
- Working in a team makes it possible to take several viewpoints into account
- Discussions (the sharing of viewpoints) are promoted
- Good practises related to error correction exist
- It is certified that local practises are taken into account in design
- Other professional organisations to support safety are used when needed

As a whole, the opportunities found in interviews range from Finnish requirements and principles to developing departments and permanent processes in the organisation in a quite general level (such as assuming good practises for recruiting people) to more detailed practises, closer to the everyday performance such as working in a team or using multifaceted safety and evaluation practises.

5.4.4 Discussion of the opportunity-related results

Results reflect opportunities for design as they appear in the design organisation and especially in the network having a touch point with design. The parties in current study have been operating organisations, affecting design with requirements, in planning, verification and validation of design; national regulator setting general requirements and inspecting design, and certifying organisation certifying the quality of design.

Regarding the actual classification, most opportunities revealed concentrating on factors of (1) understanding work and (2) organisational systems and practises. This may reflect the fact that safety-enhancing (3) mindset, values and norms do not emerge easily in a discussion unless especially sought for. This was the case in present interviews where opportunities in design was not a theme to be asked from all interviewees. Additionally, mindset-related matters may be hard to trace in any case. Still one interpretation is that they are not so strong in the organisations that were investigated. In this case it is credible to assume mindset is not emphasised in the results because it is hard to evaluate one's own mindset and such things do not become conscious unless especially called for.

However, mindset is an important determinant for maintaining the readiness for appropriate action in a situation (resilience) and it also affects decisions that may have long-lasting effects. Thus, mindset should not be forgotten in safety-promoting design activities in organisations. The results don't mean either that other factors (understanding and organisational systems) would be of ideal state as the study was not designed to answer such a question.

Most statements related to existing values, understanding, systems etc., not ideal ones, and were about matters that are realised in own organisation. This is an understandable result and also shows realism in conceptions – e.g. no wishes for another organisation to act were emphasised.

5.5 Results: Human Factors Engineering

The topic of HFE was addressed in altogether 10 interviews covering all the participating organizations.

5.5.1 Reported HFE conceptualizations and practices

In the interview data there were somewhat different conceptualizations of what actually constitutes HFE. The conceptualizations can be divided into two main classes:

1. HFE is about designing human system interfaces (HSI)
2. HFE is (also) a quality control process of design in general

These classes of conceptualizations were interpreted and derived from the interview answers to the HFE related questions. It was evident that none of the participating organizations had their own specific definition of what HFE means. The regulator and two power companies shared the conceptualization 1 and one power company represented the conceptualization 2.

The conceptualization 1 stating that HFE is about designing human system interfaces and control rooms was evident in some of the interviews of the representative of the power companies. When asked about the how human factors are/should be taken into account in design, they immediately considered design of control rooms in particular. Below is an interview quote representing conceptualization 1 from a power company:

> *"We have acknowledged that it [taking human factors into account in design] is an area that we should improve if, we're talking about HF's then, of course, we should perhaps have, specific resources for designing the control room and the control system, that would only focus at this stage together with the plant suppliers on going through what they plan to do on this front to optimise things"*

In the regulator interviews the issue was addressed in connection to reviews that the regulator conducts. It was discussed whether the material sent in for review contains the perspective of usage or operations to be considered in the safety review. An interview quote representing conceptualization 1 from the regulator:

> *Q:"So operation is not a perspective used in automation inspections?"*
>
> *A:"No, we have a separate group for looking at the operating side of things. Some people in the automation office are able to look at the user interface and operating side. Now we have the simulator as well. However, the YVL guidelines do not set many requirements on operation, the user interface or the control room, which is a deficiency."*

In another quote a regulator representative expressed that Human Factors is a separate issue from Safety inspections:

> *"This side of things [effect on operation] does not really show to us directly in any of the system alteration materials that we receive. How they would've been considered in*

> *the design. If you think purely of –as we should do– safety at the plant, for us a system where the operator has to run all over the facility to use the system could be just as safe from our point of view as some more user-friendly solution. In that sense, the materials delivered to us don't really present these matters at all. And I'm not so sure they should, either. If you think purely about our safety requirements. In that sense you don't really even need to present that information to us."*

The conceptualization 2 which considers HFE as a more general quality related matter was expressed in all the interviews of one particular power company. An interview quote representing conceptualization 2 of HFE from a power company:

> *"I think it's more that, for example in larger projects well we have to consider beforehand where we need which types of resources, we have to create the plan beforehand, where we're going to get them from and how we're going to train them. How will we keep them in the project, at what point will we need the users, at what point the maintenance people and so on and so forth."*

None of the organizations had defined their own particular HFE processes. Most of the representatives recognized this as an area of improvement which should be treated in the future. For example a power company representative expressed that the concept of ergonomics is not really fully developed in the organization:

> *"The first goal of Human Factors Engineering is that the ergonomics requirements must be fulfilled. Just so. I think it is a simple way to put it but contains a lot of meaning. A lot still needs to be done before the concept of ergonomics is understood as widely as it should be understood today. Back in the day, in a control room from the Chaplin era, it was a pretty simple thing. Nowadays cognitive ergonomics are very heavily involved, as well as organisational ergonomics."*

A mapping of the interview remarks concerning HFE was made to the HFE process and activities model presented in NUREG-0711. This was a simple analysis in which it was recognized which activities the interviewees brought up when practices of HFE were asked about. The result of the mapping is presented below (Figure 9). It shows that not all the activities identified by NRC in the guideline were mentioned in the Finnish interviews. The activities which were mentioned are: staffing and qualification, treatment of important human actions, HSI design, training program development, and HFE verification and validation. This consideration of the scope of HFE activities may well be a reflection of the conceptualization of HFE being related mostly to control room design. However, the fact that e.g. operating experience review and human performance monitoring were not considered reflects that perhaps the linkages from these activities to design are un-specified in the organizations.

The somewhat narrow scope demonstrated for HFE in the interviews may of course be a reflection of the scope of the design interviews conducted in general. It is also possible that the particular interviewees were not aware of the full scope of HFE in the respective organization.

