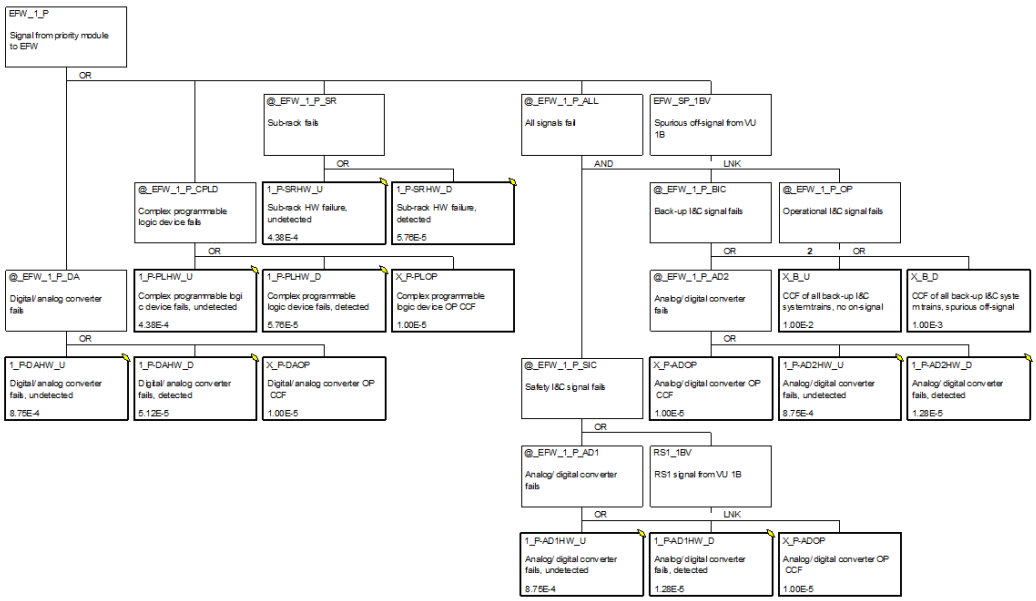
RESEARCH REPORT

VTT-R-00940-22



Probabilistic risk assessment studies for digital I&C: detected failures and priority unit

Authors: Tero Tyrväinen

Confidentiality: VTT Public

VTT

beyond the obvious

Report's title	
Probabilistic risk assessment studies for digital I&C: detected failures and priority unit	
Customer, contact person, address VYR	**Order reference** SAFIR 3/2022
Project name New developments and applications of PRA	**Project number/Short name** 131764/NAPRA
Author(s) Tero Tyrväinen	**Pages** 21/4
Keywords Probabilistic risk assessment, digital I&C, priority unit, spurious signal	**Report identification code** VTT-R-00940-22

Summary

In this report, probabilistic risk assessment (PRA) modelling studies of digital I&C are conducted as complementary to the OECD/NEA WGRISK's DIGMAP project. One goal is also to prepare for the PRA modelling work in the WGRISK's DIGMORE project, which has recently started. In this report, first, the risk contribution of detected failures causing spurious off-signals are studied by extending the PRA model of a fictive reactor protection system (RPS) developed in the DIGMAP project. Second, a fault tree model is developed for a fictive priority unit, which is also connected to the DIGMAP model.

Detected hardware failures causing spurious off-signals for safety functions are added to the DIGMAP model, as they were not included in the original study, whereas they had been found important in the previous DIGREL study. In this case, the detected hardware failures have significance only with regard to spurious off-signals causing initiating event, whereas they have little importance with regard to safety function failures. The importance of detected failures with regard to digital I&C related risk is sensitive to detection coverage parameters and fail-safe behaviour. Also, the diversity (or lack of diversity) between subsystems has significance for this matter.

A fault tree model is developed for a priority unit based on some early design ideas from the DIGMORE project. The priority unit gets its input signals from an RPS, back-up I&C system and operating I&C system. The most important contributors to the analysed safety function failure are specific failures in the priority units, but also spurious off-signals caused by detected hardware and software failures in the RPS are important. Other contributors are almost negligible. Detected RPS failures dominate over undetected failures in this case, because the detected failures can alone cause the safety function failure through the spurious off-signals, whereas undetected RPS failures only "pass the control" to the back-up I&C. However, this depends on the definition of the voting logic and the priorities of signals.

Confidentiality	VTT Public

Espoo 13.12.2022

Written by	**Reviewed by**
Tero Tyrväinen, Research scientist	Kim Björkman, Research scientist

VTT's contact address
VTT Technical Research Centre of Finland Ltd, P.O. Box 1000, FI-02044 VTT, FINLAND

Distribution (customer and VTT)

SAFIR2022 RG2 members, VTT archive

Approval

VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD

Date:	14 December 2022
Signature:	DocuSigned by: Nadezhda Gotcheva E21E683840FD424...
Name:	Nadezhda Gotcheva
Title:	Research Team Leader

Contents

1. Introduction

Reliability analysis of digital I&C systems is a challenging topic because the systems are very complex, the field is evolving, and there is very little failure data available. Software failures are particularly challenging to model because they can have many kinds of effects on the system, they are systematic in nature (unlike mechanical failures) and they are caused by mistakes in requirements specification, design or programming, etc. Lack of data is also a problem in the modelling of common cause failures (CCFs) between hardware components. High reliability is required from digital I&C, and it is not acceptable to use too conservative failure probability estimates in PRA. The topic has been studied for a long time, some practical methods have been developed specifically for the PRA of reactor protection systems (Authen et al., 2015), and digital reactor protection systems have been modelled in the PRAs of some nuclear power plants. However, international consensus on the analysis methods has not yet been achieved, and therefore, digital I&C is modelled in overly simplified and conservative manner in most PRAs currently, if modelled at all.

OECD NEA Committee on the Safety of Nuclear Installations (CSNI) Working Group on Risk Assessment (WGRISK) has organised digital I&C PRA related research for a long time. A project that surveyed available methods and information sources for the quantification of the reliability of digital I&C was finished in 2009 (OECD NEA CSNI, 2009). The DIGREL project continued the work and developed a failure mode taxonomy for the PRA of the digital I&C systems of nuclear power plants (OECD NEA CSNI, 2015). During years 2017-2021, a benchmark study on PRA modelling of a digital reactor protection system was performed with an international consortium in the DIGMAP project (OECD NEA CSNI, 2022a). In the project, six participants from different countries modelled the same reactor protection system based on common system specification and reliability data. The study showed that the same results can be produced with very different modelling approaches, such as a very detailed PRA model or a very simple PRA model with extensive background analyses. However, a detailed understanding and analysis of the system is required in any case. The modelling can focus on CCFs because only those are typically relevant for the overall results.

In parallel with the DIGREL project, a Nordic project (also called DIGREL) developed guidelines for failure modes and effects analysis of digital I&C, a software reliability analysis method, and an example PRA model for a digital reactor protection system (Authen et al., 2015; Bäckström et al., 2015). We refer to this example model as the DIGREL model. The DIGMAP benchmarking case was developed based on the DIGREL model, but it was simplified for some parts and some new details were added. Spurious signals were completely omitted in DIGMAP, whereas spurious off-signals (e.g. spurious stop of a pump) for safety functions were modelled in the DIGREL model. In the DIGREL model, the I&C related risk was dominated by detected failures causing spurious off-signals.

In 2022, a new WGRISK task called “DIGMORE – A realistic comparative application of DI&C modelling approaches for PSA” was started. It will also contain a benchmark study with participants from several countries. In the DIGMORE project, the reference case is extended compared to DIGMAP to cover new modelling aspects, such as priority logic, back-up systems and spurious actuations. The plan in DIGMORE is to define the benchmark case in early 2023 and start the PRA modelling after that.

The goals of this report are to perform simplified evaluation of the importance of detected failures causing spurious off-signals with the DIGMAP model, and to develop a preliminary fault tree model for a priority unit in order to support VTT’s participation in the DIGMORE project. Section 2 briefly presents the DIGMAP model. Detected failures causing spurious off-signals are evaluated in Section 3, and the priority unit is modelled in Section 4. Section 5 concludes the study.

2. DIGMAP model

In this section, the DIGMAP reference case and the VTT's PRA model are briefly presented. More detailed description of the reference case and analyses can be found from (OECD NEA CSNI, 2022a; OECD NEA CSNI, 2022b).

2.1 Reference case

The plant is a generic and simplified boiling water reactor plant. The layout of the main safety systems is presented in Figure 1. The safety systems are listed in Table 1. Each safety system, except for the reactor protection system, contains only one train.

