NKS-301
ISBN 978-87-7893-377-5

Improving design processes in the nuclear domain. Insights on organisational challenges from safety culture and resilience engineering perspectives

Luigi Macchi[1]
Nadezhda Gotcheva[1]
Håkan Alm[3]
Anna-Lisa Osvalder[2]
Elina Pietikäinen[1]
Pia Oedewald[1]
Mikael Wahlström[1]
Marja Liinasuo[1]
Paula Savioja[1]

[1] VTT Technical Research Centre of Finland
[2] Chalmers University of Technology
[3] Luleå University of Technology

February 2014

Abstract

Design flaws have been contributing to major industrial accidents. However, design activities are understudied in human and organisational factors studies. In the nuclear power domain, both pre-operational design and design of modifications depend on a network of organizations, and aim at developing solutions which meet different criteria. Nuclear power companies often outsource the design work to organisations, which might not be hitherto familiar with the safety requirements of nuclear industry.

The final phase of SADE project focused on testing and evaluating the results of the first two phases through in depth analysis of case studies conducted in Finland and Sweden. The study aimed at providing insights on the inter-organizational challenges related to design activities, which could potentially affect safety of the Nordic nuclear power plants. In 2013 we carried out 14 semi-structured interviews with representatives of power plant organisations, design organisations and regulators. Interviews of the Finnish case studies were complemented by one group interview each.

The study indicated that design-related challenges in the nuclear domain are mainly inter-organizational. This implies that safety management and safety culture approaches should take better into account the inter-organisational nature of work processes. For some of the challenges (e.g. coordination) many coping practices exist throughout the network, whereas for others (e.g. shared understanding) just a few were mentioned. This signifies that design organisations have learned the consequences of insufficient coordination in previous projects, while reaching a shared understanding proves to be challenging.

The design process involves both rational and creative approaches to deal with real-life problems. In nuclear industry, designers face the need to balance between fulfilling requirements and doing an extensive amount of paperwork, and creating new, safe and functional solutions. To better manage safety culture in design activities in a networked context, nuclear power companies and design supply chains need to reach a shared understanding on achieving this balance. Finally, the study provides a set of recommendations to support and improve the design process and to help anticipate emerging risks in the nuclear industry.

Key words

Safety culture, design, nuclear power industry, organizational challenges, networks

NKS-301
ISBN 978-87-7893-377-5

Electronic report, February 2014

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

Improving design processes in the nuclear domain

Insights on organisational challenges from safety culture and resilience engineering perspectives

Final Report from the NKS-R SADE activity
(Contract: AFT/NKS-R(13)97/14)

Luigi Macchi[1]
Nadezhda Gotcheva[1]
Håkan Alm[3]
Anna-Lisa Osvalder[2]
Elina Pietikäinen[1]
Pia Oedewald[1]
Mikael Wahlström[1]
Marja Liinasuo[1]
Paula Savioja[1]

[1]VTT Technical Research Centre of Finland
[2] Chalmers University of Technology
[3] Luleå University of Technology

Abstract
Design flaws have been contributing to major industrial accidents. However, design activities are understudied in human and organisational factors studies. In the nuclear power domain, both pre-operational design and design of modifications depend on a network of organizations, and aim at developing solutions which meet different criteria. Nuclear power companies often outsource the design work to organisations, which might not be hitherto familiar with the safety requirements of nuclear industry.

The final phase of SADE project focused on testing and evaluating the results of the first two phases through in depth analysis of case studies conducted in Finland and Sweden. The study aimed at providing insights on the inter-organizational challenges related to design activities, which could potentially affect safety of the Nordic nuclear power plants. In 2013 we carried out 14 semi-structured interviews with representatives of power plant organisations, design organisations and regulators. Interviews of the Finnish case studies were complemented by one group interview each.

The study indicated that design-related challenges in the nuclear domain are mainly inter-organizational. This implies that safety management and safety culture approaches should take better into account the inter-organisational nature of work processes. For some of the challenges (e.g. coordination) many coping practices exist throughout the network, whereas for others (e.g. shared understanding) just a few were mentioned. This signifies that design organisations have learned the consequences of insufficient coordination in previous projects, while reaching a shared understanding proves to be challenging.

The design process involves both rational and creative approaches to deal with real-life problems. In nuclear industry, designers face the need to balance between fulfilling requirements and doing an extensive amount of paperwork, and creating new, safe and functional solutions. To better manage safety culture in design activities in a networked context, nuclear power companies and design supply chains need to reach a shared understanding on achieving this balance. Finally, the study provides a set of recommendations to support and improve the design process and to help anticipate emerging risks in the nuclear industry.

Keywords: Safety culture, design, nuclear power industry, organizational challenges, networks

Table of Contents

1. Introduction

Design issues have often been found as a contributing cause to accidents across different industrial domains: 55 percent of accidents in chemical industry and 46 percent of accidents in nuclear industry can be attributed at least partially to design errors (Taylor, 2007). Some examples are Turkish Airlines Flight 981 crash in 1974, the Challenger space shuttle explosion in 1986, Piper Alpha oil rig explosion in 1988, the capsize of the MS Estonia ferry in 1994, or the Wenzhou high speed train collision in 2011. In the nuclear industry, between 1985 and 1997, more than 3100 licensee event reports have identified design-based issues (Lloyd et al., 2000). In particular, the analysis of the Three Mile Island reactor accident (1979) revealed a basic design flaw for pressurizer relief valve (which failed open instead of closed), as well as design problems in the control room. Various design issues (e.g. the height of the tsunami protection wall, the location of the emergency diesel generators) emerged in the analysis of the Fukushima nuclear disaster (2011) as well.

Nordic nuclear power plants have also encountered design-related problems. In 1992 in Sweden, a safety valve of the main steam system opened at Barsebäck unit 2 causing the disintegration of coverings and insulation materials from adjacent pipelines (www.analys.se, 2004). Parts of disintegrated material ended up in the reactor containment and caused clogging of the strainers for the emergency core cooling system. In 2008 in Finland, the reactor trip at Olkiluoto 1 resulted from a design issue with the generator voltage regulator (Kainulainen, 2009). In 2010 in Sweden, a possible common cause related design flaw on four valves caused an abrupt stop of the steam to the condenser leading to a short and relatively high pressure spike in the Oskarshamn 3 reactor (www.archive-se.com, 2010).

Design error is defined as “a feature of a design which makes it unable to perform according to its specification” (Taylor, 2007a: 62). The study of design errors has recently received increased attention in the field of safety science and strategies for preventing their occurrence have been proposed (Hatamura, 2009). The role of human and organizational factors (HOF) and the contribution of safety culture to the safe operation of nuclear power plants have been acknowledged (IAEA, 2005). Human factors and ergonomics are usually considered when conceiving and designing tools, interfaces and systems to provide *end-users* with artefacts satisfying usability criteria (e.g. context of use, easiness of use, learnability, satisfaction, etc.). Still, the design organisations and design processes have seldom been the subject of human factors or safety culture studies.

2. Project objectives

A jointly funded SAFIR2014 and NKS-R project has been established in 2011 to identify organizational challenges associated with design and implementation activities, and to provide recommendations to the nuclear industry community to support and improve the design process and to anticipate emerging risks. The research project approached design from safety culture and resilience engineering perspectives. The following three research questions were set at the beginning of the project:

1. What are the current organizational challenges (trade-offs, user involvement, supply chains, design errors, etc.) in the design and implementation activities and how they ultimately affect the safety of the operating power plant?
2. What kind of safety culture characteristics (risk understanding, mindfulness, etc.) are required during the design of new technological and organisational solutions in order to contribute to resilient nuclear power plants?

3. How can the Resilience Engineering and the safety culture theory (Rollenhagen, 2010; Reiman et al., 2012) contribute to improving design and implementation practices when hindsight data are not available?

3. Design in the nuclear industry as an object of study

In general, *design* can be conceived as the process of inventing, creating, and implementing (technical) artefacts (Bergman et al., 2007). This process takes place under uncertainty (Norros, 2004), relates to innovation and rational decision making (Aspelund, 2006), and incorporates aspects of planning, decision making, and management (Trueman, 1998). In the nuclear power industry, the term "design" has been used to refer both to the process of designing something and to the end product of this process. Therefore, when discussing about safety of design and safety culture in design the two meanings have to be clarified and considered because the two meanings are intertwined.

On the one hand, *when the concern is design as end product*, its safety and risks that its introduction in nuclear power systems can create, the focus is in improving design by letting the designers consider the future usage of the designed system already in the design phase. Human Factors Engineering (HFE) represents a well-established body of knowledge and expertise for this purpose. International regulator guidelines emphasize the need to consider HFE issues at different phases of the design process. According to EPRI-1008122, the application of HFE aims to ensure that a) the roles and tasks of NPP personnel are clearly defined, b) staffing levels and qualifications are adequate to fulfil the requirements of human tasks and, c) task performance requirements and human psychological and physiological characteristics are considered in the design of human-system interfaces (HSIs), procedures and training.

The Human Factors Engineering Program Review Model has been applied worldwide to evaluate the benefits of inclusion of HFE principles and methods in the design of HSIs, and to evaluate the implemented design. Several stakeholders are concerned with the area of HFE but Human Factors Engineering is mainly related to the activity of the design organization. HFE in the design organization focuses on the organization's way of taking the usage point of view into account in design. Accordingly, well defined HFE processes are a nominal feature of safety culture in design. The extent to which HFE is taken into account varies between utilities and different projects within a specific utility. The amount of HFE focus seems to be increasing in recently started projects though. The Regulator's role in nuclear domain is to monitor, inspect and follow that all regulations are fulfilled by the production and design organizations, that is, to maintain oversight of that HFE principles are being conducted in the design organization.

