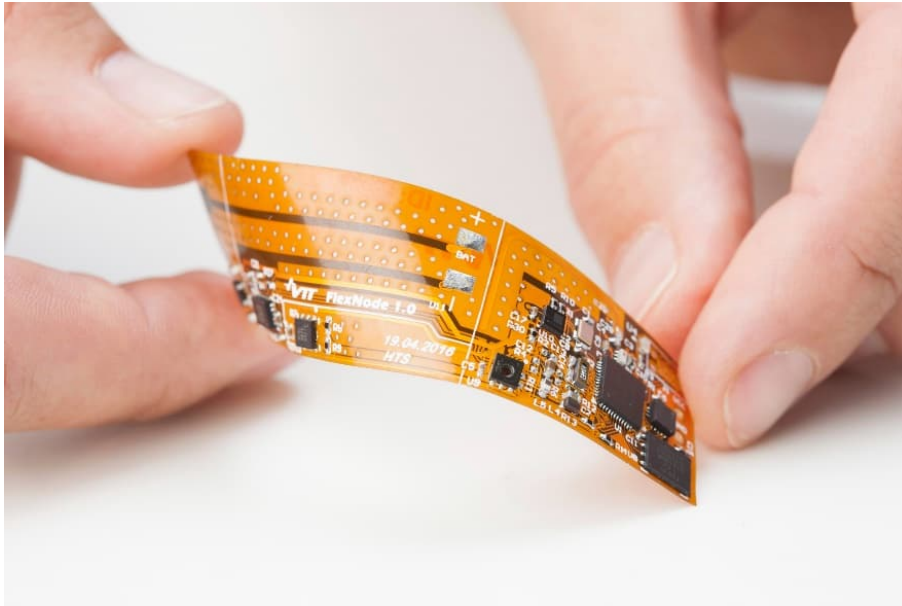


RESEARCH REPORT

VTT-R-00677-23



I&C system architecture PRA – Literature review

Authors: Kim Björkman

Confidentiality: VTT Public

Version: 4.12.2023



| | |
|---|---|
| Report's title I&C system architecture PRA – Literature review | |
| Customer, contact person, address VYR | Order reference SAFER 7/2023 |
| Project name Probabilistic Risk Assessment Labour, Improvements and Extensions | Project number/Short name 135903/PRALINE |
| Author(s) Kim Björkman | Pages 15/ |
| Keywords probabilistic risk assessment, instrumentation and control system, architecture | Report identification code VTT-R-00677-23 |
| <p>Summary</p> <p>Probabilistic risk assessment (PRA) modelling of digital instrumentation and control (I&C) systems has been studied for a long time in research projects. Some real-life applications have also been developed during the past decades. Traditionally, PRA has focused mainly on modelling defence in depth (DiD) levels 3 and 4. From I&C perspective this means that mainly the reactor protection system (RPS) has been explicitly modelled. Therefore, the research has also focused on modelling the RPS in PRA.</p> <p>Based on our review, the literature regarding PRA of the overall I&C architecture is rather scarce. A large part of the literature focuses on I&C common cause failure assessment. Some literature regarding PRA assessment of DiD levels (on a general level) can be found. Features of overall I&C architecture PRA have mainly been considered within Nordic co-operation and within SAFIR-projects. They have also been taken into account in real-life application. However, from these cases there is only a limited amount of information publicly available.</p> <p>The current Working Group on Risk Assessment task DIGMORE considers PRA of I&C systems from a bit broader scope. The study includes modelling aspects, such as priority logic, back-up systems and spurious actuations. The goal of DIGMORE is to achieve an in-depth understanding of PRA relevant impacts of interactions within the entire I&C architecture.</p> | |
| Confidentiality | VTT Public |
| Espoo 4.12.2023 | |
| Written by | Reviewed by |
| Kim Björkman Research Scientist | Tero Tyrväinen Research Scientist |
| VTT's contact address VTT Technical Research Centre of Finland Ltd, P.O. Box 1000, FI-02044 VTT, FINLAND | |
| Distribution (customer and VTT) SAFER2028 TAG1.1 members, VTT archive | |
| <p><i>The use of the name of "VTT" in advertising or publishing of a part of this report is only permissible with written authorisation from VTT Technical Research Centre of Finland Ltd.</i></p> | |



Approval

VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD

Date:

18 December 2023

Signature:

DocuSigned by:
Teemu Kärkelä
E7B76042F134471...

Name:

Teemu Kärkelä

Title:

Research Team Leader



Contents

| | |
|---|----|
| 1. Introduction..... | 4 |
| 2. Overall I&C architecture..... | 4 |
| 3. International cooperation within PRA of digital I&C..... | 5 |
| 3.1 OECD NEA CSNI WGRISK projects..... | 5 |
| 3.2 Nordic cooperation | 6 |
| 4. I&C architecture PRA..... | 6 |
| 4.1 PRA assessment of defence in depth..... | 6 |
| 4.2 I&C common cause failure assessment..... | 7 |
| 4.3 PRA of I&C features affecting several DiD levels..... | 9 |
| 4.4 PRA of I&C systems in existing plant PRAs..... | 9 |
| 4.4.1 PRA of NuScale small modular reactor I&C | 9 |
| 4.4.2 PRA of U.S. EPR I&C..... | 9 |
| 4.4.3 PRA of APR-1400 I&C | 10 |
| 4.4.4 PRA of ESBWR I&C..... | 10 |
| 4.4.5 PRA of OL3 I&C..... | 10 |
| 4.4.6 PRA of UK EPR I&C..... | 10 |
| 4.5 Miscellaneous..... | 10 |
| 5. Conclusions..... | 11 |
| References..... | 12 |

1. Introduction

Instrumentation and control (I&C) systems play a crucial role in the safe operation of nuclear facilities [1]. The overall I&C architecture (the organization of the complete set of I&C systems important to safety [2]) should consider several key principles in its design and implementation. The application of defence in depth (DiD) is the principal mean of preventing accidents and mitigating their effect [3]. Both deterministic and probabilistic analysis methods need be utilized in the assessment of DiD requirements [3].