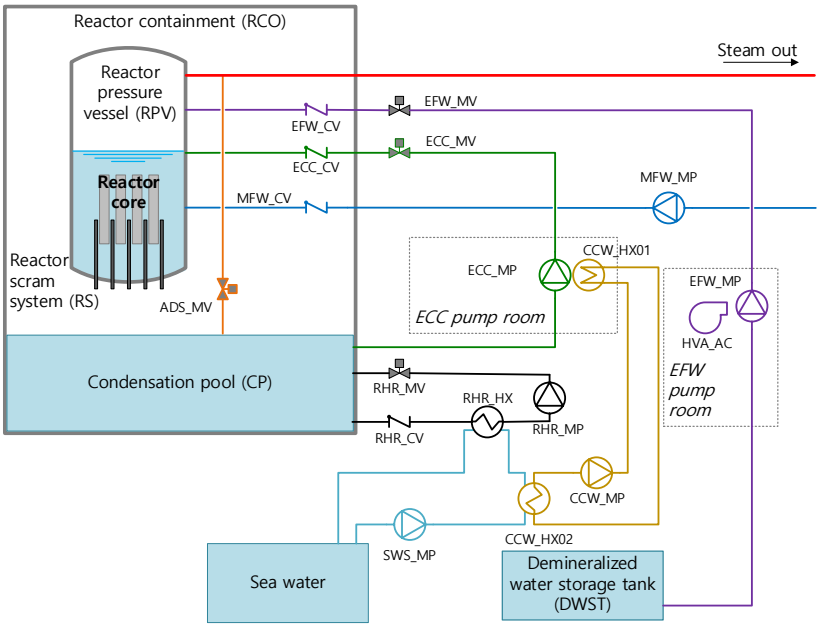


Figure 1: The layout of main safety systems (OECD NEA CSNI, 2022a).

Table 1: Safety systems.

System	Acronym
Automatic depressurization system	ADS
Component cooling water system	CCW
Emergency core cooling system	ECC
Emergency feed-water system	EFW
Service water system	SWS
Heating, venting and air conditioning system	HVA
Main feed-water system	MFW
Residual heat removal system	RHR
Reactor scram system	RS

The reactor protection system (RPS) consists of two diverse subsystems, RPS-A and RPS-B. Both subsystems contain four divisions. Each division contains its own measurement sensors, acquisition and

processing unit (APU), voting unit (VU) and sub-rack (SR). Each unit contains a processor module (PM) and a communication link (CL) module. Each APU contains analog input (AI) modules for receiving signals from measurement sensors, and each VU contains a digital output (DO) module for sending signals to the actuators. In the PM of each VU, 2-out-of-4 voting is performed based on inputs from the APUs of all divisions. The layout of the reactor protection system is presented in Figure 2. A safety function is actuated if any of the divisions sends it an actuation signal. The actuation signals of process components are summarised in Table 2.

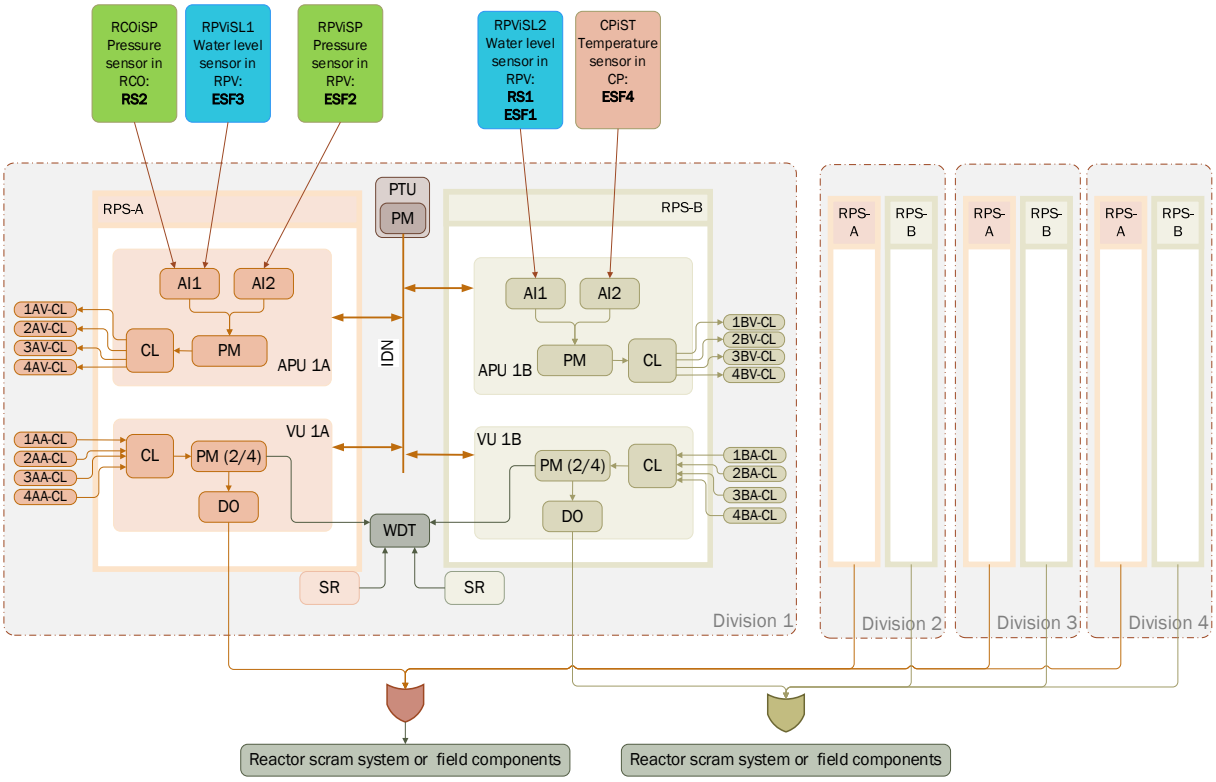


Figure 2: Reactor protection system layout (OECD NEA CSNI, 2022a).

Each division contains a periodic testing unit (PTU) that is common to both subsystems. Some of the I&C hardware (HW) failures can be detected by periodic testing that is performed every 24 hours. The PTU gathers the information from I&C components through intra-division network (IDN). Each division also contains a watchdog timer (WDT) that is common to both subsystems. The WDT can detect some of the HW failures in the PMs of the VUs and SRs in real time.

I&C modules consist of HW and operating system/platform software (OP). Processor modules include also application software (AS). For each module, the model description (OECD NEA CSNI, 2022a) specifies fictive reliability parameters for HW, OP and AS. OP and AS failure probabilities are defined on demand basis. For HW failures, failure rates are divided for failures detected by different fault tolerant features, which are automatic testing, periodic testing and full-scope testing. All HW failures are detected by full-scope testing performed every half a year if they are not detected earlier by other features.

The two subsystems are assumed to be of the same design, i.e. there is only functional diversity between the subsystems. CCFs of identical hardware components in different subsystems are modelled with the alpha-factor model. CCFs of software in similar modules in different subsystems are mostly modelled with a beta-factor of 1.

Table 2: Actuation signals (OECD NEA CSNI, 2022a).

System	Component	Control	Conditions	Signal
RS	Control rods	Open	RS1: low water level in reactor RS2: high pressure in containment	RS1 + RS2
EFW	Pump	Start	RS1: low water level in reactor ESF1: extreme low water level in reactor	RS1 + ESF1
	Motor-operated valve	Open	RS1: low water level in reactor ESF1: extreme low water level in reactor	RS1 + ESF1
HVA	AC cooler	Start	RS1: low water level in reactor ESF1: extreme low water level in reactor	RS1 + ESF1
ADS	Pressure relief valve	Open	ESF2: high pressure in reactor	ESF2
ECC	Pump	Start	ESF3: low water level in reactor	ESF3
	Motor-operated valve	Open	ESF3: low water level in reactor	ESF3
RHR	Pump	Start	RS2: high pressure in containment ESF4: high temperature in condensation pool	RS2+ESF4
	Motor-operated valve	Open	RS2: high pressure in containment ESF4: high temperature in condensation pool	RS2+ESF4
CCW	Pump	Start	RS2: high pressure in containment ESF4: high temperature in condensation pool	ESF3
SWS	Pump	Start	RS2: high pressure in containment ESF4: high temperature in condensation pool	RS2+ESF3+ESF4

2.2 Event tree

Loss of main feed-water is the only accident scenario analysed in the benchmark study. The event tree is presented in Figure 3 and it is also given in the model description [3] to the participants of the benchmark study.

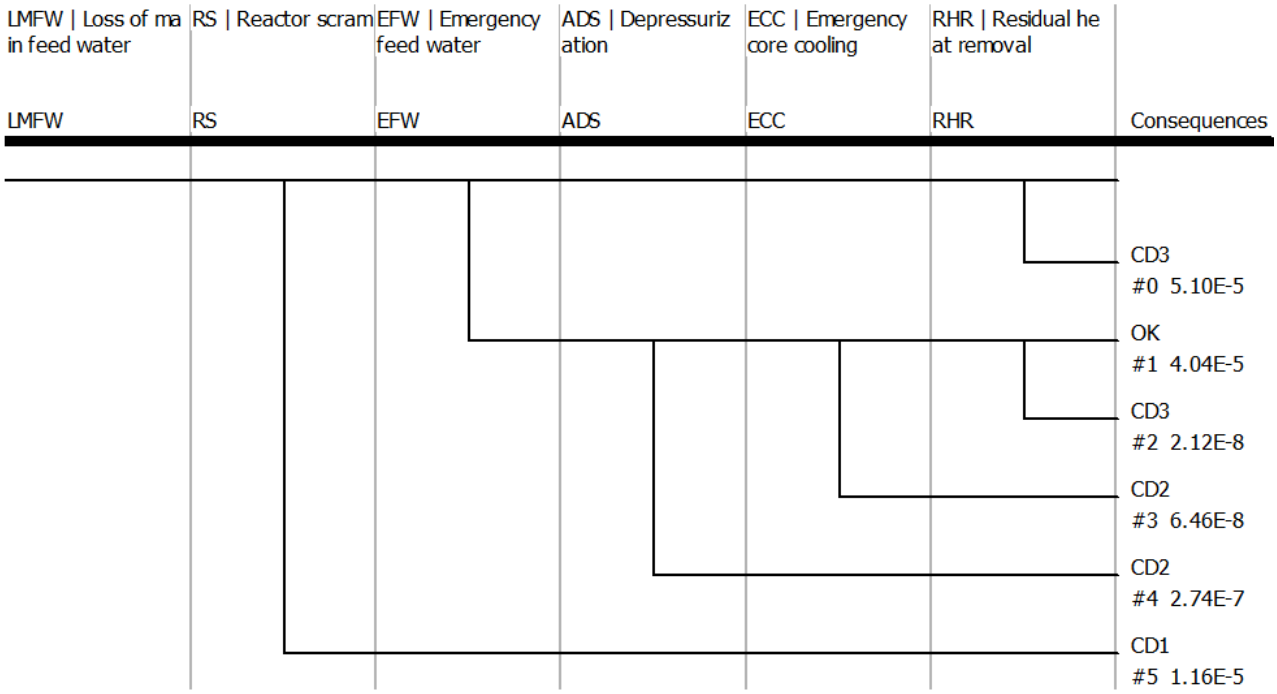


Figure 3: Event tree for loss of main feed-water accident.

