NKS-263
ISBN 978-87-7893-336-2

Organizational factors in design and implementation of technological and organizational solutions in the nuclear industry

L. Macchi (1)
T. Reiman (1)
P. Savioja (1)
U. Kahlbom (2)
C. Rollenhagen (3)

1 VTT - Technical Research Centre of Finland
2 Risk Pilot, Sweden
3 Vattenfall, Sweden

February 2012

Abstract

Design is often found as one of the contributing factors in accident in the nuclear industry. The design of new technological systems and organisational structures has to take into account and be driven by the future users' needs and has to consider how their role and work practices within the organisation will be affected. The SADE project explores to which extend the concepts of safety culture and resilience engineering can contribute to the prevention of design errors when no hindsight data are available.

In 2011, the SADE project focused on gathering experience and clarifying the current issues and challenges related to the design process. During 2011 seventeen interviews have been conducted in Finland and Sweden to identify some of the major challenges the nuclear industry is currently facing. At the same time a literature review has been conducted to establish a sound common theoretical ground. This progress report presents some of the relevant theoretical findings and preliminary results from the interviews.

Key words

Design, Safety culture, Resilience Engineering, Human Factors Engineering

NKS-263
ISBN 978-87-7893-336-2

Electronic report, March 2012

NKS Secretariat
P.O. Box 49
DK - 4000 Roskilde, Denmark

Phone +45 4677 4041
www.nks.org
e-mail nks@nks.org

Progress report of

Organizational factors in design and implementation of technological and organizational solutions in the nuclear industry (NKS-R/SADE 2011)

L. Macchi, VTT- Technical Research Centre of Finland, Finland

luigi.macchi@vtt.fi

T. Reiman, VTT- Technical Research Centre of Finland, Finland

teemu.reiman@vtt.fi

P. Savioja, VTT- Technical Research Centre of Finland, Finland

paula.savioja@vtt.fi

U. Kahlbom, Risk Pilot, Sweden

ulf.kahlbom@riskpilot.se

C. Rollenhagen, Vattenfall, Sweden

carl.rollenhagen@vattenfall.com

Abstract

Design is often found as one of the contributing factors in accident in the nuclear industry. The design of new technological systems and organisational structures has to take into account and be driven by the future users' needs and has to consider how their role and work practices within the organisation will be affected. The SADE project explores to which extend the concepts of safety culture and resilience engineering can contribute to the prevention of design errors when no hindsight data are available.

In 2011, the SADE project focused on gathering experience and clarifying the current issues and challenges related to the design process. During 2011 seventeen interviews have been conducted in Finland and Sweden to identify some of the major challenges the nuclear industry is currently facing. At the same time a literature review has been conducted to establish a sound common theoretical ground. This progress report presents some of the relevant theoretical findings and preliminary results from the interviews.

Keywords: Design, Safety culture, Resilience Engineering, Human Factors Engineering

Contents

1. Introduction....4
2. The research design and scope of the progress report....6
2.1 Overall project structure and scope....6
2.2. Methods for year 2011....7
3. Findings from literature review....7
3.1 Design as an object of study....7
3.2 Events where design issues were contributing factors....10
3.3. Previous research on design....15
3.4 Human Factors Engineering....17
4. Preliminary findings from interviews and workshops....17
4.1 Findings concerning challenges in design....18
4.2 Findings concerning Human Factors Engineering oversight Finland....21
4.3 Findings concerning Human Factors Engineering oversight Sweden....23
5. Conclusions....23
5.1 Human Factors Engineering....23
5.2 Safety culture in design....24
References....25

1. Introduction

Weaknesses in design (including both technology and organizational structures) have often played a significant part in major accidents (Rollenhagen, 2010). Study of design errors have recently received increased attention in the field of safety science. Taylor (2007a, p. 62) defines design error as " *a feature of a design which makes it unable to perform according to its specification*". Accident analysis data clearly point to the relevance of design for system safety: 55 % of the accidents in chemical industries and 46 % of the accidents in the nuclear industry can be attributed at least partly to design errors (Taylor, 2007).

However, for most systems, there are usually a very large number of requirements which are included in the specification by reference, or are implicit. In addition, in modern complex socio-technical systems what works according to specification, i.e. it is reliable, does not necessarily mean that it is safe and the other way around. As acknowledged by the safety culture and the resilience engineering approaches, safety emerges from the non-linear interaction of multiple system components. A specific design can therefore endanger system safety even when it works according to specification, if it fails in properly interacting with the other system components. This poses a major challenge for the entire design process; it is not enough to design components without acknowledging the context in which they will be used, maintained and modified.

A better ‘‘safety culture" has sometimes become a standard response for coping with observed deviations (Rollenhagen, 2010). Such a quest for safety culture has the drawback of shifting the focus for improvements from design issues to "safety culture" issues, usually interpreted to mean behaviour or attitude modifications at worker level. On the other hand, the special nature and requirements of safety culture in design organizations have received little attention.

Rollenhagen (2010) argues that design organisations are often unbalanced towards technology issues, i.e. they put too little emphasis on the people that should operate and maintain the equipment. The introduction of new technologies to support operators' activity has to take into consideration the changes it will induce in operators' role. With an increased level of technology and automation, it is likely that operators will be more and more out of the control loop. Already in 1983 Bainbridge pointed out the ironic effects of introducing automation and technology for the purpose of reducing human contribution to risk. Bainbridge argued that the assumption that operators are basically unreliable and inefficient, and therefore they should be substituted by automating the system as much as possible, was fundamentally wrong. The oversimplified assumption about human capabilities is one of the reasons for this phenomenon. In addition, humans are still required for all the tasks that designers are not able to automate or for the tasks in which human supervision is required. According to Hollnagel (2011) the use of automation often introduces new problems without really solving the old ones. The introduction of automation results in operators forced to adopt a more passive role in controlling the industrial process. At the same time, in highly

automated socio-technical systems operators, while being mainly passive controllers of the process, still have to be active actors when technology and system fails.

According to Hollnagel's (2011) definition of resilience as "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions", it is necessary that the operators acting in the system are able to interact and deal with technology when under pressure, in degraded conditions or when facing disturbances.

For this reason, the design of new technological systems has to take into account and be driven by the future users' needs and has to consider how their role and work practices within the organisation will change (Laarni et al. 2010, Norros and Savioja, 2006). Norros and Savioja (2006, p. 277) remind that human performance may be considered from two points of view in design: Traditionally human behaviour has been perceived from the perspective of causing risk to the proper and safe functioning of the system. The other perspective emphasises the positive contribution of human performance for productivity and safety (cf. Hollnagel 2009). Thus, they advocate the use of a concept of "systems usability" as the ultimate quality attribute and target of human factors engineering. To accomplish the above, a sound (safety) management process is required for both design and implementation activities.

This management process and the design and implementation organisation have to be able to deal with the fact that all new systems exist in the beginning only on the drawing board and the fact that all designs are empirically unproven until they are put into practice. Thus *de facto* it is impossible to rely on historical data and/or experience feedback systems to support the design of new technological and organisational solutions and to assess risks associated with their introduction in the nuclear energy production system. The need to look at safety in other ways than solely on hindsight and error tabulation has to be satisfied (Woods et al, 2011).

