A Model Driven Approach for Early Assessment of Defense in Depth Capabilities of Complex Sociotechnical Systems

Conference Paper · August 2017

DOI: 10.1115/DETC2017-67257

5 authors, including:

Nikolaos Papakonstantinou
VTT Technical Research Centre of Finland
81 PUBLICATIONS **1,045** CITATIONS

SEE PROFILE

Bryan O'Halloran
Naval Postgraduate School
64 PUBLICATIONS **476** CITATIONS

SEE PROFILE

Douglas Lee Van Bossuyt
Naval Postgraduate School
135 PUBLICATIONS **936** CITATIONS

SEE PROFILE

Proceedings of the ASME 2017 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference
IDETC/CIE 2017
August 6-9, 2017, Cleveland, Ohio, USA

DETC2017-67257

A MODEL DRIVEN APPROACH FOR EARLY ASSESSMENT OF DEFENSE IN DEPTH CAPABILITIES OF COMPLEX SOCIOTECHNICAL SYSTEMS

Nikolaos Papakonstantinou
VTT Technical Research Centre of Finland
Vuorimiehentie 3
Espoo, Finland
nikolaos.papakonstantinou@vtt.fi

Teemu Tommila
VTT Technical Research Centre of Finland
Tekniikankatu 1
Tampere, Finland
teemu.tommila@vtt.fi

Bryan O'Halloran
Department of Systems Engineering
Naval Postgraduate School
Monterey, California 93943
bmohallo@nps.edu

Jarmo Alanen
VTT Technical Research Centre of Finland
Tekniikankatu 1
Tampere, Finland
jarmo.alanen@vtt.fi

Douglas L. Van Bossuyt
KTM Research
18280 SW 108th Ave.
Tualatin, OR 97062
douglas.vanbossuyt@gmail.com

ABSTRACT

Defense in Depth (DiD) is a key design principle helping to improve the safety of complex systems in domains like nuclear power, oil and gas, and mining. DiD affects the basic design of the system because it contains requirements for isolation, diversity and safety divisions. If the DiD assessment happens late in the design process, there is a risk of costly redesign and project delays. To avoid this issue, this paper refines a set of early DiD assessment design rules and proposes a model-driven methodology for early assessment of the implementation of the DiD capabilities of a complex system design. The topology of the different design aspects of the system under study (mechanical, electrical, human factors, and others) and the dependencies between system elements are captured in a High Level Interdisciplinary Model (HLIM) that also holds DiD specific attributes. The resulting system model is assessed against the proposed set of DiD rules and requirements, and then it can be improved according to the results. The methodology is applied to a case study of an early nuclear power plant model of a spent fuel pool cooling system. The proof-of-concept software tool developed for early DiD assessment and presented in this paper is able to identify undesired dependencies between system elements of redundant systems, of different defense lines and other DiD related weaknesses. This provides practitioners with insights into potential vulnerabilities in the design and enables focused redesign to address the identified problems early in the design process.

INTRODUCTION

The design of complex, safety-critical, and sociotechnical systems is challenging because of the system's emergent behaviors and unexpected events that can lead to system failure. In particular, complexity is caused by interactions between different elements of the system such as process, electrical, and automation systems; the environment; and human users. Examples of major accidents show that interdisciplinary failure propagation paths can contribute significantly to emergency situations [1]. In these cases, we believe that traditional reliability-based safety assessment methodologies are not enough to capture complex emergent system failure behaviors and new design principles should be introduced [2].

Defense in Depth (DiD) is a set of design principles that are widely applied in industry to control risks [3]. It is also required by regulators in critical domains like the defense industry, oil and gas, and nuclear power [4]. DiD principles affect the basic structure of the system under design and it is not easy to add them later in the design process without very costly redesign. Therefore, there is a need for early assessment of the overall safety architecture.

In this paper we propose a model-based, computer supported, multidisciplinary methodology for early assessment of a subset of DiD capabilities. We demonstrate the method on a spent fuel storage pool at a nuclear power plant.

LITERATURE REVIEW

Introduction to DiD principles

Defense in Depth (DiD) is an approach to control risks with multiple layers of protection. While historically conceived as a military strategy, DiD in now widely used in industry and society. Typical domains that use DiD design principles are the process industries [3], oil and gas [5], mining [6], and medicine [7]. For decades, DiD has been the cornerstone of nuclear safety as well [8].

The core principle of DiD is that a variety of systems are put in place to control different potential situations that range from normal plant operation to the management of accidents. These systems are layered in DiD levels. The tasks of each DiD level are performed by systems arranged as independent and consecutive *defense lines*. If one defense line fails, the following defense line is designed to prevent or mitigate the consequences of the first failing. In addition to physical barriers against release of radioactive material (e.g. fuel cladding, primary coolant boundary, and containment structure) in nuclear power plants, DiD covers various technical and organizational means; for example, separate systems for normal operation, reactor protection and emergency situations, plant layout (safety divisions), access control, and emergency response organizations. While the application of DiD has been widely accepted, the Fukushima disaster shows the importance of external events, organizational factors, emergency preparedness and spent fuel pool safeguards [9]. Thus, a multidisciplinary approach is needed in the design and analysis of the overall DiD architecture.

Various intended and hidden dependencies are a major source of complexity in safety-critical, and sociotechnical systems. The IAEA and EPRI have good coverage of DiD requirements and regulations for the nuclear power industry [10-12]. The requirements and regulations can be summarized as requiring independence between DiD systems, safety critical systems should be independent from secondary systems not critical to the safe operation of the plant, systems performing safety functions must have at least two and preferably three independent redundant systems, and Common Cause Failures (CCFs) due to identical hardware across redundant safety systems must be minimized. These requirements and regulations outline the need to understand dependencies. While interactions are necessary for system functionality, unnecessary and potentially dangerous dependencies must be identified and removed early in the design process. Therefore, dependencies are a key issue in DiD analysis.

The many requirements and recommendations from the nuclear power industry are concerned with the existence and degree of various types of dependencies in plant design. In addition, the possibility of CCF is a major concern in safety analysis. Safety classification is used to identify the most critical parts of a system's design. Today, Probabilistic Risk Analysis (PRA) and related methods are typically used for the analysis of DiD capabilities [8, 13]. While PRA captures many DiD issues and helps plant designers to assess the safety of a nuclear power plant, we state that structured models and reasoning rules need to be developed to give answers to questions such as "Are these systems independent?" or "Are the regulatory DiD requirements satisfied?" early in the design process before large architectural decisions have been made.