Traditionally, probabilistic risk assessment (PRA) has focused mainly on modelling DiD levels 3 and 4 [4]. In addition, level 5 may have been modelled if level 3 PRA is required, whereas levels 1 and 2 are often implicitly covered by initiating event analysis. From I&C perspective this means that mainly the reactor protection system (RPS) has been explicitly modelled. However, a more detailed analysis of I&C systems involved in the DiD levels 1 and 2 could provide valuable information both for plant safety and availability perspectives [4]. In consequence, also the overall I&C architecture would need to be considered in PRA.

PRA modelling of digital I&C systems is a challenging task, because, e.g., the systems are very complex, there is very little failure data available and because of software. The topic has been studied for a long time (e.g. [5], [6]). However, mainly approaches to model the RPS have been considered [5, 7]). Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI) Working Group on Risk Assessment (WGRISK) task DIGMORE – A realistic comparative application of DI&C modelling approaches for PSA, started in 2022, extends the scope a bit by including also new modelling aspects, such as priority logic, back-up systems and spurious actuations. The work should achieve an in-depth understanding of PRA relevant impacts of interactions within the entire I&C architecture.

In this study, we perform a literature review on I&C architecture related PRA. The rest of this report is structured as follows. In section 2, we give a general level introduction to I&C system architecture. We summarize past digital I&C related WGRISK tasks and Nordic cooperation in section 3. In section 4, we review the literature related to I&C architecture PRA. Section 5 concludes this study.

2. Overall I&C architecture

According to [2], the overall instrumentation and control (I&C) architecture of a nuclear power plant “*is the organization of the complete set of I&C systems important to safety.*” In addition, non-safety I&C systems that are interconnected with I&C systems important to safety are often included in the overall I&C architecture. The architecture provides a high-level view of the individual I&C systems and how they relate to one another. It also specifies the allocation of plant functions to individual I&C systems and the specification of the interface requirements of the individual I&C systems [8]. The I&C system architecture has three primary functions [9]:

1. to provide the sensory (e.g., measurement and surveillance) capabilities to support functions such as monitoring or control and to enable plant personnel to assess the plant status,
2. to provide automatic control, both of the main plant and of many auxiliary systems,
3. to protect the plant from the consequences of any malfunction or deficiency of plant systems or human errors.

The overall I&C architecture should consider several key principles in its design and implementation [2], such as, DiD, protection against common cause failures (CCF), independence, diversity, and reliability [8]. Defence in depth is the principal means of preventing accidents and mitigating the potential consequences of accidents [3].



The DiD levels suggested by the Western European Nuclear Regulators' Association (WENRA) for new reactor designs are [3] (the bullet points under each level describes issues related to the design of I&C for the different levels as identified in [10]):

1. Prevention of abnormal operation and failures (normal operation)
 - Normal operation I&C should be designed to achieve good availability of the plant (low frequency of initiating events), and to eliminate the propagation of failures to safety I&C.
 - Operational I&C functions can have safety-related functions.
 - Systems/functions are not necessarily only non-safety classified.
 - Potential common cause initiator (CCI). It should be demonstrated that normal I&C cannot interfere safety I&C.
 - Could operational I&C be credited in safety analysis (usually not in deterministic safety assessment but maybe in PRA)?
2. Control of abnormal operation and detection of failures (anticipated operational occurrences)
 - Includes a number of preventive functions to avoid operational transients.
 - Also important to the availability of the plant and has functional dependences with level 1.
 - Functions are safety classified but not in the highest safety category. It has joint objectives with DiD level 3 and can have functional dependencies.
 - Plays usually minor role in PRA (part of the initiating event frequency).
 - Redundancy (1-out-of-2 success criterion) may be required.
3. Control of accident to limit radiological releases and prevent escalation to core melt conditions (3.a postulated single initiating events, 3.b postulated multiple failure events)
 - Includes reactor trip system (RTS) and engineered safety features actuation system (ESFAS) and belongs to the highest safety class.
 - Nowadays four-redundant systems.
 - In addition diversity may be required.
4. Control of accidents with core melt to limit off-site releases (postulated core melt accidents)
 - From I&C point of view many functions are rather simple both including passive features (no or little I&C), manual functions (relying on monitoring of status of the plant).
 - Safety classification varies.
 - DiD level 3 functions/systems play significant role at this level, too.
5. Mitigation of radiological consequences of significant releases of radioactive material
 - Includes alarming, monitoring and communication functions.
 - May be considered quite separate from the other systems.

3. International cooperation within PRA of digital I&C

3.1 OECD NEA CSNI WGRISK projects

OECD NEA CSNI WGRISK has organized research related to PRA modelling of digital I&C systems. The work started with identifying the current methods and information sources used for quantitative evaluation for digital I&C systems PRA of nuclear power plants (NPPs) [11].