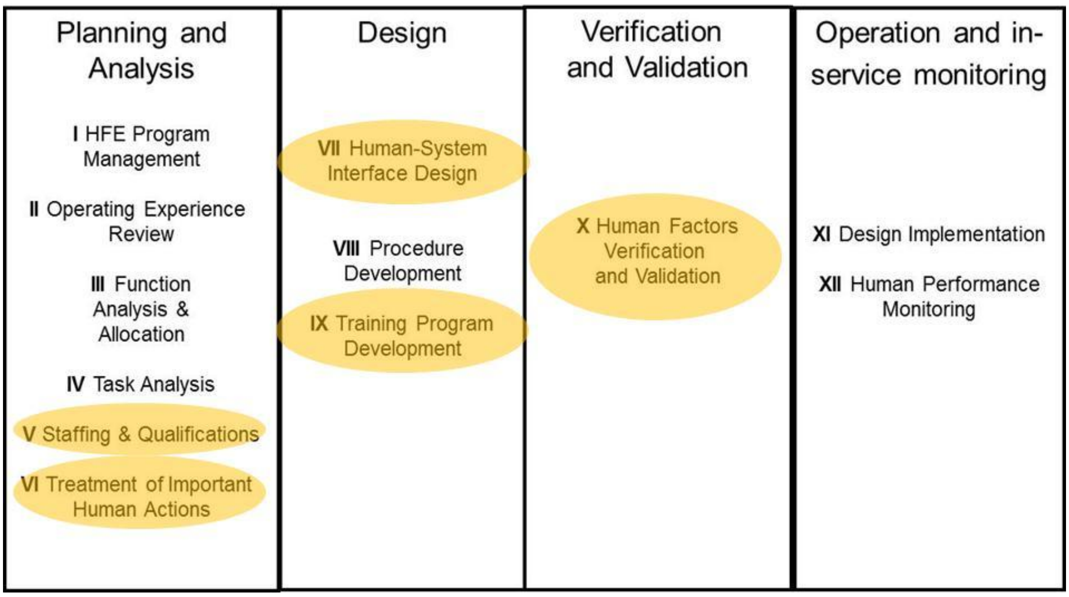

Planning and Analysis
I HFE Program Management
II Operating Experience Review
III Function Analysis & Allocation
IV Task Analysis
V Staffing & Qualifications
VI Treatment of Important Human Actions
Design
VII Human-System Interface Design
VIII Procedure Development
IX Training Program Development
Verification and Validation
X Human Factors Verification and Validation
Operation and in-service monitoring
XI Design Implementation
XII Human Performance Monitoring

Figure 9. The scope of HFE reported in the interviews. The NUREG-0711 Figure 8. The proceeding of data analysis for HFE activities which were mentioned by the interviewees when discussing HFE, are marked with colour orange.

5.5.2 Discussion and conclusions concerning HFE

Based on the interviewees conducted in the Finnish nuclear community, it is evident that the maturity of organizations concerning HFE varies. As even the conceptualisation of what constitutes HFE varies between organisations it is not necessarily sure that organizations are addressing the same issues when they are discussing HFE related matters. For this purpose the adoption of concept as it is defined in the international literature (e.g. NUREG-0711) could provide a starting point.

As none of the organizations had clear and shared conceptualizations of what constitutes HFE, and as there were no defined processes concerning it, there is clearly room for development. The organizations viewpoint to HFE varies depending on how involved they are in the design and review of the plant, its systems, and components. Regardless of the different viewpoints all the nuclear organizations have some kind of relation to design and thus they should also have a process of adopting human factors knowledge in the design process i.e. a HFE process.

The NUREG-0711 may be applied as a starting point for developing HFE processes in the organizations. Activities defined in the guideline may be interpreted to be part of good safety culture in design because they aim to foresee the potential consequences of the products already during the design phase. However, the NUREG-0711 process is quite heavy and involves wide participation from the organization. In some cases this may be necessary but it must be acknowledged that a HFE process should always be graded according to the scope and safety significance of the particular design object.

One of the topical issues in development of HFE is the connection to the technical design. Even the NUREG-0711 does not take a stance concerning how the interaction between e.g. automation and control room design should be handled. It is clear that both design process influence one another but the identification of the specific interaction points would require further knowledge concerning best practices.

6. The Fukushima accident from the network safety culture perspective

In this chapter we discuss the Fukushima nuclear power accident that took place in Japan in 2011. We explore it based on the review of the following seven accident analysis reports:

- The National Diet of Japan The official report of the Fukushima Nuclear Accident Independent Investigation Commission (2012)
- The Tokyo Electric Power Company, Inc. (2011). Fukushima Nuclear Accident Analysis Report. (Interim Report).
- The Tokyo Electric Power Company, Inc. (2012): Fukushima Nuclear Accident Analysis report. Summary.
- IRSN, (2012) Fukushima, one year later Initial analyses of the accident and its Consequences Report IRSN/DG/2012-003
- Carnegie Endowment for International Peace (2012). Why Fukushima was preventable
- Epstein, S. (2011) A Probabilistic Risk Assessment Practitioner looks at the Great East Japan Earthquake and Tsunami. A Ninokata Laboratory White Paper. Tokyo Institute of Technology
- USNRC (2012. Enhancing Reactor Safety in the 21st Century. The near-term task force review of insights from the Fukushima Daiichi accident.

The reports dug into the multiple causes that contributed to the accident. Technical aspects and human and organisational factors were addressed in the reports, and recommendations for improving safety in nuclear power plants by different authorities and experts were issued. The identified issues range from improving the regulatory framework to ensure adequate protection based on the defence-in-depth principle (USNRC, 2011) to strengthening the company risk management (e.g. TEPCO, 2012), from improving the performance of technical equipment during the accident (e.g. TEPCO, 2011, 2012) to addressing human and organisational factors of TEPCO, the Japanese regulatory body and of the Federation of Electric Power Companies (The National Diet of Japan - The Fukushima Nuclear Accident Independent Investigation Commission, 2012). Needs for future research to improve nuclear safety and emergency management have also been identified (IRSN, 2012).

For the scope of this report, we want to focus our review of the accident analysis reports in the light of the network safety culture approach and the results of the interview study described in chapter 5. We do not want here to discuss the appropriateness of the technical solutions adopted at the Fukushima power plants *per-se*, but rather to illustrate how some of the challenges emphasised by the network safety culture approach (chapter 4.4) and identified in the interview study (chapter 5) contributed to the implementation of dysfunctional design for protecting the plant from tsunamis.

6.1 Description of the Fukushima accident

In the following we describe briefly the accident that took place in Fukushima. We describe the event as it was presented in the accident analysis report conducted by the responsible power company Tokyo Electric Power Company (2011, 2012).

The Fukushima Daiichi nuclear power plant is located on the Pacific coast of Fukushima Prefecture in Japan. The power station has six boiling water reactors (BWRs) that started their commercial operations in 1970’s. The Fukushima Daini nuclear power plant is located approximately 12 km south of the Fukushima Daiichi power station. It has four BWRs that started operation in 1980’s.

On March 11 2011, units 1, 2 and 3 of the Fukushima Daiichi power plant were in operation. Units 4 to 6 were shut down for periodic inspection outage. At Fukushima Daini Nuclear power plant all four units were in operation. At 14:46, due to the Tohoku-Chihou-Taiheiyo-Oki Earthquake, the largest earthquake ever recorded in Japan, all of the operating reactors were automatically shut down. At Fukushima Daiichi power plant, all the off-site power supply was lost due to the earthquake. However, electric power necessary to maintain reactor safety was kept with the emergency diesel generators. On the other hand, at Fukushima Daini, off-site power supply was not lost.

