MORE REQUIREMENTS, MORE SAFETY? CHALLENGES IN COMBINING STRINGENT REGULATION WITH RESILIENT DESIGN

Mikael Wahlström, Pia Oedewald, Nadezhda Gotcheva, Kaupo Viitanen

VTT Technical Research Centre of Finland Ltd, Vuorimiehentie 5, FI-02150, Espoo, Finland

mikael.wahlstrom@vtt.fi

www.vtt.fi

Abstract

This paper discusses safety-relevant threats involved in highly regulated design. The study draws from an interview study regarding two design projects, a minor modification and a large waste management system, at two nuclear power plant (NPP) sites in Finland. The cases portray some main elements in NPP design, among which are stringent regulation, time-consuming document drafting, and throrough requirement management. We identify relevant trade-offs related to design of this kind and discuss the possible threats involved. The trade-offs include a rigid model of design and time-consuming document-based communication. The implied (though not empirically demonstrated) threats include insufficient iteration of the design idea, lack of holistic focus on the end-product, sharing the design authority with the regulator, and challenges in creating design solutions that promote resilience through operators' positive contribution to safety. Overall, we suggest that stringent regulation, comprehensive requirement management, and up-to-date reguirements are not sufficient in providing safe designs. Mindfulness of the identified threats, safety culture emphasizing the design organization responsibility, and leadership that ensures system thinking are needed as well.

1 INTRODUCTION

This paper reports on an interview study on design activities in the nuclear domain in Finland. The aim of the study is to identify possible threats, which should be taken into consideration in order to avoid the generation of failed designs. This is important because weaknesses in design have played a part in major accidents in the NPP domain (Rollenhagen, 2010). Our arguments, however, do not merely apply to the NPP context, but various safety-critical domains as well where designing is done 'by the book', and therefore are of interest for a wider audience. By design, in turn, we refer to activities such as idea conception, planning, problem solving, and decision making concerning technical modifications and development of new technological solutions, and the overall management of these activities (e.g., Aspelund, 2006). Based on the interviews, the NPP design practices in Finland seem to entail several positive elements, which are of key value for safety, such as thoroughness, stringent regulation and adherence to the international standards.

One might indeed immediately assume that safe designs can be achieved simply by the means of comprehensive and up-to-date set of requirements and by stringent regulatory overview. However, in order to expand the view and to provide a critical approach, we assume that this is not the whole truth. These elements certainly contribute to the safety of the end-product, but they may also come with some trade-offs and effects that have the potential to be negative for safety as it is understood in resilience engineering perspective (Hollnagel et al., 2011) and in other practical terms. The argument goes that if the design activity entails huge amount of technical requirement management and drafting precise documents for the regulator, a trade-off emerges: either too little effort might be dedicated to iterating the design idea and to considering the design in terms of usage at a system level, or the design process might become extremely time and resource consuming.

We will firstly provide a description of the basic working practises in Finnish NPP design and after that consider some possible drawbacks. We do not criticise the way nuclear projects, new builds or modifications, are actualized in Finland as such, since it seems that requirements and standards are considered with precision by both the regulator agency and the power companies. However, when it comes to the NPP domain especially, one should be open-minded in considering possible sources of incidents and failed designs.

Regarding the research approach, the present study is thus somewhat speculative as it draws from empirical findings in order to identify logically plausible hypotheses on as to why designs could fail rather than directly identifies empirical precedents. In our view, however, this is an acceptable approach in studying high-risk domains: NPPs are built to withstand harsh physical conditions that are unlikely and do not have notable

precedents, but which are nevertheless in principle possible; one could imagine the example of a huge earthquake in the stable tectonic plate under Finland – extremely unlikely but something to be prepared for. The same reasoning applies to human error issues and design: one should consider human behaviours, which perhaps have not taken place, but which seem plausible given the actual working conditions. In addition, we will shortly contrast the existing design practices to the concept of resilience engineering – we discuss that it could be challenging to design in a manner such that supports operators' capability to provide positive contribution to safety in unexpected situations.

2 THE TWO BASIC ELEMENTS IN NPP DESIGN: REGULATION AND DOCUMENTATION

Our study draws from interviews on two design cases, which are explained here only briefly. The method and the cases are explained more comprehensively elsewhere (Wahlström, in press). The first NPP design task could be considered fairly simple: it included a minor modification to a pump functionality and did not require designing new components as changes to circuit diagrams were sufficient. In contrast, the second design case was a major long-term project: the overall design for management of a specific kind of waste and the associated infrastructure. The interviewees were involved in the design work and included eight energy company workers and a governmental regulator representative. In the following we will explicate some of the basic findings based on the interviews regarding the case studies.