2.3 Fault trees

Some selected fault trees are presented here from a new version of VTT's DIGMAP model. This model is not as simplified as the model used in the official DIGMAP benchmarking (OECD NEA CSNI, 2022a; OECD NEA CSNI, 2022b). In this model, single failures are modelled for each module and division, and CCFs are generated automatically by FinPSA (previously, this was not possible, because CCF groups of eight components could not be modelled that way in FinPSA, but now the maximum CCF group size of FinPSA has been increased to eight components). This new model and the simplified model give nearly identical results, even though the level of detail of minimal cut sets is different.

Fault trees for a VU and an APU are presented in Figures 4 and 5. The fault trees include links to module specific fault trees that include the failures related to the module under an OR gate. A fault tree of a processor module is presented in Figure 6, and the others are similar or even simpler. The fault trees are similar to those presented in (Tyrväinen, 2020), even though the data are partly different.

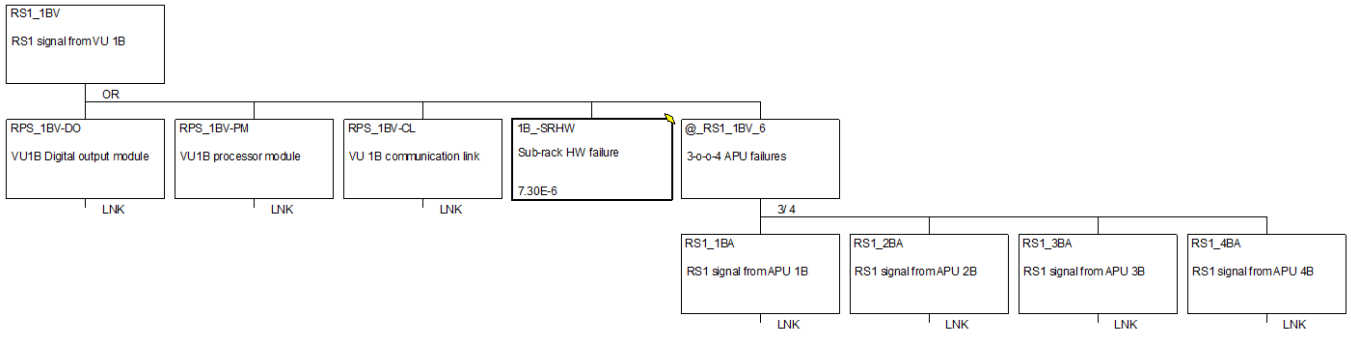


Figure 4: Fault tree for a VU.

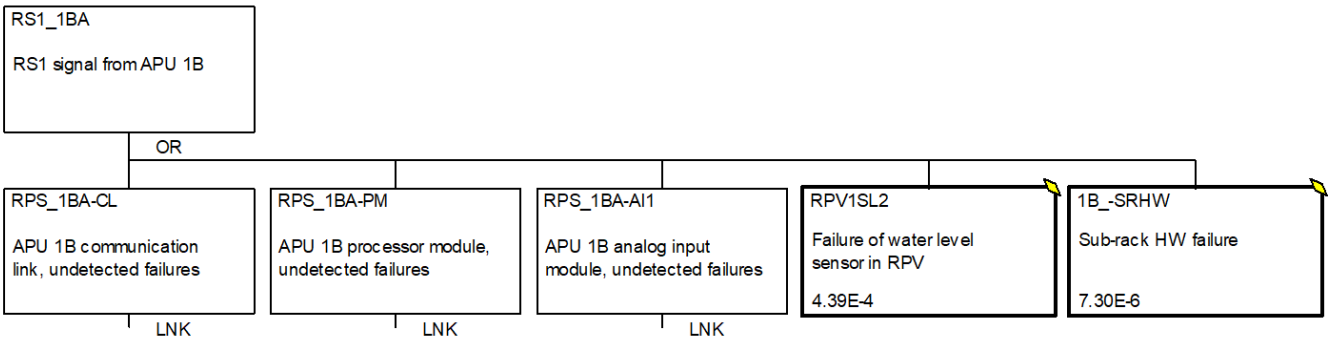


Figure 5: Fault tree for an APU.

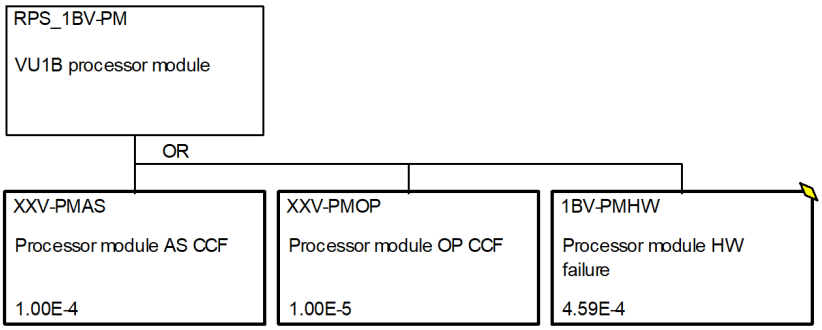


Figure 6: Fault tree for a processor module in a VU.

In the model, all hardware failures of a module are merged into one basic event, including undetected and detected failures. The total failure probability of the hardware of a module is calculated using a stand-alone fault tree that does not appear in the main PRA model. The detection coverages of different fault tolerant techniques and failures of testing equipment are modelled in such fault trees. This type of fault trees could also be included in the main PRA model and were included in some DIGMAP models (OECD NEA CSNI, 2022a; OECD NEA CSNI, 2022b), but this approach reduces the modelling work as otherwise the fault trees would need to be developed for each division in both subsystems. The failure probabilities of most modules are dominated by “undetected failures” that can only be detected by full-scope testing every half a year. More information about this modelling approach can be found in (Tyrväinen, 2020; OECD NEA CSNI, 2022b).

Spurious signals were not included in the model. Changing voting logic due to detected failures was also not modelled in this model but was modelled in some other DIGMAP models (OECD NEA CSNI, 2022a; OECD NEA CSNI, 2022b). The impact of changing voting logic was found negligible in DIGMAP. Therefore, it was possible to merge undetected and detected failures in this model. However, when spurious signals are modelled, detected failures need to be treated separately. Therefore, the modelling approach is slightly changed for the models used in the next sections. In the following, there are two hardware related basic events corresponding to undetected and detected failures for each relevant module, as was also in the DIGREL model.

3. Detected failures

3.1 Spurious stop signals for safety functions

One result from the Nordic DIGREL project was that detected failures can be important or even dominate digital I&C related risk (Authen et al., 2015 & 2016). 95% of the reactor protection system related core damage frequency was due to spurious off-signals. About half of this contribution consisted of detected hardware failures and the other half consisted of software failures.

On the other hand, in the DIGMAP project, spurious off-signals were not modelled, and the contribution of detected failures was very small. Therefore, we performed a limited study to test how important detected hardware failures could be in the DIGMAP case. Spurious off-signals caused by software failures were not included in this evaluation, because software failures are not divided into different failure types, such as fatal and non-fatal failures, in DIGMAP.

In the DIGREL model, important detected failures were those that were related to the signal for very high water level in the reactor pressure vessel. Two detected failures in APUs in redundant divisions could cause spurious closures of motor-operated valves in all trains of the EFW system, and, thus, cause the entire system to fail. CCFs of two hardware components were therefore important risk contributors. Detected failures causing spurious off-signals for other systems were not important, because either four detected failures were required for complete system failure (one detected failure stopped one train), or the systems themselves were not important.

The failure of the EFW system due to spurious high water level signals was added to the DIGMAP model with similar 2-out-of-4 failure condition. The signals were assumed to originate from the same sensors as ESF1 and RS1 signals. Detected VU failures were assumed not to cause the off-signal, because the most sensible system failure condition would be 4-out-of-4 and four detected VU failures were already modelled to cause failures of all EFW on-signals in the model (as they were merged with undetected failures for simplification). The fault trees for spurious off-signals from the VU and APU of division 1 are presented in Figures 7 and 8. Detected failures of measurement sensors were excluded, because those were specified only to be detected by the full-scope testing in the DIGMAP case. A mission time of 24 hours was specified for the detected failures along with the repair of 8 hours that was used in DIGMAP.