On the other hand, *when design is considered as an activity,* the central question is how to make sure that the outcome of the design process is going to be safe. An implicit assumption of this is that the quality and safety of the end product is influenced by the design process itself. Aspelund (2006) described the design process as consisting of ideas conception, 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, by also taking into account planning and management (Trueman, 1998). Furthermore, Mark et al. (2007) define "design" as the practice of inventing, creating, and implementing (technical) artefacts that depend upon, integrate, and transform heterogeneous and uncertain domains of knowledge. Design process aims at designing several different elements or components of a system, from training to human system interfaces, to procedures or structures etc. Design in an industrial context can be viewed as an iterative process, which aims at creating an artefact

to solve an expressed problem or to meet a certain need. This process is a combination of analytical problem solving and innovative creation of new features and combinations. The resulting artefact cannot be known in detail in advance but the function(s) that the artefact should fulfil can be known and should be specified early in the process. The different steps in a design process can be summarised as follows:

1) Identification and development of requirements for the end product;
2) Development of conceptual design ("rough" picture of the design).This is especially needed when the designed component is supposed to interact with other loosely defined components and systems;
3) Development of detailed design of the component or system;
4) Evaluation of the detailed design (and its functions with the other interdependent components/systems);
5) Implementation of the component/system;
6) Testing the component during its usage.

Design process is 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 of the nuclear industry. Rather, the design process can be understood as a complex interaction and negotiation process between different experts and organisations. We have identified the key organisations involved in design processes in the nuclear industry and their main tasks (see Macchi et al., 2013). People doing the actual hands-on design work can be in-house personnel of the nuclear power company but often the design work is outsourced in design organisations, which usually provide services for other industries as well. Therefore, design organizations are not necessarily familiar with the nuclear industry context and its specific requirements.

Design in the nuclear industry is highly regulated. Depending on the function and safety class of the system to be designed it may be that 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. The interpretation of this concept has evolved during the years, and in practice it is used with several but closely connected meanings. In the IAEA's (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."* 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 the harmful effects of radiation.

Other important safety principles in the nuclear industry are *redundancy, diversification* and *physical separation*. In general, 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 refers to existence of several systems that carry out the same

function; however, their 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. For exact definitions of the terms *redundancy*, *diversification* and *physical separation*, please refer to the STUK's YVL guide B.1/15.11.2013 and Government Decree 717/2013.

Although each design domain can be expected to manifest unique characteristics for the particular skills needed, some general psychological features can be identified. Design activities are associated with *open problem spaces rather than closed ones*. 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 different than technical-rational problem solving. According to him, a process skill should be core competence of a designer, e.g. the designer needs to "think on his feet" when immersed in *active, flexible, reflective exploration of the problem space*.

A closer look reveals an interesting dynamics between "conservatism" and "flexibility" when positioning design in the specific context of the nuclear power industry. Navigating in an open and dynamic problem space involves uncertainty. Still, incremental changes in existing structures (hardware, software, organisational, etc.) can be challenging from a safety point of view as well. This dynamics is relevant for issues about safety culture in design: we would expect that designers of safety critical systems are facing tensions between their roles as innovators, and the limitations set by rules and regulations due to nuclear power specific technical design principles.

In design of safety critical systems it is often a good practice to develop *transparent decision-making processes.* If information is properly documented and stored, it is easier to change the system later. However, from a psychological perspective, it could be challenging for a designer to continuously document the design process and why e.g. one solution is preferred to another. Documentation takes time and may be perceived as unnecessary and disturbing. Also, there might be more uncertainty behind design decisions than a designer wants to reveal. In safety critical 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.

4. Improving design by managing safety culture

Since its introduction after the Chernobyl accident, the concept of *safety culture* has been increasingly applied in research and practice in different industrial settings (IAEA, 1986). The concept was 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 main body of research and practical applications associated with safety culture are mainly focused on "sharp end" activities in the operational context rather than technological design. We stated that criteria for good safety culture in different industrial domains are the same but the manifestations of those may differ, as well as the associated challenges.

Despite the different approaches and definitions, the concept of safety culture facilitates the possibilities to address different "soft" aspects of safety management, such as norms, attitudes, behaviour and expectations. However, the concept of safety culture has not been applied extensively in the context of design activities. The people taking part in the design process are human too and cultural phenomena affect them just as much the people in

operation and maintenance. Common to most definitions of safety culture is that they consider culture as a *collective* attribute; 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 as 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. In networked design context, subcultures could turn into a challenge when the aim is to assess safety culture. That is, both the concepts of organizational culture and safety culture include the subculture issue; it is even harder to implement the concept of organizational culture in networked environments.

Many generic models of organisational culture have been proposed. One of the more influential models was developed by Schein (1992) who differentiates among several layers of organisational culture. At the deepest level, an organisational culture is assumed to be characterised by a set of basic assumptions (e.g., 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). Artefacts (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? 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 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 an idealistic view on what people can accomplish in a certain context – a focus on basic assumptions may reveal distorted world views which make a design less optimal for operation. Reason (1998) argues that a safe organisation is characterized by an *informed culture*, which continuously collects and shares information about hazards. This means both to collect information about own and others' events, as well as to perform risk analysis activities. Both processes constitute a cornerstone in safety management systems. However, for external design organisations these features of safety culture are not always easy to manage because information about events usually resides in the operating organisations. Consequently, to develop an informed culture, providers of nuclear designs must develop a network of contacts with operators.

Design processes can be perceived as distributed decision making where a number of different stakeholder has to cooperate in order to reach a safe and reliable design. 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 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 (1991:9) 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"*.

A central factor to achieve goals in a distributed network of actors is communication. Nowadays the wide availability of various communication technologies facilitates easy contacts. Still, in a distributed network of several stakeholders, constructing coherent and shared plans can be challenging because different participants have their limited view of the situation. 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 multi-agent plan specifying future actions, resources, etc. This rather common approach has 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. The system boundary is drawn widely to include a number of different stakeholders of relevance for the success of a safety-critical project. 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).

Traditionally, the concept of safety is applied to individual organisations. Also, 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. We find it thus important to expand the concept of safety culture towards a network where each stakeholder constitutes a culture of its own (containing subcultures). We can think of a network of safety culture and a set of activities (e.g. nuclear design/modifications) by identifying some of the critical safety culture factors for such a network. Based on the literature on distributed decision making, it could be suggested that one of the key factors for understanding safety culture in a network is *cooperation and communication in the network.* Three main factors are suggested to influence the communication coherence in a network: *relevance, timeliness* and *completeness* (Durfee et al., 1989, cited in Brehmer, 1991). 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 in a timely manner to have a positive effect on the (design) process. *Completeness* refers to sharing a common mental model by all the actors in the network. It appears that Reason's (1989) concept of "informed culture" (e.g. knowledge about events and risks, others' tasks, etc.) could be seen as an important factor for a network safety culture. This, in turn, evokes all the issues associated with communication among the stakeholders in the network, including setting up an efficient communication structure. This feature of a network safety culture also triggers a need to develop a *systemic model of nuclear safety* including a broad set of factors important for safety management. An ethical aspect is also relevant for a network safety culture: stakeholders should develop a shared understanding on the ethical code for resolving trade-offs and negotiations in the network.

Recently, an attempt to define the basics of *network safety culture* in the nuclear domain was made by Gotcheva et al. (2012). Drawing on the work of Reiman and Oedewald (2009) and Oedewald et al. (2011) they have suggested that a network of organizations should be taken as the *unit of analysis* from the very beginning in order to analyse the predominant (presumably shared and somehow mutually accepted) views or conceptions, or their lack thereof, which affect the behaviours and produce certain outcomes in the organizational network with regard to safety.

Because of the complexity of activities, organisations face various 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 (Perrow, 1999; Woods and Branlat, 2011; Reiman and Rollenhagen, 2012). Centralized control in a nuclear power plant organization stems from the need to have an overall picture or understanding of different parts of the system. The justification for having decentralized control is that a single centralized unit might not identify the cause of a disturbance if it relates to interactions within or between sub-systems; they could be best dealt by implementing expert solutions by personnel working directly with the sub-systems. Another typical conflict an organisation has to solve is the need to 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).

Such 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 need to be constantly taken into consideration in the design process.

5. Methods

The objectives of this project were achieved by a number of case studies performed in Finland and Sweden. The case studies consisted of carrying out interviews with representative from power plant organisations, design organisations and regulators. In 2013, fourteen interviews were carried out. The semi-structured interviews followed the interview scheme presented in the Appendix. The set of questions were adapted depending on the topics discussed and complemented by other questions for deepening the understating of some specific aspects discussed during the interviews. The in-depth interviews of the Finnish case studies were also complemented by one group interview each. Their scope was to gather an overview picture of the design project and to provide background information for the following interviews.
Since the main scope of the current study was to test and validate the relevance of the previously identified challenges, the analysis of the interviews started from the preliminary

results of the DESIGN SADE project. This was done by checking the responses interviewees gave at the explicit question "Do you agree with the following statement: (*challenge 1, 2, 3 etc.)*". Indications of the agreement or disagreement with the statement have then analysed from the interviews. Every time an interviewee expressed concern about some parts of the design process, or referred to obstacles or problems hindering the execution of the design project, it categorised as *hinders*, if and as appropriate, in the different categories of challenges. At the same time, all the indications of things going well, or considered potentially beneficial, have been collected and also categorised, as *facilitators*, according to the five macro-challenges. *Facilitators* are aspects that can enhance the design process and help in dealing with challenges, while *hinders* complicate the design process and impede the ability to deal with challenges. The possibility to revise the macro-challenges or to create new ones has been kept into consideration during the analysis.

To understand the features of a good design safety culture, we referred to the six criteria for good safety culture developed at the VTT Technical Research Centre of Finland (Reiman and Oedewald, 2009; Oedewald, et al., 2011; Reiman, et al., 2012):

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.

The criteria have been further summarised into three cornerstones of safe activities: mindset, understanding and organisational systems and structures (Figure 1).