The pump functionality modification case, despite being technically a fairly simple task, took 17 months of research and communication before the actual work could be initiated. First, two months of internal decision-making took place within the power company and after that a comprehensive 21 page plan, called 'preliminary plan' was drafted for 10 months. This included a major effort in studying the requirements involved in the modification work. The document drafting took a considerable amount of time from an engineer and also included the circulation of the text in-house within experts from different fields who commented the plan. After that the document was sent to the safety authorities who gave their first response in three months. The governmental regulator representative concluded that the document is not sufficiently comprehensive, as it did not include sufficient details on testing the new design for verifying its functionality. The issue was then addressed and the project was finalized successfully. As seen in this design case, the relation between the power company and the regulator could be described as formal: the decisive communication takes place with detailed documents. They communicate in other ways as well, that is, by telephone, by more casual emails and sometimes face-to-face even, but the final decisions are based on the documents. It seems that this formality has not always been the only way of working in Finland:

> *'We also have experienced people here, quite a few of them, and they're used to calling the authorities and simply telling them that we've thought about implementing this kind of a system, sounds good, doesn't it? And the authorities say splendid, and they implement it. I mean this is how it was done 10 years ago. But it doesn't work like that anymore, so what happens is, these, how should I put it, old dogs, they'd like to keep doing things the old way, like they used to, without sending this and that and the other thing there. But we do have to do it now.'* (Energy company employee, the modification case)

Overall, it seems, in the pump functionality modification case the biggest challenge and effort were the document drafting and communication of the plans with the authorities.

> *'Let me put it this way, if we were producing dairy products here and not nuclear power, the design would have been pretty much there already, but we have to write a mountain of documents in addition to this.* […] *If you want a challenge, 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. […] And also, in addition to the extra, in addition to the usual circulation, we had three or four internal review cycles at the office, checking everything from spelling to comprehension, so I'd say all of this has made the document clearer, easy to understand.'* (Energy company employee, the modification case)

The importance of formal and precise documents is clear throughout the interviews. There was some variation in the connections with the regulator, however, as in the larger waste management project, a dedicated person from the regulator organization was available for the project and could provide feedback more efficiently. Nonetheless, also in that project, requirement management as well as general project management were time-consuming and challenging efforts. In other words, what is very descriptive of the design processes in the nuclear domain is the vast number of requirements that have to be taken into account as the

documents are drafted. This could be seen as an evolving phenomenon, as the number of requirements has been on the rise. It was mentioned in particular that after the Fukushima Daiichi disaster in 2011, more and more safety requirements were introduced.

Overall, three distinctive characteristics are descriptive of design in NPP domain in Finland, these being 1) meticulous management of up-to-date set of appropriate requirements, 2) clear documents for transparency and 3) thorough regulatory oversight. Though these phenomena are positive in ensuring that the design solutions are safe, they might entail some counterproductive elements as well.

3 POSSIBLE DRAWBACKS AND THREATS

There are at least two possible conditions, in which the combination of stringent regulation and the plurality and complexity of requirements could be insufficient in providing successful designs. Firstly, one could see these issues as 'trends' that increase hand-in-hand with the line of time, and especially if major incidents occur, such as the one at Fukushima; in view of the interviews, this kind of progression has been taking place. New requirements can be necessary, but at the same time one should consider that, in principle, there must be a limit beyond which the number of requirements produces negative effects: this is because eventually the requirement management and document communication process could become so effortful that the design process becomes too 'rigid' in a practical sense. Secondly, it is notable that human activity is never perfect and at times mistakes occur, especially under stress, such as when working with multiple tasks parallel, or when having to balance with various, partly conflicting goals of the different stakeholders. We will discuss that 'losing the big picture' could be a plausible cause of mistakes in design in extremely regulated and complicated technology domains.

3.1 Lack of flexibility and the effortfulness of iteration

The working practice in NPP design where perfect and comprehensive plans are needed prior to implementation suggests that near perfect foreknowledge on the state of affairs at the plant are needed as well. Given that drafting of these plans takes several months, it implies that the designers have to be able to 'foresee' months or years into the future. They have to have all the details beforehand. Could this then be a problem? One may ask whether the plans could become somehow outdated during the process of their writing and during the waiting for the regulator feedback? Obviously, the plans can be modified during the document drafting if, for example, new requirements are introduced. Nonetheless, it seems that the design concept is quite fixed to the original plan; the design idea as a whole cannot be conveniently changed after the initiation of the document drafting and requirement study.

