Nuclear Engineering and Technology 55 (2023) 4367–4381

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

International case study comparing PSA modeling approaches for nuclear digital I&C – OECD/NEA task DIGMAP

Markus Porthin [a,*], Sung-Min Shin [b], Richard Quatrain [c], Tero Tyrväinen [d], Jiri Sedlak [e], Hans Brinkman [f], Christian Müller [g], Paolo Picca [h], Milan Jaros [e], Venkat Natarajan [f], Ewgenij Piljugin [g], Jeanne Demgné [c]

[a] Paul Scherrer Institut (PSI), Forschungsstrasse 111, 5232, Villigen PSI, Switzerland
[b] Korea Atomic Energy Research Institute (KAERI), KAERI, Daedeok-daero 989beon-gil, Yuseong-gu, Daejeon, Republic of Korea
[c] EDF R&D, EDF Lab Paris-Saclay, 7 boulevard Gaspard Monge, 91120, Palaiseau, France
[d] VTT Technical Research Centre of Finland Ltd (VTT), P.O. Box 1000, FI-02044, Espoo, Finland
[e] ÚJV Řež, a. s., Hlavní 130, Řež, Husinec, 250 68, Czech Republic
[f] NRG, Utrechtseweg 310, B50-West, 6800 ES, Arnhem, the Netherlands
[g] Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Forschungszentrum, Boltzmannstr. 14, 85748, Garching, Germany
[h] Office for Nuclear Regulation (ONR), Merton Road, Bootle, L20 7HS, United Kingdom

ARTICLE INFO

Keywords:
Digital I&C
Probabilistic safety assessment
Nuclear power plant
Case study
Reliability
Benchmarking

ABSTRACT

Nuclear power plants are increasingly being equipped with digital I&C systems. Although some probabilistic safety assessment (PSA) models for the digital I&C of nuclear power plants have been constructed, there is currently no specific internationally agreed guidance for their modeling. This paper presents an initiative by the OECD Nuclear Energy Agency called "Digital I&C PSA – Comparative application of DIGital I&C Modelling Approaches for PSA (DIGMAP)", which aimed to advance the field towards practical and defendable modeling principles. The task, carried out in 2017–2021, used a simplified description of a plant focusing on the digital I&C systems important to safety, for which the participating organizations independently developed their own PSA models. Through comparison of the PSA models, sensitivity analyses as well as observations throughout the whole activity, both qualitative and quantitative lessons were learned. These include insights on failure behavior of digital I&C systems, experience from models with different levels of abstraction, benefits from benchmarking as well as major contributors to the core damage frequency and those with minor effect. The study also highlighted the challenges with modeling of large common cause component groups and the difficulties associated with estimation of key software and common cause failure parameters.

1. Introduction

The instrumentation and control (I&C) systems represent key elements for the actuation of safety features in nuclear power plants. I&C components can be found in field instrumentation (e.g., sensors, actuators) as well as in processing units and human machine interfaces. Similarly to the trend in other industrial applications, the I&C in the nuclear sector is undergoing a significant shift towards digitalization. While several opportunities can be identified when using digital systems (e.g., new functionality, additional diagnostic, more user friendly interface), this brings also new challenges compared to relay based systems traditionally used in the nuclear industry.

The modeling of digital I&C systems in probabilistic safety assessment (PSA) represents an area where there is currently limited international consensus. On the one hand, the variety of failure modes of a digital I&C system makes its reliability modeling not straightforward. On the other hand, the rapid evolution of digital systems (e.g., new components or software updates) introduces also additional challenges compared to analog technology, where the operational experience provided a more robust basis for an estimation of key reliability parameters. Even if computerized I&C systems are generally reliable and

* Corresponding author.
E-mail addresses: markus.porthin@aalto.fi (M. Porthin), smshin@kaeri.re.kr (S.-M. Shin), richard.quatrain@edf.fr (R. Quatrain), tero.tyrvainen@vtt.fi (T. Tyrväinen), jiri.sedlak@ujv.cz (J. Sedlak), brinkman@nrg.eu (H. Brinkman), christian.mueller@grs.de (C. Müller), paolo.picca@onr.gov.uk (P. Picca), milan.jaros@ujv.cz (M. Jaros), natarajan@nrg.eu (V. Natarajan), ewgenij.piljugin@grs.de (E. Piljugin), jeanne.demgne@edf.fr (J. Demgné).

https://doi.org/10.1016/j.net.2023.08.012
Received 11 January 2023; Received in revised form 6 July 2023; Accepted 4 August 2023
Available online 7 August 2023

Abbreviations

A	automatic testing
ADS	automatic depressurization system
AI	analog input module
APU	acquisition and processing unit
AS	application software
CCCG	common cause component group;
CCF	common cause failure
CCW	component cooling water system
CDF	core damage frequency
CL	communication link
CSNI	Committee on the Safety of Nuclear Installations
DIGMAP	Digital I&C PSA – Comparative application of DIGital I&C Modelling Approaches for PSA
DO	digital output module
ECC	emergency core cooling system
EFW	emergency feed-water system
F	full-scope testing
FMEA	failure modes and effects analysis
FTT	fault tolerant technique
HVA	heating, ventilation and air conditioning system
HW	hardware
I&C	instrumentation and control
IAEA	International Atomic Energy Agency
IDN	intra-division network
LMFW	loss of main feed-water
MFW	main feed-water system
NEA	Nuclear Energy Agency
OECD	Organisation for Economic Co-operation and Development
OP	operating system/platform software
P	periodic testing
PM	processor module
PSA	probabilistic safety assessment
PTU	periodic test unit
RHR	residual heat removal system
RPS	reactor protection system
RPS-A	reactor protection system subsystem A
RPS-B	reactor protection system subsystem B
RS	reactor scram system
ry	reactor year
SR	sub-rack
SWS	service water system
VU	voting unit
WDT	watchdog timer
WGRISK	Working Group on Risk Assessment

offer widespread possibilities of diagnostics with features like fault tolerance and even self-healing, they are also strongly interconnected and their failure could cause a loss of several safety functions across the plant, e.g., due to common cause failures (CCF).

Since the early 1990s, practitioners have been facing the emerging challenge of incorporating the risk contribution of digital I&C in the PSAs in an adequate yet practical way. There is plenty of literature related to reliability modeling of digital I&C [1–4], both using traditional static methods, such as fault trees, and dynamic methods. Several references have also addressed PSA modeling of a digital reactor protection system (RPS) [5–18], which is the most relevant I&C system for nuclear power plant PSA. Most of the analyses presented in literature are simplified. Most comprehensively the topic has been studied in the NKS-330 report [19], which presents guidelines for performing failure modes and effects analysis (FMEA) for digital I&C, and an example PSA model, where a digital RPS has been modeled in detail. To our knowledge, there has not been any large-scale comparison of PSA modeling approaches for RPS prior to the one presented in this paper. While working groups on modeling digital I&C reliability are active, e.g., within the International Atomic Energy Agency (IAEA) and the Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA), it is generally recognized that a widely accepted industrial best practice is still missing in the nuclear sector, resulting in models prepared by different organizations being difficult to compare. Although a technical explanation of the differences is generally possible, this can typically undermine the confidence in the models.

This paper presents the results of a recent initiative by the OECD/NEA Committee on the Safety of Nuclear Installations (CSNI) Working Group on Risk Assessment (WGRISK) that strived to progress towards internationally agreed principles on modeling of digital I&C within the PSAs conducted for nuclear power plants. The task called “Digital I&C PSA – Comparative application of DIGital I&C Modelling Approaches for PSA (DIGMAP)” was carried out in the period 2017–2021 as a cooperation between eight organizations each representing different OECD member states. This task group followed on from previous NEA activities on digital I&C systems. In 2009, WGRISK completed an activity on methods and information sources for the quantification of the reliability of digital I&C systems in PSA for nuclear power plants [20]. In 2014, it completed the work on failure mode taxonomy for reliability assessment of digital I&C systems for PSA (DIGREL) [21]. DIGMAP’s ambition was to build from this work, focusing on the comparison of the reliability modeling practices in different countries. Six of the organizations developed independently their own PSA models based on the reference case description. A regulator was involved in the development of the case study, on the interpretation of the results and on the lessons learned process. Based on comparison of the models, the task group identified a set of insights on digital I&C modeling approaches, including main risk contributors, limitations of PSA modeling techniques when applied to digital I&C systems, and remaining challenges going forward.

The full documentation of the DIGMAP task can be found in the CSNI report [22,23] and summaries have been published in conference proceedings [24–26]. The motivation of this paper is to revisit the key learnings from the CSNI report along with some new insights from this activity, both from a technical and process perspective. The presentation of the work is partly restructured, highlighting the key aspects of interest for the scientific community. Chapter 2 discusses static and dynamic reliability models of digital I&C and motivates why the static PSA approach was chosen in this work. Chapter 3 presents the general process followed as part of this initiative. Chapter 4 presents the reference case used in the task and Chapter 5 summarizes the key features of the PSA models developed by the different organizations. Chapter 6 describes the approach for comparison of the different PSA models and Chapter 7 presents the results, including sensitivity analyses on key parameters and assumptions. Chapter 8 discusses the key lessons learned and insights from this comparison exercise, adding reflections on assumptions and modeling aspects not included in the CSNI report. Chapter 9 concludes the paper.

2. Static vs. dynamic modeling of digital I&C

The limitations of traditional static PSA methods, e.g., fault trees, in modeling digital I&C systems have been discussed in scientific literature [3,27–29]. These include the capability to model dynamic interactions between hardware and software, interactions between digital I&C and the plant processes and operator, time-dependent behavior, and multiple states of a component. Several dynamic methods have been proposed to overcome these limitations [3,28,30], e.g., dynamic flowgraph methodology [31], Markov/cell-to-cell mapping [32], and Petri nets

[33]. However, there have not been large-scale real-life applications of dynamic methods to digital I&C systems in the context of nuclear power plant PSA.

In this study, we have selected to apply conventional fault tree modeling techniques to a fictive RPS due to the following reasons. An objective of the study has been to compare PSA modeling approaches that have already been tested in real-life projects or could be applied in real-life projects without significant additional research efforts. While the authors acknowledge that dynamic methods could, in theory, enable more realistic modeling of digital I&C, dynamic methods are not seen as mature enough for large-scale real-life application. One difficulty in the PSA modeling of digital I&C is the lack of failure data. It is important to acknowledge that PSA model parameters related to digital I&C are inevitably very uncertain, and therefore, also the risk estimates are bound to be very uncertain. The use of dynamic methods would require even more uncertain parameters and assumptions. Despite of more realistic and detailed modeling, the risk estimates would anyway be very uncertain. Therefore, it can be questioned if it is worthwhile to perform detailed dynamic modeling when the uncertainties are bound to be large in any case due to lack of failure data. The authors believe that given the current failure data simplified static modeling is the most practical approach to perform PSA modeling of a digital RPS. Another benefit of the static approach is that the model can easily be integrated to the PSA model of the nuclear power plant.

There are also some aspects related to RPS failures that support the use of static methods. Failures are typically of on demand type, i.e., hardware components fail undetected before the initiating events and prevent a safety function actuation when a demand occurs, or a software fault prevents an actuation signal when it is demanded. The benefits of dynamic methods in modeling this type of failures are unclear. As stated in Ref. [34], after the actuation of safety functions, the feedback from the plant has no effect on the RPS meaning that there are no dynamic interactions. In Ref. [27], modeling of initiating events related to a digital feedwater control system was demonstrated with two dynamic methods. Indeed, dynamic methods can have more benefits in modeling control system failures.