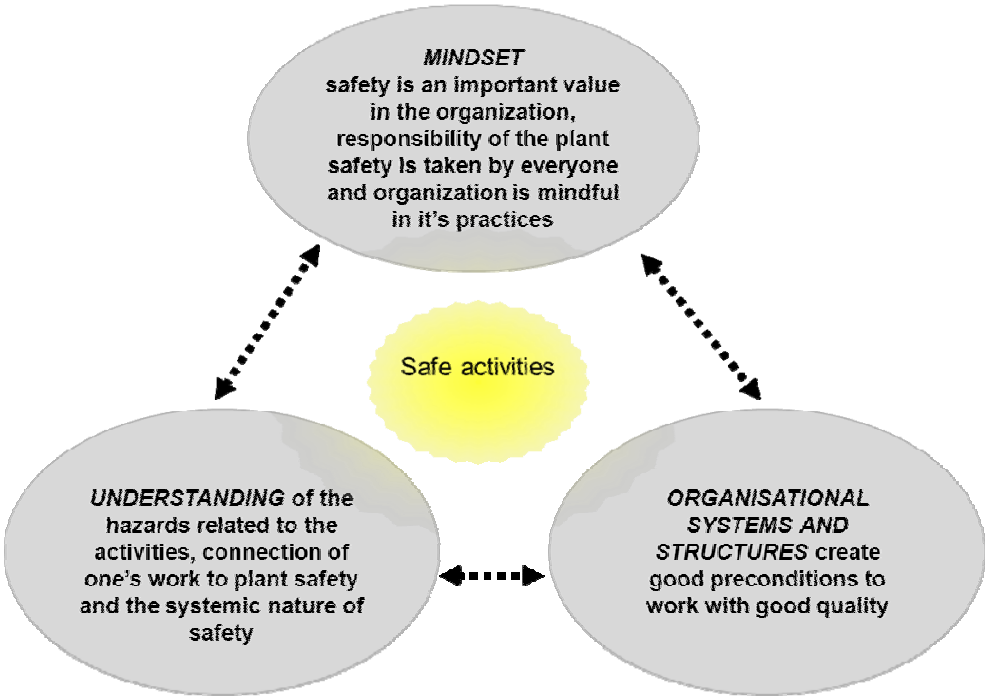

Figure 1. Cornerstones of safe activities (Oedewald, Pietikäinen & Reiman, 2011).

These criteria have been utilized for evaluating safety culture at Nordic nuclear power plants (e.g. see Oedewald et al., 2011), and can be applied for design safety culture as well. It can be

argued that design organisations, both in-house units or contractor companies, should have a certain shared mindset, where safety is valued, responsibility for the safety of the whole plant that will be utilising the designed object is taken, and constant vigilance or mindfulness is maintained.

6. Results from the case studies

The results of the different case studies performed in Finland and in Sweden during 2013 are presented in this chapter. As previously mentioned, the results are combined to avoid the possible identification of the design projects which have been studied in details and therefore to protect the anonymity of participants and organisations.

The results are organised according to the following logic: for each challenge identified in the second phase of the NKS-R SADE project, it is first discussed if and why it was recognized and acknowledged by the interviewees. Then, for each challenge, more concrete and empirical evidence based on the collected data are presented. Finally, specific coping strategies or practices suggested by the interviewees as means they have been using or they consider useful for dealing with the challenges are presented.

The five challenges identified in 2012 were as follows (see Macchi et al., 2013):

1. Safety is not always the first and most important guiding value in the design process;
2. Understanding the context where the designed end-product will be utilized may be difficult for the designers and this may lead to dysfunctional designs;
3. Organisations do not always share the same safety philosophies and understand safety requirements in the same way;
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.

We suggest that the five challenges could be related to the three cornerstones of safety culture as depicted in the following figure:

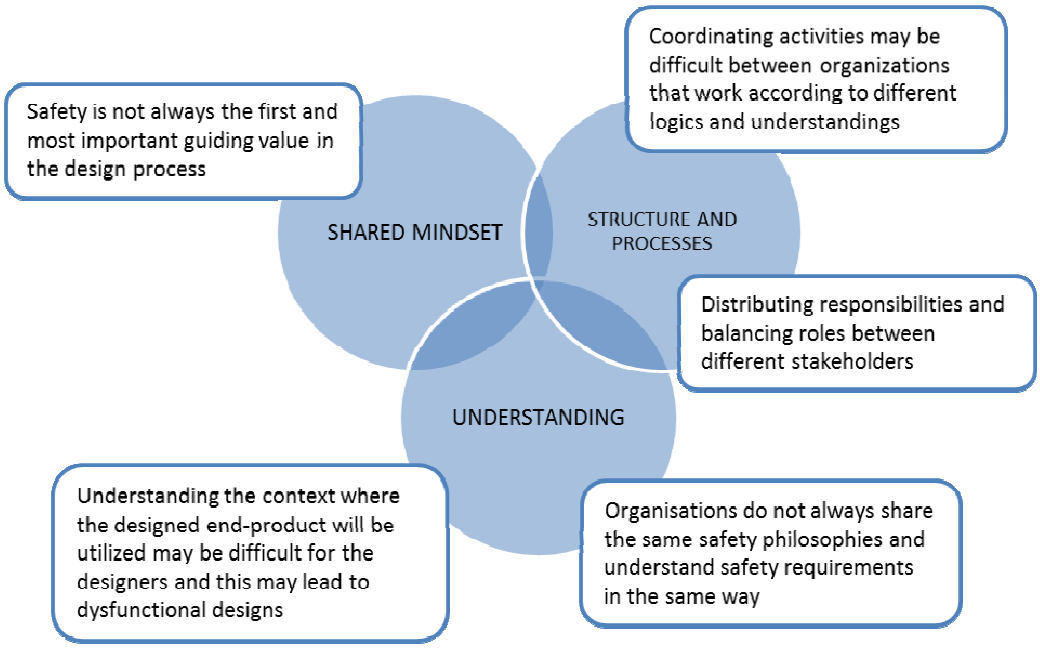

Figure 2. Macro challenges and cornerstones of safety culture.

6.1. Challenge 1: Safety is not always the first and most important guiding value in the design process

Safety should be a top priority when designing, operating and maintaining nuclear power plants. However, Macchi et al. (2013) concluded that the appropriate balance between safety and economics is not always easy to maintain, often due to the wide variety of actors involved in the design process, and their different values and missions. For example, when signing contracts with design organisations, power companies aim at a good bargain, and design organisations, especially when they act as consultants and/or subcontractors, consider the economic aspects of the deal to ensure their survival and sustainability in the short and long run. While sometimes power companies tend to sign contracts with design organizations without explaining in detail all the possible risks and complexities related to design projects in NPPs, there is also the tendency from design organisations to be reluctant to take into account new requirements once the contract is signed. From the regulator's perspective, as reported during the interviews, it is challenging to carry out detailed inspections and to make demands while realising the strong commercial pressures power companies face. All in all, while balancing between competing values of safety and economics is a typical potential challenge that most complex systems face in their activities, our study indicated that the in reality interviewees have difficulties in recalling specific work situations, in which they had to make compromises.

When asked if they personally have experienced situations in which compromises on safety had to be taken for cost related matters, or if they have ever heard something on this line going on in their company, most of the interviewees clearly said "no". For example, one automation engineer expressed his/her opinion as follows: "*I wouldn't say that. I've always got what I've wanted. Never experienced this"*. Another interviewee, also an automation engineering working as inspector at one of the companies' nuclear reactor regulator department said "*[…] I've experienced, for example, you could have a supervisor or a manager who makes financial decisions and they'll say something along the lines that wouldn't this do instead. Because they're motivated by cost savings. But even in that case, the suggestion didn't go through, safety was the priority"*. And he/she continues acknowledging that "*[…] a technical-financial comparison is made if requested or, in case of tenders, the emphasis is on certain functionality, what it costs and what can be achieved with it. And there's a limit after which additional spending won't increase nuclear power safety that much, so you need to consider whether the additional investment makes sense. At some point you make your mind up that that'll do. No experience of this but endless spending might not increase safety"*.

This later perspective on the need to find a balance between safety and costs of design projects is very clear from one interview with a designer. The need to achieve reasonable and acceptable safe solutions considering financial and temporal pressures is summarised in his/her words as "*sometimes it's not practical or… reasonable to (?) ask even the safest thing*".

Talking in detail about a project he/she has been involved in the last years he/she said: "*For example, this XXX project, we didn't, choose the, best or, safest, situation I must say. But on the other hand, in this modification... How can I say it? For example, in this time schedule we had no even possibility to choose that safest situation. […] We choose that we will just modify this (*component, Ed.*), in this XXX project, and other choice was that we will break it down and build three different (*components, Ed.*) over there. But, it has cost five to ten times more. Of course we had to, then we have designed and built totally new different kind of (*components Ed.*), but on the other hand it's, it was, it might be a little bit safer, but still it is*".

Regarding keeping a balance between competing aspects and finding acceptable solutions, an interviewee explains the way this decision-making process takes place in his/her organisation: "*We make preliminary designing work, and we had three to four different options, and we calculate the price of those and think about the safety, and then inside the project we choose one what we think that it's best, option. And after that we present our opinion to the group (*Steering group, Ed.), *then they know why we chose it and how come it and that's why. It's more likely that they will say that's OK and then we can start."*

In design processes it seems that the critical moment for safety is the development of preliminary planning. The preliminary plans are, however, often developed under economical and/or temporal pressure. As one designer pointed out "*the more time you have to plan and consider things, the better it will work, but if you have to push it and work quickly, if for some reasons we have to complete it quickly […]mistakes can happen. […]But luckily this rarely happens*". In addition, as already mentioned, the need to implement new requirements in the actual design is not well seen by designers. New requirements can come from two sources: a) the power company that provides new details once a design contract is signed, and b) the regulator. As one automation designer stated "*New ones* (of authority regulations Ed.) *are introduced constantly and finding a way to implement them here* (is a challenge Ed.)*"*. The importance of preliminary planning was discussed as: "*but it is more likely that mistakes occur in those jobs that have the lowest safety classifications. And this is usually because, the paperwork that we need, the preliminary plans are much less extensive. […] For many jobs which are class four there may be practically no preliminary planning. […]the best thing to do, of course, would be to write the preliminary plan for every job, and there's no one saying you shouldn't, but there's not always enough time for that*." It should be noted that preliminary planning cannot completely eliminate all possible surprises; therefore they should be taken into account in the beginning of the design process by considering e.g. "slack" resources or agreement between the parties involved on some specific ways for dealing with surprises.