The main objective of the project is **to identify the organizational challenges** associated with design and implementation activities and contribute toward better evaluation of the risks linked to new designs. The study will also seek to **provide information to support and guide the design process** from the human factors point of view, and to anticipate emerging risks in during the design process or in the implementation phase.

To contribute to prevent design errors when no hindsight data are available, in this project, the concepts of Resilience Engineering and safety culture are applied. The Resilience Engineering approach has not been so far thoroughly applied in the context of design. As well, the concept of safety culture has to be adapted to meet the particular characteristics of the design and implementation process. Partly different dimensions and approaches have to be scrutinised than those used for safety culture in the operation context. Particular attention has to be paid to the trade-offs occurring between innovation, operational and safety needs.

This project tackles the following research questions:

a) 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?

b) 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?

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

To address the research questions the study is structured into three phases that entail both theoretical and development issues.

2. The research design and scope of the progress report

The scope of this progress report is to present the achievements of the project work in 2011 and their implications for the continuation of the project in 2012.

This publication presents some of the preliminary findings from the activities performed both in Finland and in Sweden. The scope of the work done in 2011 was mainly to set sound foundations for future tackling the research questions of the SADE project. In this publication the research methods, their application for data collection and the preliminary results from the data analysis are presented.

2.1 Overall project structure and scope

The SADE project is divided into three phases.

The first phase (January 2011- December 2011) is focused on theoretical concepts and methods available to prevent design errors and to assess risks related to the implementation of technological and organisational solutions. This first research phase aims at **gathering experience** and **clarifying the current issues** and **challenges** related to the design process. Starting from the applied concepts and approaches actually used for assessment designs, this phase highlights their limitations by pointing to the corrective actions that had to be undertaken in response to unexpected drawbacks. The Resilience Engineering and the safety culture concept will be investigated for exploring their potential contributions to design activities.

The second phase (starting Jan 2012) consists in the theoretical contribution to both the Resilience Engineering and to the safety culture concepts and the **provision of information to support and guide the design process** and to anticipate emerging risks.

The third and concluding phase (Jan 2013-Dec 2013) of this study constitutes the **evaluation of the envisaged contribution** to contribute to improving design and implementation practices. The evaluation phase allows the identification of the strong points and the added value of the adoption of the safety culture and the resilience engineering approach with respect to the established practices.

2.2. Methods for year 2011

In order to achieve the envisaged results of the project for 2011, i.e. to gather experience and clarify the current issues and challenges, the two research methods have been utilised. The analysis and review of the relevant scientific literature and case studies was conducted first. The literature review covered the particularities of safety culture in design and the topic of resilience engineering with its implications in the design activities. The review showed that design activities have not been studied much from either safety culture or resilience point of view. The literature review was joined by field interviews.

Two groups of professionals were part of the interview sample. First, experts from the nuclear domain were interviewed either informally or as part of an introductory workshop. The contribution of these interviews was mainly in terms of identification of relevant questions to consider in main interviews, identification of the relevant cases to consider, as well as in finding the relevant persons to be interviewed. The second set of interviews addressed experts of actual design of new systems. In the interviews, in addition to design-specific questions, two questions were asked that were identical to those in the previous NKS study MOSACA (see Reiman et al. 2011): 1) "how do you define nuclear safety?" and 2) "what things you would consider if you would have to evaluate nuclear safety of an operating plant?" This allows us to compare the design experts' view on nuclear safety to those 30 experts interviewed previously from the various organisations in the nuclear field. In total 17 interviews were carried out in Finland and Sweden (STUK 4, Fennovoima 3, Fortum 3, Vattenfall 4, E.ON 3). These interviews dealt with the following themes: respondent's work and tasks, definition of nuclear safety, evaluation of nuclear safety, contribution of design to nuclear safety, understanding of design principles, human factors engineering, and safety culture in design organizations.

Workshop interviews concerning Human Factors Engineering practices were also conducted with the national regulator. The reason to utilize the workshop type of interview is that it was conducted in an exploratory phase of the research and thus preparation of an in-depth interview would have been premature. Also, the questions that the interview dealt around were rather factual and did not involve non-disclosure or personal issues which would have required a more confidential interview. The interview was conducted according to the themes so that the theme under discussion was projected to a white board so that all participants could always be aware of the theme under discussion currently. The themes covered in the workshop were Organization of the oversight of HFE in STUK; Personnel's conceptions regarding HFE; HFE practices in the on-going design projects at the utilities, and Future plans concerning regulatory requirements on HFE.

3. Findings from literature review

3.1 Design as an object of study

Reviewing the literature on design indicates that there is no common agreement on the definition (Trueman, 1998). One way to start is, however, to glance at the etymology of the word design. The Latin word *designare* means both to define and to draw, or to put forward

and give to form. One way of understanding the word is to draw with an intention of give form to something. Design can thus be seen as both process and a result which aims to express something (Borja de Motoza, 2003). In the context of the present report, the most relevant aspect is the process view of design. One broad definition of design is to conceive ideas, to plan and explain, to make decisions related to the development of the ideas and to solve the problem (Aspelund, 2006). The first part of the above broad definition of design is related to innovation, and the later part (and actually, also the first part), is related to rational decision making. One can also consider even broader aspects of design as a process, also taking into account planning, decision making, and management (Trueman, 1998). Bergman et al (2007) define design as the practice of inventing, creating, and implementing (technical) artefacts that depends upon, integrates, and transforms heterogeneous and uncertain domains of knowledge. This definition emphasizes that design is a *practice* taking place under uncertainty (cf. Norros 2004).

Based upon the literature a tentative description of the design process is presented in Figure 1. On the y-axis, the objects of design are reported. A design process can aim at designing several different elements or components of a system, from training to human system interfaces to procedures or structures etc.

On the x-axis, the temporal aspects of the design process are indicated. It seems to be relevant to first address the requirements of the design (which, depending on the problem area, can be dealt with as an innovation process or as a "predefined" task/component). Now, given the iterative nature of the design process, the next phase consists of a rather broad conceptual design which consists of a rough "picture" of the design. This is especially needed when the designed component is supposed to interact with other loosely defined components/systems etc. The next step, assuming that the conceptual design has been refined and adapted to the concept design of interdependent components/systems, is to develop the detailed design of the component/system. After developing the detailed design an evaluation of the detailed design (and its functions with the other interdependent components/systems) should be performed. After this, the actual implementation of the component/system can take place. Next the component has to be tested. The final phase of this tentative design process takes into consideration of both maintenance and upgrade of the component/system. One could of course argue that these two issues also should be taken into consideration from the beginning of the design process, i.e. being part of the areas that are presented on the y-axis.