The detected failures still did however not have significance, because in the DIGMAP model, CCFs between two subsystems dominate the RPS related risk. Therefore, similar failure criterion was also added for the ECC system, which is controlled by the other subsystem. This criterion was completely hypothetical as there was no such criterion for the ECC system in the DIGREL model. After that, there was 4-out-of-8 criterion for the failure of those two safety functions due to specific detected failures in APUs. Detected failures (causing spurious off-signals) started to have some significance in the results, but still their contribution was only 7% of the RPS related risk and 18% of the RPS hardware related risk. Undetected failures still had larger contribution.

The results from the DIGREL model and DIGMAP model are very different. Some of the difference can be explained by detection coverage parameters. The detection coverages are mostly significantly higher in the DIGREL model. Particularly, a complete detection coverage is assumed for communication links in the DIGREL model, whereas it is 80% in the DIGMAP model. Undetected failures of CL modules are the most important hardware failures in the DIGMAP model. For AI modules, the detection coverage is smaller in the DIGREL model, but there are more redundant signals using different AI modules inside a subsystem, and CCFs between different AI modules are not modelled. This reduces the risk contribution of undetected AI module failures.

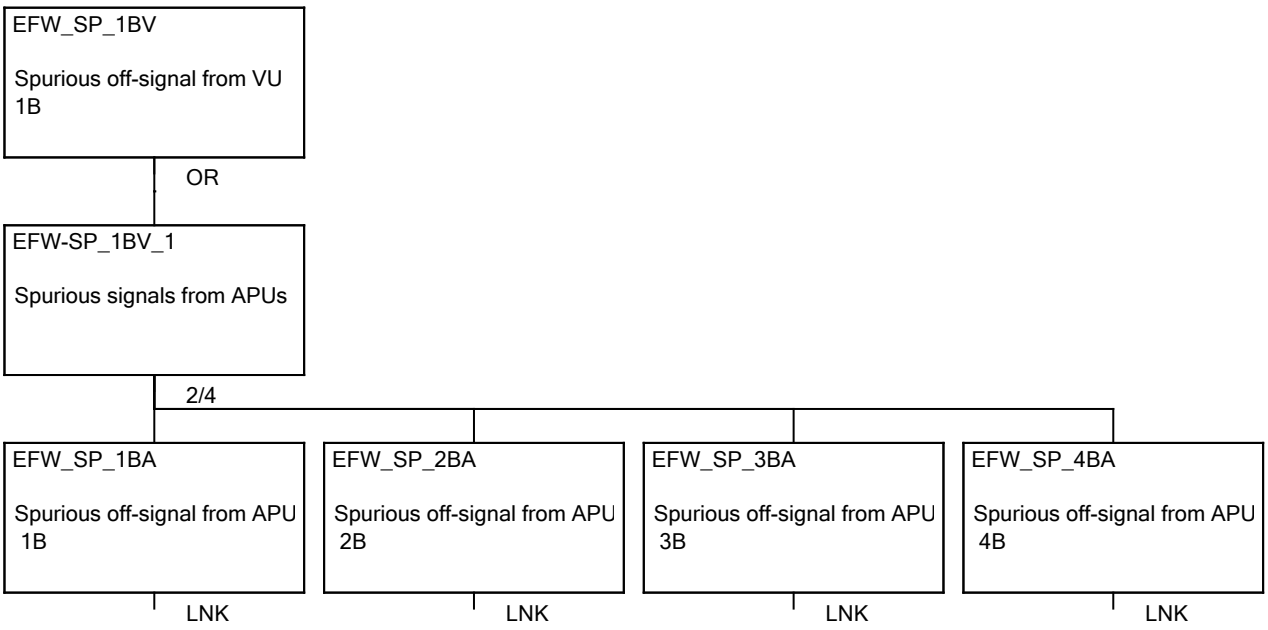


Figure 7: Spurious off-signal from voting unit.

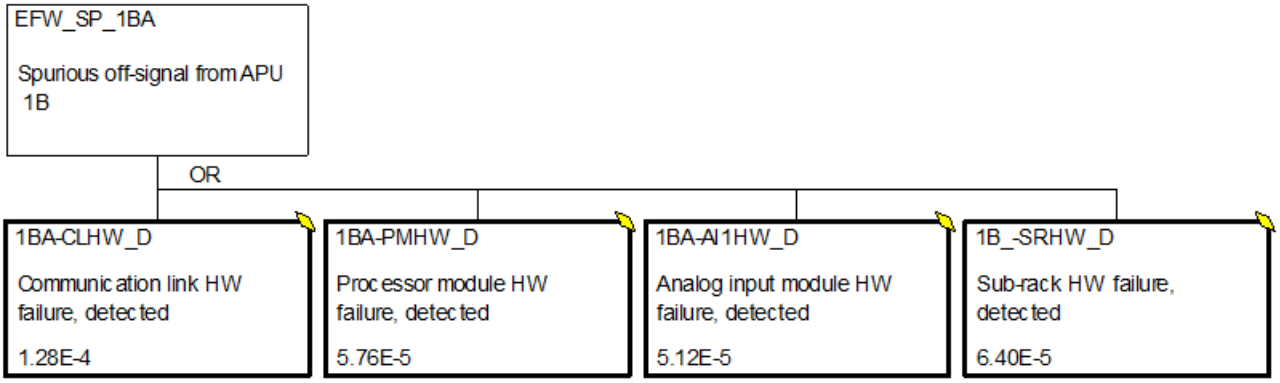


Figure 8: Spurious off-signal from APU.

It can be concluded that the risk contribution of detected hardware failures to the digital I&C related risk is highly dependent on detection coverage and fail-safe behaviour. Diversity between subsystems does also have relevance to this matter. It is possible that detected failures dominate over undetected failures or the other way round. However, it has to be noticed that detection coverage mainly affects the absolute risk contribution of undetected failures and typically has limited impact on the absolute risk contribution of detected failures, because the failure rate of detected failures is not very sensitive to the parameter when the coverages are relatively high, e.g. above 70%.

3.2 Spurious signals causing initiating event

While the loss of main feed-water scenario was modelled and stop signals were defined for the MFW system in DIGREL (Authen et al., 2015), initiating event caused by spurious stop signals for the MFW pumps was not modelled. Spurious stop signals for the pumps were modelled only in the transient and loss of offsite power scenarios. The pumps were defined to stop based on high water level in the pressure vessel and high temperature in feedwater system compartment with 2-out-of-4 criterion. Here, an evaluation is performed with the DIGMAP case on such spurious signals causing loss of main feed-water initiating event.

In the DIGMAP case, we define that high water level signals for the MFW system are processed in RPS-A and its AI1 module. Two detected failures in the APUs of RPS-A are assumed to stop the active pumps as well as cause failure to start the standby pump (the DIGREL model included two active pumps and one standby pump). Spurious off-signals for the EFW system are also considered here (as in the previous subsection), and CCFs between subsystems causing failures of both MFW and EFW are included in the analysis.

Modelling redundant failures causing an initiating event is not very handy in PRA software tools (at least not in FinPSA), because with normal modelling approach, the tool would multiply the frequencies of independent failures in minimal cut set analysis, which is not correct. Instead, the frequency of one failure should be multiplied by the probabilities of other failures, which are calculated based on the repair time of the first failure. However, if the modelling is performed that way, automatic CCF generation cannot be used. Therefore, the initiating event frequency calculations are performed in Excel in this study.

CCF calculations are performed in the same way as in the VTT's DIGMAP model described in (OECD NEA CSNI, 2022b). All CCF combinations with specific system level consequence are calculated, their probabilities are summed, and the result is used as a single basic event in the PRA model. In this case, there are two interesting system level consequences: failure of the MFW system by 2-out-of-4 criterion and failure of both MFW and EFW systems by 2-out-of-4 criterion in both subsystems. The numbers of CCF combinations with different system level consequences are presented in Table 3. Also, 3-out-of-4 and 4-out-of-4 criteria are included for sensitivity analysis. The calculations are performed separately for the AI, PM, CL and SR modules. The alpha-factor model is used with the same parameters as in the DIGMAP study (OECD NEA CSNI, 2022a). The resulting failure frequencies are presented in Table 4. It is notable that the EFW system has a relatively high conditional failure probability given the failure of the MFW system. The CCF calculations are presented in detail in Appendix.

Table 3: Numbers of CCFs causing failure of MFW or both MFW and EFW.

Number of failures	Only MFW fails 2-o-o-4	Both MFW and EFW fail 2-o-o-4	Only MFW fails 3-o-o-4	Both MFW and EFW fail 3-o-o-4	Only MFW fails 4-o-o-4	Both MFW and EFW fail 4-o-o-4
1						
2	6					
3	28		4			
4	17	36	17		1	
5	4	48	28		4	
6		28	6	16	6	
7		8		8	4	
8		1		1		1

Table 4: Frequencies (1/year) of CCFs causing failures of the MFW and EFW systems.