Later, at the Fukushima Daiichi, the subsequent arrival of the large tsunami caused by the earthquake caused flooding of cooling seawater pumps, emergency diesel generators and power panels. The size of the tsunami was M9.1 on the tsunami magnitude. It was the fourth-largest tsunami ever recorded in the world and the greatest tsunami to reach Japan. It caused the black out of Fukushima Daiichi units 1-5. All cooling functions using AC power were lost in these units. Also, due to the flooding of the cooling seawater pumps by the tsunami, the function of the auxiliary cooling system to remove residual heat from the reactor to the sea was lost. In addition, at units 1 to 3, the loss of DC power resulted in the sequential shut down of core cooling functions which were designed to be operated without AC power supply. An alternative water injection of freshwater and seawater using fire engines through the fire protection line was conducted as a flexible applied action. However it turned out, that the water could not be injected into the reactor pressure vessels in units 1 to 3 for a certain period of time. Consequently, the fuel in each unit was exposed from water, and the fuel cladding was damaged. The radioactive materials in the fuel rods were released into the reactor pressure vessels, and the chemical reaction between the fuel cladding and steam caused the generation of a substantial amount of hydrogen. This caused the release of radioactive materials and hydrogen from the reactor pressure vessels into the primary containment vessels through the main steam safety relief valves, and the internal pressure of the primary containment vessels increased. In units 1 and 3, the pressure of the primary containment vessels decreased through venting operations (the operation in which gas inside the primary containment vessel is discharged into the atmosphere in order to prevent damage to the vessel). However, in unit 2, the pressure decrease of the primary containment vessels through the venting was not confirmed. Later, in units 1 and 3, explosions which appeared to be caused by hydrogen leakage from the primary containment vessels, destroyed the upper structures of their reactor buildings. In addition, another explosion occurred at the upper structure of the reactor building in unit 4 where all the fuel had been removed from the reactor and stored in the spent fuel pool.

In Fukushima Daiichi units 5 and 6, one of the emergency diesel generators for unit 6 was in operation. By tying a power cable to unit 5, water could be supplied into the core of both units. After the recovery of the residual heat removal function from the reactor to the sea, units 5 and 6 reached cold shutdown. At the Fukushima Daini, off-site power was continuously supplied and the scale of the tsunami was relatively small compared to the Fukushima Daiichi. As a result of emergency responses, such as the restoration of temporary power of the emergency seawater system, cold shutdown was achieved for all the units there. However, at the Fukushima Daiichi units 1 to 3, the accident escalated and developed into a serious nuclear disaster.

6.2 Network safety culture aspects contributing to the Fukushima accident

The network safety culture approach described in chapter 4 and utilised in the interview sutyd (chapter 5) project led to the identification of five major challenges that may affect the design process in the nuclear industry. The identified challenges are:

1) Safety is not always the first and most important guiding value in the design process and commercial pressures may hinder safety
2) Understanding the context where the design will be utilized may be difficult for the designers and this may lead to dysfunctional designs
3) Safety philosophies may differ between different organizations
4) Coordinating activities may be difficult between organizations that work according to different logics and understandings
5) Distributing responsibilities and balancing roles between different stakeholders needs careful consideration

The significance of these challenges with respect to the design process and how they may have played a role in the Fukushima is exemplified through some of the conclusions reached in the accident analysis reports.

In the aftermath of the accident that occurred on March 11 2011 it became evident that the height of the wall constructed to protect the Fukushima Daiichi power plant from the effects of a large tsunami was not sufficient to avoid flooding of cooling seawater pumps, emergency diesel generators and power panels which should have provided the cooling of the core.

The decision to build a 5.7 meters high wall for protecting the Fukushima Daiichi Unit No.1 from tsunamis is rooted in the 1960s. The supplier and designer for the nuclear power plant was the American company General Electric. The architectural design was developed by the American company Ebasco. The construction was carried out by the Japanese Kajima. The tsunami wall, intended to protect the power plant from the effects of large tsunamis, was constructed in 1966. The original design basis tsunami was estimated to have a maximum height of 3.1 meters above mean sea level. One of the official reasons for that decision was the calculation of the appropriate height of the wall based on a tsunami wave of that height hitting Fukushima cost after an earthquake off the coast of Chile in 1960 (TEPCO, 2011, 2012). In order to build the plant upon the solid bedrock, the construction site of the Fukushima Daiichi plant was excavated. Before starting the construction of the buildings, the altitude above sea level of the construction site was lowered by 25 meters above. This resulted in locating the seawater intake buildings at 4 meters above sea level and the main plant buildings at 10 meters above sea level. The decision of doing so was due to the need to protect the facility against earthquakes. The decision to build the plant on the bedrock was sound with respect to standards and regulation concerning protection from severe earthquakes. Nevertheless the decision to reduce the altitude above sea level was a risky one with respect to protection from tsunamis. This solution also resulted in a cost reduction of building construction and of seawater pumps (Epstein, 2011). In 2002, on the basis of a new methodology for assessing tsunami safety developed by the Japan Society of Civil Engineers, TEPCO voluntarily re-evaluated the tsunami hazard and adopted a revised design-basis tsunami height of 5.7 meters. However, the actual maximum height of the tsunami that hit the plant should have been 13.1 meters, more than twice the revised design basis.

It is possible to relate the decision about the height of the tsunami wall to **insufficient understanding of the operational context of the plant**. Despite that IAEA recommends the collection of data on prehistorical and historical earthquakes and tsunamis in the region of a nuclear power plant, both TEPCO and NISA (Nuclear and Industrial Safety Agency) have been criticised for not giving sufficient attention to historical evidences of severe earthquakes and tsunami in the area (Carnegie Endowment, 2012). Epstein (2011) reports the following statement of Dr. Ryohei Morimoto, emeritus professor of geology at Tokyo University: "*I've heard the government and TEPCO say they couldn't predict the tsunami would reach that high, but that is ridiculous, as any history book would have set them straight and even if they could not predict, they should have been prepared for waves similar to the past*". Carnegie

Endowment (2012) suggests that both TEPCO and NISA should have taken into consideration the historical record of tsunamis in Japan and have defined the design-basis requirements taking into consideration that for example since 1498 six tsunamis higher than 10 meters and six higher than 20 meters stroke Japanese costs.

Different safety philosophies also played a role in the design of measures to protect the plant from tsunamis. The methodology applied to perform the tsunami analysis was the one approved by the Japan Society of Civil Engineers and accepted by NISA as a standard. Nevertheless the choice of using that methodology has been questioned by PRA practitioners (Epstein, 2011). The adopted methodology is based on a deterministic approach for risk assessment, while a probabilistic approach was going to be approved by the end of 2011 and therefore the latter was not adopted in the tsunami analysis. In this respect The Fukushima Nuclear Accident Independent Investigation Commission, (2012) states that: *"TEPCO also argued that basing any safety assessment against tsunami on a probabilistic approach would be using a methodology of technical uncertainties, and used that argument to postpone considering countermeasures for tsunami."*.