Four concepts in DiD are important to mention in the context of this paper including redundancy, physical separation, functional isolation, and diversity. *Redundancy* refers to the existence of more than one means for performing a required function [14]. A common example is the "m out of n" structure, wherein at least m of the total n items must be functioning to maintain the ability to perform the required function.

Physical separation refers to the separation of systems or components from one another by means of adequate barriers, distance or geometry, or combinations thereof [4, 11]. In our understanding, the key idea is to prevent propagation of harmful physical phenomena. Examples include flooding, fire, missiles, and chemical explosions [12].

Functional isolation is defined by [4] as "prevention of influences from the mode of operation or failure of one circuit or system on another". Functional independence is a condition that exists when successful completion of a system's required functions is not dependent upon any behavior, including failures or normal operation, of another system, or upon any signals, data or information derived from the other system [12]. Stated in the context of this paper, the purpose of functional isolation is to reduce dependencies (e.g. information flows, synchronization issues, common cause failures) between functions instead of system components. The means can be purely functional (no signals), software-based (protocols) or physical (one way links or no signal paths).

In general, *diversity* refers to the condition of being composed of differing elements. The IAEA [4] characterizes diversity as "presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure". There are many types of diversity based on operating principles, design methods and organizations, and implementation technologies [15]. The purpose of diversity is to improve system dependability by limiting the risk of CCFs, especially systematic CCFs.

Related work

To support DiD assessment, we have developed tools to analyze dependencies in the overall system architecture at the early stage. In this, we have applied existing research and technologies. For example, dependency modelling has been an active research field in multiple domains such as critical infrastructure protection [16] and [17]. In addition, our approach is based on Model-Based Systems Engineering (MBSE). We define MBSE as INCOSE does: "MBSE is the formalized application of modeling to support system requirements, design, analysis, verification and validation [activities] beginning in the conceptual design phase and continuing throughout development and later life cycle phases" [18]. The difference between MBSE

and traditional system engineering is in the use of formalized or semi-formalized machine-readable models instead of non-structured drawings and word processing documents. This does not mean that documents are not used in MBSE, but it does mean that MBSE is based on structured models rather than on documents.

Models enable computer-assisted verification & validation and system analysis, including safety analysis (i.e. Model-Based Safety Analysis, MBSA), such as FMEA (Failure Modes and Effects Analysis) using the Unified Modelling Language (UML) [19], formal (mathematical) modeling [20] and special purpose modeling (e.g. Module-based Failure Propagation (MFP) modeling used by Noh et al. [21]). Sandberg et al. [22] apply architecture modeling using the EAST-ADL2 architecture description language to assist Preliminary Hazard Analysis (PHA) of automotive embedded systems. Zhang et al. [23] apply Architecture Analysis and Design Language (AADL) to create both a control software model and its error model, and they finally apply a Markov chain model derived from the AADL models to compute the probabilities of error states of components and thereof of the whole system. Several metrics have been proposed for measuring the dependency between system modules [24]. In this paper, we use UML metamodeling for early system architecture models that enable computer assisted identification of DiD requirement violations.

METHODOLOGY

The proposed methodology provides a framework for early assessment of DiD design of complex cyber-physical and sociotechnical systems. The primary contribution of this research is a method for assessing DiD during early system design so that redesign can be performed before significant architectural decisions have been made.

An overview of the methodology is presented in Fig. 1. There are four major elements required to successfully employ this method including a system model, a technique to assess the system specifically for interdependencies, and a set of criteria used to interpret the results of assessment technique. The research in the paper clearly defines the first two, while we understand the third is clearly and highly dependent on the context. As an example of the third, the level of allowed dependency is contingent on the level of system safety. Thus, a nuclear power plant would be stricter than an autonomous vehicle used for mapping terrain. As a result, the methodology presented in this section focuses on describing the system models and the technique developed to assess them.

The overall process used to employ this methodology starts with the early design of the system under study. The practitioner then gathers the DiD requirements relevant to the system. These requirements are then mapped to rules that can be checked against the High Level Interdisciplinary Model (HLIM) of the system. The HLIM is a new model proposed as a part of this research. This model contains:

1. a functional model to capture the functional decomposition of the system, a basic functional hierarchy, and mark the points of functional redundancy,

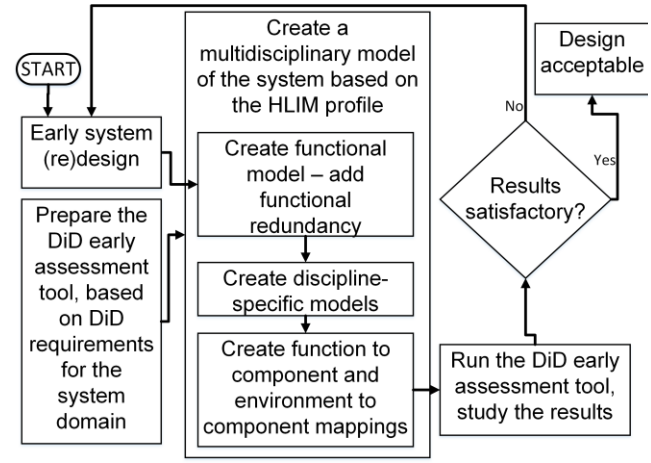

Figure 1 Flow chart showing the overview of the proposed iterative early DiD assessment methodology

2. a diagram for every design discipline (e.g., electrical, process, human factors, environment, automation) with the basic system topology and with links to elements of other disciplines when needed,
3. diagrams which model the mappings between function and system components, and the environment and system components.

The generation of these dependency diagrams can be facilitated by the use of the engineering database of the system under development as a data source, if it is available. When this modelling work is done, the DiD rules can be checked using a software that will treat the HLIM as a graph and try to find dependencies that break the DiD rules and also consider DiD related system component attributes, such as the technology used for the implementation and the allocation into safety divisions. The feedback of this assessment needs to be evaluated, and either the early design is considered acceptable or changes need to be made. Changes at this early phase of the design are much more efficient than later in the design process [25].