In some studies [11,16,35], Markov methods have been applied to model state transitions related to failure modes, failure detection and component repairs. These approaches overcome simplifications made in static fault tree analysis. However, in some cases [11,16], exclusion of CCFs has been a major limitation, as CCFs tend to dominate PSA results. Son et al. [35] included also CCFs in their Markov model, but it remains unclear if the results would be different using the fault tree analysis. In the case where a single CCF event causes the system to fail, Markov modeling makes no difference compared to fault tree modeling, as long as the components participating in the CCF are assumed to fail simultaneously, which is a standard assumption in PSA. Therefore, Markov modeling of failure-detection-repair processes is expected to have only a marginal impact on overall results when CCFs dominate.

There are a few other references where dynamic methods have been applied to an RPS. Fahmy [13] applied a dynamic fault tree to a simplified RPS. The dynamic modeling focused on voting logic changes due to tests and maintenance. Compared to static fault tree modeling, the fault tree structures were simpler, whereas approximately same results were calculated using both approaches. Shouman et al. [18] have developed a hybrid machine learning model to analyze the reliability of an RPS, but the benefits compared to static fault tree analysis remain unclear.

3. Outline of the DIGMAP task

As stated in the introduction, the main objective of the DIGMAP task was to collect experience on digital I&C modeling from a case study. Representatives from different research organizations independently developed PSA models for a commonly agreed reference case constituting of a simplified representation of the main safety systems of a nuclear power plant. The reference case included a digitalized RPS, fictive reliability parameters and specification of the accident scenario to be modeled. Most of the work was carried out independently by the various participants, while face-to-face and online meetings were used for those activities requiring interaction between the participants. The main activities of the task were:

1. Definition of the reference case: At the beginning of the task, the reference target was selected. In this step the details of the reference case were defined, both in terms of accident scenario and system functionality. More specifically, discussions on exclusion, inclusion, and simplification of the system details were mainly carried out to focus on modeling digital features. Through such discussions within the task group, the first version of the reference case was prepared in the early stages of the task.
2. Convergence on a common interpretation of the reference case: This step was carried out in the initial phase of the modeling and in the initial comparison of the results. Clarifications on a number of points were required, including agreement on some general modeling assumptions, to ensure that the models of different participants were actually comparable and that there was a common understanding of the system to be modeled. Several iterations between steps 1 and 2 were needed, as the convergence on the interpretations resulted in additional clarity on the reference case definition.
3. Independent PSA modeling: This step required detailed PSA modeling by each actively involved organization. While there was some communication between participants in this step, the adopted approaches were set out independently, based on the experience and the best practice on digital I&C modeling in each organization.
4. Comparison of results and analysis of sensitivities: In this step, the results by each organization were interpreted and compared. This required in-depth analyses and some level of understanding of each model. In some cases, this also required to confirm the overall assumptions. Sensitivity analyses with regard to key parameters and assumptions were also conducted.
5. Consolidation of lessons learned: Main findings that have been confirmed through the overall work process and the comparison of various modeling approaches were formulated into two categories: qualitative and quantitative lessons learned.

The work process was not totally linear, but there were iterations especially between the reference case definition and its interpretation (steps 1 and 2) as well as refinements of them based on the comparison

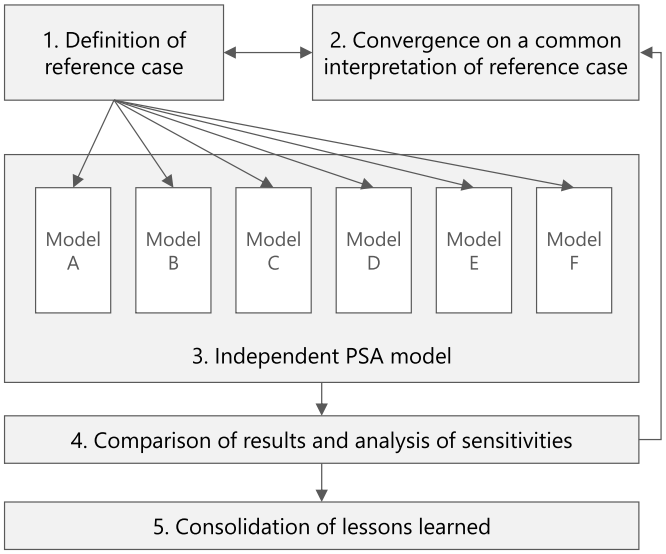

Fig. 1. Outline of the DIGMAP work.

of initial results (step 4), as illustrated in Fig. 1.

A part of the iterative process was due to the consolidation of assumptions in the interpretation of the reference case as part of the modeling. Interestingly, a similar process is often typical when developing a new PSA model for a new nuclear power plant or a refurbished digital I&C system, where PSA practitioners need to interface with I&C experts to understand the functionality of the I&C system in different operation modes or failure configurations.

An example of this process can be illustrated with the model calibrations that took place based on preliminary results. Because the main software failures (such as the malfunction of the operating system) would result in the overall failure of the protection system, the question of the weight of software failures in the results immediately arose, and the discussion allowed to converge towards illustrative failure probabilities, if not consensual. Later, the tentative results of the first model versions made it possible to reconsider the reliability parameters of the mechanical systems, to keep a balanced proportion between mechanical failures and I&C failures in the results. This was needed because the simplified front-line safety system consists of only a single channel while the digital I&C system consists of four divisions.

Another important feedback of the results on the modeling took place after the first comparison of global results. The choices different participants made to define the groups of redundant components for which they modeled CCFs caused an extreme variability of results. This variability could prevent learning from all other aspects of modeling; to avoid this, the participants agreed on a shared (conservative) definition of these common cause component groups (CCCGs). One of the assumptions causing largest variability in the results was whether or not to assume CCF between the two RPS subsystems. Both views having their merits, the modelers were encouraged to implement both variants, with the assumption of totally independent subsystems as a sensitivity analysis case.

4. Reference case

The reference case was developed focusing on digital I&C features based on a model developed in a Nordic research project [19,36]. For effective comparative analysis, some parts irrelevant to digital features such as the power supply system were excluded, and the analysis scope was limited to automatic safety signal generation by omitting spurious actuation and manual operation. The layout of the main safety systems is presented in Fig. 2. The systems consist of automatic depressurization system (ADS), component cooling water system (CCW), emergency core cooling system (ECC), emergency feed-water system (EFW), service

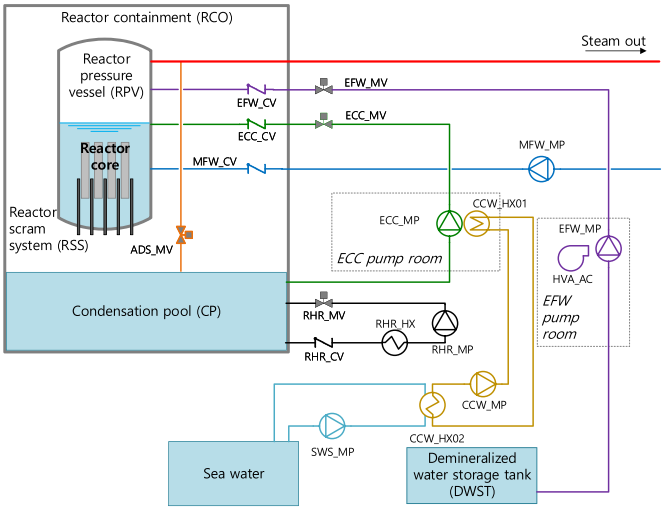

Fig. 2. Layout of main safety systems.

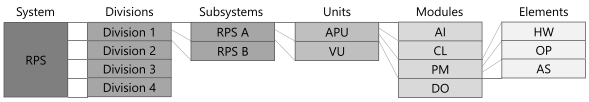

Fig. 3. Hierarchical structure of the RPS.

water system (SWS), heating, ventilation and air conditioning system (HVA), main feed-water system (MFW), residual heat removal system (RHR), and reactor scram system (RS), and each one is assumed to have only one train. Therefore, all components in a safety system should work properly in order for it to fulfil its function.

To activate each safety system, the corresponding safety signals should be generated by the RPS. The structure and layout of the RPS is given in Figs. 3 and 4, following the principles of [21]. The components of the RPS may be largely divided into parts for measuring, determining (generating) safety signals, transmitting generated safety signals, and parts supporting the aforementioned functions. Fig. 3 shows the hierarchical structure for the parts related to safety signal measurement, determination, and transmission; The RPS consists of four physically separated but functionally identical divisions (Divisions 1, 2, 3, and 4). Each division is subdivided into two subsystems (RPS-A and RPS-B) which are responsible for different functions, and each subsystem consists of an acquisition and processing unit (APU) and a voting unit (VU). The APU pre-determines the generation of a safety signal through comparison of the measured value with the setpoint, the VU performs voting logic based on inputs (pre-determined values) from all APUs of all divisions in the same subsystem. In the VU, the original 2-out-of-4 voting logic is degraded to 2-out-of-3 or 1-out-of-2 if there are one or two detected failures in the APUs, respectively. In addition, if three or more failures are detected the safety signal is generated.

In the more detailed level, APU and VU contain several modules. Both units have a processor module (PM) and a communication link (CL) module. Additionally, the APU has an analog input module (AI) for receiving sensing signals, and the VU has a digital output module (DO) for sending actuating signals. Each module consists of some of the following elements;

- Hardware board (HW)
- Operating system/Platform software (OP): for some modules, there is operating system providing the overall infrastructure for the safety functions in the specific application to work, or there is an embedded platform software that is different for each module type and non-alterable.
- Application software (AS): in the PM, AS implements the logics required by the safety functions.

The PM contains all the elements (HW, OP and AS) and the other modules (AI, CL and DO) contain hardware and OP. It is assumed that failures of two or more elements composing a module are independent of each other, and that a failure of an element leads to the failure of that module.

Other supporting parts in the RPS are as follows: Sub-rack (SR) provides power to each subsystem, and periodic test unit (PTU) and watchdog timer (WDT) are the components that perform fault tolerant functions, and intra-division network (IDN) is the medium for communication between PTU and subsystems.

The RPS is designed with three fault tolerant techniques (FTTs) providing means to detect hardware failures which are defined on failure rate basis: automatic testing (A) performed in real time (50 ms) by the AS in specific modules and the WDT (see the footnotes in Table 1), periodic testing (P) performed every 24 h by the AS of PM in the PTU by collecting information through the IDN communication, and full-scope testing (F) performed by human operators every six months (182.5 days). Although the exact mechanisms of each technique are not specified, it is assumed that some proportion of hardware failures in each

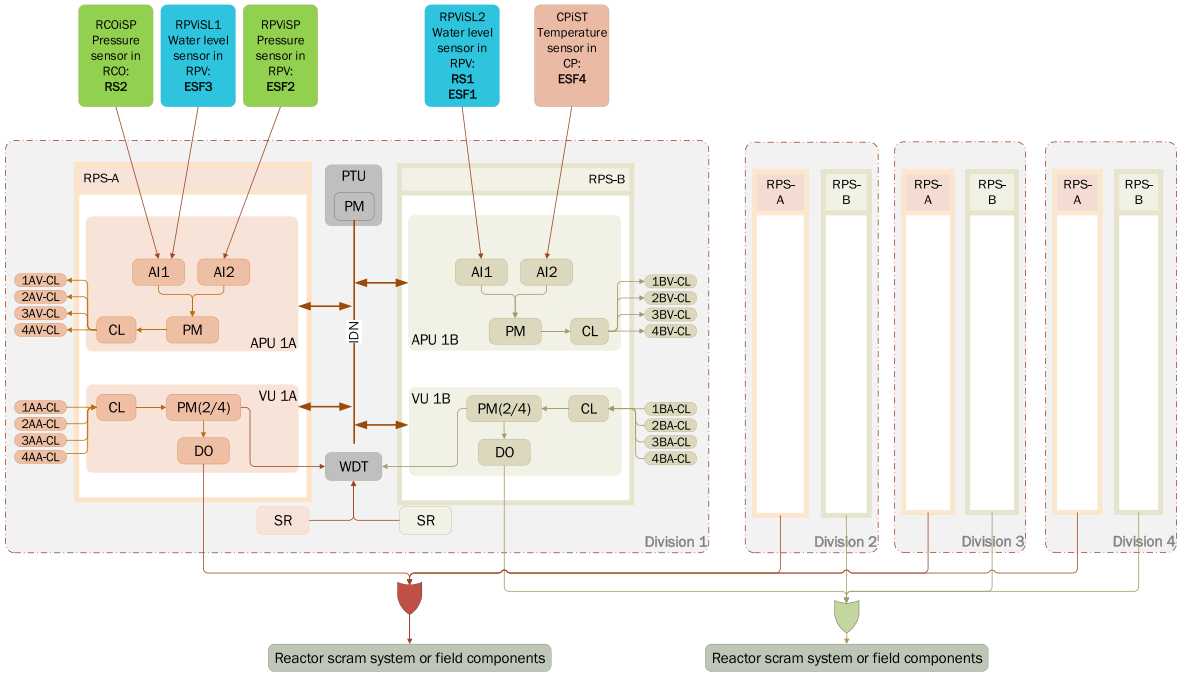

Fig. 4. Layout of the RPS

Table 1
Hardware failure rates of each module and proportion of detection coverage of FTTs.