The Fukushima Nuclear Accident Independent Investigation Commission, (2012) pointed out how **safety was not always the guiding value** of TEPCO management: "*The reason why TEPCO overlooked the significant risk of a tsunami lies within its risk management mindset — in which the interpretation of issues was often stretched to suit its own agenda- […] Rather than considering the known facts and quickly implementing counter measures, TEPCO resorted to delaying tactics, such as presenting alternative scientific studies and lobbying."*

Roles and **responsibilities of different stakeholders** of the Japanese nuclear business also influenced the design of protection measures for tsunami risks. The Japanese regulator body NISA has been criticised in the aftermath of the accident for its attitude towards tsunami risks. Japan's Nuclear Safety Commission issued guidelines (NSC, 1990) for protecting from earthquake hazards. Specific guidelines for protecting the plants from tsunami hazards were never published and this was addressed by stating that "[the effect by] *tsunami should be considered in design*" (Carnegie Endowment, 2012).

The Fukushima Nuclear Accident Independent Investigation Commission of the Diet of Japan highlighted the ineffective role of the Japanese regulator in setting new regulations and in ensuring their respect. TEPCO opposed the introduction of new safety regulations which would have interfered with plant operations and negotiated with NISA and NSC via the Federation of Electric Power Companies (FEPC). An indication of the insufficient fulfilment of the responsibilities as regulator is represented by NISA's failure to update the licensing documents for the plant following the voluntary change of design-basis of the tsunami wall (Carnegie Endowment, 2012). NISA' s reluctance in actively introducing and updating regulations is explained by the Fukushima Nuclear Accident Independent Investigation Commission as resulting from a strong belief in the safety of Japanese nuclear power plants. In addition, the regulatory body was part of the Ministry of Economy, Trade & Industry (METI), which has been actively promoting nuclear power.

7. Conclusions and discussion

Design is a practise that depends upon, integrates, and transforms heterogeneous domains of knowledge (Mark et al., 2007). This is especially true in the nuclear power context where design often requires highly specialised expertise and where the designed components are usually tightly coupled i.e. they come with several interfaces to other designed products. As design in the nuclear industry inherently involves multiple stakeholders with multiple tasks and responsibilities, the safety culture approach and – more broadly – the network safety culture approach can be considered especially relevant for improving the safety of design.

Design is also inherently a dynamic, creative cognitive act. Design is about navigating in an open problem space. As Veland (2010) states, the designers in the nuclear industry need to "think on their feet" and immerse in active, flexible, reflective exploration of the problem space. From this it follows that in order to create safe and functional end-products it is not enough to provide strict guidelines and supervision. Rather, it can be suggested that in supporting safe design it is important to develop a balanced culture that not only provides structures and rules for the work, but also supports creativity and participation in the work community. A good design safety culture does not only mean strict rules and regulations and obedience. It means an informed culture, where all the relevant actors understand the hazards related to the activities and are able to see how their own work connects to the big picture. It also means that all the relevant actors consider nuclear safety an important aspect of their work and are motivated by it and take responsibility for the overall functioning of the plant in which the designed component will be used. This responsibility also needs to be taken in a long-term way as the designed components will often be used for decades. All the relevant actors also need to be mindful in their practices. That is, they need to be constantly aware of the possibility that something surprising will turn up. There also need to be such systems and structures in place that create good preconditions to work with good quality.

How well is the nuclear industry doing in these terms then? One unfortunate example that calls for improvements in design safety culture is the Fukushima nuclear power accident. Some of the accident analysis reports point to the aspects and contributing factors that were raised up as challenges in the Finnish interview study presented in chapter 5 of this report.

The interview study described in this report revealed five main safety culture challenges relating to the interactions between the organisations in the design network. These challenges need to be solved or rather taken into account and continuously balanced between in everyday design activities. Many of the challenges identified in the interviews are rather general - similar challenges could be found in other nuclear power activities as well. However, some of the challenges most likely reflect or are strengthened by the inherent requirements of the design work - the fact that the work is strongly future oriented and deals with an open problem space.

From the interviews we also concluded a long and versatile list of opportunities in design. It seems that remedies for the challenges exist but they may locate in separate organisations, not meet each other, or the opportunities may not always be used as efficiently and systematically as possible. Additionally, the challenges can be so demanding that no single opportunity can support meeting it effectively enough. The list of opportunities drawn from the interviews can be used as a starting point to open up new ways to build solutions to support the design process.

In Table 3, the challenges and opportunities can be perceived in one glance, classified according to the cornerstones of good safety culture. A specific challenge, say, difficulty in understanding the context where the design will be utilized (category "Understanding"), might be mitigated by an opportunity of the same category, say, using people who have competence in this matter by experience, but also by an opportunity of some other category, for instance, openness and discussions that are executed among parties (category Mindset). Thus, the challenge list describes usual demands in the network contributing design, and the opportunity list describes means for tackling these challenges, means that can be used alone or as a set gathered from different categories.

In terms of HFE practices the interview study described in this report evidence that conceptualization of what constitutes HFE varies between organizations. Another finding is that the level of maturity concerning HFE in the organizations is not as high as described in international guidelines. These things need further attention and clarification in the future.

Table 3 - Challenges and opportunities presented side by side

CHALLENGES	OPPORTUNITIES
Mindset • Safety is not always the first and most important guiding value in the design process • Coordinating activities may be difficult between organizations that work according to different logics and understandings	**Mindset** • Person expresses a safety-enhancing attitude • Openness and discussions are executed among parties • Safety-enhancing support is given also when not required • New people enter the industry
Understanding • Understanding the context where the design will be utilized may be difficult for the designers and this may lead to dysfunctional designs • Safety philosophies may differ between organizations	**Understanding** • Personal and organisational competence is acquired by experience • Personal competence is acquired by the perspectives relevant to own task • Understanding has grown due to widening of the human-factors perspectives in the domain • Limitations (own and others') are understood and acted upon • Limitations in guides is overcome by personal/organisational competence • Cooperation with another type of company widens understanding • Cooperation among different professionals (users and designers) benefits understanding • The effect of people's safety orientation in spreading safety orientation is understood • New tasks in the area of human factors widen safety perspective • Safety is understood due to safety-specific work role • Safety is "sold" to another party in practises in an anticipatory manner • Safe working principles in error correction are assumed • Safety orientation is not lost with retiring personnel but is transferred to younger professionals
Structures and processes • Distributing responsibilities and balancing roles between different stakeholders requires careful consideration	**Structures and processes** • National requirements for safety are strict and include also human-factors • There is a national principle and practise of continuous development • Safety-promoting departments and other structures can be established in a NPP • Safety-promoting processes and practises for learning are/can be established

	• Good practises are used in recruiting people • Good practises in design projects (traceability and planning) are developed • Multifaceted safety monitoring and evaluation practises are/can be used • Working in a team makes it possible to take several viewpoints into account • Discussions (the sharing of viewpoints) are promoted • Good practises related to error correction exist • It is certified that local practises are taken into account in design • Other professional organisations to support safety are used when needed

7.1 Directions for future research

This study was an opening to a complex and understudied research area. The different possible theoretical perspectives on design presented in this report as well as the challenges and opportunities identified in the interview study provide direction for future research. The study covered a wide scope of different types of design processes starting from small component design and ending in design of new power plants. It aimed in providing general understanding on the design activities from the safety culture perspective. In the future more contextual studies focusing on specific design projects will help to understand the challenges and opportunities better and developing practical solutions to support the interaction between the design actors.

