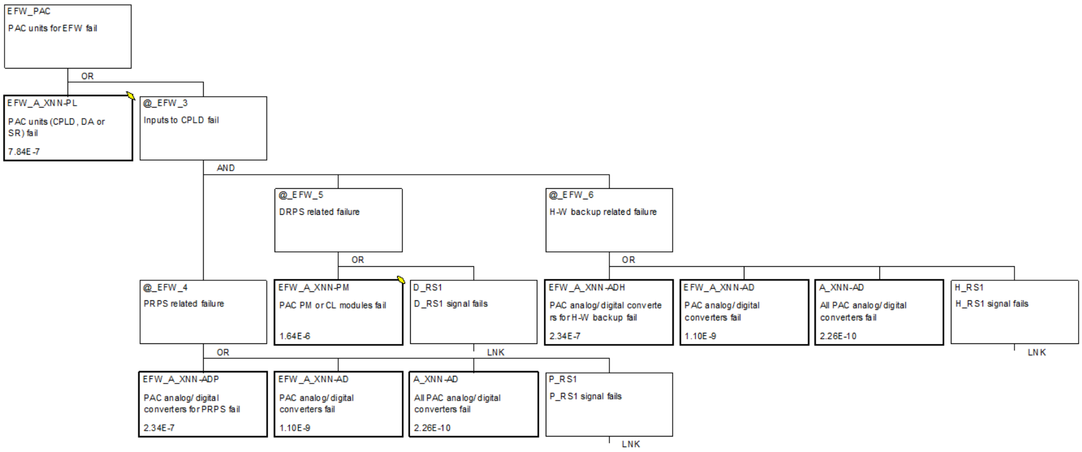
Probabilistic risk model for digital I&C architecture

Tyrväinen, Tero; Björkman, Kim

Published: 18/12/2024

RESEARCH REPORT

VTT-R-00646-24



Probabilistic risk model for digital I&C architecture

Authors:	Tero Tyrväinen, Kim Björkman
Confidentiality:	VTT Public
Version:	17.12.2024

beyond the obvious

Report's title

Probabilistic risk model for digital I&C architecture

Customer, contact person, address VYR	**Order reference** SAFER 4/2024
Project name Probabilistic Risk Assessment Labour, Improvements and Extensions	**Project number/Short name** 137917/PRALINE
Author(s) Tero Tyrväinen, Kim Björkman	**Pages** 45/7
Keywords probabilistic risk assessment, instrumentation and control, common cause failure	**Report identification code** VTT-R-00646-24

Summary

This report presents a preliminary probabilistic risk assessment (PRA) model for the OECD/NEA WGRISK DIGMORE reference case representing digital instrumentation and control (I&C) systems in a simplified boiling water reactor plant. The reference case covers an I&C architecture with several systems, such as the primary and diverse reactor protection system, operational I&C system, hard-wired backup system, and prioritization and actuation control (PAC) systems. The modelling approach selected in this study is to develop a simplified PRA model including only common cause failures (CCFs) and high-level failure events and to perform complex calculations in the background. The approach was selected due to challenges related to CCF calculations, e.g., some CCF groups include more than 8 components.

In the overall results of the PRA model, the I&C systems do not play very important role. This is however partly because of simplifications made in the reference case. Spurious signals causing the main feed-water system to stop (initiating event) are the most important I&C failure events in the results. Concerning failures of safety functions, PAC systems are the most important I&C systems, because they have less redundancy and diversity than the other systems.

In the main PRA analysis, the aim was to follow the reference case description as closely as possible meaning e.g. that the alpha-factor model was applied to hardware CCFs. However, some of the CCF calculations were very complex with the alpha-factor model. Therefore, use of the modified beta-factor model was studied in complementary analyses. It makes the modelling of CCFs much simpler. The beta-factor parameters were estimated using the partial beta-factor method. The partial beta-factor method produced mostly a bit smaller CCF probabilities than the alpha-factor model, but it depended on the assumptions used in the analysis. A complementary analysis case was also developed for spurious stop signals of safety functions.