The key to the proposed methodology is the interdisciplinary models of the system under study. In MBSE, engineers create, communicate and analyze a structured model of a future system. Various model elements represent its structure, properties, and behavior of the system. The systems that we consider here are real-world entities consisting of *system elements*, such as equipment, software and people, all located in an operational environment. A *system function* is understood here as a capability of a system to act in some way. For example, a pump has the capability to create a water flow. Manual actions and tasks are considered as "functions" of the human operator. Function is an abstract concept used for design purposes only and does not have a direct counterpart in the real system. For example, a "control temperature" function of a digital I&C system is actually realized as a software component (system element) running on a programmable controller. For a detailed background for our modelling approach see [26].

Identifying the internal topology and dependencies of the system is essential for reasoning fault propagation paths. System

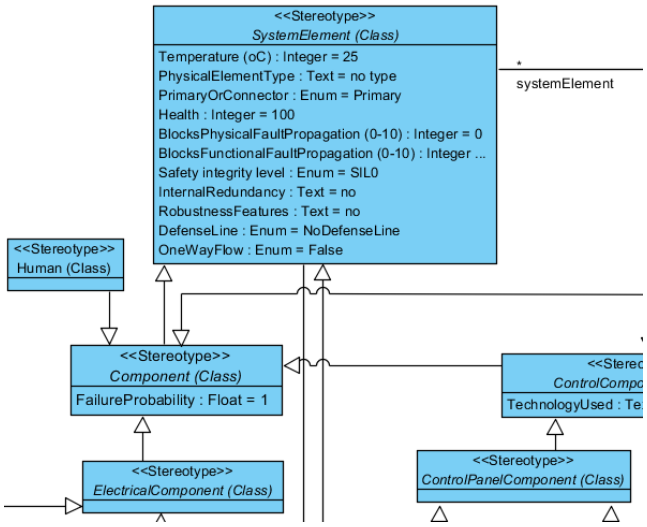

Figure 2 A UML profile for High Level Interdisciplinary Models based on UML class diagrams (partial). DiD specific attributes have been added to facilitate the DiD assessment

elements and functions are linked together with connectors (e.g. cables and pipes), flows (e.g. information transfer) and are decomposed to parts (i.e. to lower level system elements) as far as is appropriate for the design stage. Connectors perform the flows (in one or two directions) and may provide barriers against harmful physical phenomena. In the general case, the functions of parts collaborate in different configurations to perform a higher system-level function. In high-reliability systems, typical redundancy patterns, such as 2 out of 3 systems being required

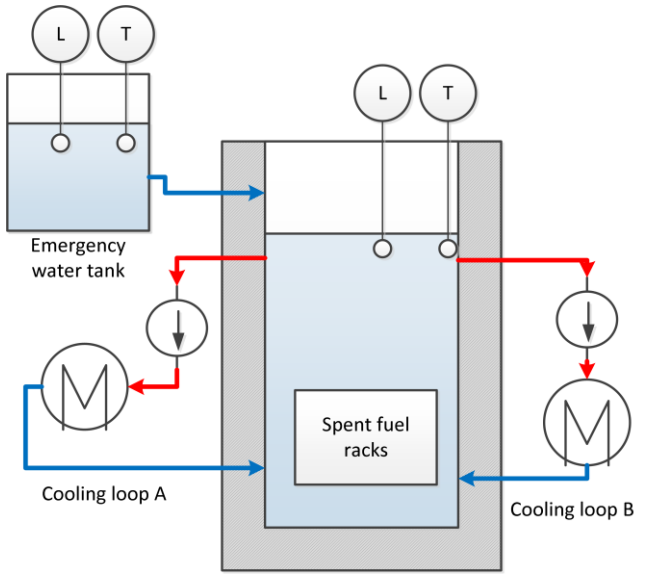

Figure 3 An overview of the case study, the spent fuel cooling system of a Nuclear Power Plant with two redundant cooling loops and an emergency cooling system

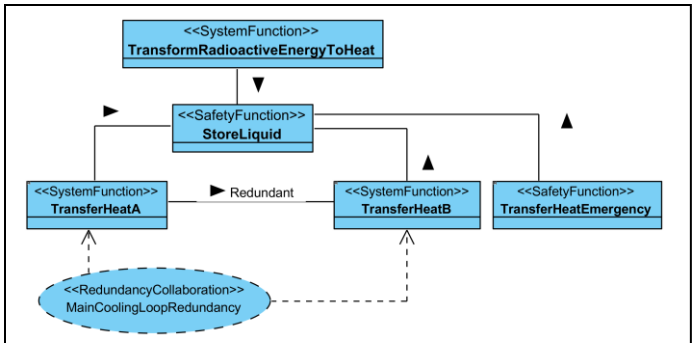

Figure 4 The simple functional model of the case study which captures the redundancy relationship between the two cooling systems

to function properly to prevent a failure, are important examples of failure tolerant configurations of system elements and functions. These patterns determine how failures in inputs can propagate to the outputs.

We consider here what kind of interdependencies might be observed in a nuclear system modelled according to the principles above. A more detailed discussion on the topic can be found, for example, in [27]. For the purposes of this paper, the following dependency types are the most relevant:

- Function → Function: Function needs material, energy or information from other functions.
- System element → Function: System element "performs" its functions, failure leads to degraded performance or total loss of the functions.
- Function → System element: To be able to operate, a system element needs services (e.g. power or cooling) from various support systems.
- System element → System element: Physical phenomena (e.g. heat or high voltage) in a system element may disturb or damage adjacent equipment or equipment physically connected to it.
- Location → System element: Captures effects of the element to the space and vice versa, e.g. effects of environmental conditions (e.g. humidity) in a space (e.g. a room) on the installed equipment.
- Technology → Function, System element: Development methods, organizations, tools and implementation technologies may lead to dependencies and Common Cause Failures (CCFs).

As described above, functional isolation, physical separation, redundancy and diversity are ways to reduce unwanted dependencies. For model-based analysis, the dependency types should be defined more exactly, for example:

- Function A is functionally dependent on function B, if the functional model contains a flow path from B to A.
- Function A is functionally dependent on system element C, if A is performed by C OR if there is a function B such that A is dependent on B AND B is "performed" by C.
- System element A is physically dependent on system element B, if there is a path of connectors from B to A OR if A AND B are located in the same space.