The following Digital System Reliability Failure Mode Taxonomy (DIGREL) task group focused on developing a taxonomy of failure modes of digital components for PRA purposes [12]. Both hardware and software components were considered. However, the taxonomy focused on the reliability analysis of the reactor protection system. A new failure modes taxonomy based on five levels of abstraction was defined: 1) system level (complete reactor protection system), 2) division level, 3) I&C unit level, 4) I&C unit modules level, and 5) basic components level.

The scope of the following DIGMAP project included a benchmark study on PRA modelling of a digital reactor protection system [13]. In the study, the same RPS system was modelled by different project participants using the common system specification and reliability data. Similar results could be computed with different modelling approaches, e.g., a very detailed PRA model vs a simplified PRA with extensive background analyses.

The current DIGMORE project extends the reference case of DIGMAP to cover new modelling aspects, such as priority logic, back-up systems and spurious actuations. The DIGMORE will also consider the overall I&C architecture more broadly, since, e.g., operational I&C will be included in the model.

3.2 Nordic cooperation

In the Nordic nuclear safety research (NKS) project DIGREL (a parallel project to the WGRISK DIGREL task group), guidelines to analyse and model digital I&C systems in PRA were developed [5]. The project consisted of three subtasks: 1) development of a failure modes taxonomy within the WGRISK DIGREL task group [12], 2) development of a digital I&C PRA model for a fictive boiling water reactor [5], and 3) development of a method for the quantification of software reliability in PRA [14]. The research project focused on modelling and analysing digital RPS for PRA purposes.

The continuation NKS project Modelling of DIGital I&C (MODIG) focused on the assessment of DiD, diversity and complexity, analysis of spurious actuations, and on software failure data [10]. A literature review regarding the role of PRA in assessing the DiD framework was performed. Considering I&C the focus has been on DiD level 3 assessment, i.e. assessment of the RPS. In the MODIG project, also DiD level 2 safety functions were considered [15]. These are discussed more in Section 4.1.

4. I&C architecture PRA

4.1 PRA assessment of defence in depth

In [10], a survey on PRA's role in assessing the DiD framework was performed. The results of the survey indicated that the assessment of DiD and diversity is quite straightforward with PRA. Typically, PRA focuses on modelling DiD levels 3 and 4. DiD levels 1 and 2 are generally implicitly included in the initiating events analysis. A conclusion of the survey [10] is that a more detailed assessment of systems and function related to DiD levels 1 and 2 could provide valuable information both from plant safety and availability points of view.

The limitations identified in [10] regarding assessment of DiD level 2 in PRA are addressed in [15]. In [15], evaluation of preventive safety functions (DiD level 2 functions) using PRA is discussed. The DiD level 2 can be interesting since it can overlap with DiD levels 1 and 3 both functionally and with respect to system arrangements [15]. I&C is in the focus of the work. In the example case of [15], the DIGREL PRA model [5] is extended to demonstrate how DiD level 2 can be included into a PRA model. In the example, the limitation function of a reactor power control system is included in the transient event tree and an example FT for the limitation function is presented [15]. The modification of the event tree to include the DiD level 2 limitation function was minor. However, since levels 1 and 2 are typically implicitly covered by the



initiating event analysis [15], the corresponding initiating events need to account for the explicit modelling of the limitation function of DiD level 2.

On a general level DiD in PRA is considered in e.g. [16] and [17]. The use of PRA in evaluating the DiD is studied in [16]. The study proposes a new framework for DiD levels to support better PRA assessment of the levels. Especially, for PRA assessment of levels 1 and 2 the International Atomic Energy Agency (IAEA) definition of the DiD [18] provide only limited support [16].

In [17], the role of PRA in evaluating the DiD is considered. A conceptual framework and related processes for the assessment of a safety architecture (i.e. the measures that encompass the different levels of DiD) implementing DiD is proposed. The assessment process consists of four main steps of which the fourth step considers the evaluation of the physical performance and reliability of the levels of DiD. An additional step performs the PRA assessment of the safety architecture (and the corresponding DiD). As the framework for the integration of DiD concept and PRA the risk space (frequency/probability of occurrence, versus consequences) is used [17].

4.2 I&C common cause failure assessment

A state-of-the-art review on probabilistic modelling of CCFs in digital I&C systems is performed in [19]. Our aim is not to repeat the review but to complement it. Based on the review in [19] there is only a somewhat limited number of literature considering hardware and software CCFs in digital I&C systems. The main challenge seems to be the lack of data. There is a need for both data collection and method development activities [19].

Diversity and DiD are used in I&C system architectures for the protection against CCFs [20]. However, it can be challenging to uphold diversity and DiD in digital systems for both hardware and software.

The U.S. Nuclear Regulatory Commission's (NRC) position on diversity and DiD focusing on digital (software) applications was reviewed in [20]. The review considered PRA in a very limited matter. However, since PRA typically considers beyond design basis events, PRA could be used also for assessing digital CCFs in this context.

In a project under the Risk Informed Systems Analysis (RISA) Pathway that is part of the U.S. Department of Energy Light Water Reactor Sustainability Program the goal is to develop a risk assessment strategy for digital upgrades and designs (see e.g. [21, 22, 23, 24, 25]). The risk assessment framework for the digital I&C systems suggested for the strategy is shown in Figure 1.