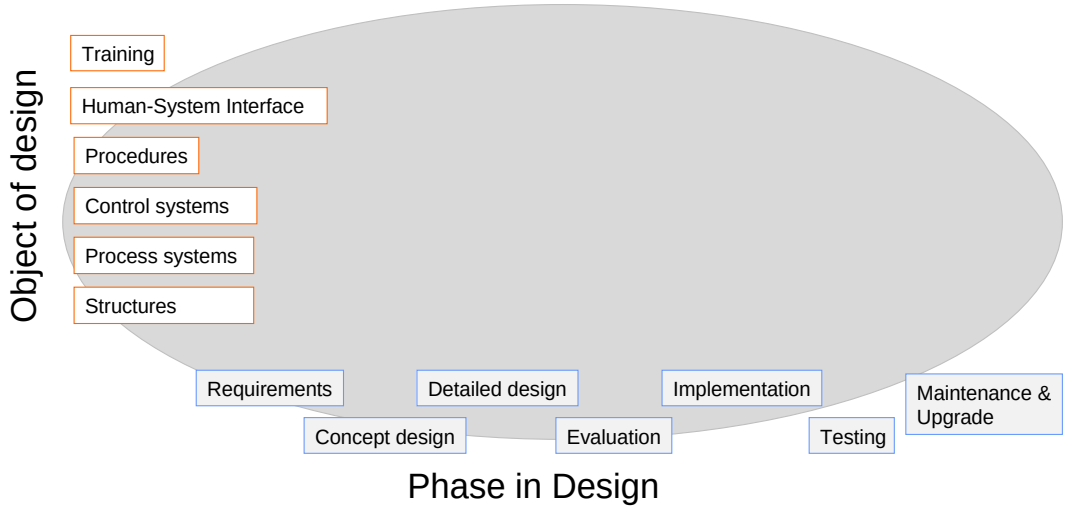

Figure 1 An illustration of design activities as composed of several phases and differing in terms of the object of design

The concept of design deals with several areas; for example organizational design and technical design. The main focus in this report deals with technical design, of course acknowledging the interrelation with Human Factors Engineering. One well known report that guides the evaluation of change-processes for design in the context of nuclear energy and Human Factors Engineering is Nureg-0711, Human Factors Engineering Program Review Model, (O'Hara et.al., 2004). NUREG-0711 consists of four general activities namely Planning and Analysis, Design, Verification and Validation, Implementation and Operation. The four activities are divided into twelve review elements. Below the four general activities and the twelve review elements are introduced, together with a preliminary mapping with the different design phases presented in Figure 1

Planning and Analysis

This general activity consists of six review elements:

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

The first element deals with the management of the HFE Program – an element which is implicit in Figure 1. The remaining five elements are concerned with establishing the requirements of the design, and thus they roughly correspond to the Requirements phase in Figure 1.

Design

The general activity design consists of three review elements:

1. Human-System Interface Design,
2. Procedure Development,

3. Training Programme Development.

The first review element, Human-System Interface, consists of for example concept- and detailed design, which maps the Conceptual design and Detailed design phases in Figure 1.

Verification and Validation

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

1. Human Factors Verification and Validation.

This element maps the Evaluation phase in Figure 1.

Implementation and Operation

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

1. Design Implementation,
2. Human Performance Monitoring.

These elements roughly correspond to the Implementation and Testing phases in Figure 1.

In a summary, design in an industrial context can be viewed as a process that has an objective of creating an artefact to solve an expressed problem or a need. This process is a combination of analytical problem solving and innovative creation of new features and combinations. The resulting 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.

3.2 Events where design issues were contributing factors

As mentioned in the Introduction of this report, the analysis of several incidents and accidents has emphasized the hazards of design based vulnerabilities for many different industrial domains. A classic example from the nuclear industry is the event at the Three Mile Island reactor in 1979. In that case a basic design flaw forced the operators to deduce the amount of coolant in the primary circuit and the core from an instrument that measured the level of water in the pressurizer.

Designing for well-defined and structured way of working can also have its drawbacks in times when novelty and improvisation is called for, such as in emergencies. As argued by Snook and Connor (2005, p. 183): “when faced with particularly ambiguous or unusual events, ones that don’t necessarily fit the original design or current method for organizing work, the very same structural mechanisms required to accomplish well-understood, cutting-edge core tasks can actually work to defeat the appropriate responses”. This is due to the fact that the appropriate response falls outside the originally designed functional boundaries. Organizational structures that affect the work practices and competence negatively in the long run have shown in many accidents (Hopkins 2000, Snook 2000).

In 1997 the United States Nuclear Regulatory Commission commissioned an engineering study of design-basis issues identified in licensee event reports (Lloyd et al. 2000). The study showed that between 1985 and 1997, more than 3100 licensee event reports identified design-basis issues. Few of the issues had direct nuclear safety significance, but still the study

concludes that design issues may be an important contributor to accident "precursor sequences".

Table 1 presents a selection of events in the Nordic power plants where design implications have been clearly highlighted during the event analysis.

Table 1 Examples of Nordic incidents where design issues have played a prominent role

Plant	System	Year	INES class	Brief description of the event	Design implications / lessons learned	Source
OL1	Reactor coolant pumps, generator voltage regulator and flywheel generator	2008	1	Reactor trip at Olkiluoto 1 as a result of a generator voltage regulator failure. The new voltage regulator was installed during the annual maintenance. The overvoltage peak caused by the opening of a plant breaker shut down all six reactor coolant pumps. The direct power supply from flywheel generators was interrupted when part of the control electronics of the reactor coolant pumps and flywheels was damaged	When the reactor coolant pumps were replaced in the 90s, it was not realised that overvoltage may, in certain situations, cut off the direct power supply from the flywheel generators to the reactor coolant pumps.	Kainulainen 2009
OL1	The blowdown system	2010	1	In a test carried out just before the shutdown of OL1 for the outage, two blowdown valves did not function as planned, so TVO decided to inspect their electrical pilot valves during the outage. The inspections revealed that three electrical pilot valves were jammed. All jammed pilot valves were of a new type.	Originally the decision to replace the valves was taken for the purpose of making their maintenance easier.	Kainulainen 2011

Plant	System	Year	INES class	Brief description of the event	Design implications / lessons learned	Source
Barsebäck 2	Containment sumps	1992		One safety valve of the main steam system opened at Barsebäck unit 2. The steam jet disintegrated coverings and insulation materials from adjacent pipelines. Parts of disintegrated mineral wool insulation was transported to the condensation pool in the reactor containment and caused clogging of the strainers for the emergency core cooling system	importance of insulation material and testing procedures	interview + http://www.analys.se/lankar/Bakgrunder/2004/Bkg%201-04.pdf
FKA	Emergency power supply system; UPS subsystem	2006	2	Degraded safety functions for common cause failure in the emergency power supply system at nuclear power plant	Importance of robust electrical systems	interviews + http://www.vattenfall.se/sv/file/content/060823-forsmarks-rapport till_11336829.pdf
FKA2	Valve upgrade at FK2	2010	-	A possible common cause related design flaw on valves lead to a power reduction for about half a year	The importance of verification of designs	Interview – see also http://www.nyteknik.se/nyheter/energi_miljo/karnkraft/article2442252.ece