The interview study described in this report was limited in terms of the number of interviewees. Even more so, the study only involved a few interviewees that carry out the actual hands-on design work. In the future understanding the designers' perspective – especially the perspective of those designers that do their work for the nuclear industry as subcontracting and might not be that familiar with the industries' context and shared principles - is important.

References

Argrys, C., Schön, D.A., (1978). Organisational learning. Reading MA: Addison-Wesley.

Argrys, C., Schön, D.A., (1996). Organisational learning II. Theory Method and Practice, Reading MA: Addison –Wesley.

Aspelund, K. (2006) The design process. Fairchild publications: USA

Brehmer, B. (1991). Distributed Decision making: Some Notes on the Litterature. In Distributed decision making: cognitive models for cooperative work. J. Rasmussen, B Brehmer and J Leplat.(eds.) New technologies and work series, John Wiley and sons.

Carnegie Endowment for International Peace (2012). Why Fukushima was preventable. Available at: www.CarnegieEndowment.org/pubs.

Colley, S.K., Lincolne, J., Neal, A., (2013). An examination of the relationship amongst profiles of perceived oraganizational values, safety climate and safety outcomes.

Durfee, E.H., Lesser, V.R., (1988). Using partial global plans to coordinate distributed problem solvers. In A.H., Bond and L.Glasser (eds.). Readings in Distributed Artificial Intelligens. San Mateo, California: Morgan Kaufman, 268-284.TT

Durfee, E.H., Lesser, V.R., Corkhill, D.D., (1989). Trends in cooperative distributed descision making. IEEE Transactions of Knowledge and Data Engineering 1, 63-68

Epstein, S. (2011) A Probabilistic Risk Assessment Practitioner looks at the Great East Japan Earthquake and Tsunami. A Ninokata Laboratory White Paper. Tokyo Institute of Technology

Fleming, M. (1999) Safety Culture Maturity Model. UK HSE Offshore Technology Report OTO 2000/049, HSE Books, Norwich.

Gordon, R., Kirwan, B. (2004). Developing a safety culture in a research and development environment: Air Traffic Management domain. Europe Chapter of the Human Factors and Ergonomic Society conference, October 27-29, 2004. EUROCONTROL Experimental Centre, BP 15, Bretigny-sur-Orge, F-91222 ,France.

Gotheva, N., Oedewald, P., Reiman, T. & Pietikäinen, E. (2012). Enhancing network safety through network governance, shared understanding and interfirm heedfulness. In Proceedings of the 11th International Probabilistic Safety Assessment and Management Conference and The Annual European Safety and Reliability Conference, Helsinki, Finland 25–29 June.

Guldenmund, F. (2010). Understanding and Exploring Safety Culture. Uitgeverij Boxpress, Oisterwijk.

Hale, A., Borys, D., (2012). Working to rule, or working safely? Part 1: A state of the art review. Safety Science (in press).

Hale, A., Borys, D., (2012). Working to rule, or working safety? Part 2; The management of safety rules and procedures. Safety Science (in press).

Hoffman, R.R., & Woods D.D. (2011) Beyond Simon’s Slice: Five Fundamental Trade-Offs that Bound the Performance of Macrocognitive Work Systems. IEEE Intelligent Systems, vol. 26, no. 6, 2011, pp. 67–71

Hollnagel, E. (2004). Barriers and Accident Prevention. Ashgate. England.

Hollnagel, E., Woods, D.D., & Leveson, N. (red.). (2006). Resilience Engineering Concepts and Precepts. Farnham: Ashgate

Hollnagel, E., Paries, J., Woods, D. D., & Wreathall, J. (red.) (2011). Resilience engineering in practice: A guidebook. Ashgate

Hoffman, R. R. and Woods, D. D. (2011). Simon's Slice: Five Fundamental Tradeoffs that Bound the Performance of Human Work Systems. 10th International Conference on Naturalistic Decision Making, Orlando FL.

IAEA (1986) Report on the Post-Accident Review Meeting on the Chernobyl Accident, Safety Series No.75-INSAG-l, IAEA, Vienna (1986)

IAEA, (1991) Safety Culture (Safety Series No. 75-INSAG-4) International Atomic Energy Agency, Vienna.

IAEA (2007) IAEA safety glossary. Terminology used in nuclear safety and radiation protection. 2007 edition. Vienna : International Atomic Energy Agency.

IAEA (2012). Safety of nuclear power plants: design. Specific safety requirements No. SSR-2/1. International Atomic Energy Agency, Vienna

IRSN, (2012) Fukushima, one year later Initial analyses of the accident and its Consequences Report IRSN/DG/2012-003

Kennedy, R.,Kirwan, B., (1995) The failure mechanisms of safety culture. In: Carnino, A. and Weimann, G., Editors, 1995.

Leveson, N.G. (2004). A new accident model for engineering safer systems, Safety Science, 42:(4), 237-270.

Leveson, N.G. (2011). Engineering a safer world. Systems thinking applied to safety. "Draft – complete but undergoing professional editing". Aeronatics and Astronautics and Engineering Systems Division. Massachusetts Institute of Technology. Available http://sunnyday.mit.edu/safer-world/safer-world.pdf [2011-08-29].

Mark, G., Lyytinen, K., & Bergman, M. (2007). Boundary objects in design: An ecological view of design artifacts. Journal of the Association for Information System, 8(1), 34.

Morgan, G., (1986). Images of organisations. Sage Publications,London.

Norros, L. (2004). Acting under Uncertainty. Core Task Analysis in ecological study of work. Espoo: VTT Publications: 546. (http://www.vtt.fi/inf/pdf/publications/2004/P546.pdf)

Oedewald, P., Pietikäinen, E. & Reiman, T. (2011). A guidebook for evaluating organisations in the nuclear industry - an example of safety culture evaluation. SSM. Available at: http://www.stralsakerhetsmyndigheten.se/Global/Publikationer/Rapport/Sakerhet-vid-karnkraftverken/2011/SSM-Rapport-2011-20.pdf

O'Hara, J.M., Higgins J.C., Persensky, J.J., Lewis, P.M., Bongarra, J.P. (2012) Human Factors Engineering Program Review Model (NUREG-0711, Revision 2). Brookhaven National Laboratory Energy Sciences and Technology Department, Upton, NY 11973-5000

Parker , S.K., Turner, N., Griffin, M.A., (2003). Designing healthy work. In Hoffman, D.A., Tetrick, L.E. (Eds.). Health and Safety in Organisations: A Multilevel Perspective. Jossey-Bass, California, p. 91-130.