Development of extensive preliminary planning is perceived challenging also for another reason. The approval process can be long and time consuming, and thus causing an overall increase in the perceived time pressure. Even if it is acknowledged that paper work is done for the sake of safety, with the increase of paperwork to prepare the plans in a way that will be acceptable for authorities it comes the fact that "*the simplest of things can be made complex, and a lot of resources are tied to processing it, and then they aren't available for the job itself*" and last minute rush can become a norm as said in one of the interview "*Well, I can't deny pressures related to schedules. There is always a rush at the last moment*". The dilemma emerging from the need to balance safety and other pressures is well exemplified from the following quote from one of the interview. M1 is a representative from a power company and Q1 is one of the interviewers.

> *M1: Well, maybe if we received a response from (the regulator) at this stage, and they'd be requesting additional information on issues related to safety, maybe then, because we aim to get the job done, and we only have a very hectic month to prepare the document to a stage that they are, that they're satisfied with it […] but anyway. I mean that it would be better to receive the response sooner, so that we'd have enough time to implement. Of course, in terms of safety culture, we should say, at that stage, we should say we're not implementing the job at all (since we won't have time for proper) planning and design. But then of course, everyone understands that there's pressure from the company, pressure to get it implemented.*

Q1: Or if…Yes, but if the objective of the modification is to improve safety…

M1: Yes, but if the modification can't be implemented…

Q1: ...and if it's not implemented, of course it's…

M1: Yes, if we can't do it now, it'll be a year from now before it's done. So that's, it'll be delayed by a year…

Approaching this kind of dilemma requires taking into consideration the bigger picture of design activities, and how they contribute to the overall availability and safety of nuclear installations. This implies that it is insufficient to focus solely on the power company activities. Instead, the broader perspective includes also the activities of the other relevant network actors involved in the design process, such as regulators and contractors.

Coping strategies associated with Challenge 1

From the analysis of the interviews it was possible to identify a number of practices that the interviewees think are of help in maintaining safety as the guiding value in design processes. In some cases those practices were practically implemented, while in other cases they are rather principles that the interviewees called for.

In the latter category goes the dealing with big external pressures for respecting schedules. It appears that it is not easy for design organizations to negotiate and to decide how to proceed with the possible safety effects of new demands or other surprises that could compromise the implementation schedule. Having more competent resources might help in keeping the schedules but it is not necessarily a solution for resisting the pressures. An interviewee stated that having more resources creates better conditions for avoiding compromises: "*Well, there should be more of us - that's my personal opinion*", which also increases opportunities for team work on executing design projects as it "*avoids being struck with one's own thoughts*".

Maintaining safety as the top priority in design work was acknowledged by the interviewees. As an interviewee puts it: "*I do trust the company enough to believe that it* (selecting suppliers) *won't be a question of small differences in the sums. It would have to be vast difference in terms of money*". Good practice one of the interviewee experienced is to have design organisation and operating organisation as part of the same company. In his/her opinion and experience this would solve the economic pressure problem because "*there is no need to fight for money, which is a very good thing. That kind of thing can never happen if there's a vendor and a client of fighting for money*".

6.2. Challenge 2: Understanding the context where the designed end-product will be utilized may be difficult for the designers and this may lead to dysfunctional designs

In nuclear power companies different departments, the regulator, consultancy companies and subcontractors play a role in the development of technological solutions. Some of the subcontractors are specialised in the nuclear domain as nuclear power have not been their core industrial domain. Consequently, some designers may have limited knowledge of operating plants layouts and strict requirements. Also for in-house technical departments it is possible that some designers based at the headquarters do not have an adequate representation of the actual plants. An interviewee put this concept in a very straightforward manner: "[…] *some (*designers Ed.*) are more willing to come here and look what is, how the real life looks. But, for some people it's enough. They have the image in their own head that this is how it works and, this is my plan how to solve it and if anybody says anything against it, he or she just doesn't understand how it is supposed to work*". This kind of potential situation can lead to different problems, ranging from delays due to the need to revise the plans to the implementation of dysfunctional designs. As an example, an interviewee stated that "*there*

might happen this kind of, behind the desk designing. […]. For example some door will open wrong direction or something like that and, that's the only thing, if you just can't go… If you won't go that place you can't see it how it works so… […] But not very big issues but still, which might…Well, if you just try and design it, again it will cost lots of lots of money so it doesn't make sense anymore". This problem could be complicated when using consultants in the design work. According to one interviewee, "*even good designers in non-nuclear areas do not know the plant and they do not know what are the requirements, so very often they produce I would say, medium-quality designs*".

The challenge of understanding appears therefore to be related to three aspects. One aspect is the context of operations of the end product, which includes the Human Factors perspective for taking into account the end-users' future use of the product. At the root of this challenge apparently there is the scarce availability in Nordic countries of people with relevant HF competences in the operating organisations, and the need to rely extensively on consultants, especially in Sweden. The overall HFE process could be jeopardized if key HF aspects are not taken into account from the very beginning of the design projects. Also, misunderstandings in classification of projects (technology vs. HF driven) could result in late involvement of HF expertise. Still, specific HF expertise is not always the solution because sometimes it is important if the designer personally visits the plant and checks the plant layout for determining, for example, how exactly a door should be opened, or is it possible to maintain a valve if it is placed in certain way. As an interviewee put it, it must be known at an early stage "*why it is designed and how it needs to work*".

The other aspect refers to the understanding of the formalisms of design processes in the nuclear industry. When compiling and preparing the approval documentation, designers that are not familiar with the nuclear domain face also other challenges in performing effectively their work. The following quotes from interviews put it very clearly: "*Many suppliers don't know what kind of documents is needed and, that is a problem*" and "*consultants who aren't involved with nuclear power compile materials with lower quality*". Consequently, design process can result in significant delays and increased time pressure.

The third aspect related to understanding refers to the effects of new design introduction into the existing system. According to one of the interviewees "*the objective* (of the design Ed.) *is usually known, but not necessarily whether they introduce some undesirable features. It may be that's what's most challenging as regards the software-side of things in this sector*". A proper understanding of consequences of a new design introduction involves uncertainty, and obviously the unwanted side effects are ultimately revealed in the testing phase.

Coping strategies associated with Challenge 2

We identified a number of practices that the interviewees considered beneficial to support understanding in design processes. The first one refers to the *understanding of the operation context* in which the end-product will eventually be deployed and used. It was stated that it is often needed to support designers from consultancy companies and subcontractors, to have personnel from the plant involved in the specification of requirements for the design. A representative from one of the power companies stated that *"if the project is big and supplier dependent, (*the power company Ed.) *is always involved;* (the power company Ed.) *representatives are there. They'll have (*The power company Ed.) *know-how at their disposal. So if they can't comment on a specific issue themselves,* (the power company Ed.*) is always involved in* (this type of projects Ed). An automation engineer from one of the companies said: "*I've been involved in practically everything, since I'm responsible for the systems related to the* (certain component Ed.)*, and I know the technology, maybe not inside out […] Then I made sure that there were free contacts for the* (component Ed.) *to retrieve data;*

whether more components are required and so on". This refers to the ways of collaboration between the power company and the contractors, and how it is reflected in commercial contracts. For instance, in some cases the power company needs to support the contractors in many aspects throughout the process, while in other cases the power company might be reluctant to intervene to contractor's areas of responsibilities. It is unclear though how this is handled in contracts, and who bears the financial responsibility if a system fails. Another interviewee reported that keeping control and oversight on the design process is an effective mean to avoid misunderstanding of the operational context and to facilitate the resolution of eventual problems: "*We have designed in practice everything. Once there's a problem, it's easy to proceed because we have the knowledge, overall responsibility, and good staff. […]We have the best knowledge of the plant"*.

The second group of supportive practices relates to *understanding the users requirements of the end-product*. It is fundamental that Human Factors competences are brought in when design contracts are written and signed: if power companies do not have sufficient in-house competences on Human Factors, they should invest resources for training and/or recruiting. A complementary strategy would be educating project participants in the basics of Human Factors knowledge to establish a shared view about the importance of this topic.

The third group of means refers to *understanding the risks and safety significance of new designs*. Decisions concerning plant modifications should be done by competent persons. The suggested means for achieving proper understanding, according to the regulator was to ensure that "*those making decisions are competent enough*" and "*they must have the understanding, and preferably also the experience […] because they decide what kind of products are developed and used at the plant*". To avoid misunderstanding of risks and safety significance, the importance of having organisational processes to keep track on previous design projects was highlighted. Documentation of previous design projects provides valuable insight on the history of some components, and how problems have been solved: "*it makes* (the design work Ed.) *easier. […] You get enough advice and you remember what was done earlier so you can utilise that […] simply find some folders there, see what was done earlier and you start to look for solutions there*."

6.3. Challenge 3: Organisations do not always share the same safety philosophies and understand safety requirements in the same way

The challenge of having different safety philosophies, or perceptions of what is affecting safety, surfaced when the organisations involved in the same design process represent different national cultures. Possible misunderstandings of the concept of continuous improvement between foreign designers and the Finnish Regulator require additional interactions and communication. Moreover, misunderstandings concerning safety requirements may occur between operating organisations and design organisations even if they are from the same country. Obviously, different organisations and project members have different focus in the project work (e.g. technical/mechanical aspects, human factors aspects, construction, electrical aspects), which could create frictions in the execution of the design work. In order to harmonize these different perspectives, multiple disciplines need to be integrated and cooperation between personnel has to take place in order to find acceptable solutions. In the interviews, this challenge has been referred to as follows: *"That's the classification documentation problem. There's a system in place, and it has a safety class, but the division into operational parts is not accurate enough. […] But that's a minor problem. In case of inaccurate documentation a minor conflict is possible between different departs"*. By dividing the design into operational parts, there is the risk of losing the big picture in terms of functionality of the design projects.

The role of regulators in the design process was brought up in the interviews as well. According to one of the interviewee, regulators tend to look too much into details "*as if they have to state an opinion"*, instead of focusing on oversight of the overall safety. Some of the interviewees perceived that an increase of the paperwork, required by the regulator, subtracts resources from the actual design work.

Further, different attitudes towards safety requirements of designers and those executing the designs in detail have surfaced. While the former emphasises conservative decision making, the latter may focus more on quality issues of their work. In one of the interview it was brought up that not only designers and operating personnel should understand the safety requirements, but also the people involved in the commercial contracts concerning the design process at the power companies.