			Proportion of detection coverage of each combination of FTTs			
Unit	Module	Failure rate (/hr)	$F\bar{A}\bar{P}$[a]	$FA\bar{P}$[b]	$F\bar{A}P$[c]	FAP[d]
APU	AI	2.0E-06	0.2	0.4[e]	0.2	0.2
	PM	2.0E-06	0.1	0.7[f]	0.1	0.1
	CL	5.0E-06	0.2	–	0.8	–
VU	DO	2.0E-06	0.2	–	0.8	–
	PM	2.0E-06	0.1	0.7[g]	0.1	0.1
	CL	5.0E-06	0.2	–	0.8	–
PTU	PM	2.0E-06	1	–	–	–
	IDN	1.0E-06	0.8	–	0.2	–
Other	SR	2.0E-06	–	0.9[g]	0.1	–

AI, analog input module; APU, acquisition and processing unit; AS, application software; CL, communication link; DO, digital output module; FTT, fault tolerant technique; IDN, intra-division network; PM, processor module; PTU, periodic test unit; SR, sub-rack; VU, voting unit; WDT, watchdog timer.

[a] Fault detectable by full-scope testing only.

[b] Fault detectable by full-scope testing and automatic testing.

[c] Fault detectable by full-scope testing and periodic testing.

[d] Fault detectable by full-scope testing, automatic testing, and periodic testing.

[e] Automatic testing for AI hardware in the APU is performed by the AS of the PM in APU (AS/PM/APU).

[f] Automatic testing for PM hardware in the APU is performed by the AS of the PM in VU. (AS/PM/VU).

[g] Automatic testing for PM hardware in the VU and SR hardware are performed by the WDT in each division.

module can be detected by each technique (see Fig. 5 and Table 1). The full-scope testing is assumed to detect any hardware failure. Fig. 5 clarifies the overlapping detection coverage of the FTTs which correspond to the notations in Table 1. Unlike the hardware failures, software (OP and AS) failure probabilities are defined on demand basis, and those failures are assumed to be undetectable by the FTTs.

The fictive failure rates assumed for the hardware failures are presented in Table 1. For OP failures and AS failures in the PMs, the failures on demand 1.0E-05 and 1.0E-04 were assumed, respectively. The

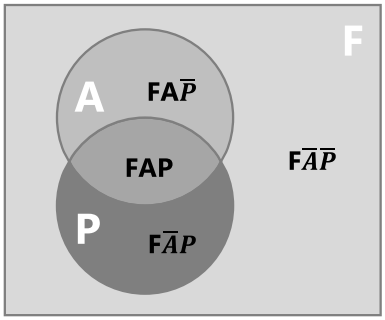

Fig. 5. Overlapping of fault tolerant techniques: (F) full-scope testing, (A) automatic testing, (P) periodic testing.

parameters were set to values regarded as reasonable by the participants and some of them were also adjusted to compensate for the simplified structure of the reference case. Recommended CCCGs were agreed upon. Hardware CCFs were encouraged to be modeled using alpha-factor models and software CCFs using beta-factor models and recommended parameters for both model types were also given.

In order to focus on the approach of digital I&C PSA model development itself, this study considered only one example initiating event: loss of main feed-water (LMFW). The event tree (Fig. 6) includes actuation of RS, EFW, ADS, ECC and RHR.

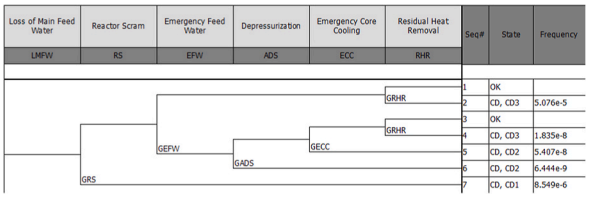

Fig. 6. Event tree for LMFW.

5. Reliability modeling

In this study, PSA models were developed based on the reference case by six organizations: EDF (France), GRS (Germany), KAERI (Republic of Korea), NRG (the Netherlands), UJV (Czech Republic) and VTT (Finland). This chapter gives an overview on the different modeling approaches used by the participants and the resulting model differences. The full model descriptions can be found in the task report [22,23]. Most of the organizations used RiskSpectrum as the main PSA modeling tool, while VTT and KAERI used the software FinPSA and AIMS-PSA, respectively. Some participants also used e.g., spreadsheets to perform supportive calculations.

Since the main focus of the task was on the modeling of the digital I&C, the models for the mechanical systems, covering e.g., valves and pumps, were commonly developed and shared between the participants so that only the models of the digital I&C would differ among the individual participants. Fault tree models were developed for RS, EFW, ADS, ECC, and RHR, corresponding to header names in the event tree (see Fig. 6). The model is simplified so that supporting systems (CCW, SWS, and HVA) do not have dedicated fault trees but are included in the main fault trees of the safety functions. A full description of the shared mechanical systems model can be found in the task report [23].

With regard to digital I&C modeling, the models produced by different organizations were quite different. For the comparison of the approaches, three modeling phases are distinguished:

- Pre-processing: This phase covers all the actions taken before the construction of the actual PSA model. Its purpose is to identify the input data and key design information needed for the development of the PSA model. This phase typically includes the development of FMEA, to characterize how the system can fail and its consequences. In some cases, it can require some background work, including the use of spreadsheets, stand-alone fault trees, or dynamic modeling (not considered in this work).
- PSA modeling: This phase covers the construction of the PSA model, typically requiring the development of event trees, fault trees and basic events with dedicated software tools. This phase also includes verification, validation and quantification of the model.
- Post-processing: This phase relates to sensitivity and uncertainty analysis and interpretation of the PSA results. Depending on the complexity of the model, detailed interpretation of the results can require some manipulation of minimal cut sets, either manually or using other software tools, e.g., to derive the risk contribution of the different elements of merged failure modes. Sensitivity analyses may also require modifications to the PSA model or background calculations.

Following this interpretation, the models developed as part of this activity can be categorized by the level of abstraction used in the modeling. In this context abstraction is defined based on the distance from the modeling of individual I&C failure modes. Three models with a low level of abstraction were prepared (KAERI, NRG, UJV), two models applied a medium level of abstraction (GRS, VTT), and one model used a high level of abstraction (EDF). Table 2 shows the main differences between the models developed by the six organizations. Among the differences, especially, the level of PSA model abstraction determines the overall process of the analysis. Depending on the analyst, if some specific characteristics of digital I&C are deemed difficult or inefficient to model in a fault tree format, the approach may be to perform a high level of PSA model abstraction instead of developing large and detailed fault tree structures. However, whatever approach is taken, valid and specific analysis results should be derived. A related discussion is made in Section 8.1.3. The different modeling approaches are discussed in the following subsections categorized by the level of abstraction.

Table 2
Summary of differences between PSA models developed.

	EDF	GRS	KAERI	NRG	UJV	VTT
Level of PSA model abstraction (Num. of basic events incl. CCF)	High (64)	Medium (460)	Low (2664)	Low (5546)	Low (5857)	Medium (72)
Detail of CCF	Abstract logic	Simplified logic	Full logic	Full logic	Full logic	Abstract logic
Consideration of voting logic	Yes	Yes	No	Yes	Yes	No
Inputs from Pre-processing	Test availability, hardware unavailability, CCF combinatory and aggregation, were calculated using separate spreadsheets.	Failure probabilities of merged basic events were calculated in separate FT models. FMEA was used for the determination of the relevant minimal cuts.	Testing interval of FTT was modified reflecting reliability of each FTT function.	None	None	Hardware failure probabilities were calculated using background FT models. CCF combinations and probabilities were calculated using separate spreadsheets.
Benefits	Simple PSA model, avoiding repetitive fault tree modeling work, customization of CCF calculations, basic results easy to interpret	Simple PSA model, avoiding repetitive fault tree modeling work, CCF calculations automated	Almost all the calculations in one model, CCF calculations automated, detailed results directly available, easy to perform sensitivity analyses	All the calculations in one model, CCF calculations automated, detailed results directly available, easy to perform sensitivity analyses	All the calculations in one model, CCF calculations automated, detailed results directly available, easy to perform sensitivity analyses	Simple PSA model, avoiding repetitive fault tree modeling work, quite detailed results directly available, customization of CCF calculations
Drawbacks	Extensive pre-processing and post-processing actions, sensitivity analyses not simple to perform, complex CCF analysis	Some pre-processing needed, extensive post-processing actions, sensitivity analyses not simple to perform, limitations in CCF modeling	Large and detailed fault tree structures, large number of minimal cut sets to interpret	Large and detailed fault tree structures, large number of minimal cut sets to interpret	Large and detailed fault tree structures, large number of minimal cut sets to interpret	Extensive pre-processing actions, some post-processing may be needed, some sensitivity analyses not simple to perform, complex CCF analysis

5.1. Low level of abstraction

When a low level of abstraction is used, almost all needed details are included in the PSA model. Separate basic events are used to model all the relevant failure modes of the RPS modules. FTTs are modeled explicitly. CCFs are fully developed, in general using the automatic CCF modeling features of the software used. The role of pre-processing and post-processing actions is limited, and the main work is related to the fault tree modeling. All sensitivity analyses can be performed by direct (or almost direct) modification of the PSA model parameters.

An interesting reflection from this comparison work is that, starting from the same assumptions and using a similar modeling philosophy (low level of abstraction) the resulting PSA models produced by KAERI, NRG and UJV are generally similar with a few minor differences, e.g.,:

- KAERI did not model active switching of the voting logic, because it was assessed insignificant for the results, whereas NRG and UJV did.
- In the modeling of FTTs, KAERI and NRG used separate basic events for failure detection coverage, whereas UJV took the detection coverages into account in the failure rates of relevant basic events representing failures.
- KAERI modeled the unavailability of testing equipment by adjusting testing intervals, whereas NRG and UJV modeled failures of testing equipment with separate basic events.
- NRG and UJV modeled the CCCG of 16 analog input modules using the automatic CCF generation feature of the RiskSpectrum code. KAERI merged module pairs to reduce the number of components in the CCCG into eight. This modeling issue is discussed in more detail in Chapters 7 and 8.

The fault trees of the PSA models with low level of abstraction include hundreds of basic events, and when CCF basic events are automatically generated, the minimal cut sets include thousands of basic events related to digital I&C itself. UJV has used this approach in the domestic nuclear power plant PSA models, keeping a level of detail relatively consistent with other systems. Nuclear power plants in the Czech Republic use extensively Living PSA and its applications in the regular decision making and the detailed PSA models help them to transparently address unavailability of individual components within the frame of e.g., risk monitoring or risk informed events evaluation and to present the results to the operational staff. A low level of abstraction was also found to be convenient from a version management point of view to have all data included in the PSA model itself.