The seven step process redundancy-guided systems-theoretic hazard analysis (RESHA) approach is used for the hazard analysis. In RESHA, fault tree analysis (FTA) and system-theoretic process analysis (STPA) [26] approaches are combined [25]. In addition, HAZCADS (hazards and consequence analysis for digital systems) [27] is used to support the construction of an integrated fault tree. The main outcomes of the hazard analysis are [28]; 1) the identification of CCFs and potential single points of failure in the digital I&C design, 2) an integrated FT containing both individual failures and CCFs of hardware and software, and 3) hazard preventive strategies.

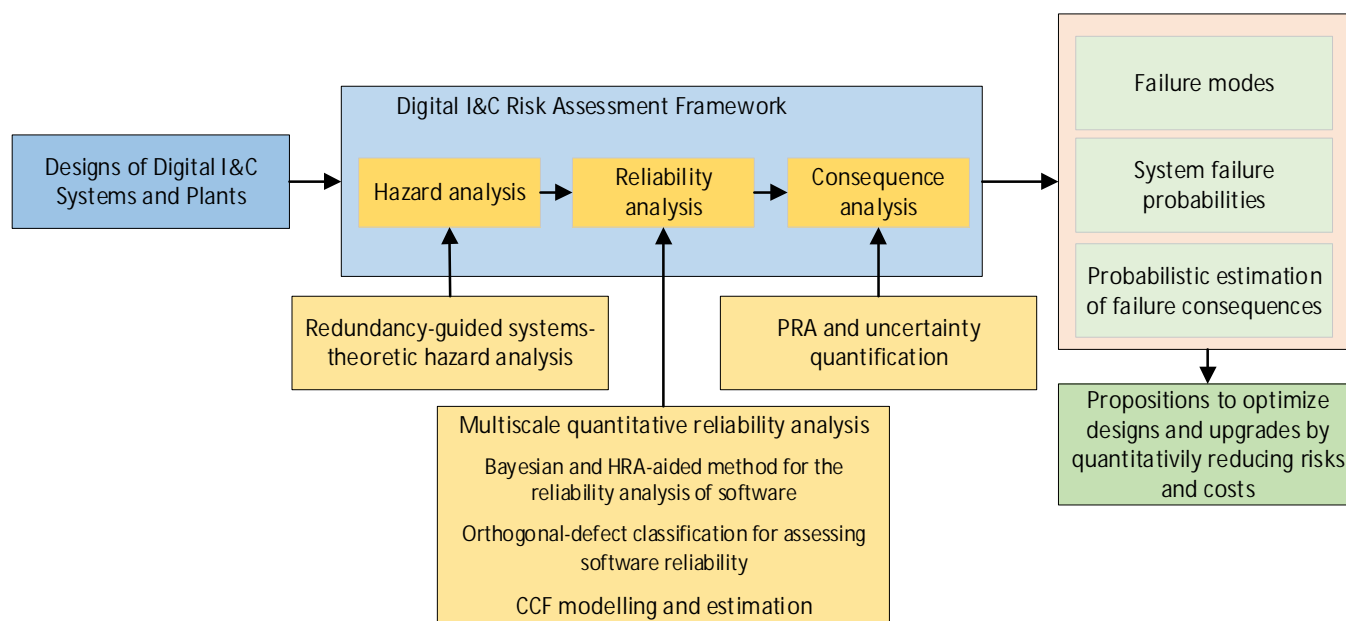


Figure 1. Risk assessment framework for high safety-significant safety-related digital I&C systems (modified from [25]).

During the reliability analysis phase either the Bayesian and HRA-aided method for the reliability analysis of software (BAHAMAS) [29] or the orthogonal-defect classification for assessing software reliability (ORCAS) approach can be used for quantifying software failure events. BAHAMAS is used when there is only a limited amount of data available, and ORCAS can be used when there is a sufficient amount of data available for detailed software reliability analysis. An approach was developed and employed for modelling and estimating both software and hardware CCFs (but especially for software CCFs). For modelling CCFs of redundant configurations a hybrid approach is used that utilises a standard and a modified beta-factor method [21]. Parameter estimation is performed by weighting different subfactors (e.g. redundancy, separation and safety culture) according to their importance based on expert judgement [28]. An approach for modelling CCFs of diverse configurations is presented in [21] and refined in [25]. When all the basic events of the integrated FT representing the entire digital I&C have been computed, it can be quantified using an FTA tool.

During the consequence analysis assessment of the impact of digital failures on plant overall risks is performed by assessing affected behaviours and responses [28]. The consequence analysis is based typically on the traditional PRA approach (i.e. event tree-fault tree approach).

In [30], risk informed methods are considered for the defence-in-depth and diversity (D3) analyses for assessing vulnerabilities to digital common cause failures. In the standard risk informed method, the existing PRA is modified to reflect digital upgrades. In the simplified risk-informed method, specific information from the existing PRA is used and combined (no need to update to PRA) and the information is conservatively treated to compute bounding estimates of potential change in key risk estimates.

In [31], the benefits of digital I&C on DiD and diversity (compared to analog I&C) were assessed from a risk perspective the focus being on software CCF. In the study, a full scope Level 1 (internal events) PRA for a typical pressurized water reactor was performed. A focus of the study was on postulated CCFs in the RTS and ESFAS [31].



4.3 PRA of I&C features affecting several DiD levels

The analysis approach for spurious actuations proposed in [10] follows the usual practice followed in PRA. Both single failures and CCFs need to be considered. In addition, both top-down and bottom-up approaches are needed. A top-down approach can be used for screening irrelevant system failures or I&C function failures. A bottom-up approach is then applied to the critical functions. Issues related to analysis of spurious actions are also identified in [10]. These issues include [10]: 1) how to identify possible common cause initiators comprehensively, 2) to what extent CCF causing a spurious actuation should be considered, 3) likelihood of a fire caused hot short, and 4) Spurious actuations caused by human errors of commission.