Module	2-o-o-4 criterion		3-o-o-4 criterion		4-o-o-4 criterion	
	MFW	MFW and EFW	MFW	MFW and EFW	MFW	MFW and EFW
AI	1.81E-3	8.13E-4	4.10E-4	2.15E-4	1.00E-4	4.82E-5
PM	2.03E-3	9.14E-4	4.61E-4	2.41E-4	1.13E-4	5.42E-5
CL	4.51E-3	2.03E-3	1.03E-3	5.36E-4	2.50E-4	1.20E-4
SR	2.26E-3	1.02E-3	5.12E-4	2.68E-4	1.25E-4	6.02E-5
Total	1.06E-2	4.78E-3	2.41E-3	1.26E-3	5.88E-4	2.83E-4

The frequency of two independent failure events (2-out-of-4 components fail due to single failures, a single failure and a CCF, or two CCFs) is 3.7E-5/year. It is so small that independent failures can be screened out from the analysis. An upper bound for the frequency of two independent failure events (a single failure and a CCF, or two CCFs) causing two failures in both subsystems is estimated as 5.6E-6/year. It can also be screened out. Only single CCF events need to be modelled.

The CCF events shown in Table 4 were added to the DIGMAP model. A fault tree was created for loss of main feed-water initiating events and it was placed in the beginning of the event tree (Figure 3). The technical initiating event of the event tree was replaced with a dummy event with a probability of 1. Initiating events that cause also failure of the EFW system were placed in the fault tree of the EFW system.

The contribution of the spurious signals to the core damage frequency was 29%. Detected failures causing only the failure of MFW and detected failures causing failures of both MFW and EFW were almost equally important. When criterion 3-out-of-4 was applied, the contribution of the spurious signals was 9%. When criterion 4-out-of-4 was applied, the contribution of the spurious signals was 2%.

4. Modelling of priority unit

This section develops a tentative fault tree model for a priority unit, which has been sketched in the DIGMORE project by Dr Christian Müller (GRS). Note that the design analysed here is simplified and only based on preliminary ideas, and will not necessarily be used in DIGMORE as such.

4.1 Priority unit design

The module structure of the priority unit is presented in Figure 9. The input connections from the RPS and back-up I&C are hard-wired. The input signals are converted into digital format by analog/digital (AD) converters. The input signals from the operational I&C (OI&C) come through network communication, a communication link (CL) and a processor module (PM) The priority logic is implemented in a complex programmable logic device (CPLD). Finally, the ‘on’ and ‘off’ signals are converted into analog format by a digital/analog (DA) converter. Each module includes operating software, but there is no customizable application software. There is also a sub-rack (SR) for power supply.

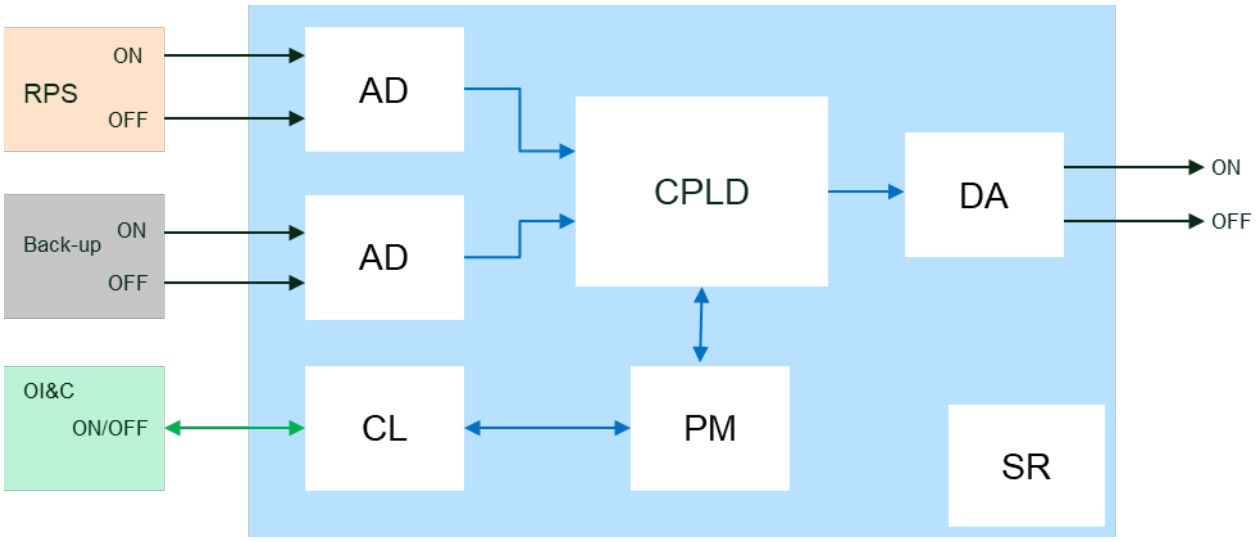


Figure 9: Module structure of the priority unit.

The priority logic is such that off-signals are prioritized over on-signals. RPS signals are prioritized over back-up I&C signals, and back-up I&C signals are prioritized over operational I&C signals.

4.2 Failure modes and effects

A simplified failure modes and effects analysis (FMEA) for the modules of the priority unit is presented in Table 3. The failure effects of the detected failures are based on assumptions of the system's fail-safe behaviour. It is assumed that the on-signal is not set based on only one detected failure. Instead, the off-signal is assumed to be set or the signals are just not set in different cases. Software failures are assumed to be fatal failures that are detected. Non-fatal software failures causing spurious signals are not included, because there is no application software in the priority unit.

Table 5: Failure modes and effects analysis for the modules of the priority unit.

Module/unit/system	Failure mode	Failure effect
Sub-rack	Hardware failure, detected	Off-signal set
	Hardware failure, undetected	No on-signal when demanded
Digital/analog converter	Hardware failure, detected	Off-signal set
	Hardware failure, undetected	No on-signal when demanded
	Software failure	Off-signal set
Complex programmable logic device	Hardware failure, detected	Off-signal set
	Hardware failure, undetected	No on-signal when demanded
	Software failure	Off-signal set
Analog/digital converter for RPS	Hardware failure, detected	Signals not set. Back-up I&C has the control.
	Hardware failure, undetected	Signals not set. Back-up I&C has the control.
	Software failure	Signals not set. Back-up I&C has the control.

Module/unit/system	Failure mode	Failure effect
Analog/digital converter for back-up I&C	Hardware failure, detected	Signals not set. Operational I&C has the control, if the RPS signal has failed.
	Hardware failure, undetected	Signals not set. Operational I&C has the control, if the RPS signal has failed.
	Software failure	Signals not set. Operational I&C has the control, if the RPS signal has failed.
Processor module	Hardware failure, detected	Off-signal set. Off-signal for the safety function, if the RPS and back-up I&C signals have failed.
	Hardware failure, undetected	Signals not set. No on-signal when demanded, if the RPS and back-up I&C signals have failed.
	Software failure	Off-signal set. Off-signal for the safety function, if the RPS and back-up I&C signals have failed.
Communication link	Hardware failure, detected	Off-signal set. Off-signal for the safety function, if the RPS and back-up I&C signals have failed.
	Hardware failure, undetected	Signals not set. No on-signal when demanded, if the RPS and back-up I&C signals have failed.
	Software failure	Off-signal set. Off-signal for the safety function, if the RPS and back-up I&C signals have failed.
RPS VU	Hardware failure, detected	Signals not set. Back-up I&C has the control.
	Hardware failure, undetected	Signals not set. Back-up I&C has the control.
	OP failure	Signals not set. Back-up I&C has the control.
	AS failure	Signals not set. Back-up I&C has the control. Spurious signal could also be possible but is not modelled.
RPS APU	Hardware failure, detected	Off-signal for safety function if two redundant modules processing the off-signal fail.
	Hardware failure, undetected	Signals not set and back-up I&C has the control, if three redundant modules processing the on-signal fail.
	OP failure	Off-signal for safety function
	AS failure	Signals not set. Back-up I&C has the control.

Module/unit/system	Failure mode	Failure effect
		Spurious signal could also be possible but is not modelled.
Back-up I&C	No on-signal on demand	Operational I&C has the control, if the RPS signal has failed.
	Spurious off-signal	Off-signal for safety function if the RPS has failed.
Operational I&C	No on-signal on demand	No on-signal when demanded, if the RPS and back-up I&C signals have failed.
	Spurious off-signal	Off-signal for safety function if the RPS and back-up I&C have failed.

The RPS, back-up I&C and operational I&C are also included in the FMEA in a simplified way. The RPS is assumed to be the same as in DIGMAP. Its failures are considered at the unit level in the FMEA. OP and AS failures are analysed separately. In DIGMAP, it was not specified how the software components fail, besides causing the failure of the subsystem. Here, OP failures are assumed to be fatal failures where the software stops operating. AS failures are assumed to be non-fatal so that the software continues operating with failed output. For back-up I&C and operational I&C, only the failed inputs to the priority unit are considered.

4.3 Fault tree model

Fault tree analysis of the priority unit is performed for the EFW related signals of the DIGMAP case. As specified in Table 2, the on-signals for the EFW are RS1 and ESF1. However, ESF1 has not been modelled separately in DIGMAP, because it comes from the same sensors as RS1. Spurious off-signal due to detected hardware failures is modelled as presented in Section 3. In addition, OP failures in RPS APU are assumed to cause the spurious off-signal as specified in the FMEA, which means that those OP failures are moved to the fault trees related to the spurious off-signal.

Mechanical components of the EFW system and support systems are excluded from the analysis. Four redundant EFW trains are assumed, and each of those has its own priority unit. Two trains are required for successful safety function, meaning that the failure criterion is 3-out-of-4.