Perrow, C. (1999). Normal Accidents. Living with High-Risk Technologies. [Rev. ed.] Princeton, NJ: University Press, Princeton.

Pidgeon, N.,O'Leary, M. (2000) Man-Made Disasters: why technology and organizations (sometimes) fail. Safety Science, 34, 15 - 30

Ponis, S. & Koronis, E. (2012) Supply chain resilience. definition of concept and its formative elements. Journal of applied business research, 28, 921-929.

Pryke, S. (2012). Social Network Analysis in Construction. Wiley.

Quinn, R.,E., Rohrbaugh, J., (1983). A spatial model of effectiveness criteria: towards a competing values approach to organisational analysis. Management Science 29, 363-377.

Quinn, R.E., Spreitzer, G.M., (1991). The psychometrics of the competing values culture instrument and an analysis of the impacts of organisational culture on quality of life. Research in Organizational Change and Development 5, 115-142.

Rasmussen, J. (1997). Risk management in a dynamic society: a modeling problem. Safety Science, 47, 183-213.

Reason, J. (1998) Achieving a safe culture: theory and practice Work and Stress, 12, 293 - 306

Reiman, T. & Oedewald, P. (2009). Evaluating safety-critical organizations – emphasis on the nuclear industry. SSM. Available at: http://www.stralsakerhetsmyndigheten.se/Global/Publikationer/Rapport/Sakerhet-vid-karnkraftverken/2011/SSM-Rapport-2011-20.pdf

Reiman, T., Pietikäinen, E., Kahlbom, U., & Rollenhagen, C. (2010). Safety Culture in the Finnish and Swedish Nuclear Industries – History and Present. NKS-213. Roskilde: Nordisk kärnsäkerhetsforskning. Available <http://www. nks.org/download/nks213_e.pdf>.

Reiman, T. Pietikäinen, E., Oedewald, P. & Gotcheva, N. (2012). System modelling with the DISC framework: evidence from safety critical domains. Work 41, 3018-3025.

Reiman, T. & Rollenhagen, C. (2012). Competing values, tensions and tradeoffs in management of nuclear power plants. *Work*, 41, 722-729.

Schein, E.H. (1992). Organisational Culture and Leadership. (2nd Edition ed.),, Jossey-Bass, San Francisco CA.

The National Diet of Japan The official report of the Fukushima Nuclear Accident Independent Investigation Commission (2012)

The Tokyo Electric Power Company, Inc. (2011). Fukushima Nuclear Accident Analysis Report. (Interim Report).

The Tokyo Electric Power Company, Inc. (2012): Fukushima Nuclear Accident Analysis report. Summary.

Thompson, RC, Hilton, TF, & Witt, LA. (1998) Where the safety rubber meets the shop floor: A confirmatory model of management influence on workplace safety. *Journal of Safety Research*, 29, pp15-24

Thompson, G. (2003). Between Hierarchies and Markets: The Logic and Limits of Network Forms of Organization

Trueman, M. (1998) "Managing innovation by design - how a new design typology may facilitate the product development process in industrial companies and provide a competitive advantage", European Journal of Innovation Management, Vol. 1 Iss: 1, pp.44 - 56

Turner, N., Chmiel, N., Walls, M., (2005). Railing for safety: job demands, job control and safety citizenship,. Journal of Occupational Health Psychology 10 (4), 504-512.

USNRC (2012. Enhancing Reactor Safety in the 21st Century. The near-term task force review of insights from the Fukushima Daiichi accident.

Veland, O. (2010). Design patterns in the nuclear domain: theoretical background and further research opportunities. OECD Halden reactor project. HWR-932.

Wasserman.S, & Faust.K. (1994). Social network analysis: methods and applications. Cambridge Univ. Press, 1998.

Woods, D.D. & Branlat, M. (2011). How human adaptive systems balance fundamental trade-offs: Implications for polycentric governance architechtures, in Proceedings of the Fourth Resilience Engineering Symposium, Sophia Antipolis, France.

Wright, C. (1986). Routine death: fatal accidents in the oil industry. Sociological Review 34 (1), 265-289.

Zohar, D. (2010). Thirty years of safety climate research: reflections and future directions. Accident Analysis and Prevention 42, 1517-1522.

Zohar, D., Luria, G. (2004). Climate as social-cognitive construction of supervisory practices: scripts as proxy of behaviour patterns. Journal of Applied Psychology 89, 322-333.

Bibliographic Data Sheet **NKS-XX**

Title	Safety culture in design
Author(s)	Luigi Macchi[1], Elina Pietikäinen[1], Marja Liinasuo[1], Paula Savioja[1], Teemu Reiman[1], Mikael Wahlström[1], Ulf Kahlbom[2], Carl Rollenhagen[3]
Affiliation(s)	1 VTT Technical Research Centre of Finland 2 RiskPilot 3 Vattenfall
ISBN	87-7893-<filled by the secretariat>
Date	08/02/2013
Project	NKS-R SADE
No. of pages	55
No. of tables	3
No. of illustrations	9
No. of references	61

Abstract
max. 2000 characters

In this report we approach design from a safety culture approach As this research area is new and understudied, we take a wide scope on the issue. Different theoretical perspectives that can be taken when improving safety of the design process are considered in this report. We suggest that in the design context the concept of safety culture should be expanded from an organizational level to the level of the network of organizations involved in the design activity. The implication of approaching the design process from a safety culture perspective are discussed and the results of the empirical part of the research are presented. In the interview study in Finland and Sweden we identified challenges and opportunities in the design process from safety culture perspective. Also, a small part of the interview study concentrated on state of the art human factors engineering (HFE) practices in Finland and the results relating to that are presented. This report provide a basis for future development of systematic good design practices and for providing guidelines that can lead to safe and robust technical solutions.

Key words Safety culture, Design, Network safety culture, HFE

APPENDIX A. INTERVIEW OUTLINE

Conceptions concerning own work

1. Professional background (education, how long worked in x, where before that, current occupation)
2. How do you define nuclear safety? What does it mean?
3. If you would have to evaluate nuclear safety in an operating power plant what kind of things would you review?
4. In your work, what is the core task? Objective, purpose, the main content etc.
5. How is your own work related to nuclear safety?