Thus, the design model applied in NPP design resembles the so-called V-model (Figure 1); it entails the assumption that the foreknowledge is perfect. Turner (2007, p. 12) describes the V-model as follows: 'we can define complete, consistent, testable, and buildable requirements; decompose perfect requirements to perfect specifications; accurately estimate effort, cost, and schedule for the specifications; schedule work according to this information early in the programme; and measure progress using earned-value management or similar techniques'. Indeed, Turner points out that the V-model can be criticised due to the lack of flexibility. This criticism concerns the NPP design as well.

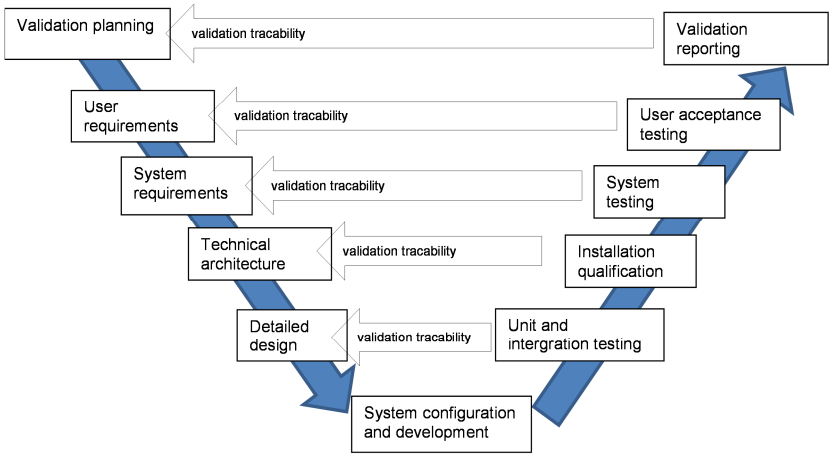

Figure 1. *V-Model of a Conventional, Large-System Development Process (adapted from Turner, 2007).*

The argument then goes that, once an agreement on the design solution has been made, a long process of requirement management and document drafting takes place – and during this requirement study and drafting phase the plans can be changed only slightly, i.e., it would be a somewhat rigid process. Alternatively, the plans could be changed more drastically but this would imply that the burdensome document drafting and requirement management process should be re-done as well. In other words, two options exist, and both could be seen as problematic: either the process is rigid and non-changeable, or the process is especially time and resource consuming.

Firstly, to address the problems of a rigid and predefined process, one should consider the issues, relevant to a NPP design solution that might vary over time, i.e., the issues that could be different than those foreseen. These unpredictable issues could include, at least requirement changes, changes in design or implementation work force, advances in technology and supplier situation. If the situation changes, while the plans have been laid down already, new plans would be needed. Additionally, parallel design projects might have an impact as well, that is, if several design projects with interlinked causal elements take place at the same time and if all of these projects progress especially slowly, managing the overall repertoire of projects might be particularly challenging.

Secondly, one may accept the fact sometimes new plans have to be made despite the great efforts involved. The safety-related problem involved is easy to identify: if things do not get done in a reasonable time, there will be delays in creating the necessary enhancements to safety. More generally, economic expenses in this approach would be considerable. To the best of our understanding, it is likely that this is actually how things are done in the NPP domain in Finland. According to our interviewees, there are sufficient economic resources to be used when dealing with design issues concerning safety.

Overall, one could conclude that iteration of design plans is effortful in NPP projects. It is thus questionable whether the designers are always when necessary willing to reconsider a design idea, if this reconsideration implies a new burdensome document-drafting and requirement management process. It is very unlikely to find data confirming this kind of behaviour, but one may consider it as a possible phenomenon seeding unsuccessful design solutions in some circumstances. This is threat that might take place in stressful or hurried work conditions.

3.2 Losing the big picture?

Understanding the overall NPP context has been found to be a significant challenge in NPP design (Macchi, et al. 2014). This is understandable in view of technical complexity. Additionally, one may thus assume that with a tremendous amount of document creation and tasks project administration tasks, the possible problem of not understanding the end-product holistically could be amplified: arguably, there could be the possibility that the design team distances itself from the actual aim, that is, the creation of a good solution, since there is so much other issues involved.