Plant	System	Year	INES class	Brief description of the event	Design implications / lessons learned	Source
OKG3	Valve upgrade at OKG3	2010	-	A possible common cause related design flaw on four of the valves that lead to an abrupt stop of the steam to the condenser. This lead to a short and relatively high pressure spike in the reactor.	The importance of verification of designs	Interview – see also http://www.okg.se/templates/NewsPage___993.aspx
RAB2	Degradation of pumps.	2008		Due to tests that were done under different conditions that were postulated in the accident analyses, it was not found out that the pumps had degraded, and thus could not provide the flow that was required according to the safety analyses.	The importance of testing the equipment (operation readiness verification) under conditions that are similar to the conditions postulated in the safety analyses.	Interview

Design issues are also commonly found during event analysis in many safety critical industries. In this report, the Challenger explosion is briefly summarised with the purpose of illustrating the challenges in performing sound and safe design, and consequences that can result from failing in doing so. It is here below also reported a brief account of the Fukushima Daiichi nuclear accident. Even in that case design issues were quickly identified.

Challenger Space Shuttle explosion

The story of NASA's space shuttle program is full of design related optimising, shortcuts and tradeoffs. The Space Shuttle was part of a larger Space Transportation System concept that arose in the 1960's when Apollo was in development. The concept originally included a manned Mars expedition, a space station in lunar orbit, and an Earth-orbiting station serviced by a reusable ferry, or Space Shuttle. The funding required for this large an effort, on the order of that provided for Apollo, never materialized, and the concept was scaled back until the reusable Space Shuttle, earlier only the transport element of a broad transportation system, became the focus of NASA's efforts. In addition, to maintain its funding, the Shuttle had to be sold as performing a large number of tasks, including launching and servicing satellites. For example, the Air Force agreed not to develop any launch vehicles of its own, provided that the Shuttle was designed to accommodate military needs. This required compromises in the design. The compromises contributed to a design that was more inherently risky than was necessary. (Leveson 2008, Rossow 2012) A further factor was that there was a pressure at the design phase to make promises about the number of launches per year and the cost per launch which quickly proved unrealistic.

Jensen (1996) provides a narrative of the accident based on secondary sources, which emphasises the influence of the political and societal factors. For example, he points out how the original design of the space shuttle by NASA did not include booster rockets using solid fuel but rather a manned mother plane. A manned mother plane carrying the orbiter proved too expensive in the political climate where NASA had to fight for its budget and justify the benefits of its space program. Reusable rocket boosters were cheaper. As the rocket boosters were designed to be reusable after being ditched into sea water on each flight, NASA did not want to consider what "all the pipes and pumps and valves inside a liquid-fuel rocket would be like after a dip in the ocean (Jensen, 1996, p. 143)". Thus it was decided that solid fuel instead of liquid should be used. Solid rocket motors had never been used in manned spaceflight since they cannot be switched off or "throttled down" after ignition. Moreover, the fact that the design had field joints at all (which were the cause of the accident) had to do with Morton Thiokol wanting to create jobs at their home in Utah, 2500 miles from the launch site. There was no way of building the booster in one case in Utah and shipping it to the Kennedy Space Center (Jensen, 1996, p. 179). Thus, the booster rocket was designed and later manufactured in several pieces which were assembled in the Kennedy Space Center – that is why the joints were called 'field joints', the booster rocket was assembled in the field and the pieces were sealed with the field joints. Also, as pointed out by Rossow (2012), shipping the SRB as a single unit (from Utah to Florida) would have meant that a large amount of rocket fuel would be concentrated in a single container—creating the potential for an enormous explosion.

Fukushima nuclear accident

Two design bases were implemented for protecting the Fukushima Daiichi nuclear power plant: an earthquake design basis and a tsunami design basis. Both design bases were derived from historical available data concerning previous earthquakes and tsunamis.

According to the INPO special report 11-005, published in November 2011, the probability of an earthquake exceeding design basis was calculated to be 10^{-4} to 10^{-6}. The INPO report states *"The March 11 earthquake occurred over the area where multiple smaller individual earthquakes had previously occurred. The interaction over a large area contributed to the earthquake being the largest Japan has ever experienced and the fourth largest recorded earthquake in the world. The design basis seismic analysis had not considered the possibility of ground motion across several areas"*. Despite that, no seismic damages were reported by operators and emergency diesel generators as well as emergency core cooling system operated as expected and designed.

The original tsunami design basis for the Fukushima Daiichi nuclear power plant was based on the Chilean tsunami of 1960. When the construction permit was issued, the tsunami design basis was 10.2 feet. The design basis was voluntarily increased by TEPCO in the beginning of years 2000s to the maximum water level of 18.7 feet. The new design basis was conceived to ensure that all the critical seawater pump motors were installed higher than the maximum estimated inundation level, but it did not accounted for the need to mitigate hydrodynamic impact forces. According to the INPO report, "*the breakwater was not modified when the new*

tsunami height was implemented because it was not intended to provide tsunami protection, but rather to minimize wave action in the harbour".

Numerical simulations of tsunamis used to develop the new design basis in 2002 considered the possibility for tsunamis generated from eight different sources near the Japanese coast. Nevertheless the tsunami of March 11 resulted to be produced by ruptures across several areas. Unfortunately this option was not considered as credible in the analysis (INPO; 2011).

3.3. Previous research on design

Star and Griesemer (1989) introduced the concept of boundary object, which is currently considered an established concept in the field of design studies (Bergman et al. 2007). A boundary object is defined as "an analytical concept of those scientific objects which both in habit several interacting social worlds … and satisfy the informational requirements of each of them. Boundary objects are objects which are both plastic enough to adapt to local needs and the constraints of the several parties employing them, yet robust enough to maintain a common identity across sites. They are weakly constructed in common use, and become strongly structured in individual-site use. These objects may be abstract or concrete." A boundary object can serve a key role in developing and maintaining coherence across different communities of practice. The concept of boundary object can be used when referring either to the design process or to the designed artefacts and their use.

Bergman et al. (2007) have identified four essential features for viable design boundary objects: 1) the capability for common representation, 2) the capability to transform design knowledge, 3) the capability to mobilize for action, and 4) the capability to legitimize design knowledge across social worlds.

Norros and Salo (2009) identified three basic assumptions of the role of the human with regard to technology. First, humans can be seen as a risk factor. In this case design should aim at minimising the potentially negative consequences of human activity by building in the system as much automation as possible. As previously mentioned this solution was already criticised in the 1980s by Bainbridge and more recently by the Resilience Engineering approach. An alternative perspective on humans is to see people as a creative factor. In this case design should aim at maximising the benefits of the user and to develop technology which support human activity. The third perspective sees humans in a co-evolution with technology. In the last case design should concern practices which create new possibilities and uses of living (Hancock and Chignell 1995; Papin 2002).