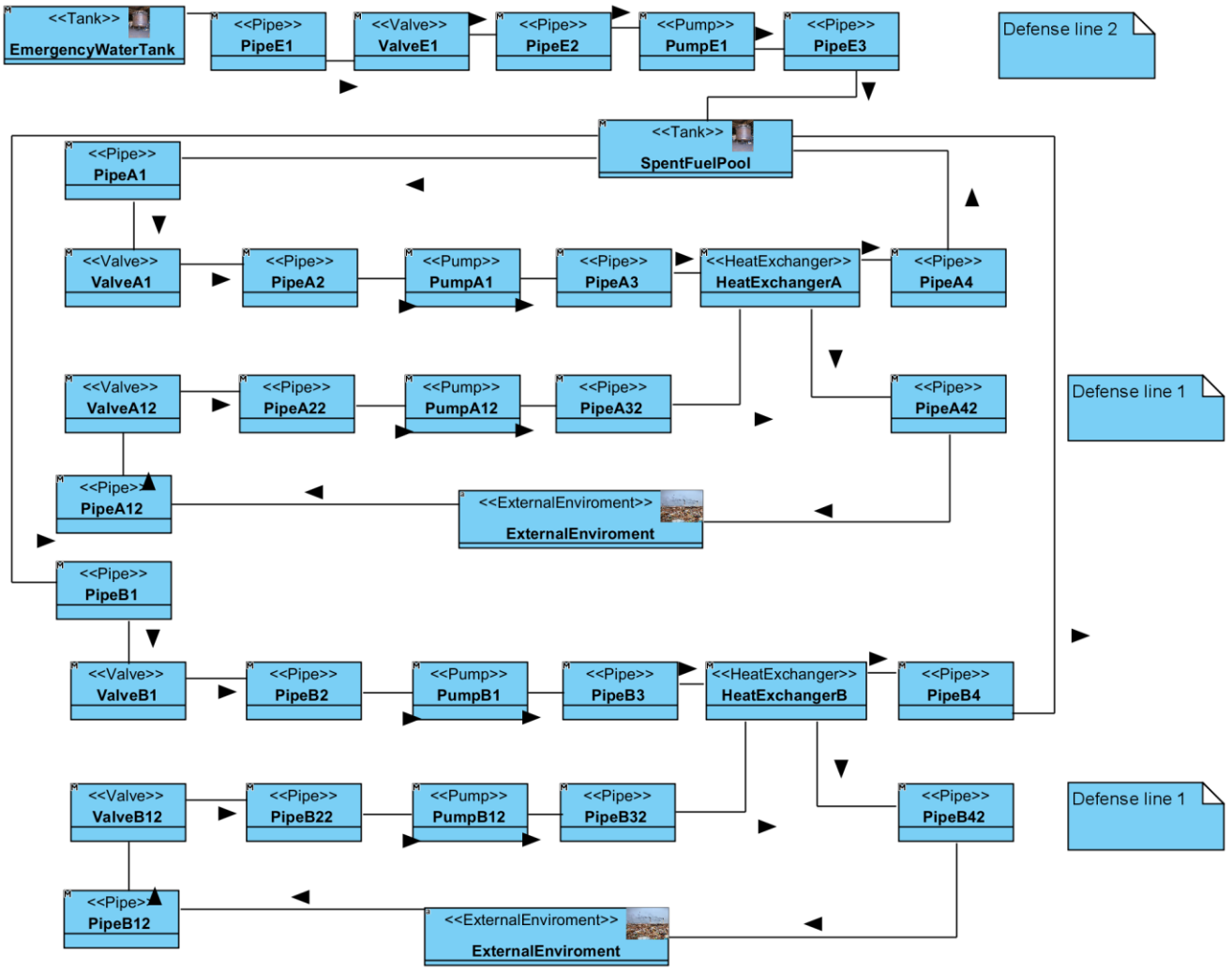

Figure 5 The process diagram of the case study. The "defense line" is an attribute of the process component, but it is also shown here as a note next the redundant cooling systems and the emergency cooling system

- System element A is physically dependent on space B if it is located in B OR if it is located in a space that is dependent of B through a path of connectors.

Instead of no or full dependency, there is a certain degree of "coupling" between system elements and functions. We propose that each direct dependency between two items in the model can be given a strength value in the range of 0…1. For longer dependency paths, the total strength can be calculated on the basis of link strengths and properties of system elements along the path. For example, redundancies have the ability to block propagation of failures. This gives a measure that can be used to rank potential problems in a design.

Different types of diversity are used to reduce the possibility of CCFs affecting systems that are redundant and isolated. Protection against CCFs is a design requirement in domains like the Nuclear [11]. To keep things simple, we consider only alternative technologies (e.g. microcontroller-based automation vs discrete logic gates) and add the following rules:

- Two system elements or functions are diverse if they are based on different technologies.
- Two system elements or functions are susceptible to CCF if they are not diverse or if they are dependent in some of the other ways listed above.

A UML profile [28] for early DiD modelling, used later in the case study, is presented in Fig. 2. This profile captures the basic ontology that implements a subset of the ideas mentioned above and facilitates the development of HLIMs for early DiD assessment. A "System of Interest" is described in terms of "Functions" and "System elements". The "System elements" can be human, electrical, control and process "Components" or various "Spaces" like rooms, corridors and staircases. With the help of a system model that follows this profile (see the diagram figures of the case study) and algorithms identifying possible dependencies, it is possible to pinpoint potential weaknesses and inconsistencies in the proposed system architecture. Rules can be used to check whether some of the regulatory requirements are satisfied. To do this, the requirements must first be interpreted