A fault tree for the priority unit of train 1 is presented in Figures 10 and 11. All failures of DA, CPLD and SR modules are assumed to lead to the failure to actuate the EFW train, either by setting the off-signal or omitting the on-signal. Spurious off-signal from the RPS also alone causes the failure of the actuation. Other RPS failures and failures of the corresponding AD module pass the control to the back-up system. In that situation, a spurious off-signal from the back-up system causes the EFW train to fail, whereas failure of the on-signal or AD failure passes the control to the operational I&C. When the operational I&C has the control, all its failures and failures of the CL and PM cause the EFW train to fail. The failures related to the different systems are modelled under an AND gate. The spurious off-signal from the back-up system is also included in the fault tree of the operational I&C, because the operational I&C cannot actuate the safety function in that situation.

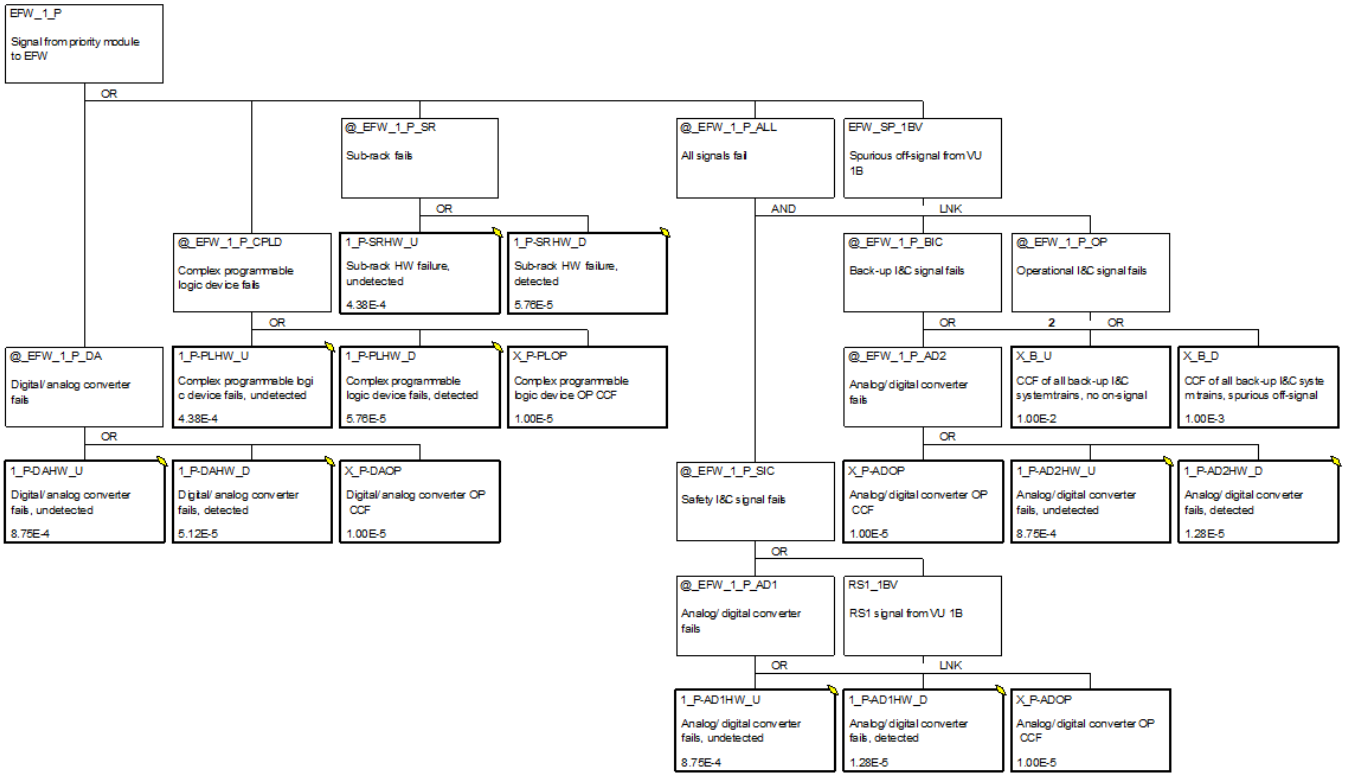


Figure 10: Fault tree for the priority unit of train 1.

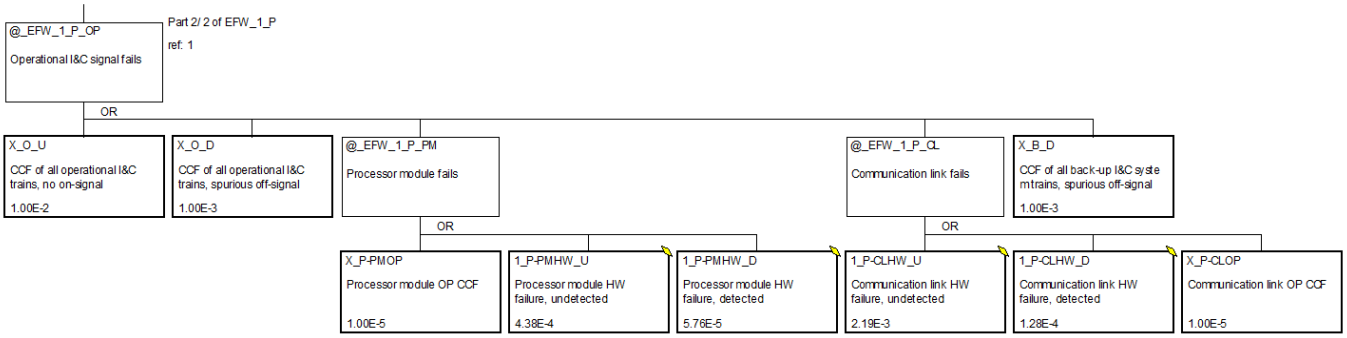


Figure 11: Fault tree for failure of a signal from the operational I&C.

The fault tree is developed a bit differently than the DIGMAP model. Here, all failures of the priority unit are in the same fault tree. The model could also be made modular with separate fault trees for different modules. This could be useful particularly if the same structures would be used in different fault trees, but here one big fault tree is convenient for the presentation of the model.

The modelling of fault-tolerant techniques is simpler than in DIGMAP. Only automatic testing and full-scope testing are considered, whereas also periodical testing was included in DIGMAP. Failures of testing equipment are also ignored here, as those had very small risk contribution in DIGMAP. The modelling of those could anyway be performed in the same way as in DIGMAP, which would add a bit more complexity to the model.

The failure rates and detection coverages of hardware failures are presented in Table 6. These are fictive numbers that are in line with the values used in DIGMAP. The detection coverage is for the automatic testing. The full-scope testing is assumed to detect all failures. For OP failures, a probability of 1E-5 is

used as in DIGMAP. For back-up and operational I&C, failure probabilities of 1E-2 for failure of on-signal on demand and 1E-3 for spurious off-signal are assumed, as the systems are not modelled in detail here. These failures of back-up and operational I&C are assumed to be common to all trains.

Table 6: Failure rates and detection coverages of hardware failures of the modules.

Module	Failure rate (1/h)	Detection coverage
AD	2E-6	0.8
CL	5E-6	0.8
CPLD	2E-6	0.9
DA	2E-6	0.8
PM	2E-6	0.9
SR	2E-6	0.9

A mission time of 24 hours is used for those detected failures that can cause spurious off-signal. For detected failures that are “ignored”, no mission time is given, because those cannot stop the safety function after it has started.

4.4 Results

The total failure probability of the I&C signals to the EFW system is 2.04E-4 (for 3-out-of-4 failure criterion). The share of the failures of the priority units is 57%, and failures of the RPS cover 43% of the total failure probability. Spurious off-signal from the back-up I&C has a contribution of 0.3%, and failure of the on-signal from the back-up I&C has a contribution of 0.03%. Operating I&C has a contribution of 0.1%. The reason for the small contribution of back-up and operating I&C is that the RPS’s contribution is dominated by spurious off-signals.

The contribution of hardware failures to the failure probability related to the priority units themselves is 83%, and the contribution of software failures is 17%. Of the hardware failures, 91% are undetected failures.

The contribution of hardware failures to the total failure probability related to the RPS is 65%, the contribution of OP is 34%, and the contribution of AS is 0.3%. Of the hardware failures, 99% are detected failures, because the detected failures cause spurious off-signals, whereas undetected failures only “pass the control” to the back-up I&C. The OP failures in APUs have also been assumed to cause spurious off-signals, which explains their dominance over AS failures.

The most important modules are the DA, CPLD and SR of the priority units. The CCFs of those alone cause the failure of the EFW system. Modules in RPS APUs are also important, because multiple detected failures in those cause spurious off-signals. The Fussell-Vesely values of 50 most important basic events are listed in the following. These correspond largely to the top minimal cut sets as e.g. the 32 most important basic events cause the top event alone. In the basic event names, ‘X_P’ refers to the priority unit, ‘XX’ refers to the RPS, and ‘XXA’ refers to RPS APU.