From a system safety perspective, design has been explored from many starting point. For example, in Normal Accident Theory (NAT), Charles Perrow argued that due to high complexity and tight coupling among components in modern technical systems, then accidents in these systems are to be expected (Perrow, 1984). This pessimistic theory about the results of design was opposed by High Reliability Organisation (HRO) theorists who argued that a proper safety culture (e.g. preoccupation with failure, technical expertise, high safety priorities, learning orientation etc.) (LaPorte and Consolini, 1991; Roberts, 1990) could contribute to the creation of more-than-expected safe organisation. These both classical accounts associated with both technical design and operating features (culture) of

sociotechnical systems have gradually been replaced by systemic perspectives on safety. Although the term “systemic” may receive different interpretations, there are some features, however, that seem to reoccur when systemic perspectives and safety are discussed. One such feature concerns the idea that safety is an emergent property involving several different hierarchical levels. This can be contrasted with a view on safety as the sum of different individual components perceived in isolation from each other. In other words: individual components may perform according to specifications (reliability) but the system may nevertheless be unsafe considering the total interactions and dynamics among the components. Another aspect characterising systemic accounts is that technical, human and organisational properties are tightly interwoven. Systemic perspectives also focus on that systems are exposed to conflicting goals and values; safety is one value that production systems must satisfy, but there are many other values as well.

One example of a systemic model is represented by Leveson´s STAMP model (Leveson, 2004). A basic idea behind STAMP is to model systems in terms of a hierarchy of organisational levels where each level is more complex than the lower one. Each of the higher levels enforces a set of constraints on the lower levels and this is how safety is controlled. Thus, upholding safety can be perceived as being basically a control problem and accidents may occur as a result of weakness/failures of control. In STAMP, “technical design errors” occur because of failures to control the design developmental process (including design, manufacturing, installation etc.). It should be noted that the concept of “control” is widely defined by Leveson and include both direct and indirect features (organisational culture such as assumptions, norms and values). One interpretation of STAMP would thus be that “safety culture” in design organisation consists of the formal and informal constraints that put constraints on the design process – what is allowed and not allowed. Such an interpretation would however be problematic because one would expect that in a design culture there is a trade-off between innovative cultural features and those features that put constraints on the design processes.

One of the most interesting features of Leveson´s model is the suggestion of two parallel tracks named “system development” and “system operation”. For both these processes, Leveson suggests a hierarchy of levels. Starting from the top, these levels are for both processes defined as (a) “Congress and legislatures”, (b) “Governmental Regulatory Agencies, Industry associations, User Associations, Unions, Insurance Companies, Courts”: (c) Company Managements. Later, downstream, in this model the processes differ between the system development track and the system operation track. Furthermore, various routes of exchange between the developmental track and the operation track is spelled out and discussed in Leveson´s model. We shall here not dwell more into this particular example, but only recognize that STAMP represent a serious effort, and a good starting point, for a further exploration into various issues of relevance for the present project. In fact, there seems to be rather few systemic models of the kind comparable with STAMP that, in the very same model, explore the exchange between design and operation in a systematic way. STAMP seems, however, still somewhat premature with respect to the complexity of various sociological and psychological factors that will influence the culture in design organisations.

It is our hope that the present focus can further dwell into some of these issues by, for example, focus on how different actors perceive the concept of safety and safety culture.

3.4 Human Factors Engineering

Human Factors Engineering (HFE) is a process the purpose of which is to enhance safety in design. The process consists of several activities which all aim at improving design by letting the designers consider the future usage of the designed system already in the design phase.

HFE provides a set of principles and methods to be used for applying human factors knowhow in the design and modification of nuclear power plants. 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 1) the roles and tasks of NPP personnel are clearly defined, 2) staffing levels and qualifications are adequate to fulfil the requirements of human tasks and, 3) 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 world widely applied to the evaluation of the successfulness of inclusion of HFE principles and methods in the design of HSIs and to the evaluation of the implemented design.

In the initial analysis of HFE issues in Finland we recognized that there are several different stakeholders that have some kind of a relationship and role in regard to Human Factors Engineering. We see that Human Factors Engineering is mainly related to the activity of the design organization. HFE is the design organization's way of taking the usage point of view in design and well defined HFE processes are a nominal feature of safety culture in design.

In Sweden, as in Finland, there are several stakeholders that are concerned with the area of HFE. The degree of how HFE is taken into account varies between different utilities and also between different projects within a specific utility. The amount of HFE focus seems to be increase for more recently started project. In at least one of the cases studied, NUREG-0711 forms the backbone of the "ideal" HFE-process.

The regulator's (nuclear authority) role in nuclear domain is to monitor and inspect and follow that all regulations are fulfilled by the production and design organizations. Thus the role of the regulator is to maintain oversight of that HFE being conducted in the design organization.

4. Preliminary findings from interviews and workshops

During 2011 seventeen interviews, both workshop and face-to-face semi-structured interviews were conducted in Finland and Sweden. The results of preliminary analysis are reported here divided into two sections. First are reported the findings concerning the issues and challenges that interviewees from the nuclear industry highlighted. Then the findings from the interviews conducted with the Finnish nuclear authority, mainly focused on HFE issues, are summarised together with reflections from the Swedish practices.

4.1 Findings concerning challenges in design

The analysis of six in-depth interviews suggested the existence of several challenges related to design in the nuclear industry.

The interviewees were asked to express their thoughts and opinions concerning three main subjects:

1. What safety culture is
2. What challenges are related to design
3. What kind of safety culture is desired for design organisations

Between different organisations and different representatives there is not, rather obviously, a clear and shared consensus of what safety culture is.

Nevertheless two themes seem to be recurrent in the interviews. First, safety culture is related to the way of thinking, to the attitudes of everyone in the organisation. For example one interviewee said: *"It's the way of thinking about, the approach to safety; the tones in which it's referred to – from coffee table conversations to official regulations. How seriously matters are approached"*. Another interviewee also considered that safety culture requires that *"no pressure comes from anyone. If someone is worried about a matter of safety, they are given time to sort out the matter. The matter is sorted without hurry."* One of the interviewee made the interesting remark that; "*When you do not need to constantly remind people about the importance of safety, then you have a safety culture*". One of the interviewees referred to the recurrent motto "safety first". What he said can be rephrased as "a safety culture that supports safety is that the organization and the staff always put safety first, and that it must be clear that management considers and prioritizes safety issues".

The second recurrent feature of safety culture relates to the more tangible factors influencing everyday activities. On one hand, as explained during one of the interview, good safety culture requires to *"have good means, practices, methods, instructions, tools, resources"* and in the meantime *"safety and financial matters support each other, which means that these two interests should not be conflicting"*.

In response to the question about what to look for in terms of safety culture in a design organisation one person said that "*I would see if they themselves would raise important issues instead of that I personally would have to remind them of these*". When it came to the suppliers' safety culture, and the possible evaluation of this, one interviewee said that it was almost impossible to imagine a way to evaluate this, but that one rough possible way was to find out how the suppliers had dealt with for example shortcomings in earlier projects. One way for the customer (the NPP) to deal proactively with the suppliers safety culture issues was, however, that the customer should be aware of the importance of supporting the suppliers safety culture by aiming for win-win contracts, i.e. having a realistic balance between resources (e.g. money to the supplier) and expected outcome (deliverables from the supplier).