PRA modelling of spurious off (stop/close) signals for safety functions resulting from detected failures and of a priority unit is considered in [32]. The work was complementary to the DIGMAP project [13]. Spurious off signals were added to the DIGMAP model and their impact to the results were assessed. They were modelled in accordance with [5]. Considering the priority unit, a fault tree model of the unit was developed [32]. The input signals for the priority unit come from an RPS, back-up I&C system and operating I&C system. In the PRA model, only the RPS is modelled in detail. The back-up system and the operating I&C system are accounted for only in a simplified manner.

The common position of Multinational Design Evaluation Programme – Digital Instrumentation and Controls Working Group [33] gives assessment guidance to evaluate the sources of spurious actuations, the consequence of identified spurious actuations, and measures to prevent and respond to spurious actuations to maintain plant safety. The common position does not recommend any specific approach for the evaluation. The generic framework presented in [34] focuses especially on evaluating consequences associated with spurious actuation.

4.4 PRA of I&C systems in existing plant PRAs

4.4.1 PRA of NuScale small modular reactor I&C

The U.S. NRC has published sections of the NuScale small modular reactor Design Certification Application (DCA) online [35]. The only I&C system modelled in the PRA is the module protection system (includes both the RTS and ESFAS) [36]. In addition, the plant control system is credited in the single module model in the context of an initiating event. The I&C is modelled at the digital module level. I&C related behaviour that could have a negative impact on system operation or plant response have been modelled explicitly in the PRA. The PRA model includes basic events for actuation priority logic modules. Related to multi-module PRA the plant wide I&C systems are considered in the shared systems hazard analysis [36].

4.4.2 PRA of U.S. EPR I&C

The U.S. NRC has published sections of the US variant of the European Pressurized Water Reactor (U.S. EPR) Final Safety Analysis Report (FSAR) online [37]. The protection system (PS) is the most important I&C system to the PRA and, thus, it is the only I&C system that is modelled in detail (to the level of detail of the rack mounted TELEPERM XS (TXS) modules) [38]. I&C systems modelled at a lower level of detail include the safety automation system (SAS), process automation system (PAS), and the diverse actuation system (DAS). For the SAS and PAS conservative failure rates are used in the PRA. The models of PAS and SAS are combined with power supplies and sensor inputs that could be shared with the PS to account for dependencies. A beta factor is used to include DAS in the PRA model to account for potential software



CCF with the corresponding PS functions. For the PS, the PRA model includes two categories of software CCFs; CCFs of the operating system software and CCF of the application software [38].

4.4.3 PRA of APR-1400 I&C

The U.S. NRC has published sections of the Advanced Power Reactor 1400 (APR1400) Design Control Document [39]. In the PRA model, the plant protection system (PPS) (includes RTS and ESFAS) and the diverse actuation system (of which the diverse protection system (DPS) is the most relevant part) are included [40]. Operating system software and applications system software CCFs are assumed for both the PPS and DPS. However, software CCFs only affect the specific system, similarly to hardware CCFs. In addition, component interface modules (CIM) (performs signal prioritization) are considered in the PRA. A CIM is a hardware based device and, thus, it is not subject to software CCF. Each CIM is connected to one component and is included in the boundary of the component.

4.4.4 PRA of ESBWR I&C

The U.S. NRC has published sections of the Economic Simplified Boiling-Water Reactor (ESBWR) Design Control Document [41]. The RPS and the DPS are included in the PRA model [42].

4.4.5 PRA of OL3 I&C

The PRA of the Olkiluoto (OL3) I&C for the operating license is briefly addressed in [43]. The I&C modelling is based on the failure mode and effect analysis of the I&C systems. The I&C modelling is done at different phases and levels. The detailed fault tree (FT) models of I&C functions developed for reliability analysis for verifying unavailability targets functions as the basis for I&C modelling in PRA. At this phase, basic events are modelled at the hardware module level. In addition, software failure modes are considered in the model. For the actual I&C modelling in the PRA, so called super-components are used. Super-component FTs are used to create super-component basic events that represents the failure of I&C system units. These FTs are not directly linked to PRA model, but are used to compute the failure probability of the basic events in the PRA.

4.4.6 PRA of UK EPR I&C

For modelling the I&C in the UK EPR an approach referred to as the Compact Failure Model (CM) is used [44]. In the CM approach, a digital I&C system is divided into elementary I&C functions (channels) that are represented by specific fault trees in the PRA. The I&C functions are split into instrumentation, processing and actuator parts. In the processing part the processing functions of the PS, the SAS, the PAS, the Reactor Control Surveillance and Limitation System (RCSL) and the Severe Accident I&C (SA I&C) are considered. For example, CCFs are considered for systems based on the same platform (e.g., the RCSL, SA I&C and RPS are part of the TXS platform). The human machine interface and non-computerised safety system are modelled similarly to digital I&C systems.

4.5 Miscellaneous

A risk informed approach for probabilistic design and optimization of I&C architectures in research reactors is presented in [45]. In the approach, after an I&C architecture has been formulated it is converted into a reliability block diagram (RBD). The RBD is then transformed into a Bayesian network model that is used



for the reliability analysis. In parallel to the reliability analysis, the cost of the I&C architecture is estimated. Based on the reliability analysis and the cost estimates, different risk metrics are used to determine an optimized architecture. The approach should be applicable to I&C systems of different DiD levels. However the case study only considers the RPS [45].