5.2. Medium level of abstraction

When applying the medium level of abstraction, significant simplifications are made in the PSA model, such as merging of failure modes related to a specific module. Pre-processing involves considerable amount of work and some post-processing work is also typically needed. The PSA modeling part is significantly smaller compared to using the low level of abstraction, because the model includes a significantly smaller number of basic events and gates. There are different ways to apply the medium level of abstraction. The models by VTT and GRS differ considerably from each other as explained in the following.

In VTT's approach, hardware failure modes of a module are merged in the PSA model. The total unavailability of hardware in each module type is calculated in the pre-processing phase using a stand-alone fault tree. The FTTs are also modeled in these fault trees. Hardware CCF calculations are also performed in the pre-processing phase using spreadsheets. All CCF combinations, related to a specific module type, with the same impact are merged for the PSA model. The basic events of the PSA model represent CCFs between modules only, and independent failures are not modeled. Active switching of the voting logic is not modeled. The number of resulting minimal cut sets is significantly smaller than with the low level of abstraction, but still relatively detailed minimal cut sets are produced. The model of VTT includes only 72 basic events even when automatically generated CCFs are included. Post-processing of the results of the PSA model is needed if the risk contributions of individual hardware failure modes or FTTs are of interest. Hardware and FTT related sensitivity analyses require modification of the background models as well as of the PSA model.

In the GRS approach, failure modes related to each unit (acquisition unit, processing unit, voting unit or sub-rack) are merged including hardware and software in different modules of the unit. However, detected (self-signaling) and undetected (non-self-signaling) failures are treated separately. For detected and undetected failures, the total unavailability of each unit type is calculated in pre-processing using a stand-alone fault tree, where also FTTs are modeled. CCFs between units are modeled using the automatic CCF modeling feature of the PSA software tool. System level FMEA is used to determine relevant failure combinations concerning the active switching of the voting logic, and those failure combinations are then modeled in the PSA model with some simplifications. The fault trees of GRS's model include only dozens of basic events, and the minimal cut sets include hundreds of basic events when automatically generated CCFs are added. Post-processing of the results of the PSA model is needed to calculate risk contributions of individual modules, component types and failure modes. All sensitivity analyses require modification of the background model.

The GRS and VTT approaches were developed during this study and have not been applied elsewhere yet. Both approaches are actually combinations of different simplifications that could also be applied independently of each other. For example, the approach by GRS to use system level FMEA to model active switching of the voting logic could be combined with detailed modeling that corresponds to the low level of abstraction, or VTT's approach to merge hardware failure modes of a module could be applied without performing the CCF calculations in pre-processing.

5.3. High level of abstraction

When using the high level of abstraction, all failures with the same overall consequence are merged together in the PSA model. Most of the calculations are performed in pre-processing using spreadsheets, including the unavailability of each module type taking into account FTTs and CCF combinatory. The PSA model itself is very simple and includes a small number of basic events representing system level failure modes. Only CCFs are modeled. Hardware and software failures are included in the same basic event when they have the same impact. The model of EDF includes 64 basic events in total. Post-processing of the results of the PSA model is needed to calculate risk contributions of individual modules, component types and failure modes. All sensitivity analyses require modification of the background model.

EDF has used this compact modeling approach for a long time. The objectives are to avoid costly complexity in the PSA model with no significant added value, but also to stick to basic concepts clear for PSA analysts, to avoid an excessive number of minimal cut sets with specific I&C failure basic events, and to enable I&C modeling already in an early design stage. However, with the simple PSA model comes also higher effort in pre- and post-processing.

It can be noticed that the model of VTT is not much larger than the one of EDF. The model of VTT includes only eight more basic events. The main difference between the models is that the model of EDF focuses on system level failure modes, whereas the model of VTT includes separate basic events for different module types making the minimal cut sets more detailed. Based on the level of modeled failure modes, the level of abstraction of the VTT's model has been defined as medium, but concerning the model size, the difference to high level of abstraction is quite small. The main reason for the small size of VTT's model is that quantitatively negligible single failures and partial CCFs with no system level impact are omitted (i.e., only significant CCFs are modeled), and CCF combinations with same impacts are merged.

Table 3
Minimal cut sets of APU processor modules CCFs causing complete RPS loss (NRG).

MCS n°	pfd	BE1	BE2	BE3
21	1.51E-06	FTT_F_PM	XXA-PMHW_DET_FT-ALL	
41 to 48	3.54E-07	FTT_F_PM	XXA-PMHW_DET_FT-7AH	
	[…]	[…]		
	3.54E-07	FTT_F_PM	XXA-PMHW_DET_FT-7AF	
50 to 65	1.48E-07	FTT_F_PM	XXA-PMHW_DET_FT-6AS	
	[…]	[…]		
	1.48E-07	FTT_F_PM	XXA-PMHW_DET_FT-6AX	
69	3.92E-08	FTT_PF_PM	PT_SUCCESS	XXA-PMHW_DET_PT-ALL
sum	**6.75E-06**			

BE, basic event; MCS, minimal cut set; pfd, probability of failure on demand.

6. Comparison approach

To compare the results of the different models, the participants agreed to provide the overall core damage frequency (CDF) and the on-demand failure probabilities of the ADS signal (actuated by one non-redundant signal), RS signal (two redundant signals) and SWS signal (three redundant signals) as well as the first 100 minimal cut sets for all of these four events.

The description of the different approaches (see Chapter 5) shows that there is a real challenge in implementing this comparison. Different levels of detail of the models are not the only differences. Within the detailed models, different choices of simplification are made, e.g., whether to model failures of FTTs explicitly with basic events or by adjusting testing interval parameters. Intermediate level models implement also different strategies, aggregating in a preliminary evaluation each complete CCF with the partial CCFs having the same effects at the system level (VTT); or aggregating the hardware and software failures causing the loss of function of an APU or a VU in a division (GRS). EDF aggregates all the CCFs (hardware and software) according to their effects at the system level, with more abstract basic events than the other participants. It should also be noted that partial CCFs are, in most cases, automatically generated and coded according to calculation software conventions (especially with RiskSpectrum or AIMS-PSA), which requires careful interpretation.

However, some particularities facilitate the comparison. On the one hand, in a redundant system such as an RPS, the unreliability is mainly due to CCFs making a function unavailable on too many of the redundant modules. On the other hand, the failures detected online, the most common in a digital system, are in effect only for a relatively short time. Furthermore, FTTs reduce their effect on availability (reconfiguration of the voting logic) and direct, in the event of accumulation, the action of the RPS towards the least dangerous situation. This means that the average hardware unavailability is mainly due to undetected failures (i.e., failures detected only by the F test). In the end, undetected CCFs of identical modules, as well as CCFs of a software nature, can be expected to represent the main I&C loss scenarios.

Indeed, when analyzing the first 100 minimal cut sets of the various undesirable events considered for each of the detailed models, only CCFs of identical modules, and combinations with a partial CCF and an independent failure of a module of the same CCCG are found. In each combination, the failure and detection mode are the same for both events so that the minimal cut sets can be grouped based on the module and the failure/detection mode for the interpretation of the results.

CCFs on redundant modules sufficient to cause system level failure of a safety function are therefore the central pivot for a comparison. While some models (EDF, GRS) combine heterogeneous failure modes (even hardware and software) for model simplification purposes, it is more practical to focus on elementary CCFs of modules of the same nature (which is a main principle of VTT's method) to facilitate a detailed comparison of the results and identify the possible causes of differences. It is straightforward to interpret those elementary CCFs, and to characterize their effects on the RPS. This settles analysis, moreover, at the intermediate level of the models proposed: the basic events of EDF can easily be divided into groupings of these elementary CCFs, and these elementary CCFs can be used as a basis for grouping the detailed minimal cut sets that include different partial CCFs. Only the GRS model, which first aggregates heterogeneous failure modes within a division and then models their CCF, will require more "translation" effort.

Table 4
Minimal cut sets of APU processor modules CCFs causing complete RPS loss (KAERI).

MCS n°	pfd	BE1
21	1.51E-06	XXA-PMHW-12345678
52 to 59	3.55E-07	XXA-PMHW-1234678
	[…]	[…]
	3.55E-07	XXA-PMHW-1234567
99	1.49E-07	XXA-PMHW-123458
100	1.49E-07	XXA-PMHW-123456
sum	**4.65E-06**	

BE, basic event; MCS, minimal cut set; pfd, probability of failure on demand.

For example, if the macro failure of the CCFs of APU processor modules causing a complete failure of both subsystems RPS-A and RPS-B is considered, it will be represented in VTT's 100 first minimal cut sets for RS failure, by a single basic event (XXA-PMHW-AB) of probability 7.88E-06. This will be compared to the corresponding (and more detailed) minimal cut sets of NRG, KAERI and UJV. Results are shown for the two first ones in Table 3 and Table 4.

For EDF, CCFs of APU processor modules are only a contribution among others to the basic event of complete loss of the RPS. However, an intermediary calculation is precisely the estimate of the share allocated to the processor modules (equal to 7.08E-06). Finally, GRS also handles basic events grouping heterogeneous failure modes (but by division). The PM contribution is reconstituted by multiplying the basic unavailability of a processor module by a beta-factor, to obtain 1.84E-05.

From a practical point of view, it was possible to sort out the correspondences between the models only thanks to shared basic event naming conventions.

Table 5 is a summary table of the comparisons of the estimated probabilities of the CCFs leading to the RPS loss. Intermediate columns are added for EDF and GRS to allow comparison at the intermediate level. As VTT's method tries to evaluate exactly the aggregation of the elementary CCFs of modules of the same nature, their results are taken as a reference. Values that deviate from them by a factor 2 (and require then investigation) are highlighted in **bold** (high value) or underlined (low value) and will prompt a search for an explanation. For example, NRG's and UJV's results for CCFs of SRs are low, because some of the order 6 or 7 CCFs are beyond the first 100 minimal cut sets (and then ignored), while KAERI's same result is even 0, because none of the SR CCFs appear in the first 100 minimal cut sets.

In contrary, if going to a higher level of abstraction, the sum of the elementary CCFs of VTT leading to the loss of the RPS (2.37E-04) can be compared to the value of the RPS loss event of EDF (2.50E-04).

To complete the comparisons of results, other similar tables were

Table 5
Comparison of the estimated probabilities of the macro-failures leading to the RPS loss.

Macro-failure in both subsystems	EDF	*EDF interm.*	GRS	*GRS interm.*	KAERI	NRG	UJV	VTT
HW: 6oo16 CCFs of AI	2.50E-04	*2.64E-05*	3.79E-05	***3.75E-05***	1.61E-05	**3.29E-04**	**3.28E-04**	1.56E-05
HW: CCFs of 6oo8 APU/PM		*7.08E-06*	1.22E-04	***1.84E-05***	4.65E-06	6.75E-06	6.71E-06	7.88E-06
SW: CCFs of APU AS		*0*		***4.20E-06***	0	0	**5.00E-06**	0
HW: CCFs of 6oo8 APU/CL		*3.57E-05*		***9.76E-05***	3.40E-05	3.46E-05	3.42E-05	3.92E-05
SW: generic OP failure of AI, PM, CL modules in APUs		*3.00E-05*		*1.26E-06*	3.00E-05	2.80E-05	5.25E-06	3.00E-05
SW: generic OP failure of CL, PM, DO modules in VUs		*3.00E-05*	1.61E-04	*1.26E-06*	3.00E-05	2.70E-05	5.25E-06	3.00E-05
HW: CCFs of 8oo8 VU/CL		*8.02E-06*		***9.76E-05***	7.93E-06	8.41E-06	7.79E-06	8.81E-06
HW: CCFs of 8oo8 VU/DO		*3.21E-06*		***3.92E-05***	3.02E-06	3.32E-06	3.12E-06	3.53E-06
HW: CCFs of 8oo8 VU/PM		*1.58E-06*		***1.84E-05***	1.51E-06	1.68E-06	1.56E-06	1.74E-06
SW: CCFs of VU AS		*1..00E-04*		*4.20E-06*	1.00E-04	1.00E-04	5.00E-05	1.00E-04
HW: CCFs of 6oo8 SR		*3.57E-07*	3.75E-07	*3.75E-07*	0	1.57E-07	8.64E-08	3.92E-07

AI, analog input module; APU, acquisition and processing unit; AS, application software; CCF, common cause failure; CL, communication link; DO, digital output module; HW, hardware; OP, operating system/platform software; PM, processor module; SR, sub-rack; SW, software; VU, voting unit.

established: for the independent loss of a subsystem, for the failure of the AS triggering a signal or activating a mechanical system, and for redundant groups of four input cards or of four sensors.