In other words, as it takes time in document drafting and requirement management, it might be that these activities become the focus of design work – the actual usage of the final technical solution could remain secondary. This could be seen as a leadership issue: a good leader would maintain an overall understanding and responsibility of the actual solution rather than focus on project and requirements management. The following account exchange concerns initially good cooperation, but then goes beyond that in discussing leadership.

> Researcher: *'Can you think about any practical way of making sure that there is no break [in cooperation]?'*
>
> Interviewee: *'Yeah. It's what we have now. [Project leader name], he's in charge of the project. During the implementation of the project, there was no such person. So somebody has to have an interest in what's being done. So that's the basic element that, there's one person who feels that this is mine, on the operator side, who feels that now I'm responsible; my team will operate this plant. Then, the approach is completely different. If nobody's nominated, then who should care what's being done. Nobody. Would we have been, or would we have had such a person during the project, it would have been a bigger success.'* (Energy company employee, the waste management system case)

Understandably, in large and complex projects the leader cannot maintain a specific understanding of all the relevant technical issues. Challenging and important design tasks, that is, those with significant safety and/or economic implications, are typically organized as projects. The projects would thus have to be viewed from a sufficiently broad level of abstraction. The project leadership should maintain an overview of who understands

the issues relating to its more specific subdomains. The leader should also make sure that these individuals communicate with each other and the leader should maintain the big picture sufficiently.

Another issue that could possibly induce the lack of maintaining the big picture is shared responsibility. Arguably, the fact that the power companies in Finland rely on the authorities in checking that designs are acceptable, could mean that the power companies, in a sense, share responsibility and 'design authority' with the regulator agency. In a high reliability organization someone should have to have the final word and the responsibility in ensuring that the design solution works – someone has to maintain the 'big picture'. As expressed in an IAEA report (2003), and according to the regulations, the operating organizations, that is, the power companies, have the responsibility to maintain design authority. This is to say that they have to formally approve all the design changes and also have to maintain the needed knowledge. However, the regulator agency in Finland has responsibilities that could be seen as overlapping as it also accepts the plans. In some instances this could imply a loss of design authority in the actual working practices of power company workers, i.e., the designers could start thinking that 'if the regulator accepts, the design is ok'. Actually the regulator does not only accept the plans, but also influences the design process. This could also imply a decrease in undivided design authority in reducing power company autonomy.

> *'The authorities give us our marching orders for these things, we have to work according to that and also, [power plant name] has established their own guide-lines accordingly and, how the design work, what kind of documentation is required, so I'm not sure whether there's anything, they work well or don't, but we'll have to do them anyway. We cannot take any short cuts; we must follow the specified procedures. We cannot establish our own design methods in that sense.'* (Energy company employee, the waste management system case)

In communicating with some power company workers, however, this issue of 'shared design authority' was promptly rejected: it was stated that the design authority clearly lies within the power companies. This could very well be true, but the current workers cannot speak on behalf of the future ones; if the plausible conditions for shared authority exist, the power companies should be conscious so that the responsibility of the end-product as a whole never slips away in daily design practices. This is indeed important because shared responsibility can sometimes mean that nobody takes the final responsibility of maintaining an overall understanding of the design process.

To summarize, the following possible causes imply that failing to maintain the understanding and responsibility of the overall project and end-product could be a plausible reason for unsuccessful designs in the NPP domain:

1. The threat of lack of focus on the end-product holistically due to the burdensomeness of documentation as well as project and requirements management.
2. The threat of sharing the design authority with the regulator, i.e., nobody would maintain the final and complete responsibility in actual design activities.
3. Technical complexity and the sheer size of some projects.

4 CONCLUDING INTERPRETATIONS: ACHIEVING RESILIENT DESIGNS?

This study is relevant in view of managing resilience as it discusses the shortcomings and trade-offs related to managing design in safety critical domains by stringent regulation and by increasing requirements – understanding the designed solutions holistically can be compromised due to the tediousness of requirement management and document drafting; yet, holistic understanding would be needed in creating resilient systems. We do not oppose thorough governmental regulation in safety critical domains, but, at the same time, one should ensure that gaining the regulator acceptance does not become the focus of design activity: safety and functionality should be the main design goals. Resilience engineering is to say that safety is not to be understood solely as the absence of accidents and other negative events but as a capability to perform successfully (Hollnagel et al., 2011). However, designing for capability of this kind can be in practice challenging if requirement management and precise document drafting are emphasized – this is because iteration of plans becomes more challenging; it might be hard to conceive how to operate a system in the best possible manner prior the first versions of the systems.