In many of the interviews, uncertainty was expressed when the question concerned definitions of nuclear safety in general and safety culture in particular. This is of course not a

surprising finding in view of the many different meanings these concepts have been given – not even academics in safety culture research agree about what the concept of safety culture should mean. The idea that safety culture covers both assumptions, values, attitudes, norms and similar "people oriented" factors, as well as tangible factors such as the quality of various means (tools, instructions etc.) is present in many responses. The difference sometimes made between safety culture and safety climate, was not made by any of the respondents.

These findings are in line with our previous study on safety culture in the Nordic nuclear branch (Reiman et al. 2011). In that study the interview sample did not have specialists from design. A further analysis of the combined interview sample of 40 interviewees showed that people seem to emphasize certain aspects of nuclear safety – some technical, some organizational and some issues related to operating experience (Reiman et al. in press).

Challenges related to design can be clustered according to four topics: (1) knowledge and experience; (2) taking into account future needs and requirements; (3) specification of requirements; (4) new technology and integration of new technology with old technology.

The fundamental role that **knowledge and experience** in designing, and the potential lack of them, especially in newcomers in the industry, has been reported in several interviews as a worrying challenge. *"It might be quite difficult to design the I&C system, unless you do not have experience from operating power plants. I know there are designers who have never been in the operating power plants or haven't done any design for operating power plants"* said one interviewee. *"If you put the limit high, or high enough, then this is automatic that they [the limits] will be followed. Of course if you have problem in nuclear safety you lose the availability […] Somehow this is not so clear. Maybe because of no experience to build any plant. Because it's also suppliers' problem, they don't have experienced people anymore"* reported another interviewee.

Since, as remarked during one of the interviews, design aims at *"achieving a desired result"* it is crucial to define the result as detailed as possible and as early as possible in the design process. This implies that designer should be able to **understand** and take into account **needs and requirements.**

As an example, one interviewee said: *"we must naturally always have a defined goal when we start designing something. The goal must be defined at least in reasonable detail in the beginning, and the goal usually becomes clearer during the process; it might not always be that precise in the beginning. Sometimes, it may be necessary to even change it as the design progresses"*. Similar concerns was expressed during another interview in which it was stated: *"A designer who has not so much experience, makes some reservation and this is also what I see, it's very difficult for [certain] people for instance to have this kind of vision for longer time. They are making the design so that they do the design when they know, but if you don't know, they don't do"*

Tightly related to the ability of understanding needs and requirements is the challenge of **specifying the correct requirements** to be met in the design. The following quote extracted from one of the interviews describes well the magnitude of this challenge: *"The problem will be that the erection and installations starts before all the necessary design and procedures,*

instructions have been completed. That causes a mess. […] But if you are starting, finalizing layout and making civil drawings,[…], it might happen so that, and the design mature enough, it might happen that you will end up with solution that you find out, that you can fulfil the independence and separation criteria, with this layout, with these buildings already designed and the worst case, even the construction works started, then you are in big trouble, in very big trouble."

A similar concern was raised in another interview: "*The design processes to a great extent concerns the development of specifications, and as everybody knows, it costs way too much money to develop complete specifications in advance….so that when the actual design work has started, the specification is complemented. I mean, you really cannot do a complete specification from the beginning, it has to be a part of the rest of the process… and here, I don't really know, how we do in order to do this rock steady…. "*

The presence of "new technology" is a challenge for design and redesign of nuclear power plants. Introduction of digital equipment raises several new issues, such as how to validate software, how to go about in changing software, new error modes, etc. In upgrading projects there is the potential difficulty to understand how a new installation will fit with old installations. One of the interviewees remarked that there is a risk that the old principles have become forgotten with time. In particular the electrical systems are important to understand. One of the respondents meant that "There have been some substantial changes with respect to electrical issues – before, one took these things as more or less granted, none were particularly interested in those things then – everybody thought that they should just work. But there is a substantial change in that we must understand the electrical systems in a deeper sense".

In addition to the four above mentioned challenges related to design, a fifth one deserves to be mentioned. This challenge is specific for the **organisations of large design projects**, both NPP in-house and customer / supplier projects. In one of the interviews, a concern was expressed about the integration of the line-organization in the project organisation in order to increase the speed of the projects. The problem here was that this integration made it harder to guarantee that the line organization kept on having a critical perspective regarding the project outcome, and that it was harder to guarantee a critical and "separate" review process. In a second case it was reported how in some supplier organizations seemed to be shortcomings regarding experienced personnel, and that there was a need for the customer to support the supplier. The problem here was also concerned with how to guarantee that the NPP-project customer organization kept having a critical perspective on the supplier project organizations deliverables. In another interview in which the above issues were raised, the interview acknowledged the above challenges, but emphasised that the NPP organization always had the total responsibility regarding the safety: "*But even if we do buy from a supplier there is still a big and important role for the NPP organization to fulfil. It is still the case that the technical department are responsible for the design. And this does not only mean that we should check that the design we buy fulfils and established specifications, but also that we should do analyses that verifies this…. And that we should identify and verify which specifications that should be fulfilled."*

One theme that is common both to the above discussion of the role of the line organization and role of new technology is the question about the fulfilment of the basic safety principles in design: redundancy, diversity and separation. These principles should be fulfilled in the finished design, but also the design process itself should adhere to some common safety principles. However, in practice it quickly becomes clear that even these principles are not clear cut and trade-offs are necessary to meet the several requirements of the design process (schedule, costs, safety, reliability, functionality, maintainability, acceptability).

4.2 Findings concerning Human Factors Engineering oversight Finland

In STUK Human Factors Engineering is considered to encompass activities of the utilities that are related to design and modification of control rooms.

Currently, HFE oversight related work is organized so that there is one person whose responsibility HFE oversight mainly is, but in addition there is an organizational virtual team which is responsible for monitoring utilities in all matters concerning control rooms. This virtual team also reviews all issues concerning control rooms. This group is called Control Room Group and it consists of four individuals the expertise areas of whose cover psychology, nuclear physics, automation, and accident and safety analysis.

In STUK the term human factors (HF) is used broadly. It covers both organizational and human factors. In the operational safety team there are four additional people (in addition to the aforementioned Control Room Group) who are monitoring the organizational issues in the plants both in the operating and under construction phases. The expertise areas in this team include engineering, educational science, production economy, and health science. This means that altogether there are 7-8 people in STUK whose work is related to either human factors or Human Factors Engineering oversight.

Regarding international connections STUK has cooperation with the Swedish regulatory authority SSM about HFE oversight matters. All the cooperation is informal; there are no official forms for the cooperation such as established working groups or regular meetings. In addition there have been meetings with the safety authorities in France as the interest of EPR type plants is shared between the Finnish the French, and the British authority. STUK has also taken part in IAEA's meetings concerning HFE. It is also known that STUK actively participates in the OECD/NEA Working Group for Human and Organisational Factors that has HFE on its agenda

It was regarded as a special challenge related to HFE oversight in STUK that there is no official definition of HFE in STUK. This means that neither general agreement of what HFE means, nor what it comprises of, exists. This might lead to confusion about which reviews are such that they require HFE oversight activities in addition to technical reviews.