This process allowed correction of anomalies in the models, e.g., related to unit interpretation in reliability data (/h instead of/d), test scheme parameter, preliminary high order CCF calculation and conservative grouping of failure modes. The remaining differences between the models are results of deliberate methodological choices, which are discussed in the following chapters.

7. Results

7.1. Main results

The main results of the six PSA models are presented in Table 6 and Fig. 7. In addition to the CDF per reactor year (ry), the failure probabilities of safety signals RS, ADS and SWS are presented. NRG's model has the highest CDF and failure probabilities. UJV's results are also significantly larger than the results of the other models. The reason why NRG's and UJV's results stand out is the very conservative modeling of CCFs of the analog input modules as will be discussed later. EDF, KAERI and VTT have quite similar results due to similar modeling assumptions, despite of different levels of abstraction used in the modeling. GRS's ADS failure probability is smaller than in the other models, while GRS's results are otherwise third largest. This is because GRS used quite different assumptions in modeling software failures compared to the others.

The main issue causing differences between the results of different models is the CCF modeling of 16 analog input modules. No PSA software tool offers the capability to manage all CCF combinations of an alpha-factor group of 16 components. Therefore, different workarounds were used in the models:

- NRG and UJV used RiskSpectrum's simplification where all CCF combinations with at least four components were combined into one basic event and treated as a full CCF. This approach appeared to be very conservative resulting in about ten times larger risk contribution of AI modules compared to the other models, because most CCF events with at least four components do not really cause complete system failure.
- EDF and VTT calculated all AI CCF combinations in a spreadsheet, grouped combinations with the same impact and summed the probabilities of relevant combinations to calculate probabilities for CCF basic events used in the model. This approach is otherwise accurate, except that it leaves out single failures and partial CCFs that would have an impact on the system only if multiple such events would occur.
- KAERI merged AI module pairs for CCF modeling so that the group of 16 components was reduced into a group of 8 components. The new alpha-factors were calculated based on the original alpha-factors so that the new alpha1 is alpha1+alpha2, the new alpha2 is alpha3-+alpha4, etc. This is not an exact solution, but it produced a result only slightly smaller than the results of EDF and VTT.
- GRS did not model the CCCG of 16 components, but two CCCGs of eight components. GRS applied the beta-factor model instead of the alpha-factor model.

Software failure modeling also caused differences in the results. The main differences were the following:

- The most popular option applied by EDF, GRS, KAERI, NRG and VTT was to use an additive approach to CCF probabilities meaning that the given AS failure probability was applied to each AS module and the given OP failure probability was applied to each OP module.
- UJV used a distributive approach were the given AS and OP failure probabilities were divided between different AS/OP modules, i.e., the given probability was interpreted as the total AS/OP probability covering all modules. This lowered UJV's results compared to the other models and explains the differences compared to NRG's results.
- Most participants applied a beta-factor of 1 (or close to 1) to software CCFs, but GRS applied significantly smaller beta-factors resulting in a very small risk contribution of software failures.

Fig. 8 presents the probabilities that the RPS is lost completely due to hardware, AS and OP failures respectively. NRG's and UJV's hardware contributions are large due to the conservative AI CCF modeling. UJV's AS and OP failure probabilities are smaller due to the different approach

Table 6
Core damage frequency and failure probabilities of the RS, ADS and SWS signals from each model.

		EDF	GRS	KAERI	NRG	UJV	VTT
CDF [1/ry]	LMFW	6.33E-05	6.68E-05	6.28E-05	7.78E-05	7.30E-05	6.32E-05
Signal generation failure probability [−]	RS	2.50E-04	3.21E-04	2.38E-04	5.40E-04	4.50E-04	2.37E-04
	ADS	5.27E-04	3.44E-04	4.77E-04	7.77E-04	6.30E-04	5.10E-04
	SWS	2.50E-04	2.83E-04	2.24E-04	5.40E-04	4.50E-04	2.37E-04

ADS, automatic depressurization system; CDF, core damage frequency; LMFW, loss of main feed-water; RS, reactor scram system; ry, reactor year; SWS, service water system.

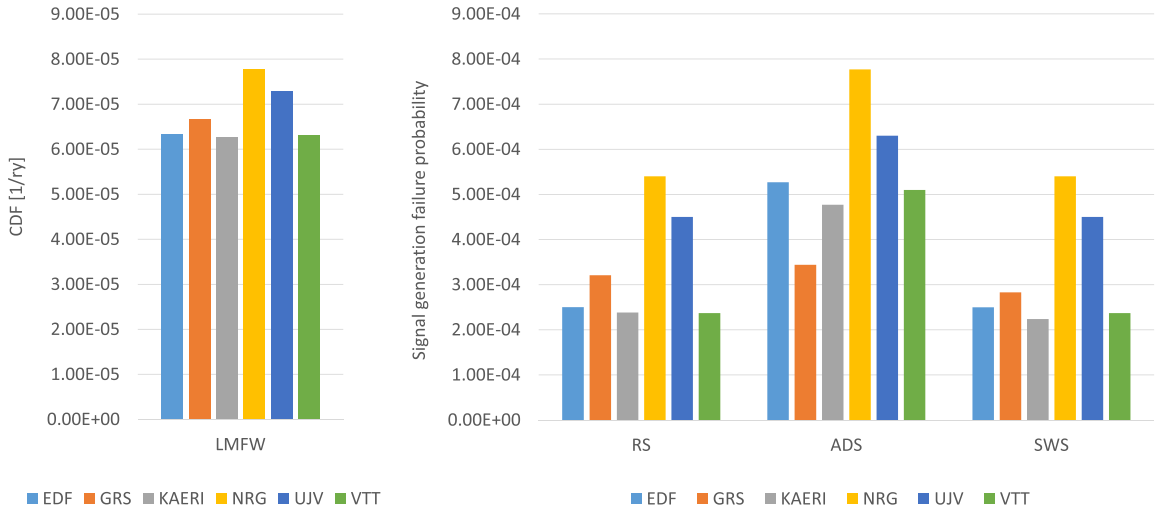

Fig. 7. Core damage frequency and failure probabilities of the RS, ADS and SWS signals from each model.

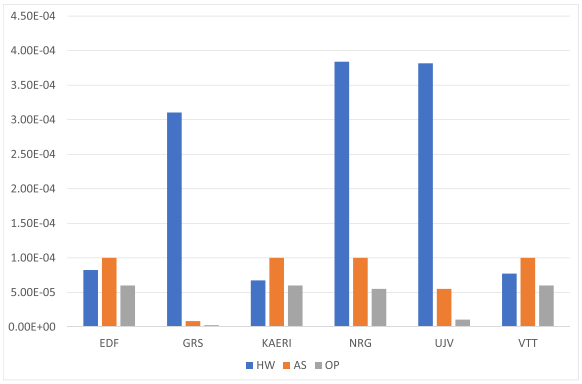

Fig. 8. Probability of complete loss of the RPS by hardware (HW), AS and OP failures.

in software modeling. GRS's AS and OP failure probabilities are very small due to the use of small beta-factors. On the other hand, GRS's hardware contribution is large due to the use of the beta-factor model. EDF's, KAERI's and VTT's failure probabilities are similar and quite balanced.

All the differences in the results can be explained by differences in the modeling assumptions, parameters and CCF modeling workarounds (a detailed comparison is found in the task report [22]). The selected levels of modeling detail or the overall modeling approaches did not cause any significant differences in the results. Even though the models of EDF and VTT were simplified so that single failures of digital I&C components were not modeled, their results were completely in line with the results of the detailed models, because CCFs totally dominated the digital I&C related risk. The modeling approach of GRS was an exception, because it is restricted to apply the same CCF model to hardware and software, and therefore, it would not be possible to produce the results of the other participants by that approach. However, if hardware and software were separated in GRS's unit level modeling, the approach could also produce approximately same results.

Active switching of the voting logic due to detected failures was modeled by four participants. It did not have any significant impact on the results, because such conditions last only a short time as detected failures were assumed to be repaired in 8 h. Therefore, it is not necessarily worthwhile to model logic switching. The need for such detailed modeling should be considered carefully because it is quite complex. In some applications, like risk monitor, the modeling might anyway be beneficial.

7.2. Sensitivity analyses

7.2.1. Software failures

The sensitivity of the results on variations in AS and OP failure probabilities was studied by each participant. The results for the CDF and the failure probability of the RS signal are presented in Fig. 9. In most models, software failures dominate the results when their probabilities are 1E-3 or larger. The previously discussed differences in the modeling of software failures also affect these results so that the sensitivity is the smallest in the model of GRS, and also UJV's results are below the results of others.

7.2.2. Fault tolerant techniques

To study the impact of failure detection coverages to the results, a set of sensitivity analysis cases was prepared. In order to simplify the analysis, the detection coverages of periodical testing were firstly set to 0 to create a test reference case. This means that failures that would be detected only by periodical (P) testing or full-scope testing were now assumed to be only detected by full-scope testing (hence notation "P => F"), and failures that would be detected by all testing alternatives were now assumed to be detected only by automatic testing or full-scope testing. Secondly, the detection coverages of automatic testing were varied for those modules subject to automatic testing to create sensitivity analysis cases. The detection coverages in different cases are presented in Table 7. It specifies for each parameter set (from A = 0 to A = 1) the proportion of failures detected both by full-scope testing and automatic testing (noted FA). The complementary proportion of failures, i.e., 1 – FA, are detected by full-scope testing only. Failures in the modules not subject to automatic testing (see Table 1) were assumed to be detectable by full-scope test only in all of the sensitivity cases.