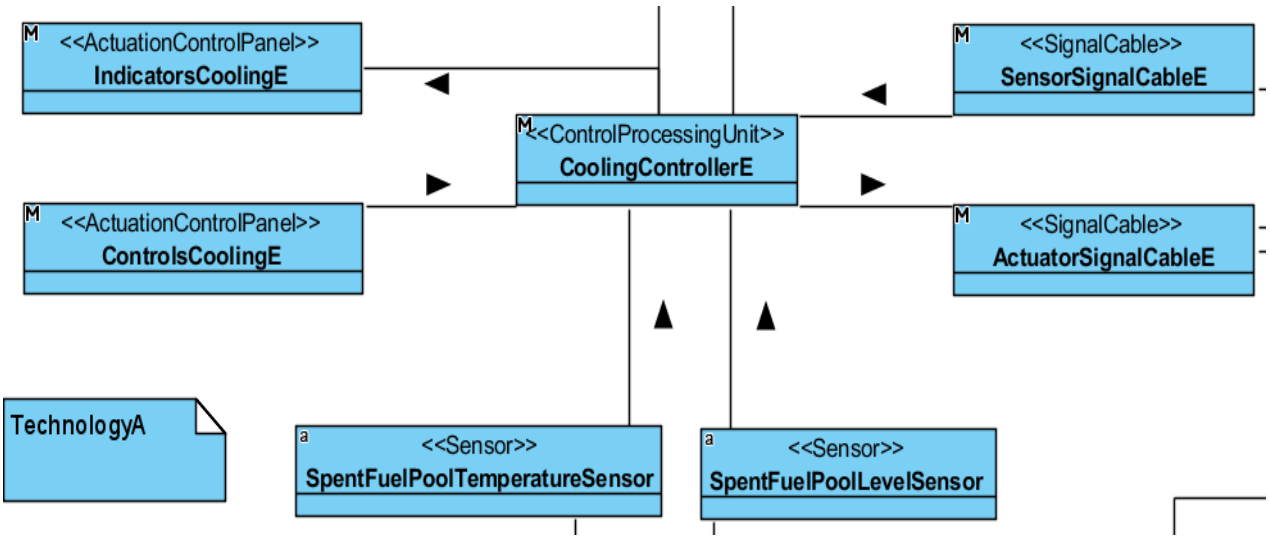

Figure 6 The automation diagram of the case study (partial). The controller contains the "diversity" DiD attribute (e.g. micro-controller, simple Boolean logic or analog relays). All automation components have safety classification

and formalized in a way that enables automated verification. In the following we will give a small example that demonstrates the basic idea.

CASE STUDY AND RESULTS

The case study is applied to the cooling system of a spent fuel pool of a Nuclear Power Plant and is used to demonstrate the methodology. An overview of this system is shown in Fig. 3. Two redundant cooling loops (A and B) are used to circulate water through heat exchangers. Even though both loops are normally used, one is enough to keep the temperature at a safe level. If the temperature is too high or the water level drops below a safety threshold, an emergency system is activated to add water to the pool.

The HLIM of the fuel pool was created in the Visual Paradigm UML drawing tool [29]. It contains a functional model that captures the redundancy relationship between the cooling loops A and B (see Fig. 4), simple models of the process (see Fig. 5), automation (see Fig. 6), electrical supply (see fig. 7), environment (see Fig. 8) and human users (see Fig. 9). Additional diagrams model the function to system element (see Fig. 10) and environment to system element dependencies (see Fig. 11).

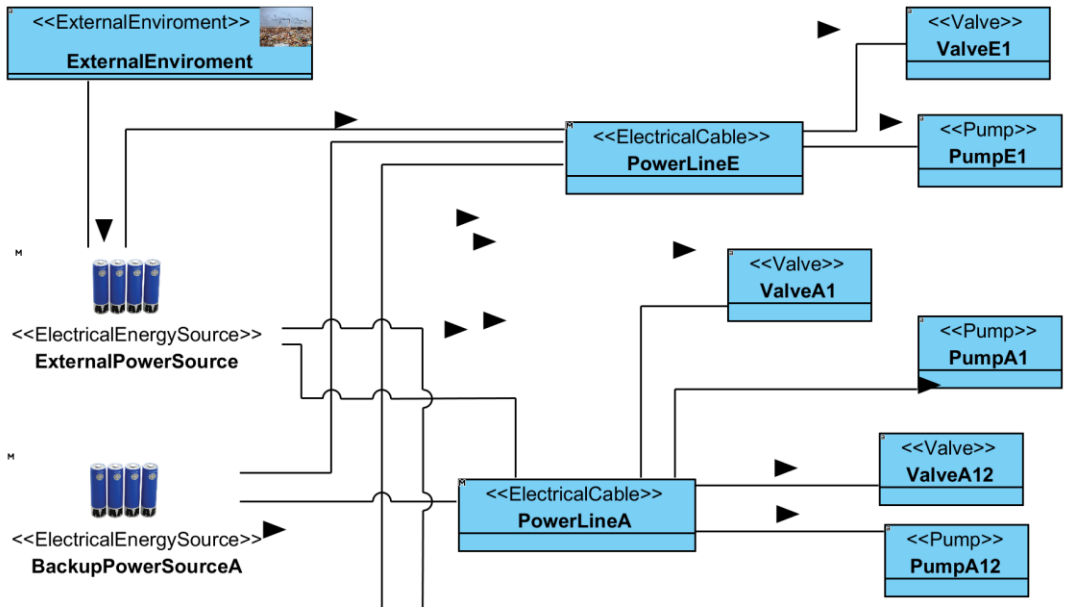

Figure 7 The electrical diagram of the case study (partial). The process components shown here are references to the process diagram. There is a component-level redundancy here, the two backup power sources (the second is not shown)