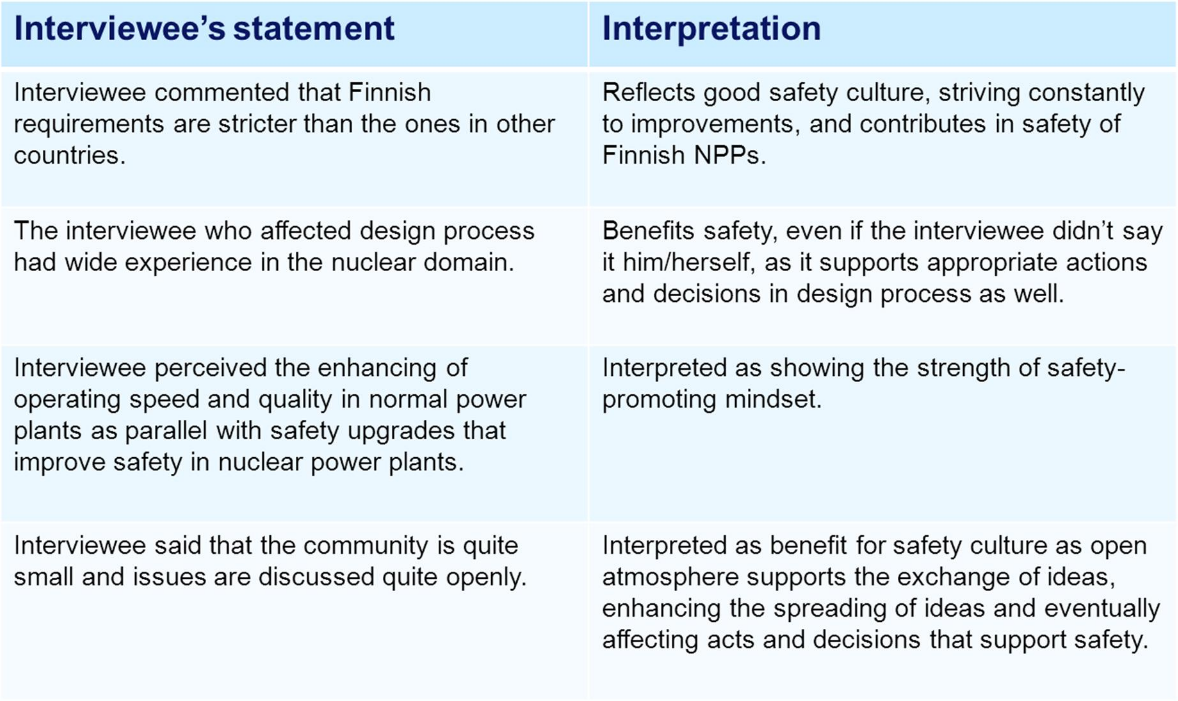
Conceptions concerning design and safety in design

6. What is the role of design in terms of nuclear safety?
7. How are design activities broadly organized in your company? What are the pros and cons of the current way of organizing?
8. For what purposes do you use PRA/PSA in design? The value of probabilistic versus deterministic analysis? What about HFE?
9. How do you utilise experience feedback in design? How is that organised in your company?
10. Given that designs are never perfect, are you aware of an example of a design flaw with some nuclear safety significance that was discovered in a NPP; how it was found out, what was done, what was learned in terms of new designs
11. What are the means for evaluating the safety of a proposed design? How can the designer him/herself evaluate safety?
12. How important is it for the design personnel to understand the contribution of the component/system to the operating plant?
    a. What practical implications can good / bad understanding have?
    b. What practical implications can bad understanding have?
13. How important is it for the operating personnel to understand the design basis?
    a. What practical implications can good / bad understanding have?
    b. What practical implications can bad understanding have?
14. What do you associate with safety culture?
    a. Have you been “educated” in safety culture issues?
15. When/If you inspect an organization designing a retrofit or a new build, what kind of safety culture characteristics you want that organization to have?
16. How does a good safety culture in design stage differ from good safety culture in operation?
17. When you buy a new design, what kind of safety culture characteristics you want the supplier to have?
18. On an individual level, how is good safety culture portrayed in “day-to-day” design work
    a. Can it be perceived in the design documents
    b. Can it perceived in the design output (e.g. component, system, plant)
19. In your view, how has the thinking about the design process and realised design changed during the years?
20. How has the definition of acceptable design / radicality of design changed? What is now considered normal that was once radical, and what are the current controversies?
    a. technical lessons?
    b. project management?
    c. human and organizational factors?

21. In your view, how has the institutional environment (political, markets, workforce) changed during the years and how it has affected design activities?

APPENDIX B. CLARITY OF RESULTS

In the table below, such statements are presented that have required specific interpretation by the analyser.



Interviewee's statement	Interpretation
Interviewee commented that Finnish requirements are stricter than the ones in other countries.	Reflects good safety culture, striving constantly to improvements, and contributes in safety of Finnish NPPs.
The interviewee who affected design process had wide experience in the nuclear domain.	Benefits safety, even if the interviewee didn't say it him/herself, as it supports appropriate actions and decisions in design process as well.
Interviewee perceived the enhancing of operating speed and quality in normal power plants as parallel with safety upgrades that improve safety in nuclear power plants.	Interpreted as showing the strength of safety-promoting mindset.
Interviewee said that the community is quite small and issues are discussed quite openly.	Interpreted as benefit for safety culture as open atmosphere supports the exchange of ideas, enhancing the spreading of ideas and eventually affecting acts and decisions that support safety.