The sensitivity analysis results for all models are presented in Fig. 10. In the models of UJV and NRG, a significantly larger sensitivity is observed, as the RPS has a much larger risk contribution in those models (around 50% for the CDF) than in other models (25% for the CDF). This is caused by the conservative AI CCF modeling. For other participants, the sensitivity is more or less at the same level, even if the GRS's results are at a higher level. It can also be observed that setting the detection coverage of periodical testing to 0 increases the CDF. Periodical testing actually has larger impact on the results than automatic testing, because the coverage of the periodical testing is larger; even in case A = 1, the

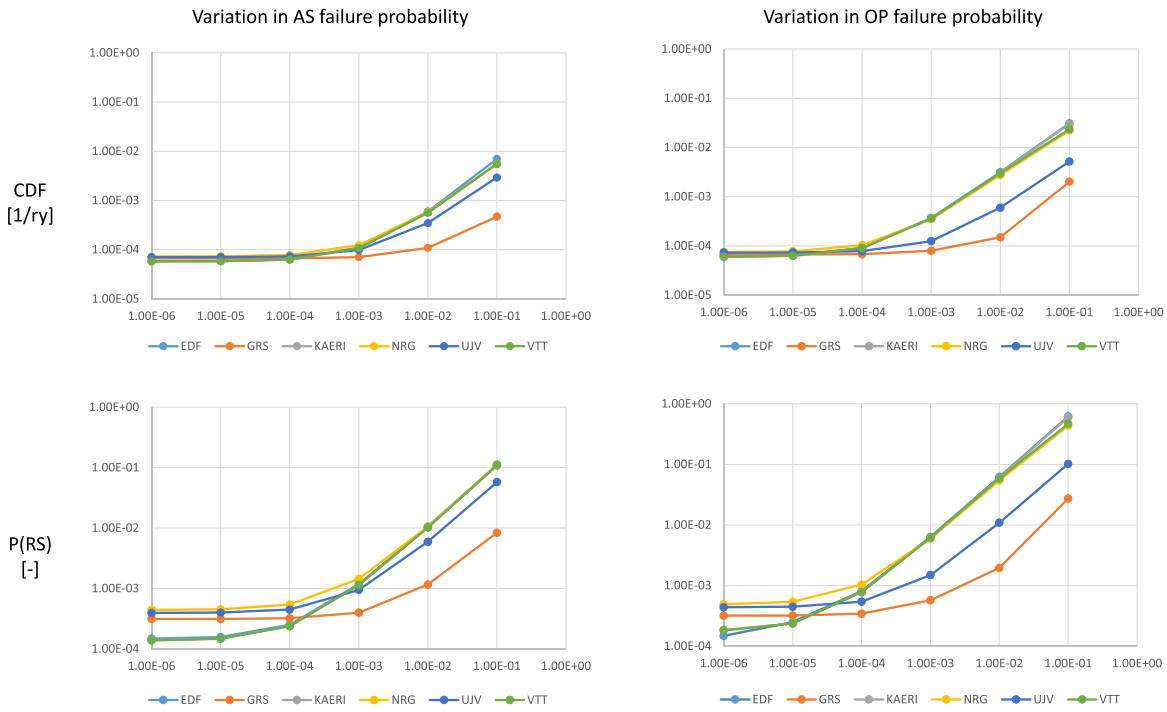

Fig. 9. Sensitivity of CDF and RS signal failure probability with regard to variation in AS and OP failure probability.

Table 7
Sensitivity cases for fault detection coverage.

	Parameter Set	A = 0	A–	A-	Test Reference Base (P => F)	A+	A++	A = 1
Unit	Module	FA: Proportion of failures detected by both F and A						
APU	AI	0	0.15	0.30	0.6	0.80	0.90	1
	PM	0	0.20	0.40	0.8	0.90	0.95	1
	SR	0	0.225	0.45	0.9	0.95	0.95	1

A, automatic testing; AI, analog input module; APU, acquisition and processing unit; F, full-scope testing; P, periodic testing; PM, processor module; SR, sub-rack.

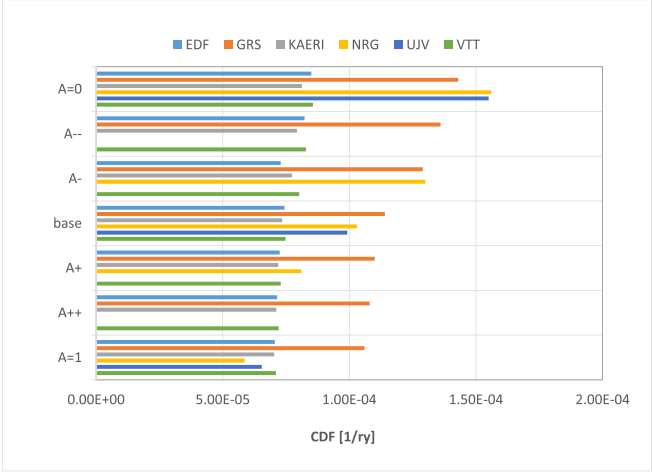

Fig. 10. Results of fault detection coverage sensitivity cases.

risk is higher than in the baseline model, because periodical testing was removed from the model. All in all, the results highlight the importance of good coverage of periodical and automatic testing, because the interval of full-scope testing is much longer. In the baseline model, the unavailability related to failures not detected by periodical and automatic testing dominates the risk contribution of hardware components.

7.2.3. *Diversity between subsystems*

In the baseline models, it was assumed that the subsystems (RPS-A and RPS-B) are identical, except that they implement different safety signals. Therefore, CCFs between the subsystems were modeled and they dominate the results. A sensitivity case was developed by revising this assumption so that the subsystems were assumed to be completely independent, with no possibility of CCFs between them. The results of this sensitivity case are presented in Table 8. The failure probabilities of the RS and SWS signals are reduced by three decades, when the possibility of CCFs between the subsystems is eliminated, and the contribution of the RPS to the CDF becomes very small. The failure probability of the ADS signal, on the other hand, does not change, because only one subsystem

Table 8
Results for the case with full diversity between subsystems.

		EDF	GRS	KAERI	NRG	UJV	VTT
CDF [1/ry]	LMFW	5.08E-05	5.08E-05	5.09E-05	5.09E-05	5.10E-05	5.08E-05
Signal generation failure probability [−]	RS	2.76E-07	1.64E-07	3.26E-07	3.40E-07	1.20E-07	2.53E-07
	ADS	5.25E-04	4.05E-04	5.06E-04	4.99E-04	3.50E-04	5.03E-04
	SWS	2.00E-07	1.55E-07	3.14E-07	3.28E-07	1.10E-07	2.42E-07

ADS, automatic depressurization system; CDF, core damage frequency; LMFW, loss of main feed-water; RS, reactor scram system; ry, reactor year; SWS, service water system.

is used to generate it.

8. Discussion

The main findings identified during the process of comparing various modeling options and evaluating the quantitative results of the reference case were summarized by the task group into a set of lessons learned:

- Qualitative lessons learned: These lessons capture the findings from the modeling exercise, i.e., they are related to the process required to reach a consensus on the interpretation of the system to be modeled and produce comparable results.
- Quantitative lessons learned: These lessons have been derived from the PSA quantification.

Whether or not the findings can be directly transferred and applied to other cases and problem settings needs to be verified on a case-by-case basis. However, in the opinion of the task group, the reference case reflects practice sufficiently to be an appropriate reference for comparison of alternative PSA modeling options.

In addition to these lessons, the selection of modeling and parameter assumptions in the work is reflected upon.

8.1. Qualitative lessons learned

This section presents main findings which were identified from the process of modeling the of reference case.

8.1.1. Interpretation of the digital I&C system

The modeling effort required by the task group members showed that the interpretation of how the digital I&C system behaves in different failure scenarios is not trivial. In fact, it requires understanding of various aspects of the digital I&C specification, the system design and operation including maintenance and testing regimes, which may not be documented in a format easily useable by a PSA practitioner. For example, while the design documentation is typically focused on how the system should work, the PSA specialist is generally more interested in understanding if and how its functionality could be affected by failures. Therefore, the task group considers close cooperation between digital I&C engineers and PSA experts to be required in order to model the digital I&C correctly and adequately in PSA. This cooperation can be beneficial both in terms of developing an accurate PSA model but also to inform digital I&C engineers how the reliability of the digital I&C systems could be improved.

8.1.2. Value of benchmarking

The comparison work within the task group highlighted the value of benchmarking between different models. In fact, the iterations needed to consolidate the assumptions in the reference case helped identifying problems and improvements to the PSA models. This is important particularly in case of digital I&C systems, because of their complexity and the multitude of the possible failure mechanisms of components, and the complex and highly redundant system architecture.

Therefore, the task group can recommend developing and comparing different PSA models at various phases of the design (e.g., digital I&C supplier model vs licensee model) and licensing (e.g., support model for regulator to inform discussions with the licensee). This could be delivered by means of an independent PSA modeling (even simplified), e.g., developed by an independent party as part of a PSA validation, by the regulator, or its technical support organization.

8.1.3. Level of modeling abstraction

The modeling approaches chosen by task group participants were different e.g., in terms of modeling details and number of basic events, as presented in Chapter 5. The various modeling approaches adopted in the task group highlighted the impact of different levels of abstraction and simplification in modeling.

The most important finding is that irrespective of the level of detail of the modeling, the results of the different models are essentially the same, provided the modeling is correct and the same set of assumptions are used. In other words, if the modeling is correct and fit for the purpose of the analysis, it is a matter of the preferences of the analyst whether to make model simplifications or not.

Another important finding is that the same level of understanding of the digital I&C system and its failure behavior is required for any level of modeling detail. At a low level of abstraction, this understanding is needed for the detailed explicit modeling of each failure mode of every component and software module in the digital I&C system. In a highly abstract model using detailed quantitative side analyses or previous experiences, the same level of understanding is needed to define the possible simplifications and translate these into a reliability model accounting for the key contributors.

The model simplifications can be made at different levels. This can save time in building and maintaining the model, at the cost of the level of detail of the results. The development of a simplified model can however require several iterations as it is not necessarily known beforehand what kind of simplifications can be made. When deciding on the abstraction level it needs to be carefully ensured that nothing important is left out. What is important depends to a large extent on the application of the PSA model.

The level of detail is not universal nor rigidly set. A pragmatic approach can be followed, by skipping details when they show to be negligible. It may also be useful to model some details in background analyses so that the PSA model itself does not become very complex.

In general, the following aspects play a role in choosing the level of modeling detail:

- PSA application: safety assessment, design evaluation, support of nuclear power plant operation, etc.: what is the required level of cut set information?
- Modeling effort (time and resources) required for detailed modeling versus expertise and skills needed in the construction of an abstract model (including R&D work).
- Possibility to re-use the structure of a compact model for several functions, to automatize the modeling, and to be flexible regarding the need for detailed modeling for specific applications of PSA.
- Ease of communication of results; detailed information vs. aggregated information.
- Level of detail of available data (depending on the maturity of the project, detailed failure data of I&C hardware and software components vs. global functional failure modes of I&C systems).
- Functional limitations of the PSA tool.
- Maintenance effort of the model (implementation of future system changes and upgrades).

8.2. Quantitative lessons learned

This section presents some insights gained from the quantification of the test case. It is worth noting that some of these findings cannot be generalized to other cases, although in the opinion of the task group this digital I&C system is a realistic enough representation of a typical system used in new nuclear power plants. Challenges related to quantification beyond this study are also discussed.

8.2.1. Common cause failures

The risk related to digital I&C was completely dominated by CCFs between redundant modules, particularly CCFs causing failures of both subsystems. This was not a surprise. The identification of CCCGs is a key issue in digital I&C PSA because digital I&C systems include typically many identical hardware and software components in redundant configurations, in different modules and in different subsystems. Different interpretations about the extent of independence and diversity to protect

against CCFs occurring within a single I&C subsystem or affecting multiple redundant subsystems (e.g., RPS and engineered safety features actuation system) can lead to very different results as demonstrated during the benchmarking process as well as by the sensitivity case assuming full diversity between subsystems.

The contributions of hardware and software varied among the models, but both were found important contributors in general. The CCF modeling of both hardware and software is, of course, an important issue, but also the failure probability of a single component is important as it affects the CCF probabilities when using a parametric CCF model.

8.2.2. Software failures

In this study, AS failures were more important than OP failures, but also OP failures had a significant risk contribution. Sensitivity analyses showed that either AS or OP failures could dominate the results if very large/conservative failure probabilities were used. On the other hand, if a beta-factor smaller than 1 can be justified for software CCFs, it can significantly decrease the risk contribution of software. When assessing software CCFs, it is important to consider two different CCF types: CCFs between redundant software modules processing identical signals/functions and CCFs between redundant software modules processing different, but (partly) redundant signals/functions. How to systematically reflect all these CCF conditions in the actual CCF parameters is challenging.