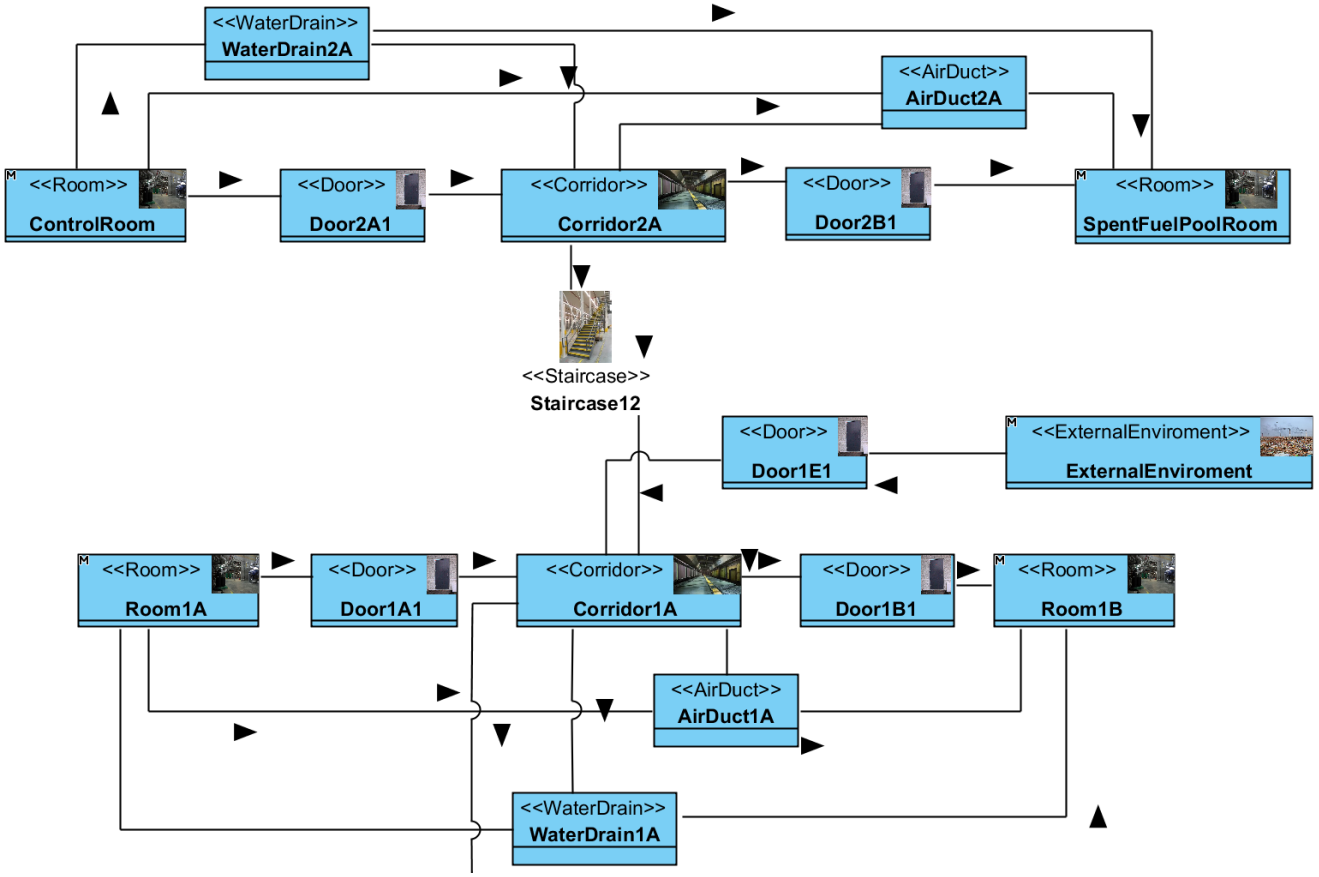

Figure 8 Part of the environment diagram of the case study. The system components are allocated to 3 levels (-1, 1 and 2). It is important to include in this diagram all possible connections between the spaces which can potentially propagate failure. The spaces are allocated to safety divisions.

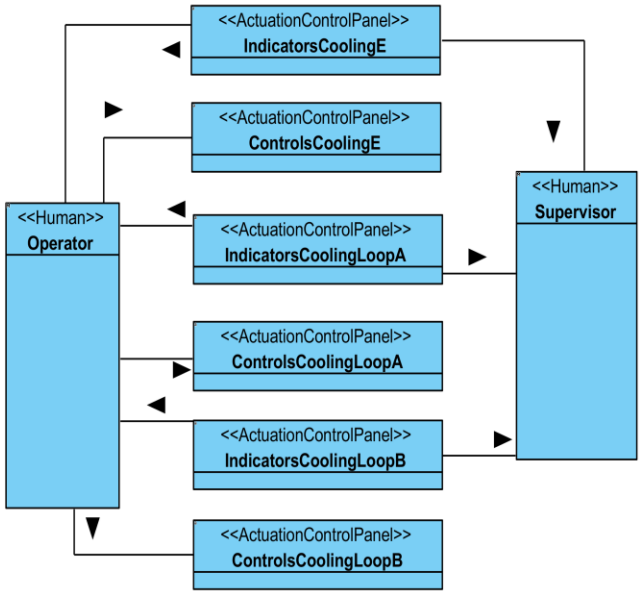

Figure 9 The human factors diagram of the case study. The fact that the case study has one control panel and one operator for all the cooling loops is flagged as an issue

A set of six rules that can be automatically assessed and are derived from the DiD requirements presented in the literature review and methodology section was compiled for the domain of our case study. The rules can be assessed against the dependency relations within the HLIM and the DiD specific attributes of the model. These rules were applied on the case of a spent fuel cooling pool in a generic power plant similar to those found in Finland although we do state here that this case study has been carefully developed to not represent real-world systems. The rules include:

1) No dependency links between components with different safety classes (represented in our case as Safety Integrity Levels, SILs).
2) System components which belong to redundant subsystems within the system should be allocated to spaces assigned to different safety divisions.
3) System components of redundant systems should not have dependencies with each other.
4) Automation components of redundant control systems should utilize diverse technology.
5) A system automation component of lower safety class can be linked to a component with higher safety class