Coping strategies associated with Challenge 3

In the analysis of the interviews it emerged that a practice for dealing with different perceptions of what is affecting safety was to closely collaborate with other partners. In this way divergences in understanding safety requirements was reduced and collaboration and cooperation run smoother. In his/her words this was "*we work together; we work together so closely that coordination is part of cooperation*". To address the problem related to having adequate understanding of the Human Factors safety requirements, it was suggested to create a common definition among design projects' participants of what is included in human factors.

6.4. Challenge 4: Coordinating activities may be difficult between organizations that work according to different logics and understandings

Coordination of activities in design processes is probably the most recognised challenge discussed by the interviewees, largely due to the nature of design activities in nuclear domain. Besides, the multiple stakeholders involved, different perspectives on this activity, iterative nature of the design work, and potential geographical distribution of partners all contribute to making coordination challenging.

Coordination of activities is perceived especially challenging when design projects involve long subcontracting chains. The main problem is that the longer the chain is, the "*the further down you go with the sub-supplier chains, the less they see the connection"* between different nuclear safety aspects. Furthermore, the regulators require operating organisations to keep control on "*everything to the last details*" and make sure that manufacturing companies have a proper understanding of nuclear safety and on the functioning principles of nuclear power plants. A representative from regulators expressed his/her point about this issue as follows: "*the challenges in the cooperation between us and the licence holder are well known, but I'd say we've managed them pretty well. What I don't know, I mean, I see people from* (consultancy company Ed.) *there at the plant, during deployment inspections, but I'm not aware of the procedures in place between them and the client, I don't know that side of things*". Actually, the challenge to understand to what extent the subcontractors are knowledgeable about the safety requirements could be related to different factors, such as unwillingness to disclose everything to the client, contractors' tailoring their competences and processes to big client's expectations to get the contracts signed, or resource issues related to inspecting and auditing potential contractors. Also, language barriers can emerge when suppliers and sub-suppliers have national background different from the purchasing organisation.

Yet another challenge is to interact and coordinate with other stakeholders, including regulators and inspectors, to gather information about nuclear safety risks due to introduction

of new designs. This potential problem is emphasised when interacting with new organisations and in case new requirements have to be taken into consideration. When asked if he/she thinks coordinating activities are challenging, a representative from regulators said: "*I agree, in particular when something new is designed, involving a new organisation and new requirements. It's easier if you've already designed the product in the same organisation and with the same requirements*"

Dealing with regulatory requirements and the interaction with regulators was often discussed by the interviewees. The interaction and communication with the regulators during different case studies did not create any major problem thanks to well-established practices, such as existing design plan paper models and the routine of phone and face-to-face interactions. Nevertheless, sometimes understanding, interpreting and timely complying with the full range of authorities' requirements and guidelines has proven to be challenging. The difficulty to write a clear plan with limited points for misinterpretations was reflected by one of the interviewees as follows: "*what's challenging is communicating with the authorities, in writing, on paper you know, since what we do is we may discuss an issue with the authorities over the phone and both parties are aware of the fact that writing unambiguously, it's incredibly difficult. It's easier to speak and explain something, to make it understandable. But since there has to be a document, we have to put it in writing and do our best to make the text as unambiguous as possible. I'd say that's the biggest challenge in these jobs*"

Following guidelines can pose challenges even when they are internal. Human Factors guidelines are not always established since the very beginning of design projects and ad hoc ones are created in the process. Design processes seldom go by the book, and time and resources can be limited. It is often the case that for example suppliers need to close issues for commercial reasons and thereby some interactions are skipped. Interestingly, it was reported in one of the interviews that for the engineering community interactions are often perceived negatively since they are seen as expression of failures. Keeping track of the different stages of design projects by the different organisations involved was also reported as a challenge potentially leading to different participants "*running their own race*". Paradoxically, when time pressure increases more reporting is needed and less time is available for doing the actual job.

Some of the interviewees reported that parties are somehow getting a bit further from each other along the execution of design processes. In one relevant example this led to lack of operators' involvement in the design process. According to one of the interviewee, during the critical period of definition of operators' requirements, the operating company "*was not actively participating in the project. Of course, say, due to our internal quality assurance procedures they were in verifying, everything that we produced but, spiritually they could've been more involved"*. Intangible aspects, as the "*personal chemistry"* between participants to avoid clashes, or the personal commitment to the projects are important contributing factors for coordinating activities.

Coping strategies associated with Challenge 4

Probably due to the relevance of this challenge for all the parties interviewed during the case studies, a high number of practices which are in place throughout the network of organisations involved in the design processes were mentioned. Few of them are overarching for most of the challenges as the desire to have extra time for reviewing documentation before sending them to authorities, and to involve designers and Human Factors experts since the very beginning of design works. Others are more specific practices ranging from management practices to availability of supporting tools for the different phases of the projects.

Working in a team and having more discussion and communication within the different teams was deemed essential for ensuring good coordination of activities. Also improving leadership aspects and sense of responsibility for the different people involved in the projects were mentioned as supportive means for making things run smoothly. Commitment of operating companies was said to be achieved in one case study by nominating the person who will be responsible for the operation of the end product, the responsible for the outcome of the project. In that case a responsible person from the operating organisation was appointed as owner of the design project.

Weekly contacts between design and operating organisations were also an established practice for supporting coordination. This routine was considered beneficial for ensuring a "*110% connection between organisations"* as a way to keep things moving in the desired direction through "*continuous meetings, discussions, etc."* From a project management perspective, having and properly using IT tools was a positive factor for better following up the plans and schedules. IT supporting tools were also considered useful for facilitating the writing of extensive preliminary planning and documentation for authorities. By the implementation of such tools, two main results would be achieved: first, the writing process would speed up allowing more available time for the actual design work; and second, the use of IT support tools for preparing the documentation makes it easier to transfer requirements from "one document to another". According to an interviewee this is especially important when the design work is subcontracted from the power company: "*When we do it like this internally […], it's quite easy to track the requirements, but if we had external parties involved, it might be, somewhat problematic at times*". In addition, a tool ensuring consistency between documents with respect to requirements is fundamental for facilitating the process of approval "*and then we write the preliminary plan, and there's a paragraph that completes the requirement. But if there's no link between them, the authority says that it's here, but I can't see that it's there, because the link is missing between them*".

Good practices are established for coordination of activities between power companies and authorities, such as informing authorities in advance about future jobs at the plants. Knowing who is responsible for what, who to call for information or clarifications clearly support the execution of design processes. Having face-to-face meeting between regulators and licensee to solve unclear points is considered from both sides a good practice. A representative from one of the regulators said that these occasions are used also for ensuring that the interpretation of guidelines is correct.

6.5. Challenge 5: Distributing responsibilities and balancing roles between different stakeholders

On one side there is the challenge of clearly defining responsibilities within one organisation and of ensuring that everyone and every department act as expected. Designers at one of the plants considered a certain project as successful despite that when tested it caused an event: designers believed though that it was not designers' responsibility but the operators'. In this respect one representative from a power company said: "*For example maintenance would like to plan our* (designers Ed.) o*perating models. Of course we listen to what maintenance has to say, and discuss things. But the way it works here is that we don't do the design based on that. We listen to other organisations, but at the end of the day, we have to make the design decisions and choose how we implement it"*. At least in one of the power companies small projects, roles and responsibilities formally are determined by the circulation of the "*folders*" (i.e. of the documentation related to design work), as there are no project groups. However, in case of large design projects involving multiple stakeholders the roles are divided since "*there's a closely knit internal organisation, but in larger, bigger modifications, project groups can be quite large, when different organisations are involved. And there are internal*

project meetings, discussing someone's opinion and we find common ground and understanding". Even if these formalisms are in place, it is still difficult to ensure that all involved partners understand the demands of the projects. In the reality of complex projects, it could happen that the project members do not know exactly who is responsible for what and who in practice is taking decisions. On the other hand, the decision-making is distributed because multiple viewpoints and competencies are needed.

Besides, there is the challenge of defining roles and responsibilities between buyers and vendors and managing the interfaces when design activities are purchased from several subcontractors. As one of the interviewees put it *"of course the, you know, customer's supplier side, they try to specify the responsibilities and roles by using different documents, such as agreements, specifications, product-related quality control and so on. But as regards design of new things... Well, it can sometimes be unclear but I wouldn't generalise it like that"*. The perceived experience of designers plays an important role in reassuring the buyers that everything has been taken into account.

Another aspect to be considered related to role and responsibilities concern the regulator *vis-à-vis* the other stakeholders involved in the design process: to what extent the regulators should oversight the design activities of subcontractors? The position of regulators in this respect is that licensees are held responsible for the work and safety culture of subcontractors and suppliers. This attitude implies that the role of regulators is limited to the oversight of final products and the activities of power companies. Therefore, licensees should have the role of requiring and verifying that the companies they interact with effectively possess appropriate systems and structures, knowledge and understanding of risks, and mindset for the performance of good work. In a way this is a relief of responsibility for regulators, but it may be a burden, not only in terms of accountability but also in terms of resources and competences, for the licensee. The overall attitude of the regulator with respect to inspections was also subject of concern for some of the interviewees. The point that was raised was if the most effective focus of attention of regulator is on technical details or rather on the overall functioning and safety of the system.

With respect to the *modus operandi* of regulators it is interesting to point out probably the main difference between the Finnish and Swedish regulatory agency. The main involvement of the regulator in the design process is in the approval of design documentation and following inspections to certify that the end-product respects the functional and safety requirements. It seems that STUK in Finland and SSM in Sweden pursue this objective in slightly different ways: STUK is involved in supporting the different stages of the design process by giving recommendations and suggestions for improvement even in informal settings, which at best leads to identifying potential problems as soon as possible.

On the other hand it is important for the regulators to play an independent evaluator's role, which is their core task. Being somehow involved in the different phases of design process questions this independency. 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? According to the interviews performed in Sweden, SSM seems to be more detached from the design process: the Swedish regulator intervenes only once the documentation is submitted for approval, which formally makes SSM more independent than STUK.