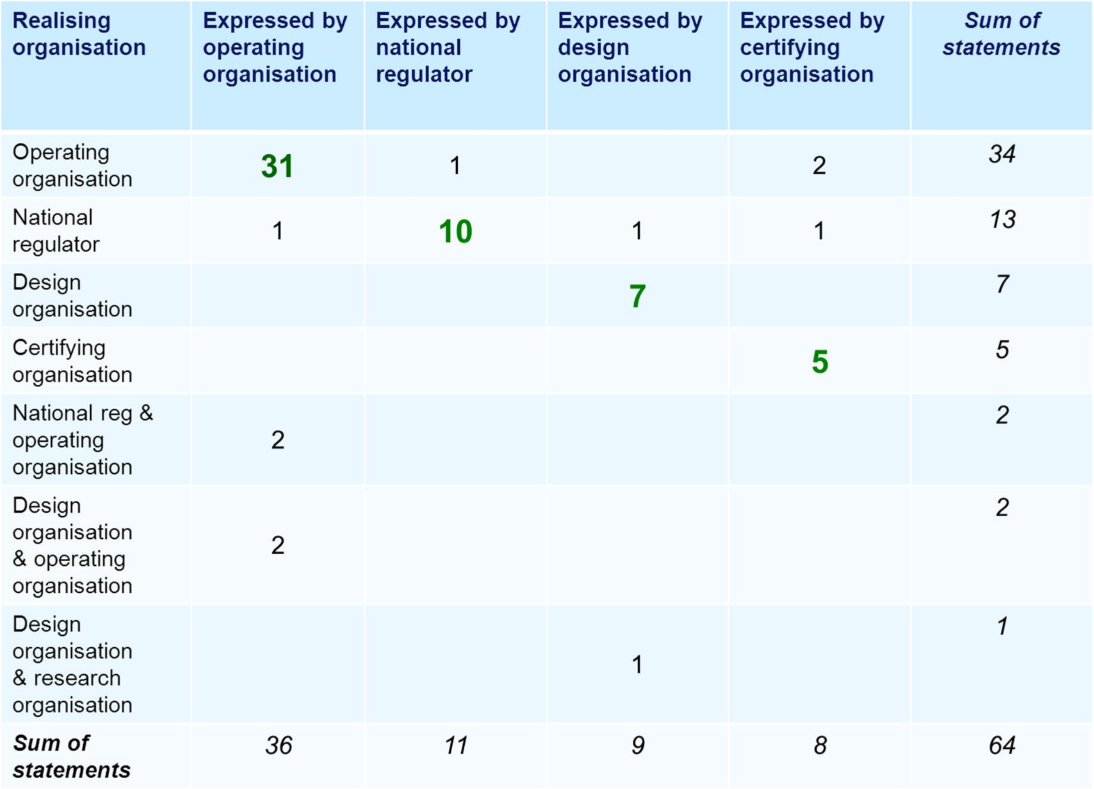
APPENDIX C. IDEAL OPPORTUNITIES

Below in the table are presented all expressions of opportunities that are not actual but ideal.

NATURE OF STATEMENT	**STATEMENT**
Will be:	There will be a process for enhancing learning from experience.
Will be:	The new guide of the national regulator will better take into account human factors engineering than the present one.
Is planned:	When acquiring the permit for deployment is near, the plant personnel aims to carry out practically all analyses so that the analysing work is done by two independent actors (the plant and the supplier company).
Could be:	A safety culture department could be established.
Could be:	Mentoring could be made a systematic practice.
Would be good:	If more workshop-type evaluation would be used in design instead of circulating files for each person separately, the existence of gaps and flaws in circulation would be more probably found as in the latter case, collaboration is enhanced and design would be regarded more as a whole instead of small slices.

APPENDIX D. LOCUS OF OPPORTUNITY-REALISING ORGANISATION

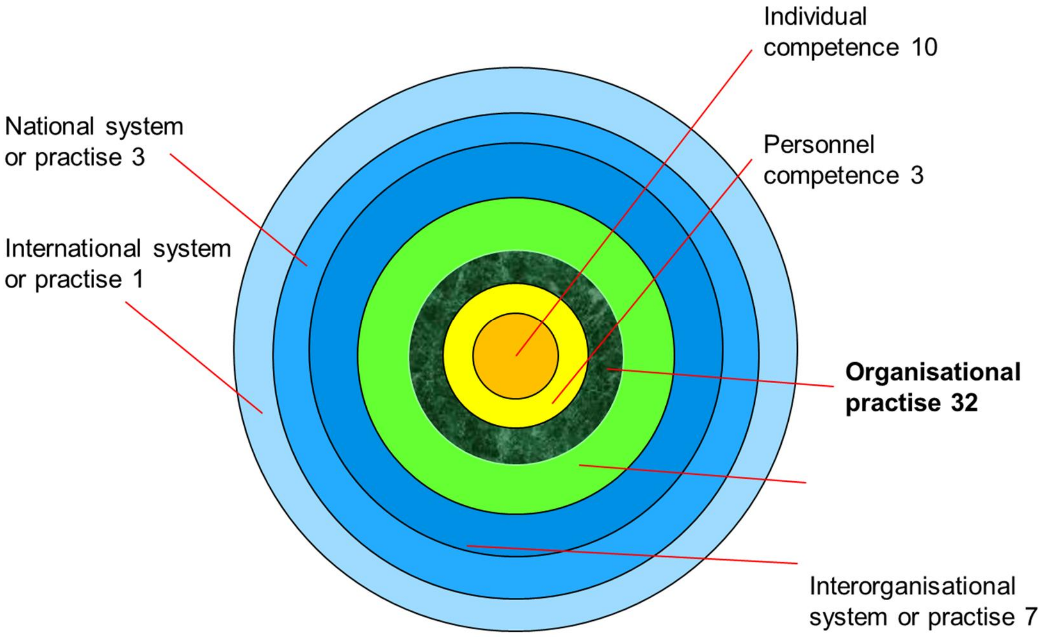
Below in the table the locus of opportunity-realising organisation is presented for all statements, classified according to the realising organisation and the origin of such statement.



Realising organisation	Expressed by operating organisation	Expressed by national regulator	Expressed by design organisation	Expressed by certifying organisation	*Sum of statements*
Operating organisation	**31**	1		2	*34*
National regulator	1	**10**	1	1	*13*
Design organisation			**7**		*7*
Certifying organisation				**5**	*5*
National reg & operating organisation	2				*2*
Design organisation & operating organisation	2				*2*
Design organisation & research organisation			1		*1*
Sum of statements	*36*	*11*	*9*	*8*	*64*

APPENDIX E. ORIGIN OF THE EXPRESSED OPPORTUNITY

In the figure below are presented the results related to the origin of the expressed opportunity.



Title	Safety culture in design

Author(s) Luigi Macchi[1], Elina Pietikäinen[1], Marja Liinasuo[1], Paula Savioja[1], Teemu Reiman[1], Mikael Wahlström[1], Ulf Kahlbom[2], Carl Rollenhagen[3]

Affiliation(s) [1] VTT Technical Research Centre of Finland
[2] RiskPilot, Sweden
[3] Vattenfall, Sweden

ISBN	978-87-7893-353-9
Date	April 2013
Project	NKS-R / SADE
No. of pages	55
No. of tables	3
No. of illustrations	9
No. of references	61

Abstract In this report we approach design from a safety culture approach As this research area is new and understudied, we take a wide scope on the issue. Different theoretical perspectives that can be taken when improving safety of the design process are considered in this report. We suggest that in the design context the concept of safety culture should be expanded from an organizational level to the level of the network of organizations involved in the design activity. The implication of approaching the design process from a safety culture perspective are discussed and the results of the empirical part of the research are presented. In the interview study in Finland and Sweden we identified challenges and opportunities in the design process from safety culture perspective. Also, a small part of the interview study concentrated on state of the art human factors engineering (HFE) practices in Finland and the results relating to that are presented. This report provide a basis for future development of systematic good design practices and for providing guidelines that can lead to safe and robust technical solutions.

Key words Safety culture, Design, Network safety culture, HFE

Available on request from the NKS Secretariat, P.O.Box 49, DK-4000 Roskilde, Denmark.
Phone (+45) 4677 4041, e-mail nks@nks.org, www.nks.org