Nevertheless, human factors and HFE oversight as part of it are valued in STUK. This is supported by the fact that the management is aware of the importance of HFE oversight. In addition, in discussions of about safety factors HF is often brought up. HF topics typically acknowledged by the management consist of experiences from OL3 (Olkiluoto 3, new EPR

being built in Eurajoki, Finland). These experiences have increased the awareness of such human factors as safety culture, training, and communication. It is also acknowledged in STUK that HFE is related to the overall safety culture of an organization. HFE is a characteristic of a strong safety culture. And as there are requirements for safety culture in the current and up-coming regulatory guides, it can be interpreted that the basis for HFE requirements already exists.

When safety culture in design was discussed more generally, it was concluded that good safety culture in design means that the designers and other experts involved in the design understand what effects their work has on safety and take it seriously. In addition processes should be well specified, people well trained etc.

In the on-going modernization and new builds projects of the industry STUK does not inspect the utilities with regard to HFE. HFE process descriptions are not required so there is no systematic reviewing either.

When the new YVL guides are published, also existing plants must show that they fulfil the new requirements. If they do not meet the requirements the matters will be handled case by case. STUK is not prepared for this phase yet.

As the modification of the regulatory guides takes place, the new requirements will ask for the coordination of all HFE processes by the utilities. Since licensees have the responsibility they should plan and carry out the process themselves. STUK would like to see that licensees carry out as much as possible of the HFE work in house in contrast to using external experts such as consultants. This is because in the end it is the licensee who is responsible for safety. There are differences in the practices of Finnish utilities and the variation in the amount of using external consultants is extensive.

The main plans of STUK concerning the future of HFE deal with the renewal of the regulatory guides. In addition it was discussed that STUK should create and specify a HFE oversight process which would describe how the regulator carries out the HFE-related reviews.

In further development it should be analyzed and specified (in the regulatory guidelines) what kinds of plant modifications require a HFE process. This type of requirement should enforce the utilities to consider all changes from a human factors point of view. This would mean considering the changes for example from the point of view of possible human errors that might be induced.

The consensus in STUK is that the Finnish regulator is still developing its HFE oversight approach. This becomes especially evident in comparison with the international collaborators. It is believed in STUK that authorities in other countries have more specific HFE oversight processes in effect and more clear understanding of HFE. The current situation in STUK is not a question of resources, more of will. It is viewed that STUK should start planning and training the personnel in HFE oversight related issues in order to increase awareness and this way proceed towards mastery of HFE oversight and also other human factor related issues.

4.3 Findings concerning Human Factors Engineering oversight Sweden

Interviews with representatives for different modernization projects in Sweden did indicate that the focus in Human Factors Engineering is increasing, and that the HFE is, to different degrees, included in at least all modernization projects that also affect the main control room. In some of the projects, HFE issues are strongly emphasized, with several full time HFE-staff employed both in the NPP project organization and also in the vendors organization.

The HFE organization in one NPP project organization consisted of three different function; Human System Interface (HIS), procedures and working methods, and training. These functions were managed in two different sub project organizations, and a HFE-coordinator was assigned to coordinate the work that was done within the different HFE-related functions, thus acknowledging that there were possible interrelated issues that concerned several different HFE-functions.

One challenge that were mentioned in one of the modernization projects was that the HFE-process are to a certain extent based upon a clear sequential process, whereas the process in reality to a certain extent was performed in parallel. One major area of focus in one of the projects was the alarm systems.

Interviews with SSM discussion Human Factors Engineering were not been performed in the first phase of the project.

5. Conclusions

5.1 Human Factors Engineering

The interviews with the Finnish authority showed how Human Factors Engineering oversight has started to gain in importance in STUK. Even though a formal definition of HFE does not exist and no processes or workflows have been specified for HFE oversight, the issue of HFE has been acknowledged as topical and is thus introduced to the new guidance that the regulator is currently renewing. This means that as the new guidance is taken into use there will be formal requirements concerning HFE that the utilities must fulfil.

The current conception of scope of HFE is not clear or unison in STUK. It is maintained that HFE is important in the matters related to the main control room and other control stations, and namely the design of user interfaces. Even within the scope of control room design HFE is considered to cover mainly the issues of verification and validation of new designs and modernizations. This scope of HFE is quite narrow. It does not take into consideration any of the activities that are related to analysis, design and operation phases of technology life cycles. Neither does it take into consideration other operational areas such as maintenance or supervision of work which might also be relevant from a HFE point of view.

Some of the future plans concerning HFE in STUK are quite clear. The intention is to include requirements for utilities in the new YVL guidance. The new guidelines are currently under public review. The next steps within own organization are a little bit unclear. The need for a specification of HFE review process was discussed in the workshop. More clear specification

of the process would be helpful also from the point of view of the utilities as it would then be clearer what is expected of them as the new guidelines are being implemented.

Human Factors issues have received more and more attention in Sweden over the years. This is manifested by, for example, a rather large HF group centrally located at Vattenfall. With respect to HF design issues the concentration has been towards the central control rooms and various systems have been developed for validation and verification of control room upgrades. Recently a new project is started to create an upgrade of a validation handbook – a projects supported by all the Swedish nuclear plants. The interviews did reveal, however, that in spite of the attention towards HF design engineering, there is still a way to go regarding integration of HF design practices and other, more conventional, design practices. The human factors aspects of design tend to come too late in the change projects, one person remarked that the HF projects seemed to live a life of their own at the side of the change projects. This fact has also been noted by the regulators.

5.2 Safety culture in design

The preliminary analysis conducted on the seventeen interviews performed during the first year of the SADE project, in conjunction with the review of literature, showed some of the challenges related to design issues in the nuclear industry.

In particular, understanding and specifying functional requirements of both products and organisations appear to be an important challenge for nuclear industry. Approaching the design process from the safety culture and the resilience engineering perspective highlights the need for good design to cope with and support the management of the complexity of the nuclear industry (Norman, 2011). From the interviews, it seems important to solve the challenges not by addressing problems one by one with new designs or more powerful technology. The call for knowledge and experience, for understanding and specification of requirements may suggest, as also indicated by Hollnagel (2011) that what is required is to achieve a better understanding of the current and future functioning of the systems. In this way the design could effectively support such functioning capacity and support humans and organisations in sustaining their activities during both expected and unexpected conditions.

Design process in nuclear power context can be seen as a combination of analytical problem solving and innovative creation of new features and solutions. This process has an objective of creating an artefact to solve an expressed problem or a need yet the exact characteristics of this artefact cannot be known in detail in advance. Only the functional requirements can be set, but these can be met in many different ways. In terms of developing a strong safety culture it should be acknowledged that instead of (or in addition to) strict instructions design activities need to be controlled by goal and direction providing “rules” and shared values. The organization should also contribute to expertise of the designers as well as to integration of different design disciplines and design of different components.