Estimation of software failure probabilities and CCF parameters is a challenge on which there is no consensus yet. Many of software reliability analysis methods can be found from literature [2,37,38], but most of the methods have not been developed for nuclear power plant PSA, and particularly lack consideration of CCFs. For nuclear power plant PSA, some methods and guidance have been developed [8,39–42], but international consensus has not been achieved yet. The data on software failures is very limited, though it has been possible to apply operating experience in some cases [43]. Typically, "standard values" or expert judgments are applied in PSA [44]. In some cases, even if there is a reliability estimate for software, it can be difficult to apportion it to AS and OP. It is therefore a good practice to perform sensitivity analyses for software failure probabilities.

8.2.3. Hardware failures

Failure rates for single hardware failures can be well estimated based on existing data, but there is little data for CCF parameters, particularly when the CCCGs are large. Options are to use generic CCF parameter values, like in this study, or apply engineering judgment -based methods [8,45]. Very large CCCGs (more than eight components) are not only a challenge for parameter estimation, but also for PSA modeling as the number of possible CCF combinations becomes too large to manage in minimal cut set computation. The alpha-factor model and other similar parametric models become impractical when the group sizes are large. The PSA analyst should be aware of PSA software tool limitations and carefully evaluate workarounds before applying them. A practical CCF model for large CCCGs would be needed, taking into account data collection challenges and that identical modules can be used for different purposes in digital I&C systems, i.e., not all CCF combinations with the same length have the same consequence. The modified beta-factor model proposed in Ref. [8] could be a solution to these challenges as it enables simple modeling of CCFs at different levels (e.g., within subsystem, between subsystems and between systems), but on the other hand, its treatment of CCF combinations is very simplified.

In line with earlier studies (e.g. Ref. [46]), the results show that hardware failure (and CCF) probabilities also depend significantly on failure detection coverages of FTTs. In this study, the contribution of the hardware resulted mostly from failures that cannot be detected by any other means than full-scope testing. The reason for this is that the full-scope testing interval of 4380 h is much longer than the testing intervals of automated tests and the repair time. This means that the portion of failures not covered by automated tests is particularly important. It makes a big difference if this uncovered portion is e.g., 1% or 10%.

8.2.4. Modeling issues with little importance

Active switching of the voting logic due to detected failures had practically no impact on the results. The main reason is that detected failures are repaired in a relatively short time, which was assumed to be 8 h, so that the alternative voting configurations are in effect only for a short time. In addition, the active switching of the voting logic was defined so that detected failures alone cannot cause the system to fail on demand, but undetected failures are also needed for that. The significance of detected failures and active switching of voting logic can, of course, depend on the parameters of the model. Furthermore, those could be more important in case of spurious actuations, which were not considered in this study, or in specific applications like risk monitors.

Failures of testing equipment had small risk contributions. The main reason is that failures of testing equipment alone do not have impact on the system, but also failures of the tested components are needed. The risk contributions of testing equipment are also dependent on model parameters, such as failure detection coverage.

8.3. Modeling and parameter assumptions

To be able to meaningfully compare the results, the participants agreed on a set of common modeling assumptions. However, the question on most appropriate assumptions remains open, and further discussion on these could be the subject of new work. Similarly, for the parameters, the set of values has been unified, but again many variations could be justified.

8.3.1. Qualitative modeling choices

Hardware CCCG definitions. Before agreeing on common CCCG definitions, the CCCG scopes varied significantly among DIGMAP participants. This demonstrated that there is a large underlying expert judgment in this regard. It concerns the distinction that can be made between the nature of a component (CCCG of all PMs) and their functional role (PMs in APUs distinguished from PMs in VUs), or even the strict identity of their function (PMs implementing the same signals). This can result in making strong and potentially excessive assumptions of independence. Conversely, a very cautious vision leads to practical problems (too large CCCG) and conservatisms that are difficult to quantify.

Software CCCG definitions. Because identical copies of OP software appear in redundant parts of a system, there might not be any problem in setting CCCGs. However, one can notice that there is never quite a consensus between the participants on how to define the CCCGs, and this is mainly due to the underlying level of granularity of analysis. At the OP level, the software can be considered globally, as a single entity that assumes the central function of managing all the other application programs, or at the firmware level of each type of component. This choice of level of detail has no consequences in principle but opens the way to significant differences in the interpretation of reliability data, e.g., it makes a significant difference whether the same OP failure probability value is applied at the OP level or at the firmware level of each component type.

For the AS, the collective choice, with one exception, was to group together in CCCGs only the exact copies for the APUs (thus separating subsystem A and subsystem B), but on the other hand all the instances of the two subsystems for VUs. The benefit of these simplifications has already been mentioned, but it can be seen that there is a deviation from reality (optimistic for APUs, and conservative for VUs). More fundamentally, a "block" view of the subsystems from the AS point of view prevents consideration of a software error that would affect a specific function, without damaging other functions implemented on the same processors. This block view is not fully realistic and prevents the claim for functional diversifications which would increase the robustness of the system.

8.3.2. Calibration of parameters

Hardware CCF parameters. The adoption of shared hardware CCF parameters was necessary to avoid too obvious differences in the results. This should not overshadow legitimate settings that may be discussed in a real project. The chosen parameters are essentially based on analog I&C operating experience. The values of the alpha parameters are a priori values supposed to be updated by the operating experience. Values for large orders are essentially constructed by a "mapping up" method, likely to be conservative.

These CCF assessments could also be put into perspective by taking into account precautionary design features or supposed operating conditions. For example, the evaluation of the CCFs of the analog acquisition modules (from the given alpha parameters) could be revised by expert judgment, when they are assigned different functions (acquisition of diverse measures), since it can be argued that generic failure modes (such as a sizing problem) do not apply uniformly. Similarly, from one subsystem to another, the application context of the PMs of the APUs could be considered sufficiently diversified to decrease the probability of a CCF that would affect both subsystems at the same time.

Software CCF parameters. As discussed before, the (relative) diversity between two AS could be represented. A relative probability of failure could be applied to AS based on different criteria (triggering AS in APU) or sending different orders (actuating AS in VU). A quantitative differentiation of the AS modules could also be considered, as for AS, the processing of the actuation of a system (once the signal is set to "true") could be judged safer than the triggering phase of the order: the first is indeed fully tested by periodic test, while the second is usually not exhaustively tested, because of the variability of the inputs.

Due to its unalterable and strictly copyable nature, there is a hesitation to consider the different instances of the same software in different divisions as distinct components, liable to fail at different times. Faced with the difficulty of characterizing the properties of the execution context that would explain differences in behavior from one instance to another, the most conservative choice (namely a full dependency) is difficult to challenge. There is however matter to discuss, for example, the partial independence of OPs between the two subsystems. The suggested value of $\beta = 1$, for the OPs, between the two subsystems, could be relaxed, because the application contexts are different (as different safety functions are implemented in each subsystem) and preventive features of diversification can be implemented (like a slight differentiation of the cycle durations between the two subsystems).

9. Conclusions

This paper summarizes the key findings from a comparative work within the OECD/NEA on digital I&C reliability modeling within the nuclear field. The approach with different organizations having independently developed their own PSA models of a simplified reference case representing a nuclear power plant with emphasis on digital I&C systems important to safety proved to be an efficient way of gaining more experience and insights on the topic.

Based on a comparison of the models and observations during the whole work process, both qualitative and quantitative lessons were learned. Various modeling approaches were categorized based on the level of abstraction of the actual PSA model, and it was concluded that similar results were obtained regardless of approach as long as the basic assumptions on the system were consistent. It was found that interpretation of the digital I&C system behavior in failure scenarios is far from trivial, in real-world cases requiring close cooperation between the PSA analyst and the I&C engineers and operation, and the benchmarking between models proved beneficial not only in comparing the modeling approaches but also in their quality assurance. From the quantitative point of view, the analysis showed which elements are dominating the results and which ones have only a minor effect. Not surprising, the definitions of CCCGs, i.e., assumptions on (in)dependencies between systems have a substantial effect on the results. This work will hopefully bring the field one step further on the path towards commonly agreed best practices in PSA modeling of digital I&C in the nuclear context.

During the work, a number of topics where further research and international cooperation would help gaining additional useful insight were identified. Following the positive response of the current activity, both within the group and from external reviewers, a follow-up task within the WGRISK was initiated in 2022 using a similar comparative approach but extending the scope towards even more realistic settings. The new task "A Realistic Comparative Application of Digital I&C Modelling Approaches for PSA (DIGMORE)" will focus on supporting the enhancement of the probabilistic assessment methodology by providing guidance for PSAs with respect to digital I&C systems. This will be achieved through an extension of the DIGMAP test case, considering additional interactions important to safety throughout the plant I&C architecture during the course of accident sequences (including, e.g., spurious actuations). It was also identified that international cooperation activities would be beneficial, with the aim to build consensus on a set of qualitative or quantitative considerations to be used for the estimation of central software and CCF parameters or to support the development of guidance, or guiding principles, for regulatory purpose regarding interpretation of the digital I&C system PSA results and integration of the analysis into the validation and verification process of the digital I&C. It was further found that the modeling of large CCCGs would benefit from methodology development to find practical and pragmatic solutions that can be implemented in PSA software tools.

Data availability

Full description of the reference case and PSA models can be found in Refs. [22,23].

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The work presented in this paper is part of the WGRISK programme of work supported by the OECD/NEA. EDF thanks IRSN for its invitation to participate in this work. National participations were particularly supported by The Finnish Research Programme on Nuclear Power Plant Safety 2015–2018 (SAFIR2018) and 2019–2022 (SAFIR2022), the National Research Foundation of South Korea Grant funded by the Korean Government (MSIT) (RS-2022-00144175), the Dutch research programme on nuclear energy and technology funded by the Ministry of Economic Affairs and Climate, the German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (Bundesministerium für Umweltschutz und Reaktorsicherheit, BMU), and the Technology Agency of the Czech Republic through the Competence Centre CANUT (Centre for Advanced Nuclear Technologies).

References

[1] Q.Z. Liang, Y. Guo, C.H. Peng, A review on the research status of reliability analysis of the digital instrument and control system in NPPs, in: IOP Conference Series: Earth and Environmental Science, Vol. 427, 2020. https://doi.org/10.1088/1755-1315/427/1/012018.

[2] T.-L. Chu, M. Yue, M. Martinez-Guridi, J. Lehner, Review of Quantitative Software Reliability Methods, Brookhaven National Lab, 2010. BNL-94047-2010, https://doi.org/10.2172/1013511.

[3] T. Aldemir, D.W. Miller, M.P. Stovsky, J. Kirschenbaum, P. Bucci, A.W. Fentiman, L.T. Mangan, Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, U.S. NRC, 2006. NUREG/CR-6901, https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6901/index.html.