For independent verification purposes of the Flamanville 3 plant PRA the Institute for Radiological Protection and Nuclear Safety (IRSN) has developed a limited scope PRA and [46] presents the preliminary I&C model part of the PRA. In the model, I&C failures are considered for the PS, SAS and MCS and MCP¹. For example, CCF between TXS and the TXP platforms are considered. Fault trees are used for the modelling.

An approach to evaluate quantitatively the importance of digital I&C system components involving complex interactions is described in [47]. Due to the complex interactions and the lack of availability of quantitative failure data for each component, analysing the importance with PRA can be challenging. In the proposed method a system model is built according to the systems-theoretic accident model and process, and weights are assigned to components based on design information and operation strategies (instead of quantitative failure data) [47]. The importance of each component is computed according to the effect of a single component failure on the overall I&C functions. In the case study related to a research reactor, the importance analysis was performed for the protections systems (RPS and alternate protection system) and monitoring systems (post-accident monitoring system, and information processing system) [47].

In [24], dynamic event trees (DET) are used to estimate failure likelihoods for digital I&C system reliability assessment. The study specifically focused on the effect of CCFs and software aging. Based on the two performed case studies, the DET approach represents reality better than traditional PRA methods. DETs can also be integrated into the traditional ET/FT analysis. In addition, [24] presents a method for evaluating the model agnostic reliability of ML models integrated in digital I&C systems.

5. Conclusions

PRA modelling of digital I&C systems has been studied for a long time in research projects. Some real-life applications have also been developed during the past decades. Traditionally, probabilistic risk assessment (PRA) has focused mainly on modelling DiD levels 3 and 4. From I&C perspective this means that mainly the reactor protection system (RPS) has been explicitly modelled. Therefore, the research has also focused on modelling the RPS in PRA.

Based on our review, the literature regarding PRA of the overall I&C architecture is rather scarce. A large part of the literature focuses on I&C common cause failure assessment. Some literature regarding PRA assessment of DiD levels (on a general level) can be found. Features of overall I&C architecture PRA have mainly been considered within Nordic co-operation and within SAFIR-projects. They have also been taken into account in real-life application. However, from these cases there is only a limited amount of information publicly available.

The current WGRISK task DIGMORE considers PRA of the I&C systems from a bit broader scope. The study includes modelling aspects, such as priority logic, back-up systems and spurious actuations. The goal of DIGMORE is to achieve an in-depth understanding of PRA relevant impacts of interactions within the entire I&C architecture.

¹ The meaning for MCP or MCS is not described in [46].

References

1. International Atomic Energy Agency (2018a), Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna.
2. International Atomic Energy Agency (2018b), Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants Nuclear Energy Series NP-T-2.1. https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1821_web.pdf
3. WENRA (2013), Safety of new NPP designs – Study by Reactor Harmonization Working Group RHWG, Technical Report, Western European Nuclear Regulators' Association. https://www.wenra.eu/sites/default/files/publications/rhwg_safety_of_new_npp_designs.pdf.
4. Holmberg, J.E., Bäckström, O., Porthin, M., Tyrväinen, T. (2016), Application of PRA for the assessment of defence-in-depth of a nuclear power plant, in: Walls L, Revie M, Bedford T, editors, Risk, Reliability and Safety: Innovating Theory and Practice. CRC Press, pp. 728–735. doi:10.1201/9781315374987-110.
5. Authen, S., Holmberg, J.E., Tyrväinen, T., Zamani, L. (2015), “Guidelines for reliability analysis of digital systems in PSA context - Final report”, NKS-330, Nordic nuclear safety research, Roskilde.
6. Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI) (2015), “Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis”, NEA/CSNI/R(2014)16, Paris, France.
7. Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI) (2022), “Digital I&C PSA – Comparative Application of Digital I&C Modelling Approaches for PSA, Volume 1: Main Report and Appendix A”, NEA/CSNI/R(2021)14, Paris, France. DRAFT.
8. Multinational Design Evaluation Programme, Common Position on Safety Design Principles and Supporting Information for the Overall I&C Architecture (2015). Tech. Rep. DICWG No. 9. OECD.
9. International Atomic Energy Agency (2011), Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants. IAEA Nuclear Energy Series NP-T-3.12. IAEA Vienna.
10. Authen, S., Bäckström, O., Holmberg, J.-E., Porthin, M. & Tyrväinen, T. (2016). Modelling of Digital I&C, MODIG— Interim report 2015. NKS-361, Nordic nuclear safety research (NKS), Roskilde.
11. Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI). (2009). “Recommendations on Assessing Digital System Reliability in Probabilistic Risk Assessments of Nuclear Power Plants,” NEA/CSNI/R(2009)18, Paris, France.
12. Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI). (2015). “Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis,” NEA/CSNI/R(2014)16, Paris, France.
13. Porthin, M., Shin, S.-M., Quatrain, R., Tyrväinen, T., Sedlak, J., Brinkman, H., Müller, C., Picca, P., Jaros, M., Natarajan, V., Piljugin, E., Demgné, J. (2023). International case study comparing PSA modeling approaches for nuclear digital I&C – OECD/NEA task DIGMAP, Nuclear Engineering and Technology, Vol. 55:12, pp. 4367-4381, ISSN 1738-5733, <https://doi.org/10.1016/j.net.2023.08.012>.