On the other hand, a remarkable amount of time and resources are invested in the development of an end product without knowing if the design is ultimately the right one. The consequences of this could be that for fully approvable designs (or which requires small modifications) the evaluation will actually be considered as fully independent. For clearly

not-approval designs, it will be required to the licensee to invest resources for correcting them. For designs which are in a grey zone of acceptability in between the two (unlikely) extremes, there may be pressures (real or perceived) for temporal or economic reasons for approving them (especially if the gain in functionality and/or safety is minor compared to the cost of e.g. rethinking the design from its basis).

Coping strategies associated with Challenge 5

Good practices for coping with the challenge of attributing responsibilities between different stakeholders and fulfilling attributed roles were suggested during the interviews. For instance, one of the case organizations developed an internal project model for clarifying the execution of the projects, while another power company increased the number of professional project managers. For what concerns the Finnish system, the practice of having regular meetings with the regulator was perceived as very supportive for the successful execution of design projects to the extent that STUK has considered including it in the future YVL guides. As one of the interviewees from a power company said: "*STUK had very good recording on what was going on, […] So I am very pleased to hear that […] this procedure […] now it's written in the future YVL guides"*. This will result in a formal recognition of the role of the regulator in the processes as being involved throughout the design projects to support the development of the end-products. To cope with the issue of knowing who is responsible for which parts of the development of the end-product in large complex projects, it was mentioned in the interviews that projects should be performed in-house: "*It would be a different thing if there were several external organisations involved, then there might be problems, establishing who's doing what*". Human resourcing, in the sense of allocating the right person to the right position, was quite obviously considered important. This was especially the case for big projects, where a clear definition of responsibilities areas is needed for coping with the complexity of the work.

6.7. The specifics of the nuclear industry as another challenge

Another challenge has been reported during the interviews: *working in a conservative industrial domain.* This is represented in the way defences and safety measures are taken, in the way regulation is written, as well as in the way changes are dealt with. In the process of conceiving, designing, installing and maintaining technology, nuclear industry tends to rely on known, tested, validated and already implemented technological solutions. Even though conservatism is usually considered essential in ensuring safety, it can also pose some challenges. Implementation of new technologies based on for example digital solutions which may be safer and more effective than the currently used is challenging because it is not tested in nuclear plants. As one of the interviewees said: "*The biggest compromise is the fact that the verification of new technologies is so complex, and expensive […] that even if we could implemented a finesse better with a new technology, it seems impossible to get it approved for use in a nuclear power plant*". The result of this conservative attitude is also that as time passes it becomes harder to find personnel, especially in the automation domain, trained and interested in dealing with old-fashioned technology. The opinion expressed in one of the interviews was that in the near future "*there will be less and less people with sufficient understanding of functioning of the currently implement technology*". To address this issue, it would be required to establish training programmes focused on the functioning and developing of technologies acceptable according to the nuclear industry standards and to look for young personnel interested in learning about them. Another impact of the conservatism of nuclear industry is that procurement activities can become complicated even for simple equipment. Almost everything installed and used in a nuclear power plant has to respect strict safety standards and requires detailed documentation. Frequently there are increased costs and delays for obtaining components, which would otherwise be relatively cheap and more easily

available in other industrial domains. A summary of the challenges, coping strategies and their relevant cultural aspect is presented in Table 1.

Table 1. Summary of identified organizational challenges, coping strategies and cultural aspects.

Specific challenge	Coping strategies	Cultural aspect
Challenge 1. Safety is not always the first and most important guiding value in the design process • To find an appropriate balance between safety and economics • To carry out detailed inspections and making demands while realising the strong commercial pressures power companies face • To achieve reasonable and acceptable safe solutions considering financial and temporal pressures • To develop extensive preliminary planning • To implement new requirements in the design • To prepare extensive paperwork for the approval results in more time pressure and less availability of resources for the actual design	• Avoid big external pressures for respecting schedules • Have more competent human resources • Have great morality, to be mindful and concerned with nuclear safety • Have design organisation and operating organisation as part of the same company	Shared mindset
Challenge 2. Understanding the context where the designed end-product will be utilized may be difficult for the designers and this may lead to dysfunctional designs • To have limited knowledge of operating plants layouts and requirements by designers • To have a not adequate representation and image of the actual plants • To include Human Factors in the end-product • To understand the formalisms of design processes in the nuclear industry • To understand the effects of the introduction of a new design in the existing system	• Have personnel from the plant involved in in the specification of requirements for the design • Keep control and oversight on the design process • Bring Human Factors competences in the process since the moment contracts are written and signed • Educate project participants in the basics of Human Factors • Select competent decision makers for plant modifications • Keep track and document previous design projects	Understanding

Challenge 3. Organisations do not always share the same safety philosophies and understand safety requirements in the same way • To consider enough buffers when designing components • To have different foci (perspectives) of attention in the project work (e.g. technical/mechanical aspects, human factors aspects, construction, electrical aspects) • To have different perceptions on what is affecting safety • To have different attitude towards safety requirements and design (conservative decision making vs. focus on quality issues)	• Have enough buffer capacity in the current and future designed systems • Create a common definition of what does human factor mean • Closely collaborate with other partners to create shared understanding on safety requirements	Mindset Understanding
Challenge 4. Coordinating activities may be difficult between organizations that work according to different logics and understandings • To manage long subcontracting chains • To deal with suppliers and sub-suppliers with different national background • To interact with new organisations with which there are no previous experiences of collaboration • To consider new requirements • To understand, interpret and comply with authorities' requirements and guidelines • To communicate the respect of requirements and guidelines to authorities • To be overconfident on the effectiveness of the guidelines for running projects • To keep track of the different stages of design projects • To avoid parties getting further from each other along the execution of design processes	• Reserve extra time for reviewing documentation • Involve designers and Human Factors experts since the very beginning • Work in teams and to have more discussion and communication within the different teams • Improve leadership and sense of responsibility • Nominate the person who will be responsible for the operation of the end product as responsible for the outcome of the project • Have weekly contacts between design and operating organisations • Use IT tools for better following up plans and schedules • Use IT tools for facilitating writing of extensive preliminary planning • Use IT tools for supporting consistency between documents with respect to requirements • Inform authorities in advance about future jobs • Have regular contacts and open relationships with the regulator, e.g. regular face-to-face meetings between the regulator and licensee could clarify unclear points and solve problems	Structure and processes Understanding

Challenge 5. Distributing responsibilities and balancing roles between different stakeholders • To define responsibilities within one organisation and to ensure that the everyone and every department act as expected • To make sure that all involved partners understand the demands of the projects • To define roles and responsibilities between buyers and vendors • To manage interfaces between organisations • To define to what extent the regulators should oversight the design activities of subcontractors • To involve the regulator in the design process	• Have regular meetings with the regulator • Perform in-house projects • Identify technical and human factors demands especially in the interaction with contractors	Structure and processes Understanding

7. Discussion and conclusions

The SADE DESIGN NKS project was structured in three phases. During the first phase (2011) we reviewed the relevant scientific literature and identified the topical human and organizational challenges related to the design process. The second phase (2012) focused more specifically on exploring the challenges and opportunities related to collaboration and communication between the designers and the end-users since design in the nuclear industry is usually performed by a network of organizations. Identifying and clarifying various tensions and trade-offs that people involved in design and management of nuclear power plants were seen as one means to resolve them. It should be noted that different network actors have different ways of balancing tendencies, and if the design network is not aware that there are tensions and different solutions to them, then miscommunication is likely to occur. We assume that the previous lessons learned have been taken into account by the design organizations in the nuclear industry.

The third and final phase of this project (2013) aimed at testing and evaluating the results of the first two phases through in depth analysis of selected design case studies conducted in Finland and Sweden. Throughout the different case studies recurrent themes emerged. We related them to systemic aspects, which frame and influence the possibilities for conducting design projects safely and effectively. Some systemic aspects refer to the existence of *temporal* and *economic pressures* which, to a certain extent, compromise the optimal execution of design processes. The intrinsic *uncertainty* of designing end-products plays a role in the way design projects are performed, that is, by involving multiple stakeholders, which calls for extra effort in coordinating, understanding requirements and preparing documentations. Unfamiliarity with nuclear requirements and operational contexts is a potential source of suboptimal solutions. The general *conservatism* permeating the nuclear industry has an impact on both the possibilities to develop and implement innovative technical solutions, and on the time required for purchasing components to be used within the plants. It turned out that power company representatives often perceived “design” mainly as paper work, e.g. drafting documents and carrying out the required checks, whereas the innovation side was almost absent from their discussions.

Design activities include developing ideas, negotiating, proposing and implementing solutions to real-life problems. However, the study indicated that the nuclear industry representatives approached the design processes mainly from “paperwork” point of view, focusing on review and approval of design plans; an approach, which is fairly insufficient. The quality of design was considered to depend largely on designer’s tacit knowledge and his/her understanding of the context and conditions where the technology/design solution is going to be implemented. However, design process involves both rational and creative approaches to a problem. Fulfilling specific requirements, including an extensive amount of paperwork, which requires time, resources and usually a long chain of approval by various stakeholders, is only part of what designers face in the nuclear industry. The other part of their work, though, refers to the need to create something new, which is both safe and functional. Thus, to better support human and organizational performance in design processes, the nuclear power companies, engineering companies and design supply chains need to nurture a culture that shares the importance of this dual perspective in a networked context.

The study revealed that safety is clearly recognized as a top priority during design, operation, and maintenance of nuclear power plants. At the same time, participants in the design projects in this study mentioned the pressure of schedules and costs, which make them feel that at

times “safety first” principle was not always easy to implement in practice in the design process. To balance between these conflicting goals it is necessary to involve people with competencies in e.g. technology, human factors and economy in the planning of projects to discuss the potential conflicting goals and find an acceptable compromise. It is recommended that people involved in the design process and decision making should have at least basic knowledge in human factors.

The need to provide all the required documents on time could also slow down the design process, especially for people not working inside the nuclear industry. The tendency to use and rely on tested and validated technology in the nuclear industry imposes a number of restrictions that may not always be known by outsiders of the industry. Organizations without knowledge of the conditions for nuclear power plants should be informed and learn about safety requirements in the industry, early in the design process, by representatives of the nuclear industry. To minimize time-consuming administrative tasks, it is recommended that appropriate IT support for documentation is used and clear working routines are established for reporting to authorities.