The argument thus goes that if the design activity focuses largely on technical requirement management and on drafting precise documents for the regulator, insufficient effort might be dedicated to iterating the design idea and to considering the design in terms of usage at a system level. Human activity would have to be considered holistically, however, if the system is to allow resilient and flexible activity; means for making sense of varied situations should be supported. These issues can be difficult to foresee in plans or to confine to

requirements.

This study questions the thinking that increasing requirements and preciseness in regulation is a simple means for producing safety – other issues are needed as well. These include the following: 1) sufficient recourses for iteration and reconsidering the design idea, 2) safety culture in design, which emphasizes the design organization responsibility in lieu of regulatory acceptance, and 3) leadership that ensures system thinking in design. As discussed already, the first point seems to be well actualized in Finland, but may also reflect economic burdens in the domain. One could also consider the so-called 'incremental commitment model' in design, which has been proposed as an alternative to the already discussed V-model (Pew & Mavor, 2007). The key idea in the incremental commitment model is that the stakeholders involved evaluate different versions of the plans in different phases; these include initial scoping and concept definition. This implies that stakeholder opinion would be used in defining the initial plans and the design concept in the very beginning of the process. It could be problematic, however, if the regulator would participate at this phase with a formal role as a requirement specialist or such, because thus the regulator's independence as a reviewer could be compromised. The second and third point, in turn, reflect the DISC model of safety culture (Reiman et al 2009, Oedewald et al. 2011), which emphasizes responsibility for the entire system, seeing safety as a complex phenomenon, mindfulness, and management of good work conditions; the threats identified in this study could be understood as some of the issues the design organizations should be mindful about.

Overall, this article provides food for thought for those involved in design activities in a highly regulated safety-critical field. In order for the threats identified in our study not to take place, good and comprehensive requirements and rigorous regulatory oversight might not suffice; issues such as pride and feeling of responsibility in maintaining safety along with excellent and broadminded technical expertise and leadership are needed as well.

Acknowledgements

This study summaries and expands a chapter of a project report (Wahlström, in press). The study was supported by the SAFIR2014 programme, the Finnish State Nuclear Waste Management Fund (VYR), Nordic Nuclear Safety Research (NKS), VTT Technical Research Centre of Finland, and Vattenfall (Ringhals).

REFERENCES

Aspelund, K. (2006). *The design process.* New York, NY: Fairchild publications.

Hollnagel, E., Paries, J., David, D. W., & Wreathall, J. (2010). *Resilience engineering in practice: A guidebook.* Surrey, UK: Ashgate Publishing.

IAEA, (2003). *Maintaining the Design Integrity of Nuclear Installations Throughout Their Operating Life.* INSAG-19. Vienna, Austria: IAEA.

Macchi, L., Gotcheva, N., Alm, H., Osvalder, A.-L., Pietikäinen, E., Oedewald, P., Wahlström, M., Liinasuo, M. & Savioja, P. (2014). *Improving design pro-cesses in the nuclear domain. Insights on organizational challenges from safety culture and resilience engineering perspectives.* Final report, Nordic Nuclear Safety Research, NKS-301. Retrieved from http://www.nks.org/en/nks_reports/

Oedewald, P., Pietikäinen, E. & Reiman, T. (2011). *A guidebook for evaluating organisations in the nuclear industry - an example of safety culture evaluation*. Stockholm, Sweden: SSM.

Pew, R. W. & Mavor, A. S. (Eds.). (2007). Human-system integration in the system development process: A new look. Washington, DC: National Academy Press.

Reiman, T. & Oedewald, P. (2009). *Evaluating safety-critical organizations – emphasis on the nuclear industry.* Stockholm, Sweden: SSM.

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

Turner, R. (2007). Towards Agile Systems Engineering Processes. *CrossTalk, Journal of Defense Software Engineering,* 9, 11–15.

Wahlström, M. (in press). More requirements, more safety? Cultural tensions in NPP design activities. In P. Oedewald, N. Gotcheva, K. Viitanen & M. Wahlström (Eds.), *Safety culture and organisational resilience in the nuclear industry throughout the different lifecycle phases* (pp. 53–71). MANSCU Final report. VTT publications.