14. Bäckström, O., Holmberg, J.-E., Jockenhövel-Bartfeld, M., Porthin, M., Taurines, A., Tyrväinen, T. (2015). Software reliability analysis for PSA — Final report. NKS-341, Nordic nuclear safety research (NKS), Roskilde.
15. Holmberg, J.-E., Helminen, A., Porthin, M. (2017). Using PRA to assess defence-in-depth — case study on level 2 of defence-in-depth. Risk Pilot Report 14127_R002. Risk Pilot.
16. Hellström, P. (2015). DiD-PSA: Development of a Framework for Evaluation of the Defence-in-Depth with PSA. SSM Report 2015:04, Strålsäkerhetsmyndigheten, Stockholm.
17. Fiorini, G.-L., La Rovere, S. (2016). The PSA assessment of Defense in Depth Memorandum and proposals (IRSN-PSN-RES-SAG--2017-00020). France.
18. International Atomic Energy Agency Advisory Group. (1999). Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1, INSAG Series No. 12, IAEA, Vienna.
19. Tyrväinen, T. (2021). Probabilistic modelling of common cause failures in digital I&C systems - Literature review. VTT Technical Research Centre of Finland. VTT Research Report No. VTT-R-00728-21.
20. Muhlheim, M. D., Wood, R., (2016). Technical Basis for Evaluating Software-Related Common-Cause Failures. United States. ORNL/SR-2016/130. <https://doi.org/10.2172/1279406>.
21. Bao, H., Zhang, S., Youngblood, R., Shorthill, T., Pandit, Pr., Chen, E., Park, J., Ban, H., Diaconeasa, M., Lawrence, S. (2022). Risk Analysis of Various Design Architectures for High Safety-Significant Safety-Related Digital Instrumentation and Control Systems of Nuclear Power Plants During Accident Scenarios, Idaho National Laboratory, Idaho Falls, ID, INL/RPT-22-70056.
22. Bao, H., Shorthill, T., Chen, E., Park, J., Zhang, S., Jayakumar, A. V., Elks, C., Dinh, N., Ban, H., Zhang, H., Quinn, E., Lawrence, S. (2022). An Integrated Framework for Risk Assessment of High Safety-significant Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants: Methodology and Demonstration, Idaho National Laboratory, Idaho Falls, ID, INL/RPT-22-68656.
23. Bao, H., Shorthill, T., Chen, E., Zhang, H. (2021). Quantitative Risk Analysis of High Safety-significant Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants using IRADIC Technology. Idaho National Laboratory, Idaho Falls, ID, INL/EXT-21-64039.
24. Zhang, H., Bao, H., Shorthill, T., Quinn E. (2023). An Integrated Risk Assessment Process of Safety-Related Digital I&C Systems in Nuclear Power Plants. Nuclear Technology, Vol. 209:3, pp. 377-389, DOI: 10.1080/00295450.2022.2076486
25. Bao, H., Shorthill, T., Chen, E., Park, J., Kim, J., Turkmen, G.S., Ban, H., Dinh, N., Aldemir, T., Zhang, S., Lawrence, S. (2023). An Integrated Framework for Risk Assessment of Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants: Methodology Refinement and Exploration. Idaho National Laboratory, Idaho Falls, ID, INL/RPT-23-74412.
26. Leveson, N. G., Thomas, J. P. (2018). STPA Handbook. https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
27. Clark, A. J., Williams, A. D. (2019). HAZCADS - Hazard and Consequence Analysis for Digital Systems. United States. <https://www.osti.gov/servlets/purl/1643085>.

28. Bao, H., Zhang, H., Shorthill, T., Chen, E., Lawrence, S. (2023). Quantitative evaluation of common cause failures in high safety-significant safety-related digital instrumentation and control systems in nuclear power plants. *Reliability Engineering & System Safety*, Vol. 230, 108973, <https://doi.org/10.1016/j.ress.2022.108973>.
29. Shorthill, T., Bao, H., Zhang, H., Ban, H. (2021). A novel approach for software reliability analysis of digital instrumentation and control systems in nuclear power plants. *Annals of Nuclear Energy*, Vol. 158, 108260, ISSN 0306-4549, <https://doi.org/10.1016/j.anucene.2021.108260>.
30. EPRI. (2004). *Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades: Applying Risk-Informed and Deterministic Methods*,” NUREG-Series Publications 1002835. EPRI, Palo Alto, CA. URL: <https://www.nrc.gov/docs/ML0505/ML050540262.pdf>.
31. EPRI. (2009). *Effects of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants*. Technical Report 1019183.
32. Tyrväinen, T. (2022). *Probabilistic risk assessment studies for digital I&C: detected failures and priority unit*. VTT Technical Research Centre of Finland. VTT Research Report No. VTT-R-00940-22
33. *Multinational Design Evaluation Programme (2017), Common Position on spurious actuation*. DICWG No 13. OECD.
34. Ismael, L., Garcia, P.E. (2017). *Spurious Actuations in Digital Instrumentation and Control Systems - Evaluation Framework*. NPIC&HMIT 2017, paper 137. United States: American Nuclear Society - ANS.
35. NuScale SMR. (2022). *Design Certification Application – NuScale*. <https://www.nrc.gov/reactors/newreactors/smr/nuscale.html>.
36. *NuScale Standard Plant Design Certification Application. (2020). Chapter Nineteen Probabilistic Risk Assessment and Severe Accident Evaluation. Part 2 - Tier 2, Revision 5*. NuScale Power LLC.
37. Areva NP. (2013). *U.S. EPR Final Safety Analysis Report*. [Online]. Available:<https://www.nrc.gov/reactors/new-reactors/design-cert/epr/reports.html>
38. Areva NP. (2013). *AREVA Design Control Document Rev. 5 - Tier 2 Chapter 19 - Probabilistic Risk Assessment and Severe Accident Evaluation*. [Online]. <https://www.nrc.gov/docs/ML1326/ML13262A290.html>
39. *Korea Electric Power Corporation and Korea Hydro & Nuclear Power Co., Ltd. (2022). APR1400 Design Control Document and Environmental Report*. [Online]. <https://www.nrc.gov/reactors/new-reactors/large-lwr/design-cert/apr1400/dcd.html>
40. *Korea Electric Power Corporation and Korea Hydro & Nuclear Power Co., Ltd. (2018). APR1400 Design Control Document, Tier 2, Chapter 19 probabilistic risk assessment and severe accident evaluation. Revision 3. APR1400-K-X-FS-14002-NP*.
41. GE-Hitachi Nuclear Energy. (2022). *ESBWR Design Control Document*. [Online]. <https://www.nrc.gov/reactors/new-reactors/large-lwr/design-cert/esbwr.html>
42. GE-Hitachi Nuclear Energy (2014). *ESBWR Design Control Document, Tier 2, Chapter #19 probabilistic risk assessment and severe accidents. 26A6642BY. Revision 10*.