The design organization and the operative organization should develop a common understanding of safety aspects in the design process. For instance, there should be communication and agreement on when a design change is a human factor or a technical issue. It is recommended to create an understanding of Human Factors and safety, which has a system perspective where both technical and human factors aspects are represented. It is also recommended that multidisciplinary groups participate in projects, where the work environment is affected by the design work. Entrepreneurs involved in large nuclear projects could also be provided with a basic education concerning safety in the nuclear domain. A safety culture should be implemented, meaning a culture where safety is a concern for all people involved in the design project. Incidents and mistakes should be reported without fear for blame or punishment. It should also be a culture where it is possible to learn from mistakes, and a culture that is flexible, where authority to make a decision depends upon expert knowledge and not on formal position in the organization.

To understand how complex organizations function, Weick (1995) introduced the concept of *sensemaking*, which usually refers to how meaning is given to past experiences in organizations. According to the interviews in this study, the need to make sense of the effects of introducing new design in an existing system was pointed out as the possible side effects of a new system may be hard to predict. A recommendation is therefore to be prepared for side effects and actively look for them. To improve the possibilities for stakeholders to understand the context for the designed end-product it is recommended to form groups of people with different competencies, technical as well as human factors competences, when modifications are planned, implemented and in operation and maintenance. Decisions should be taken by this group collectively. The availability of people with relevant Human Factors knowledge in the Nordic operating nuclear power organizations is somehow limited, so external consultants are often employed in the design process. In some cases consultants with relevant Human Factors knowledge are involved too late in the process to make any difference.

The co-existence of different safety philosophies and understanding of safety requirements emerged from the interviews, and was especially pronounced in large and complex, multi-cultural projects. Even organizations in the same country often have different perspectives, i.e., technical *vs.* organizational. The classification of safety-related problems could also vary, depending on the perspective of the classifier. Regulators are often focused on details, which create an increase in the paperwork needed. Operating personnel and designers were also reported to have different attitudes toward safety requirements: operating personnel tend to

favor conservative solutions, while designers focused on quality aspects. The demand from regulators to have optimal control over the design process can be challenging as well. Monitoring closely the progress of large and complex projects creates a risk that different stakeholders are doing their job without sufficient knowledge of the other stakeholders' progress. The coordination of activities may be more or less lost, which may lead to tensions between involved stakeholders.

Large and complex design projects in nuclear industry involve many partners with distributed work and distributed decision making. Besides, a conflict is possible between distributed and centralized decision making. Centralized decision making may increase control over the entire process but will put a strong burden on the decision makers and possibly slow down the working process. Decentralized decision making may be effective and make it easier to solve unexpected problems. A disadvantage is that it makes it harder to get a holistic view of the design process. It is recommended to create better IT support for documentation and communication of the process status.

The existing literature on Highly Reliable Organizations (HROs) states that there are five principles to guide the work:

- *Principle 1:* Preoccupation with failure

It means that any lapse may be a symptom that something may be wrong with the system, something that could have severe consequences if several small errors happened to coincide. HROs encourage reporting of errors and are aware of liabilities of success, complacency, temptation to reduce safety margins, the drift into automatic processing.
It is recommended to improve the incident and accident reporting system and closely analyze errors and do what is possible to learn from them.

- *Principle 2:* Reluctance to simplify

The world is complex, unstable, unpredictable, take steps to create a complete and nuanced picture of what you are facing. Welcome skepticism; accept diverse experience and different opinions. To recognizing something may be dangerous, superficial similarities between present and past events could lead you in the wrong direction.
It is recommended to create groups of people with different educational backgrounds, i.e., technical and behavioral, to analyze the impact of changes when modifications of NPPs are planned.

- *Principle 3*: Sensitivity to operations

Be attentive to the front line or the sharp end where the actual work is being done. The "big picture" in HROs is less strategic and more situational than in most other organizations.
It is recommended to involve operating personnel early in the planning of changes.

- *Principle 4:* Commitment to resilience

No system is perfect and we must learn from failure. The essence of resilience is the intrinsic ability of an organization (system) to maintain or regain a dynamically stable state, which allows it to continue operations after a major problem or during continuous stress. HROs develop capabilities to detect, contain, and bounce back from those inevitable errors that are a part of an undetermined world. Not error-free, but errors that do not disable it. Resilience is a combination of keeping errors small and of improvising strategies that allow the system to function. The demands are deep knowledge of technology, the system, one's coworkers, and oneself.
It is recommended to create groups of people with different backgrounds and give them the task of creating worst case scenarios and ways to cope with these scenarios.

- *Principle 5:* Deference to expertise

HROs prefer diversity because it helps them to notice more in complex organizations and to act more. Rigid hierarchies have their own special vulnerability to error. Errors at higher

levels tend to pick up and combine with errors at lower levels, making the problem bigger, harder to understand, and more prone to escalation. HROs push decision making down and around. Decisions are made on the front line, authority mitigates to the people with the most expertise, regardless of their rank. It is recommended to create an organizational structure that allows people with expert knowledge have an impact on important decisions, regardless of their position in the organizations hierarchy.

To be resilient, an organization must be able to cope with disturbances, and to have the capacity to anticipate disturbances that have never occurred before but are still possible in the future. It is recommended to create groups of employees with different backgrounds and give them the task to invent new possible disturbances with safety implications. After that, develop coping strategies for these new, more or less likely disturbances. The interviews in this study provided strong support for the importance and challenge of coordination and collaboration, especially in large complex projects with suppliers and sub-suppliers, different cultures, language barriers, and different opinions concerning safety requirements.

It is recommended to use IT support in order to monitor and visualize the project and the status of the different parts. To control a system the operator must have a mental model of the system (Conant and Aschby, 1970) and to communicate it to all involved stakeholders in a meaningful way. This is one possible way to improve the shared mental model of the stakeholders. Communication about delays and reasons for delays could possibly improve the interaction between stakeholders and reduce tensions and conflicts. The complexity of a project should have an impact on the size of the steering committee, and a multidisciplinary approach is probably the only way to proceed. Human Factors aspects should be recognized early, to avoid surprises later in the process.

Studies of dynamic decision-making (e.g. Brehmer, 1992) have identified a number of sub-optimal strategies to control large and complex projects. For instance, encapsulation, or maintaining a narrow focus on a single part of the problem and ignoring its connection to other parts have been demonstrated in experimental studies. Thematic vagabonding, meaning jumping from one topic to another topic quickly, without going into necessary detail, has also been identified. Improper delegation and shift in responsibility to others, and blaming them when things go wrong has also been identified. It seems that these strategies also may occur in real life and should be avoided.

The challenge is to clearly distribute responsibilities and balance roles between the involved stakeholders. In complex projects it is sometimes hard to know who is responsible for what and who should decide the progress of the work. A challenge has been reported when defining the responsibilities between the operating organization and their demands on a product and sellers expectations. Lack of specification of the desired product/service has sometimes caused extra discussions and negotiations, and consequently delays in the process. Another problem mentioned was the Regulators' preoccupation with technical details instead of a focus on the overall functioning of the system. The difference between authorities in Finland and Sweden, where the Finnish authorities follow the process closely and are early involved was discussed. The Swedish authorities are usually not directly involved in the process. These different strategies have both advantages and disadvantages and the question is which strategy is most efficient. To cope with the problems a strategy was to have regular meetings with the regulators. A recommendation is to make specifications of products or services more explicit to avoid long discussions concerning what was expected from the supplier.

Another challenge that emerged was the conservative nature of the nuclear domain. Since products must be tested and verified before they can be used, and operators are used to established practices and tools, the use of newer technology often is delayed. This is, of

course positive from a safety perspective, but also means that it may be hard to recruit people to an organization where the advantage of new technology takes a long time. An often reported time consuming challenge is the administrative burden of documentation. Routines and support systems could possibly make this time consuming burden less time consuming and make it possible to devote more time to the actual design work.

One of the main conclusions of this study is that challenges in the design processes in the nuclear domain are mainly inter-organizational. The previous literature seems to focus on the design process and design phenomenon itself and not on the challenges that arise in a network of organisations involved in design, which takes place when designing to a highly conservative and demanding domain. Overall, the study revealed that for some of the challenges (e.g. coordination) there are plenty of existing practices applied throughout the network of organisations involved in the design processes. However, for others, such as shared understanding, just a few coping strategies were mentioned.

The study indicated that interaction is needed between design and other organisations regarding shared and improved understanding of issues important to safety in design in the nuclear domain. This interaction should take place in the continuum of explicit requirements that all stakeholders should be aware of to the less easily expressible safety values and safety philosophy. A way or working should be shared among stakeholders that facilitate mutual understanding and knowledge transfer of acute matters as well as underlying principles and facts which may emerge as more urgent at some phase of the design process.

8. Summary of recommendations

The study provides a set of recommendations to the nuclear industry community to support and improve the design process and to anticipate emerging risks. The design process evolves in a complex system operating under uncertainties, with multiple interdisciplinary international stakeholders with conflicting goals, under time and financial pressures where safety is critically important. We recommend that to improve design processes in the nuclear domain, the nuclear industry community should concentrate on following practices:

- **Develop “design thinking”**
  - Acknowledge that designers working on safety-critical systems and components need to balance their role of innovators and rational problem solvers set by the nuclear power specific technical design principles. To develop safe and functional design in the nuclear power domain, designers need to balance between creating something new and dealing with an extensive amount of paperwork. Although in the conservative context of the nuclear industry the operators are used to well-established tools and solutions, it should be recognized that the design process it is not only about drafting documents and carrying out required checks; it is also about innovation and creating new solutions for particular problems.
  - Assist designers in strengthening their process skills by creating conditions for them to “immerse” in active, flexible and reflective exploration of the problem space he/she is working with.
- **Develop and support “design safety culture”**
  - Create blame-free environment, in which design errors are reported early and documented properly, and develop efficient systems for incident reporting and organizational learning. Recognize that leadership can shift in different situations depending on the need for specific expertise. Ensure that all people

involved in the design process and the decision making have at least basic knowledge in human factors and safety culture.

- Involve human factors expertise in negotiations and during the whole design process and highlight the positive aspects of interactions for the engineering community.