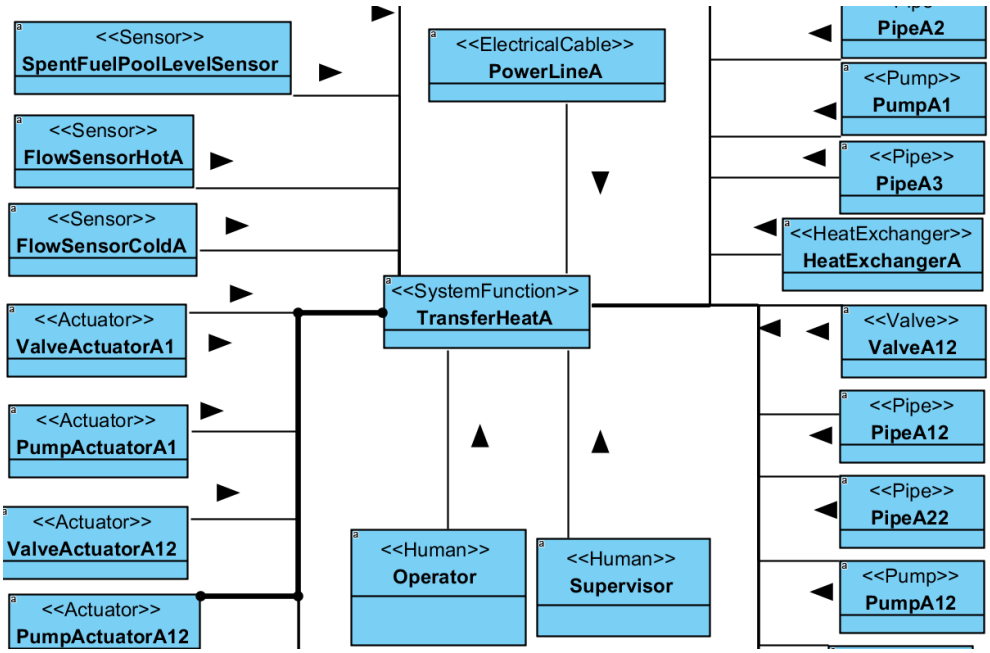

Figure 10 The dependency diagram which captures the mappings between the "Transfer Heat A" function of the case study and the system components (partial). Since the redundancy relation is captured in the functional model, these mappings show how redundancy is propagated to the system components

only if there is one-way isolated flow (e.g. optical connection against electrical hazards).

6) System components of defense lines should not have dependencies with each other.

A prototype software tool (see Fig. 12) was developed to parse the XMI representation [28] of the HLIM of the system under study and to report cases in which the rules are broken.

The DiD early assessment tool that we present here produces an output that is very strict to the six rules without any filtering. This leads to verbose output that needs human analysis to determine which cases are indeed DiD design weaknesses. An overview of the early DiD assessment results for our case study are as follows:

The results of the assessment of Rule 1 highlighted the boundaries of systems which are safety classified the non-safety classified process components. For example, the emergency tank temperature sensor classified as SIL3 is connected to the emergency water tank that has no safety classification.

The results for Rule 2 (redundancy and safety divisions) among other output, identified the fact that both redundant cooling systems are monitored and operated using the same control panel and by the same operator. This is a source of risk.

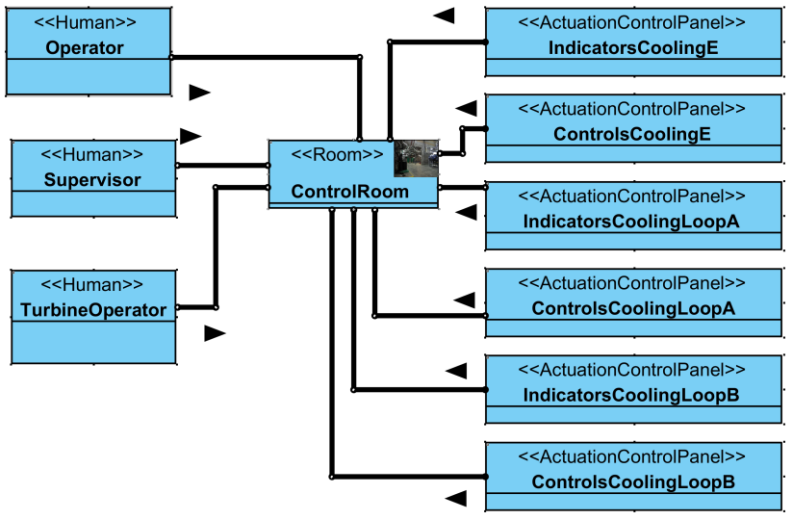

Figure 11 Example of environment to components diagram. The "Control room" space is linked to the humans included in the case study and the control panel elements (monitors and controls)

Figure 12 The prototype tool which parses the HLIM of the system and assesses it against a set of early DiD rules

Rule 3 is associated with the isolation of redundant subsystems. The tool was able to identify dependency paths between the two redundant cooling systems that included the operator, the control room, the spent fuel pool temperature and level sensors (which were shared between redundant systems) and the external environment (one water source feeds both heat exchangers).

Rule 4 checked that the automation controllers assigned to redundant functions are indeed using different technologies.

Rule 5 didn't identify any automation components which are connected but have different safety classification.

Rule 6 is related to the isolation of defense lines. In our case study, the two redundant cooling systems belong to the same defense line and the emergency system belongs to a second defense line. Some of the dependency paths identified were through the shared spent fuel pool sensors, the power lines (from grid and backup ones) and the operator.

While these results may seem obvious to nuclear power experts, the tool successfully identified these design weaknesses which gives us confidence in the tool identifying other weaknesses that are not currently identified by existing methods (e.g.: PRA, etc.).

DISCUSSION

The dependency paths mentioned in the case study section were very short (direct links or through one element). The tool can be asked to find longer dependency paths that, for example, go through the environment (doors, corridors, staircases) and link redundant systems or systems of different defense lines. These are particularly difficult to identify without a good model and an automated assessment process. Addressing these weaknesses would involve making drastic design changes such as duplicating key elements of the design. These changes can either be implemented and the design will be re-assessed or a strong justification for keeping the design as-is needs to be provided.

It should be noted that while the methodology presented in Figure 1shows a design iteration step, we do not perform a design iteration here. An engineering practitioner using this method would use the results presented in this section to iterate on the system design and re-run the proposed methodology and software tool to determine if the system design changes sufficiently increase the DiD of the system.

While the results shown here are limited in their scope, the proposed method does demonstrate its ability to find existing known design weaknesses in spent fuel cooling pools. We are currently refining the method and software tool to deploy on much larger systems, such as an entire nuclear reactor complex, to identify potential design weaknesses that have been overlooked by existing methods. The method is computationally intensive (a downside that we are working to address) and does not lend large case studies to be presented succinctly but shows significant promise in identifying potential overlooked design weaknesses.

CONCLUSIONS

The methodology proposed in this paper provides a model-driven framework for early assessment of key DiD principles. The interdisciplinary modelling approach enables the identification of dependency paths that include elements from different design domains (e.g., environment, process, electrical, human factors and automation). The early assessment of DiD can lead to system architecture modifications which would be very costly to implement later on in the design lifecycle.

The presented case study of a spent fuel pool cooling system revealed weaknesses related to the DiD principles such as in the isolation of redundant subsystems and dependencies between defense lines. The identified design weaknesses can then be addressed to strengthen the DiD of the system before major architectural decisions have been made.