43. Kollasko, H., Dirksen, G., Grygoruk, R., Pesonen, J., Tunturivuori, L., Tarkiainen, A. (2018). Main Results and Conclusions of the OL3 Level 1 and Level 2 PSAs for the Operating License in Connection with the Fulfillment of the Regulatory Requirements. In *PSAM 14 - Probabilistic Safety Assessment and Management: Papers* [268] International Association for PSAM. https://iapsam.org/psam14/proceedings/paper/paper_268_1.pdf
44. Électricité de France / Areva NP (2012). UK EPR, PCSR Sub-chapter 15.1 — Level 1 PSA, Rep. UAEPR-0002-151, Issue 05, EDF/AREVA.
45. Khalil Ur, R., Heo, G. (2015). Risk Informed Design of I&C Architecture for Research Reactors. In *IEEE Transactions on Nuclear Science*, Vol. 62, no. 1, pp. 293-299, doi: 10.1109/TNS.2014.2375361.
46. Delache, J. (2012). I&C modelling in the IRSN EPR level 1 PSA (NEA-CSNI-R--2012-2). Nuclear Energy Agency of the OECD (NEA).
47. Shin, S.-M., Lee, S.H., Shin, S.K. (2022). A novel approach for quantitative importance analysis of safety DI&C systems in the nuclear field. *Reliability Engineering & System Safety*, Vol. 228, 108765, ISSN 0951-8320, <https://doi.org/10.1016/j.res.2022.108765>.

Certificate Of Completion

| | |
|--|----------------------------|
| Envelope Id: 37BA017600BC4A0F85E462123BAD1121 | Status: Completed |
| Subject: Complete with DocuSign: VTT-R-00677-23.pdf | |
| Source Envelope: | |
| Document Pages: 16 | Signatures: 1 |
| Certificate Pages: 1 | Initials: 0 |
| AutoNav: Enabled | Envelope Originator: |
| Envelopeld Stamping: Enabled | Christina Vähävaara |
| Time Zone: (UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius | Tekniikantie 21, Espoo |
| | .., . P.O Box1000, FI-0204 |
| | Christina.Vahavaara@vtt.fi |
| | IP Address: 130.188.40.73 |

Record Tracking

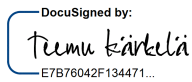
| | | |
|--------------------------|-----------------------------|--------------------|
| Status: Original | Holder: Christina Vähävaara | Location: DocuSign |
| 18 December 2023 08:31 | Christina.Vahavaara@vtt.fi | |

Signer Events

Teemu Kärkelä
teemu.karkela@vtt.fi
Research Team Leader

Teknologian tutkimuskeskus VTT Oy
Security Level: Email, Account Authentication (None), Authentication

Signature

DocuSigned by:

E7B76042F134471...

Signature Adoption: Pre-selected Style
Using IP Address: 130.188.17.16

Timestamp

Sent: 18 December 2023 | 08:32
Viewed: 18 December 2023 | 10:05
Signed: 18 December 2023 | 10:06

Authentication Details

SMS Auth:
Transaction: ab6e9d3b-4579-443d-9d68-a2de2716524e
Result: passed
Vendor ID: TeleSign
Type: SMSAuth
Performed: 18 December 2023 | 10:05
Phone: +358 40 7614199

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

| In Person Signer Events | Signature | Timestamp |
|-------------------------------------|------------------|--------------------------|
| Editor Delivery Events | Status | Timestamp |
| Agent Delivery Events | Status | Timestamp |
| Intermediary Delivery Events | Status | Timestamp |
| Certified Delivery Events | Status | Timestamp |
| Carbon Copy Events | Status | Timestamp |
| Witness Events | Signature | Timestamp |
| Notary Events | Signature | Timestamp |
| Envelope Summary Events | Status | Timestamps |
| Envelope Sent | Hashed/Encrypted | 18 December 2023 08:32 |
| Certified Delivered | Security Checked | 18 December 2023 10:05 |
| Signing Complete | Security Checked | 18 December 2023 10:06 |
| Completed | Security Checked | 18 December 2023 10:06 |
| Payment Events | Status | Timestamps |