	Name	Fuss-Ves	Comment
1	X_P-DAOP	4.89E-02	Digital/analog converter OP CCF
2	X_P-PLOP	4.89E-02	Complex programmable logic device OP CCF
3	XXA-AIOP	4.89E-02	Analog input module OP CCF
4	XXA-CLOP	4.89E-02	Communication link OP CCF
5	XXA-PMOP	4.89E-02	Processor module OP CCF
6	X_P-DAHW_U-ABC	4.33E-02	3x CCF Digital/analog converters HW, undetected
7	X_P-DAHW_U-BCD	4.33E-02	3x CCF Digital/analog converters HW, undetected
8	X_P-DAHW_U-ACD	4.33E-02	3x CCF Digital/analog converters HW, undetected
9	X_P-DAHW_U-ABD	4.33E-02	3x CCF Digital/analog converters HW, undetected
10	X_P-DAHW_U-ABCD	4.01E-02	4x CCF Digital/analog converters HW, undetected
11	X_P-SRHW_U-ABC	2.17E-02	3x CCF Sub-racks HW, undetected
12	X_P-PLHW_U-ABC	2.17E-02	3x CCF Complex programmable logic devices HW, undetected
13	X_P-SRHW_U-BCD	2.17E-02	3x CCF Sub-racks HW, undetected
14	X_P-PLHW_U-BCD	2.17E-02	3x CCF Complex programmable logic devices HW, undetected
15	X_P-SRHW_U-ACD	2.17E-02	3x CCF Sub-racks HW, undetected
16	X_P-PLHW_U-ACD	2.17E-02	3x CCF Complex programmable logic devices HW, undetected
17	X_P-SRHW_U-ABD	2.17E-02	3x CCF Sub-racks HW, undetected
18	X_P-PLHW_U-ABD	2.17E-02	3x CCF Complex programmable logic devices HW, undetected
19	X_P-PLHW_U-ABCD	2.01E-02	4x CCF Complex programmable logic devices HW, undetected
20	X_P-SRHW_U-ABCD	2.01E-02	4x CCF Sub-racks HW, undetected
21	XXA-CLHW_D-EH	6.74E-03	2x CCF Communication links HW, detected
22	XXA-CLHW_D-FH	6.74E-03	2x CCF Communication links HW, detected
23	XXA-CLHW_D-GH	6.74E-03	2x CCF Communication links HW, detected
24	XXA-CLHW_D-EG	6.74E-03	2x CCF Communication links HW, detected
25	XXA-CLHW_D-FG	6.74E-03	2x CCF Communication links HW, detected
26	XXA-CLHW_D-EF	6.74E-03	2x CCF Communication links HW, detected
27	XX_-SRHW_D-GH	3.37E-03	2x CCF Sub-racks HW, detected failures
28	XX_-SRHW_D-FH	3.37E-03	2x CCF Sub-racks HW, detected failures
29	XX_-SRHW_D-EH	3.37E-03	2x CCF Sub-racks HW, detected failures
30	XX_-SRHW_D-EF	3.37E-03	2x CCF Sub-racks HW, detected failures
31	XX_-SRHW_D-FG	3.37E-03	2x CCF Sub-racks HW, detected failures
32	XX_-SRHW_D-EG	3.37E-03	2x CCF Sub-racks HW, detected failures
33	X_B_D	3.18E-03	CCF of all back-up I&C system trains, spurious off-signal
34	XXA-PMHW_D-FH	3.03E-03	2x CCF Processor modules HW, detected
35	XXA-PMHW_D-EH	3.03E-03	2x CCF Processor modules HW, detected
36	XXA-PMHW_D-EF	3.03E-03	2x CCF Processor modules HW, detected
37	XXA-PMHW_D-FG	3.03E-03	2x CCF Processor modules HW, detected
38	XXA-PMHW_D-EG	3.03E-03	2x CCF Processor modules HW, detected
39	XXA-PMHW_D-GH	3.03E-03	2x CCF Processor modules HW, detected
40	X_P-PLHW_D-ABD	2.85E-03	3x CCF Complex programmable logic devices HW, detected
41	X_P-SRHW_D-ABD	2.85E-03	3x CCF Sub-racks HW, detected
42	X_P-PLHW_D-ACD	2.85E-03	3x CCF Complex programmable logic devices HW, detected
43	X_P-SRHW_D-ACD	2.85E-03	3x CCF Sub-racks HW, detected
44	X_P-PLHW_D-BCD	2.85E-03	3x CCF Complex programmable logic devices HW, detected
45	X_P-SRHW_D-BCD	2.85E-03	3x CCF Sub-racks HW, detected
46	X_P-PLHW_D-ABC	2.85E-03	3x CCF Complex programmable logic devices HW, detected
47	X_P-SRHW_D-ABC	2.85E-03	3x CCF Sub-racks HW, detected
48	XXA-AI1HW_D-EH	2.69E-03	2x CCF Analog input modules HW, detected failures
49	XXA-AI1HW_D-FH	2.69E-03	2x CCF Analog input modules HW, detected failures
50	XXA-AI1HW_D-EF	2.69E-03	2x CCF Analog input modules HW, detected failures

4.5 Sensitivity analysis

When the 2-out-of-4 condition for spurious off-signals based on detected failures in RPS APU is changed to 3-out-of-4, the total failure probability of the I&C signals to the EFW system is decreased by 21%. Fussell-Vesely of detected hardware failures in RPS APU is decreased by 70% from 0.28 to 0.083. The contribution of spurious off-signals based on detected hardware failures is therefore quite sensitive to the definition of the voting logic. The contribution of OP failures causing spurious off-signals, on the other hand, is not dependent on the voting logic when only complete CCFs are modelled. When 4-out-of-4 condition is applied, Fussell-Vesely of detected hardware failures in RPS APU is decreased to 0.021.

When the priority is defined for on-signals instead of off-signals, the total failure probability of the I&C signals to the EFW system is decreased by 43% and the contribution of the RPS is decreased from 43% to 0.1%. The reason for this is that spurious off-signals from the RPS cannot cause failure of the safety function alone.

5. Conclusions

In this report, PRA modelling studies of digital I&C have been conducted as complementary to the WGRISK's DIGMAP project. One goal has also been to prepare for the PRA modelling work in the WGRISK's DIGMORE project, which has recently started. In this report, first, the risk contribution of detected failures causing spurious off-signals were studied by extending the PRA model developed in the DIGMAP project. Second, a fault tree model was developed for a fictive priority unit, which was also connected to the DIGMAP model.

Detected hardware failures causing spurious off-signals of safety functions were added to the DIGMAP model, as they were not included in the original study, whereas they had been found important in the previous DIGREL study. In this case, the detected hardware failures had only little importance compared to undetected failures. The importance of detected failures with regard to digital I&C related risk is sensitive to detection coverage parameters and fail-safe behaviour. Also, the diversity (or lack of diversity) between subsystems has significance for this matter.

Detected hardware failures causing the loss of main feed-water initiating event due to spurious off-signals were also evaluated with the DIGMAP model based on definitions from the DIGREL study, even though those were not modelled in DIGREL. In this case, detected failures were found significant contributors. It is notable that a detected CCF can cause both an initiating event and failure of a safety function at the same time if no diversity is implemented between hardware components.

A fault tree model was developed for a priority unit based on some early design ideas from the DIGMORE project and an FMEA that was constructed for the modules of the priority unit. The priority unit gets its input signals from an RPS, back-up I&C system and operating I&C system. The RPS model from DIGMAP was used for the RPS signal failures, whereas the other systems were modelling in a very simplified manner. The most important contributors to the safety function failure were specific failures in the priority units, but also spurious off-signals caused by detected hardware and software failures in the RPS were important. Other contributors were almost negligible. Detected RPS failures dominated over undetected failures in this case, because the detected failures can alone cause the safety function failure through the spurious off-signals, whereas undetected RPS failures only "pass the control" to the back-up I&C. However, the contribution of detected failures depends on the definition of the voting logic and the priorities of signals.

The results of this study highlight the need to model spurious off-signals that occur due to detected failures in PRA. Spurious off-signals can be important both with regard to initiating events and failures of safety functions, even though it is not always the case.

References

Authen, S, Holmberg, J-E, Tyrväinen, T, Zamani, L. (2015), "Guidelines for reliability analysis of digital systems in PSA context - Final report", NKS-330, Nordic nuclear safety research, Roskilde.

Authen, S, Bäckström, O, Holmberg, J-E, Porthin, M, Tyrväinen, T. (2016). "Modelling of digital I&C, MODIG – Interim report 2015", NKS-361, Nordic nuclear safety research, Roskilde.

Bäckström, O, Holmberg, J-E, Jockenhövel-Barttfeld, M, Porthin, M, Taurines, A, Tyrväinen, T. (2015). “Software reliability analysis for PSA: failure mode and data analysis”, NKS-341, Nordic nuclear safety research, Roskilde.

Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI). (2009). “Recommendations on assessing digital system reliability in probabilistic risk assessments of nuclear power plants”, NEA/CSNI/R(2009)18, Paris, France.

Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI). (2015). “Failure modes taxonomy for reliability assessment of digital instrumentation and control systems for probabilistic risk analysis”, NEA/CSNI/R(2014)16, Paris, France.

Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI). (2022a). “Digital I&C PSA – Comparative application of digital I&C modelling approaches for PSA, Volume 1: Main report and Appendix A”, NEA/CSNI/R(2021)14, Paris, France. DRAFT.

Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI). (2022b). “Digital I&C PSA – Comparative application of digital I&C modelling approaches for PSA, Volume 2: Appendices B0-B6”, NEA/CSNI/R(2021)14/ADD, Paris, France. DRAFT.