[4] S. Authén, J.-E. Holmberg, Reliability analysis of digital systems in a probabilistic risk analysis for nuclear power plants, Nucl. Eng. Technol. 44 (2012) 471–482, https://doi.org/10.5516/NET.03.2012.707.
[5] S.J. Lee, W. Jung, J.-E. Yang, PSA model with consideration of the effect of fault-tolerant techniques in digital I&C systems, Ann. Nucl. Energy 87 (2016) 375–384, https://doi.org/10.1016/j.anucene.2015.07.039.
[6] Q. Liang, M. Liu, P. Xiao, Y. Guo, J. Xiao, C. Peng, Reliability assessment for a safety-related digital reactor protection system using event-tree/fault-tree (ET/FT) method, Sci. Technol. of Nucl. Install. 2020 (2020), 8839399, https://doi.org/10.1155/2020/8839399.
[7] S.H. Lee, H.E. Kim, K.S. Son, S.M. Shin, S.J. Lee, H.G. Kang, Reliability modeling of safety-critical network communication in a digitalized nuclear power plant, Reliab. Eng. Syst. Saf. 144 (2015) 285–295, https://doi.org/10.1016/j.ress.2015.07.029.
[8] H. Bao, S. Zhang, R. Youngblood, T. Shorthill, P. Pandit, E. Chen, J. Park, H. Ban, M. Diaconeasa, N. Dinh, S. Lawrence, Risk Analysis of Various Design Architectures for High Safety-Significant Safety-Related Digital Instrumentation and Control Systems of Nuclear Power Plants during Accident Scenarios, U.S. Department of Energy, 2022. INL/RPT-22-70056.
[9] J.H. Bickel, Risk implications of digital reactor protection system operating experience, Reliab. Eng. Syst. Saf. 93 (2008) 107–124, https://doi.org/10.1016/j.ress.2006.10.015.
[10] H.G. Kang, S.-C. Jang, A quantitative study on risk issues in safety feature control system design in digitalized nuclear power plant, J. Nucl. Sci. Technol. 45 (2008) 850–858, https://doi.org/10.1080/18811248.2008.9711486.
[11] A.S. Saber, M.K. Shaat, A. El-Sayed, H. Torkey, M.A. Shouman, Reliability analysis model of the digital reactor protection system, in: 2020 37th National Radio Science Conference (NRSC), Cairo, Egypt, 8-10 Sept, 2020, https://doi.org/10.1109/NRSC49500.2020.9235117.
[12] H. Torkey, A.S. Saber, M. Shaat, A. El-Sayed, M.A. Shouman, Bayesian belief-based model for reliability improvement of the digital reactor protection system, Nucl. Sci. Tech. 31 (2020), https://doi.org/10.1007/s41365-020-00814-6.
[13] R.A. Fahmy, Development of dynamic fault tree model for reactor protection system, Process Saf. Prog. 40 (2021), e12201, https://doi.org/10.1002/prs.12201.
[14] Z. Ma, H. Yoshikawa, M. Yang, Reliability model of the digital reactor protection system considering the repair time and common cause failure, J. Nucl. Sci. Technol. 54 (2017) 539–551, https://doi.org/10.1080/00223131.2017.1291375.
[15] J. Zhao, Y.-N. He, P.-F. Gu, W.-H. Chen, F. Gao, Reliability of digital reactor protection system based on extenics, SpringerPlus 5 (2016) 1953, https://doi.org/10.1186/s40064-016-3618-y.
[16] Y. Bulba, Y. Ponochovny, V.V. Sklyar, A. Ivasiuk, Classification and research of the reactor protection instrumentation and control system functional safety markov models in a normal operation mode, in: International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications, Kyiv, Ukraine, June 21-24, 2016.
[17] I. Ahmed, E. Zio, G. Heo, Risk-informed approach to the safety improvement of the reactor protection system of the AGN-201K research reactor, Nucl. Eng. Technol. 52 (2020) 764–775, https://doi.org/10.1016/j.net.2019.09.015.
[18] M.A. Shouman, A.S. Saber, M.K. Shaat, A. El-Sayed, H. Torkey, A hybrid machine learning model for reliability evaluation of the reactor protection system, Alex. Eng. J. 61 (2022) 6797–6809, https://doi.org/10.1016/j.aej.2021.12.026.
[19] S. Authén, J.-E. Holmberg, T. Tyrväinen, L. Zamani, Guidelines for Reliability Analysis of Digital Systems in PSA Context — Final Report, Nordic nuclear safety research, Roskilde, Denmark, 2015. NKS-330, https://www.nks.org/en/nks_reports/view_document.htm?id=111010212773211.
[20] NEA, Recommendations on Assessing Digital System Reliability in Probabilistic Risk Assessments of Nuclear Power Plants, OECD/NEA/CSNI, Paris, France, 2009. NEA/CSNI/R(2009)18, https://www.oecd-nea.org/jcms/pl_18874/recommendations-on-assessing-digital-system-reliability-in-probabilistic-risk-assessments-of-nuclear-power-plants.
[21] NEA, Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis, OECD/NEA/CSNI, Paris, France, 2015. NEA/CSNI/R(2014)16, https://www.oecd-nea.org/jcms/pl_19588/failure-modes-taxonomy-for-reliability-assessment-of-digital-instrumentation-and-control-systems-for-probabilistic-risk-analysis.
[22] NEA, Digital I&C PSA – Comparative Application of Digital I&C Modelling Approaches for PSA, Main Report and Appendix A, 2023. NEA/CSNI/R(2021)14. will be available at: www.oecd.org.
[23] NEA, Digital I&C PSA – Comparative Application of Digital I&C Modelling Approaches for PSA, Appendices B0-B6, 2023. NEA/CSNI/R(2021)14/ADD. will be available at: www.oecd.org.
[24] M. Porthin, S.M. Shin, T. Tyrväinen, C. Mueller, E. Piljugin, J. Stiller, R. Quatrain, L. Granseigne, H. Brinkman, P. Picca, J. Gordon, J. Sedlak, Comparative application of digital I&C modeling approaches for PSA, in: International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2019), Charleston, SC, April 28-May 3, 2019, in: https://www.ans.org/pubs/proceedings/article-45687/.
[25] S.M. Shin, M. Porthin, T. Tyrväinen, C. Mueller, E. Piljugin, J. Stiller, R. Quatrain, J. Demgné, H. Brinkman, V. Natarajan, P. Picca, J. Gordon, J. Sedlak, M. Jaros, An international joint research to explore the method for Digital I&C reliability assessment: OECD/NEA DIGMAP, in: Asian Symposium on Risk Assessment and Management (ASRAM 2019), Online, September 30-October 2, 2019.
[26] M. Porthin, S.-M. Shin, M. Jaros, J. Sedlak, P. Picca, R. Quatrain, J. Demgné, H. Brinkman, V. Natarajan, T. Tyrväinen, C. Müller, E. Piljugin, WGRISK DIGMAP: Comparison of PSA modeling approaches for digital I&C, in: 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021), Online, June 14–17, 2021. https://doi.org/10.13182/T124-35036.
[27] T. Aldemir, S. Guarro, J. Kirschenbaum, D. Mandelli, L.A. Mangan, P. Bucci, M. Yau, B. Johnson, C. Elks, E. Ekici, M.P. Stovsky, D.W. Miller, X. Sun, S.A. Arndt, Q. Nguyen, J. Dion, A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems, U.S. NRC, 2009. NUREG/CR-6985, https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6985/index.html.
[28] M. Tripathi, L.K. Singh, S. Singh, P. Singh, A comparative study on reliability analysis methods for safety critical systems using petri-nets and dynamic flowgraph methodology: a case study of nuclear power plant, IEEE Trans. Reliab. 71 (2022) 564–578, https://doi.org/10.1109/TR.2021.3109059.
[29] D.K. Shukla, A. John Arul, A review of recent dynamic reliability analysis methods and a proposal for a smart component methodology, in: Reliability, Safety and Hazard Assessment for Risk-Based Technologies, Singapore, 2020, https://doi.org/10.1007/978-981-13-9008-1_22.
[30] T. Aldemir, S. Guarro, D. Mandelli, J. Kirschenbaum, L.A. Mangan, P. Bucci, M. Yau, E. Ekici, D.W. Miller, X. Sun, S.A. Arndt, Probabilistic risk assessment modeling of digital instrumentation and control systems using two dynamic methodologies, Reliab. Eng. Syst. Saf. 95 (2010) 1011–1039, https://doi.org/10.1016/j.ress.2010.04.011.
[31] C.J. Garrett, S.B. Guarro, G.E. Apostolakis, The dynamic flowgraph methodology for assessing the dependability of embedded software systems, IEEE Trans. Syst. Man Cybern. 25 (1995) 824–840, https://doi.org/10.1109/21.376495.
[32] J. Yang, B. Zou, M. Yang, Bidirectional implementation of Markov/CCMT for dynamic reliability analysis with application to digital I&C systems, Reliab. Eng. Syst. Saf. 185 (2019) 278–290, https://doi.org/10.1016/j.ress.2018.12.024.
[33] R.B.N. Vital, P.F. Frutuoso e Melo, J.A.C.C. Medeiros, M.A.B. Alvarenga, Availability assessment of a nuclear reactor limitation system by a Timed Petri Net, Prog. Nucl. Energy 152 (2022), 104380, https://doi.org/10.1016/j.pnucene.2022.104380.
[34] T.-L. Chu, M. Yue, G. Martinez-Guridi, K. Mernick, J. Lehner, A. Kuritzky, Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods, U.S.NRC, 2009. NUREG/CR-6997, https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6997/index.html.
[35] K.S. Son, S.H. Seong, H.G. Kang, G.S. Jang, Development of state-based integrated dependability model of RPS in NPPs considering CCF and periodic testing effects at the early design phase, Reliab. Eng. Syst. Saf. 193 (2020), 106645, https://doi.org/10.1016/j.ress.2019.106645.
[36] J.-E. Holmberg, DIGREL Example PSA Model Description, Risk Pilot, Stockholm, Sweden, 2016. Report 14127_R001.
[37] Y. Cai, Y. Wu, J. Zhou, M. Liu, Q. Zhang, Quantitative software reliability assessment methodology based on Bayesian belief networks and statistical testing for safety-critical software, Ann. Nucl. Energy 145 (2020), 107593, https://doi.org/10.1016/j.anucene.2020.107593.
[38] J. Seo, H.G. Kang, E.-C. Lee, S.J. Lee, Experimental approach to evaluate software reliability in hardware-software integrated environment, Nucl. Eng. Technol. 52 (2020) 1462–1470, https://doi.org/10.1016/j.net.2020.01.004.
[39] S. Authén, O. Bäckström, J.-E. Holmberg, M. Porthin, T. Tyrväinen, Modelling of DIgital I&C, MODIG — interim report 2015, Nordic Nuclear Safety Research, Roskilde, Denmark, 2016. NKS-361, https://www.nks.org/en/nks_reports/view_document.htm?id=111010213493819.
[40] EPRI, Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments, 2012, 1025278. Palo Alto, CA, USA, https://www.epri.com/research/products/1025278.
[41] M. Jockenhövel-Barttfeld, O. Bäckström, J.-E. Holmberg, M. Porthin, A. Taurines, T. Tyrväinen, Modelling software failures of digital I&C in probabilistic safety analyses, ATW - Int. J. Nucl. Power 60 (2015) 151–158. https://www.kernd.de/kernd-en/fachzeitschrift-atw/hefte-themen/2015/03_mar.php.
[42] H.G. Kang, S.H. Lee, S.J. Lee, T.-L. Chu, A. Varuttamaseni, M. Yue, S. Yang, H. S. Eom, J. Cho, M. Li, Development of a Bayesian belief network model for software reliability quantification of digital protection systems in nuclear power plants, Ann. Nucl. Energy 120 (2018) 62–73, https://doi.org/10.1016/j.anucene.2018.04.045.
[43] AREVA, AREVA Design Control Document Rev. 5 - Tier 2 Chapter 19 - Probabilistic Risk Assessment and Severe Accident Evaluation, U.S.NRC, 2013. ML13262A290, https://www.nrc.gov/docs/ML1326/ML13262A290.html.
[44] O. Bäckström, J.-E. Holmberg, M. Jockenhövel-Barttfeld, M. Porthin, A. Taurines, T. Tyrväinen, Software Reliability Analysis for PSA: Failure Mode and Data Analysis, Nordic Nuclear Safety Research, Roskilde, Denmark, 2015. NKS-341, https://www.nks.org/en/nks_reports/view_document.htm?id=111010213008953.
[45] IEC, Functional Safety of Electrical/electronic/programmable Electronic Safety-Related Systems - Part 6: Guidelines on the Application of IEC 61508-2 and IEC 61508-3, IEC 61508-6, 2010. https://webstore.iec.ch/publication/5520.
[46] M.C. Kim, J. Seo, W. Jung, J.G. Choi, H.G. Kang, S.J. Lee, Evaluation of effectiveness of fault-tolerant techniques in a digital instrumentation and control system with a fault injection experiment, Nucl. Eng. Technol. 51 (2019) 692–701, https://doi.org/10.1016/j.net.2018.11.012.