This DiD early assessment presented here will be combined in future research with failure propagation assessments and probabilistic safety assessment methods to develop a more complete evaluation of the safety level of the system design. A possible direction future is the generation of evidence supporting safety cases about the design of the system. In addition to supporting the design process, the method presented here may find use in safety cases presented to nuclear regulators and regulators in other industries to demonstrate a system's DiD as being sufficient to meet both the letter and spirit of the regulations.

ACKNOWLEDGEMENTS

This research was funded by the Finnish Research Programme on Nuclear Power Plant Safety 2015-2018 (SAFIR2018, http://safir2018.vtt.fi).

REFERENCES

[1] U. S. N. R. C. (NRC). (2013). Three Mile Island Accident. Available: http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.pdf

[2] N. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety: MIT Press, 2011.

[3] R. Squillante Jr, D. J. S. Filho, R. M. da Silva, J. A. L. Souza, F. Junqueira, and P. E. Miyagi, "A Novel Safety Control Hierarchical Architecture for Prevention and Mitigation of Critical Faults in Process Industries based on Defense-in-depth, Reactive Systems and Safety-diagnosability," IFAC-PapersOnLine, vol. 48, pp. 1326-1331, // 2015.

[4] IAEA, "IAEA Safety Glossary 2007 Edition," ed, 2007.

[5] J. H. Saleh, R. A. Haga, F. M. Favarò, and E. Bakolas, "Texas City refinery accident: Case study in breakdown of defense-in-depth and violation of the safety–diagnosability principle in design," Engineering Failure Analysis, vol. 36, pp. 121-133, 1// 2014.

[6] J. H. Saleh and A. M. Cummings, "Safety in the mining industry and the unfinished legacy of mining accidents: Safety levers and defense-in-depth for addressing mining hazards," Safety Science, vol. 49, pp. 764-777, 7// 2011.

[7] A. M. Sholukh, J. D. Watkins, H. K. Vyas, S. Gupta, S. K. Lakhashe, S. Thorat, M. Zhou, G. Hemashettar, B. C. Bachler, D. N. Forthal, F. Villinger, Q. J. Sattentau, R. A. Weiss, G. Agatic, D. Corti, A. Lanzavecchia, J. L. Heeney, and R. M. Ruprecht, "Defense-in-depth by mucosally administered anti-HIV dimeric IgA2 and systemic IgG1 mAbs: Complete protection of rhesus monkeys from mucosal SHIV challenge," Vaccine, vol. 33, pp. 2086-2095, 4/21/ 2015.

[8] IAEA, Assessment of Defence in Depth for Nuclear Power Plants, 2005.

[9] WENRA, Report Safety of new NPP designs - Study by Reactor Harmonization Working Group RHWG, 2013.

[10] EPRI, "Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environments," 21-Nov-2014 2014.

[11] STUK, GUIDE YVL B.1 Safety design of a nuclear power plan, 2013.

[12] IAEA, Design of Instrumentation and Control Systems for Nuclear Power Plants. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2016.

[13] EPRI, "Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades: Applying Risk-Informed and Deterministic Methods," 13-Dec-2004 2004.

[14] IEC, "IEC IEC 60050-192:2015 International electrotechnical vocabulary - Part 192: Dependability," ed, 2015.

[15] NRC, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems (NUREG/CR-7007, ORNL/TM-2009/302)," 2010.

[16] R. Bloomfield, N. Chozard, and P. Nobles, "Infrastructure interdependency analysis: introductory research review," 2009.

[17] O. N. Philip, "Protecting Critical Infrastructure by Identifying Pathways of Exposure to Risk," Technology Innovation Management Review, vol. 3, 2013.

[18] S. Friedental, R. Griego, and M. Simpson, "INCOSE Model Based Systems Engineering (MBSE) Initiative," presented at the INCOSE2007, San Diego, 2007.

[19] M. Chaari, W. Ecker, C. Novello, B. A. Tabacaru, and T. Kruse, "A model-based and simulation-assisted FMEDA approach for safety-relevant E/E systems," in 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2015, pp. 1-6.

[20] P. Struss and A. Fraracci, "Automated Model-based FMEA of a Braking System," IFAC Proceedings Volumes, vol. 45, pp. 373-378, 1// 2012.

[21] K.-W. Noh, H.-B. Jun, J.-H. Lee, G.-B. Lee, and H.-W. Suh, "Module-based Failure Propagation (MFP) model for FMEA," The International Journal of Advanced Manufacturing Technology, vol. 55, pp. 581-600, 2011// 2011.

[22] A. Sandberg, D. Chen, H. Lönn, R. Johansson, L. Feng, M. Törngren, S. Torchiaro, R. Tavakoli-Kolagari, and A. Abele, "Model-Based Safety Engineering of Interdependent Functions in Automotive Vehicles Using EAST-ADL2," SAFECOMP 2010, Vienna, Austria, September 14-17, 2010. Proceedings, E. Schoitsch, Ed., ed Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 332-346.

[23] T. Zhang, Y. Jiang, J. Ye, C. Jing, and H. Qu, "An AADL Model-Based Safety Analysis Method for Flight Control Software," in 2014 International Conference on Computational Intelligence and Communication Networks, 2014, pp. 1148-1152.

[24] K. Hölttä-Otto, N. A. Chiriac, D. Lysy, and E. Suk Suh, "Comparative analysis of coupling modularity metrics," Journal of Engineering Design, vol. 23, pp. 790-806, 2012/11/01 2012.

[25] N. Papakonstantinou, S. Sierla, J. Alanen, and K. Koskinen, "Reducing redesign of safety critical control systems by early risk assessment," INDIN 2010, Osaka, Japan, 2010.

[26] T. Tommila and J. Alanen, "Conceptual model for safety requirements specification and management in nuclear power plants," VTT - VTT Technology: 238. 120 p. + app. 26 p., Espoo, 2015.

[27] J. M. Torry-Smith, N. H. Mortensen, and S. Achiche, "A proposal for a classification of product-related dependencies in development of mechatronic products," Research in Engineering Design, vol. 25, pp. 53-74, 2014.

[28] OMG. (2015). OMG Unified Modeling Language TM (OMG UML) specification version 2.5. Available: http://www.omg.org/spec/UML/2.5/PDF

[29] Visual Paradigm. (2016). Visual Paradigm homepage. Available: https://www.visual-paradigm.com/