- **Improve communication and coordination of activities**
  - Since challenges in the design processes in the nuclear domain are mainly inter-organizational, safety management and safety culture approaches should take better into account the inter-organisational nature of the work processes in design.
  - Develop transparent decision-making processes.
  - Document and store properly the information. Support designers in using IT tools for continuously documenting the design process, including providing arguments for design decisions, e.g. why one solution is preferred to another. Allow sufficient and realistic time for performing documentation tasks. Make sure the information is structured in such a way that makes it easy to find and follow up the history of specific design decision.
  - Keep track on the different stages of design project; avoid different organisations involved in the design process to "run their own race".
  - Acknowledge the possible risks involved: increased communication should not lead to "group think" situations because this might produce imperfect or even wrong design solutions.
- **Create a shared understanding** of safety conditions and operational requirements in nuclear industry for all stakeholders involved in the design process.
  - Construct shared plans for future actions, resources, etc. in a distributed network of several stakeholders by applying e.g. multi-agent planning approach. Provide each stakeholder with timely and correct information about the other relevant actors, as well as means to resolve conflicts. Acknowledge that information is spreading also largely through informal networking.
  - In dynamic and complex environments, use partial global planning approach by continuously updating the information and reformulate shared plans in view of new information. Recognize that local actors need freedom to build their own plans and these are shared with others in the network to improve coordination. Create conditions and shared spaces for technicians and HF people to work together. Involve end-users and operators in all phases of the design process, if relevant.
  - To better manage safety culture in design activities in a networked context, nurture a shared understanding between the nuclear power companies and design supply chains on the "dual perspective" of design - improve the understanding that design process involves both rational and creative approaches to a real-life problem.
- **Develop a systemic perspective** throughout the design process
  - Develop a holistic overview of the design process - draw the system's boundary widely to include relevant interdisciplinary and international stakeholders important for the success of a safety-critical design project.
  - To help imagine short-term and long-term consequences of design solutions, acknowledge the interrelations of technical, human and social issues and their effects on the outcome of the design process.

Acknowledgments
NKS conveys its gratitude to all organizations and persons who by means of financial support or contributions in kind have made the work presented in this report possible.

Disclaimer
The views expressed in this document remain the responsibility of the authors and do not necessarily reflect those of NKS. In particular, neither NKS nor any other organisation or body supporting NKS activities can be held responsible for the material presented in this report.

References

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

Brehmer, B. (1991). Distributed Decision making: Some Notes on the Literature. 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.

Brehmer, B. (1992). Dynamic decision making: Human control of complex systems. Acta Psychologica, Vol. 81, pp. 211-241.

Conant, R.C. and Aschby, W.R. (1970). Every good regulator of a system must be a model of that system. Int. J. System Sci., vol 1, No 2, 89-97.

Durfee, E.H. and 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 Intelligence. San Mateo, California: Morgan Kaufman, 268-284.

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

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

Hale, A.R., and Hovden, J. (1998). Management and culture: the third age of safety. A review of approaches to organizational aspects of safety, health and environment. In: Feyer, A.-M., Williamson, A. (Eds.), Occupational Injury: Risk, 142 Prevention and Intervention. Taylor and Francis, London.

Hatamura, Y. (2009). Learning from design failures. Springer ISBN 978-4-431-25372-3

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

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

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 (2005). Safety culture in the maintenance of nuclear power plants. Safety reports series, ISSN 1020-6450 ; no. 42— Vienna : International Atomic Energy Agency, 2005. ISBN 92–0–112404–X

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

Kainulainen, E. (Ed.) (2009). Regulatory control of nuclear safety in Finland. Annual report 2008. STUK-B 105. Säteilyturvakeskus, Helsinki

Lloyd R., Boardman, J. and Pullani S. (2000). Causes and Significance of Design-Basis Issues at U.S. Nuclear Power Plants. NUREG-1275. U.S. Nuclear Regulatory Commission, Washington, D.C.

Macchi, L., Reiman, T., Savioja, P., Kahlbom, U. and Rollenhagen, C. (2012). Organizational factors in design and implementation of technological and organizational solutions in the nuclear industry, Progress report, NKS-R/SADE 2011.

Macchi, L., Pietikäinen, E., Liinasuo, M., Savioja, P., Reiman, T., Wahlström, M., Kahlbom, U. and Rollenhagen, C. (2013). Safety culture in design. Final Report from the NKS-R SADE activity, AFT/NKS-R(12)97/13).

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

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. and 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

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

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

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

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

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

Reiman, T., Pietikäinen, E., Kahlbom, U. and 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>.

Rollenhagen, C. (2010). Can focus on safety culture become an excuse for not rethinking design of technology? Safety Science, 48, 268-278.

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

Taylor, J.R. (2007). Statistics of design error in the process industries. Safety Science

Thompson, R., Hilton, T. and Witt, L. (1998). Where the safety rubber meets the shop floor: A confirmatory model of management influence on workplace safety. Journal of Safety Research, 29, 15-24.

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, issue 1, 44-56.

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

Weick, K. (1995). Sensemaking in organizations. Thousand Oaks, CA: Sage

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

www.analys.se (2004). Analysgruppen Bakgrund [Online, in Swedish] Available from: http://www.analys.se/lankar/Bakgrunder/2004/Bkg%201-04.pdf.

www.archive-se.com (2010). [Online, in Swedish] Available from: http://archive-se.com/page/147799/2012-07-18/http://www.okg.se/templates/NewsPage____993.aspx

Appendix – Interview scheme

Baseline: recorded group interview. A timeline with events will be made with start date and (previsioned) future end date. Beforehand needed: permission needed for the recordings and the participants should be asked to *prepare* to talk about how the project has proceeded in the past and will proceed in the future.

First questions:

- Object of design: what is the object of the design? What is the significance of the design for nuclear safety (safety class) and for the functioning of the plant? What is the scale (small – medium – large) of the design? Type of the design (muutostyyppi)? What types of technical disciplines or competences/expertise are needed for the design (automation, mechanical, electrical, human factors, experience from operators etc.)? At what stage is the design?
- Why the design? What initiated it? When did it start and what was the reason for starting it? (e.g. the original design of the plant, deficiencies found during the use of the plant, new requirements, operating experience review in the industry, production or financial drive)?

Secondly, a spread sheet (Excel sheet) will be filled jointly; guidelines for the making:

- Building timeline of the project with relevant episodes that interviewees bring up and description of the episodes (what was done by whom (in collaboration with whom))?

1) In-depth interview (individual interview)

Baseline: individual interview with audio recording.

<u>Background of the interviewee</u>

- Educational background /degree
- Title
- Position in the company (to which group/unit does the interviewee belong to)
- Years working in the company
- Years working in similar kind of work
- If there is other relevant work experience, what is it?

<u>The design process story from the perspective of the interviewee</u>

The jointly made "Project timeline" will be used as a reference here.

1) Can you define design (work)? How do you understand what design is about? (is there any special features of designing?)
2) Can you describe in your own words and from your own perspective, how has this design process proceeded, is there anything you would like to amend at this point or do you concur with the sheet?
3) What have been the most challenging events or episodes (on the spread sheet)? -> If nothing has been challenging, ask for (three of) the most challenging. -> Describe reasons as to why they have been challenging and how have you dealt with these challenges.
4) What have been especially well accomplished events, what has been done especially well? -> Why?
5) What have been badly or non-optimally accomplished events, what has not been done right? -> If none, mention the least successful event. -> Explain further, why?

6) Were there challenges in collaboration between the different actors? What were these challenges like? How did you deal with the challenges?
7) Were there any specifically good practices ("erityisen toimivia tähän suunnittelutyöhön liittyviä käytäntöjä/ toimintatapoja") that you would like to mention at this point (in addition to those that have been already noted)?
8) Were there any specifically bad or imperfect practices ("jotain suunnittelukäytäntöjä, jotka eivät ole olleet hyviä tai jotka voisivat olla parempia") that you would like to mention at this point (in addition to those that have been already noted)?
9) Can you compare the way this design work has been carried out with other projects and/or other experiences you have been involved in?

2) Challenges

Continuation in individual interviews.
Preparation: "Next we will present some provocative statements about NPP design in general (that is not related to your current design case) and would like your comments on them." (Each statement will be presented on a sheet of paper.)
Statements:

A. Ei aina täysin ymmärretä, mitä lopputarkoitus varten ydinvoimalassa jokin asia suunnitellaan ja tämä voi johtaa epäonnistuneisiin suunnitteluratkaisuihin. (Eng. It is not always completely understood why, that is, to which final purpose in NPP, certain issue is designed for and this causes poor design outcomes.) (Understanding the context where the design will be utilized may be difficult for the designers and this may lead to dysfunctional designs.)
B. Käsitys hyvästä turvallisuudesta ja turvallisuuteen vaikuttavissa asioissa vaihtelee eri organisaatioissa; tämä tuottaa ongelmia ydinvoimalaitoksen suunnittelussa. (Eng. Understanding on good safety ja on issues that influence safety varies in different organisations; this causes problems for NPP design.) (Safety philosophies may differ between different organizations.)
C. Ydinvoimalaitoksen suunnitteluun liittyvien aktiviteettien koordinointi on hankalaa, koska eri organisaatiolla on erilaisia käsityksiä ja toimintalogiikoita. (Eng. Coordinating activities related to NPP design is difficult because different organisations have different understandings and activity logics.) (Coordinating activities may be difficult between organizations that work according to different logics and understandings.)
D. Tehtävien ja roolien jako eri organisaatioiden kesken vaatii tarkkaa harkintaa ydinvoimalaitoksen (tai jonkin sen osan) suunnittelussa. (Eng. The distribution of tasks and roles among different organisations is challenging in NPP design (or in designing something for NPPs). Distributing responsibilities and balancing roles between different stakeholders needs careful consideration.
E. On tilanteita, joissa kustannuksiin liittyvät tekijät vaikuttavat ydinvoimalan suunnittelussa siten, että tehdään kompromisseja turvallisuuden suhteen eli kaikkein turvallisinta vaihtoehtoa tai toimintatapaa ei valita. (Eng. There are situations in NPP design in which issues related to cost-effectiveness influence so that compromises regarding safety are made, that is, the safest option or practice will not be selected.) (Safety is not always the first and most important guiding value in the design process and commercial pressures may hinder safety.)