Tyrväinen, T. (2020). “Probabilistic risk model of digital reactor protection system for benchmarking”, VTT-R-01028-19, VTT Technical Research Centre of Finland Ltd, Espoo.

Appendix: Common cause failure calculations

Table 7: Annual frequencies of independent detected failures.

Module	Failure rate (1/h)	Detection coverage	Frequency (1/year)
AI	2E-6	0.8	0.0140
PM	2E-6	0.9	0.0158
CL	5E-6	0.8	0.0350
SR	2E-6	1.0	0.0175
Total			0.0823

Table 8: Alpha-factor parameters.

Alpha1	Alpha2	Alpha3	Alpha4	Alpha5	Alpha6	Alpha7	Alpha8
9.32E-01	4.20E-02	1.44E-02	6.55E-03	2.35E-03	1.32E-03	9.01E-04	4.79E-04

Alpha-factor model:

$$Q_k = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t,$$

where Q_k is the probability/frequency of a specific CCF combination with k components, m is the number components in the CCF group, Q_t is the total failure probability/frequency of one component, and

$$\alpha_t = \sum_{k=1}^{m} k \cdot \alpha_k.$$

Table 9: Frequencies (1/year) of CCF events of different orders.

Module	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
AI	1.17E-2	1.51E-4	2.59E-5	9.41E-6	4.22E-6	4.74E-6	1.13E-5	4.82E-5
PM	1.32E-2	1.70E-4	2.91E-5	1.06E-5	4.75E-6	5.33E-6	1.27E-5	5.42E-5
CL	2.93E-2	3.77E-4	6.46E-5	2.35E-5	1.05E-5	1.18E-5	2.83E-5	1.20E-4
SR	1.46E-2	1.89E-4	3.23E-5	1.18E-5	5.27E-6	5.92E-6	1.42E-5	6.02E-5

Table 10: Numbers of CCFs causing failure of MFW or both MFW and EFW.

Number of failures	Only MFW fails 2-o-o-4	Both MFW and EFW fail 2-o-o-4	Only MFW fails 3-o-o-4	Both MFW and EFW fail 3-o-o-4	Only MFW fails 4-o-o-4	Both MFW and EFW fail 4-o-o-4
1						
2	6					
3	28		4			
4	17	36	17		1	
5	4	48	28		4	
6		28	6	16	6	
7		8		8	4	
8		1		1		1

Table 11: CCF frequencies (1/year) for AI module.

Number of failures	Only MFW fails 2-o-o-4	Both MFW and EFW fail 2-o-o-4	Only MFW fails 3-o-o-4	Both MFW and EFW fail 3-o-o-4	Only MFW fails 4-o-o-4	Both MFW and EFW fail 4-o-o-4
1						
2	9.05E-4					
3	7.24E-4		1.03E-4			
4	1.60E-4	3.39E-4	1.60E-4		9.41E-6	
5	1.69E-5	2.03E-4	1.18E-4		1.69E-5	
6		1.33E-4	2.84E-5	7.58E-5	2.84E-5	
7		9.06E-5		9.06E-5	4.53E-5	
8		4.82E-5		4.82E-5		4.82E-5
SUM	1.81E-3	8.13E-4	4.10E-4	2.15E-4	1.00E-4	4.82E-5

Table 12: CCF frequencies (1/year) for PM.

Number of failures	Only MFW fails 2-o-o-4	Both MFW and EFW fail 2-o-o-4	Only MFW fails 3-o-o-4	Both MFW and EFW fail 3-o-o-4	Only MFW fails 4-o-o-4	Both MFW and EFW fail 4-o-o-4
1						
2	1.02E-3					
3	8.14E-4		1.16E-4			
4	1.80E-4	3.81E-4	1.80E-4		1.06E-5	
5	1.90E-5	2.28E-4	1.33E-4		1.90E-5	
6		1.49E-4	3.20E-5	8.53E-5	3.20E-5	
7		1.02E-4		1.02E-4	5.10E-5	
8		5.42E-5		5.42E-5		5.42E-5
SUM	2.03E-3	9.14E-4	4.61E-4	2.41E-4	1.13E-4	5.42E-5

Table 13: CCF frequencies (1/year) for CL module.

Number of failures	Only MFW fails 2-o-o-4	Both MFW and EFW fail 2-o-o-4	Only MFW fails 3-o-o-4	Both MFW and EFW fail 3-o-o-4	Only MFW fails 4-o-o-4	Both MFW and EFW fail 4-o-o-4
1						
2	2.26E-3					
3	1.81E-3		2.59E-4			
4	4.00E-4	8.47E-4	4.00E-4		2.35E-5	
5	4.22E-5	5.06E-4	2.95E-4		4.22E-5	
6		3.32E-4	7.11E-5	1.90E-4	7.11E-5	
7		2.26E-4		2.26E-4	1.13E-4	
8		1.20E-4		1.20E-4		1.20E-4
SUM	4.51E-3	2.03E-3	1.02E-3	5.36E-4	2.50E-4	1.20E-4

Table 14: CCF frequencies (1/year) for SR module.

Number of failures	Only MFW fails 2-o-o-4	Both MFW and EFW fail 2-o-o-4	Only MFW fails 3-o-o-4	Both MFW and EFW fail 3-o-o-4	Only MFW fails 4-o-o-4	Both MFW and EFW fail 4-o-o-4
1						
2	1.13E-3					
3	9.05E-4		1.29E-4			
4	2.00E-4	4.23E-4	2.00E-4		1.18E-5	
5	2.11E-5	2.53E-4	1.48E-4		2.11E-5	
6		1.66E-4	3.55E-5	9.48E-5	3.55E-5	
7		1.13E-4		1.13E-4	5.66E-5	
8		6.02E-5		6.02E-5		6.02E-5
SUM	2.26E-3	1.02E-3	5.12E-4	2.68E-4	1.25E-4	6.02E-5

The frequency of two independent failure events (2-out-of-4 components fail due to single failures, a single failure and a CCF, or two CCFs):

$$6 \cdot \frac{0.0823}{year} \cdot \frac{\frac{0.0823}{year}}{365 \cdot \frac{24h}{year}} \cdot 8h \approx 3.72 \cdot 10^{-5}/year,$$

where 6 is the number of combinations with two components, $0.0823/year$ is the total failure frequency of one module (any module), and $8h$ is the mean time to repair.

An upper bound for the frequency of two CCFs causing 2-out-of-4 components to fail in both subsystems:

$$4 \cdot 4 \cdot \frac{0.0823}{year} \cdot 0.068 \cdot \frac{\frac{0.0823}{year} \cdot 0.068}{365 \cdot \frac{24h}{year}} \cdot 8h \approx 4.58 \cdot 10^{-7}/year,$$

where $4 \cdot 4$ is the number of ways to select one component from both subsystems (it can be counted that one CCF is associated to one subsystem, even though a CCF event can include failures in both subsystems), and 0.068 is the portion of CCF events of the total failure frequency of one module.

An upper bound for the frequency of a combination of a single failure and a CCF causing 2-out-of-4 components to fail in both subsystems:

$$2 \cdot 4 \cdot 4 \cdot \frac{0.0823}{year} \cdot 0.026 \cdot \frac{\frac{0.0823}{year}}{365 \cdot \frac{24h}{year}} \cdot 8h \approx 5.15 \cdot 10^{-6}/year,$$

where $2 \cdot 4 \cdot 4$ is the number of ways to select the single failure from one subsystem and one component from the other (it can be counted that the CCF is associated to the other subsystem even though there has to be another failure also in the subsystem with the single failure), and 0.026 is the portion of CCF events with at least three components of the total failure frequency of one module.

DocuSign

Certificate Of Completion

Envelope Id: B38DA55A15F940A398CE013E2CC2CA32
Subject: Complete with DocuSign: VTT-R-00940-22.pdf
Source Envelope:
Document Pages: 26 | Signatures: 1
Certificate Pages: 1 | Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius

Status: Completed

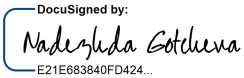
Envelope Originator:
Christina Vähävaara
Vuorimiehentie 3, Espoo,
., . P.O Box1000,FI-02044
Christina.Vahavaara@vtt.fi
IP Address: 130.188.17.16

Record Tracking

Status: Original
13 December 2022 | 07:42

Holder: Christina Vähävaara
Christina.Vahavaara@vtt.fi

Location: DocuSign

Signer Events	Signature	Timestamp
Nadezhda Gotcheva Nadezhda.Gotcheva@vtt.fi Research Team Leader Security Level: Email, Account Authentication (None), Authentication	DocuSigned by:  E21E683840FD424... Signature Adoption: Pre-selected Style Using IP Address: 91.157.225.98	Sent: 13 December 2022 | 07:45 Viewed: 14 December 2022 | 09:31 Signed: 14 December 2022 | 09:31

Authentication Details
SMS Auth:
Transaction: 66143E247B5C1804919300312F8A08E2
Result: passed
Vendor ID: TeleSign
Type: SMSAuth
Performed: 14 December 2022 | 09:29
Phone: +358 40 1326030

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	13 December 2022 | 07:45
Certified Delivered	Security Checked	14 December 2022 | 09:31
Signing Complete	Security Checked	14 December 2022 | 09:31
Completed	Security Checked	14 December 2022 | 09:31

Payment Events	Status	Timestamps