One aspect of design as practice that differentiates it from other forms of practice taking place in the nuclear power domain (such as maintenance or operations) is that the work is highly conceptual and not easily observable. Further, it is more individually oriented than many other forms of occupation. There is a need for methods to facilitate shared view of the

entire activity of design. Thus, the concept of 'boundary object' is relevant also for nuclear power domain; an interesting discussion is what types of boundary objects are needed for facilitating a shared understanding of the nuclear safety significance of the given design.

The role of the organization in creating and maintaining 'boundary objects' such as safety principles and more abstract safety related values and norms should also be further elaborated. A further tension is created by the fact that safety culture requirements for operations and maintenance might differ from those of design organizations; what kind of boundary objects could maintain their common identity in all those contexts yet be flexible enough to influence the activity in each setting? The concept of safety culture in its current ambiguous usage is not an adequate boundary object. One can even ask if the concept should be specified to each context (operations, maintenance, design) without an attempt to find overarching safety culture principles? These questions will be elaborated in the continuation of the SADE project in 2012.

References

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

Bainbridge L (1983) Ironies of automation. Automatica 19(6):775–779

Bergman, M., Lyytinen, K. & Mark, G. (2007). Boundary Objects in Design: An Ecological View of Design Artifacts. Journal of the Association for Information Systems, 8, 546-568.

Borja de Motoza, B. (2003) *Design management: using design to build brand value and corporate innovation.* Canada, Alworth Press

Hancock P, Chignell M (1995) On human factors. In: Flach J, Hancock P, Caird J, Vicente KJ (eds) Global perspectives on the ecology of human–machine systems, vol 1. Lawrence Erlbaum, Hillsdale, pp 14–53

Hollnagel, E. (2009). The ETTO principle: Efficiency-thoroughness trade-off. Farnhamn: Ashgate.

Hollnagel, E (2011) Coping with complexity: past, present and future. Cognition Technology and Work DOI 10.1007/s10111-011-0202-7

Hopkins, A. (2000). Lessons from Longford. The Esso gas plant explosion. Australia: CCH.

INPO (2011) Special report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station.

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

Kainulainen, E. (Ed.) (2011). Regulatory control of nuclear safety in Finland. Annual report 2010. STUK-B 134. Säteilyturvakeskus, Helsinki.

Jensen, C. (1996). No downlink. A dramatic narrative about the Challenger accident and our time. New York: Farrar Straus Giroux.

Laarni, J., Norros, L., Salo, L. & Koskinen, H. (2010). OPRACTICE summary report: Designing large-screen overview displays for nuclear power plant control rooms. In E.K. Puska (Ed.), SAFIR2010. The Finnish research programme on nuclear power plant safety 2007-2010. Interim Report. VTT Research Notes 2466. Espoo: VTT.

LaPorte, T.R. & P. Consolini (1991), Working in practice but not in theory: theoretical challenges of high reliability organizations, Journal of Public Administration Research and Theory, vol. 1, pp. 19-47.

Leveson, N.G. (2002). Technical and Managerial Factors in the NASA Challenger and Columbia Losses: Looking Forward to the Future. In: Kleinman, Cloud-Hansen, Matta, and Handelsman (editors), Controveries in Science and Technology Volume 2, Mary Ann Liebert Press

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

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

Norros, L. & Savioja, P. (2006). Integrated validation of complex human-technology systems – development of a new method. In H. Räty & E.K. Puska (Eds.), SAFIR. The Finnish Research Programme on Nuclear Power Plant Safety 2003– 2006. Final Report. VTT Research Notes 2363. Espoo: VTT.

Norros, L., Salo, (2009). Design of joint systems: a theoretical challenge for cognitive systems engineering. Cognition Technology and Work (2009) 11:43–56 DOI 10.1007/s10111-008-0122-3

Norman D (2011) Living with complexity. The MIT Press, Cambridge

Papin B (2002) Integration of human factors requirements in the design of future plants. Paper presented at the Enlarged Halden Programme Group Meeting, Storefjell

Perrow, C. (1984). Normal Accidents: Living with high risk technologies. Princeton: Princeton University Press.

Reiman, T., Kahlbom, U., Pietikäinen, E. & Rollenhagen, C. (2011). Nuclear Safety Culture in Finland and Sweden – Developments and Challenges. NKS-239. Nordic nuclear safety research NKS, Roskilde, Denmark.

Reiman, T., Rollenhagen, C. and Pietikäinen, E. (in press). Professionals' Beliefs about Nuclear Safety – An interview study in the Nordic nuclear branch. 11th International Probabilistic Safety Assessment & Management Conference, 25-29 June 2012, Helsinki, Finland.

Roberts, (K.H) 1990 "Managing high reliability organizations". California Management Review 32(4): 101–114.

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

Rossow, M. (2012). Engineering Ethics Case Study: The Challenger Disaster. CED Engineering.Com.

Snook, S. A. (2000). Friendly fire. The accidental shootdown of U.S. Black Hawks over Northern Iraq. New Jersey: Princeton University Press.

Snook, S.A. & Connor, J.C. (2005). The price of progress: Structurally induced inaction. In: W.H. Starbuck and M. Farjoun (eds.), Organization at the limit. Lessons from the Columbia disaster. Oxford: Blackwell.

Star, S. L. and Griesemer, J. R. (1989): ‘Institutional ecology, 'translations' and boundary objects: amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39’, Social Studies of Science, vol. 19, no. 3, pp 387-420.

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

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

Woods, D., Branlat M. (2011). Basic patterns in how adaptive systems fail. In Resilience engineering in practice: A guidebook. Farnham, UK: Ashgate.

Title	Organizational factors in design and implementation of technological and organizational solutions in the nuclear industry.
Author(s)	L. Macchi [(1)] T. Reiman[(1)] P. Savioja[(1)] U. Kahlbom[(2)] C. Rollenhagen[(3)]
Affiliation(s)	(1) VTT- Technical Research Centre of Finland, Finland (2) Risk Pilot, Sweden (3) Vattenfall, Sweden
ISBN	978-87-7893-336-2
Date	March 2012
Project	NKS-R / SADE
No. of pages	27
No. of tables	1
No. of illustrations	1
No. of references	33

Abstract

Design is often found as one of the contributing factors in accident in the nuclear industry. The design of new technological systems and organisational structures has to take into account and be driven by the future users' needs and has to consider how their role and work practices within the organisation will be affected. The SADE project explores to which extend the concepts of safety culture and resilience engineering can contribute to the prevention of design errors when no hindsight data are available.

In 2011, the SADE project focused on gathering experience and clarifying the current issues and challenges related to the design process. During 2011 seventeen interviews have been conducted in Finland and Sweden to identify some of the major challenges the nuclear industry is currently facing. At the same time a literature review has been conducted to establish a sound common theoretical ground. This progress report presents some of the relevant theoretical findings and preliminary results from the interviews.

Key words Design, Safety culture, Resilience Engineering, Human Factors Engineering