Confidentiality	VTT Public

Espoo 18.12.2024

Written by	**Reviewed by**
Tero Tyrväinen, Research Scientist	Ilkka Karanta, Senior Scientist

VTT's contact address

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

Distribution (customer and VTT)

SAFER2028 TAG1.1 members, VTT archive

Approval

VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD

Date:	18 December 2024
Signature:	DocuSigned by: Teemu Kärkelä E7B76042F134471...
Name:	Teemu Kärkelä
Title:	Research Team Leader

Contents

List of acronyms

Acronym	Meaning
AC	Air cooler
AD	Analog/digital converter
ADS	Automatic depressurisation system
AI	Analog input
APU	Acquisition and processing unit
AS	Application software
CCF	Common cause failure
CCW	Component cooling water system
CD	Core damage
CDF	Core damage frequency
CL	Communication link
CP	Condensation pool
CPLD	Complex programmable logic device
CV	Check valve
DA	Digital/analog converter
DI&C	Digital instrumentation and control
DO	Digital output
DRPS	Diverse reactor protection system
DWST	Demineralized water storage tank
ECC	Emergency core cooling system
EFW	Emergency feed-water system
ESF	Engineered safety features
HVA	Heating, venting and air conditioning system
HW	Hardware
HWBS	Hard-wired backup system
H-W	Hard-wired
HX	Heat exchanger
I&C	Instrumentation and control
IDN	Inter-division network
LMFW	Loss of main feed-water
MCR	Main control room
MFW	Main feed-water system
MP	Motor-operated pump
MV	Motor-operated valve
NEA	Nuclear energy agency
NPP	Nuclear power plant
OECD	Organisation for economic co-operation and development
OIC	Operational instrumentation and control
OS	Operating system
OP	Operating system/platform software
PAC	Priority and actuation control
PM	Processor module
PRA	Probabilistic risk assessment

Acronym	Meaning
PRPS	Primary reactor protection system
PSA	Probabilistic safety assessment
PTU	Periodic testing unit
RCO	Reactor containment
RHR	Residual heat removal system
RPV	Reactor pressure vessel
RS	Reactor scram system
RTS	Reactor trip system
SL	Sensor measuring water level
SP	Sensor measuring pressure
SR	Sub-rack
ST	Sensor measuring temperature
SWS	Service water system
VU	Voting unit
WDT	Watchdog timer
WGRISK	Working group on risk assessment

1. Introduction

Reliability analysis of digital instrumentation and control (I&C) systems is challenging 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. 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 systems that are used to actuate safety functions in nuclear power plants, and it is not acceptable to use too conservative failure probability estimates in probabilistic risk assessment (PRA). The topic has been studied for a long time (Chu et al., 2010; Liang et al., 2020; Tyrväinen, 2021; Björkman, 2023), some practical methods have been developed specifically for the PRA of digital reactor protection systems (Authen et al., 2015), and digital I&C 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 often modelled in overly simplified and conservative manner in PRAs.

Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI) Working Group on Risk Assessment (WGRISK) 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, 2024a; Porthin et al., 2023). 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 similar 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, detailed understanding and analysis of the system is required in any case. The modelling can usually focus on CCFs because only those are typically relevant for the overall results.

In 2022, a new WGRISK task called DIGMORE – A realistic comparative application of DI&C modelling approaches for PSA was started. It also contains 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 work should achieve an in-depth understanding of PRA relevant impacts of interactions within the entire I&C architecture. The overall goal is to provide recommendations for the development of PRA models concerning digital I&C systems.

This report develops a PRA model for the DIGMORE reference case (OECD NEA CSNI, 2024c). The model is developed for the ‘base case,’ which has been finalized. The DIGMORE reference case will also cover various different architecture and design alternatives that have not been defined at this point and are therefore not modelled. However, in this report, complementary analyses are also performed for the reference case, including comparison of different CCF models and modelling of additional spurious signals.

2. Reference case description

This chapter gives a brief description of the DIGMORE reference case (OECD NEA CSNI, 2024c).

2.1 Reference plant

The reference plant is the same as in the DIGMAP project (OECD NEA CSNI, 2024a). It is a generic and simplified boiling water reactor plant. The layout of main safety systems is presented in Figure 1. The safety systems are listed in Table 1. For simplicity, each safety system, except for the I&C systems, contains only one train. However, the failure rates/probabilities of the components have been multiplied by 0.01 so that the failure probabilities of the safety systems are at a more realistic level.

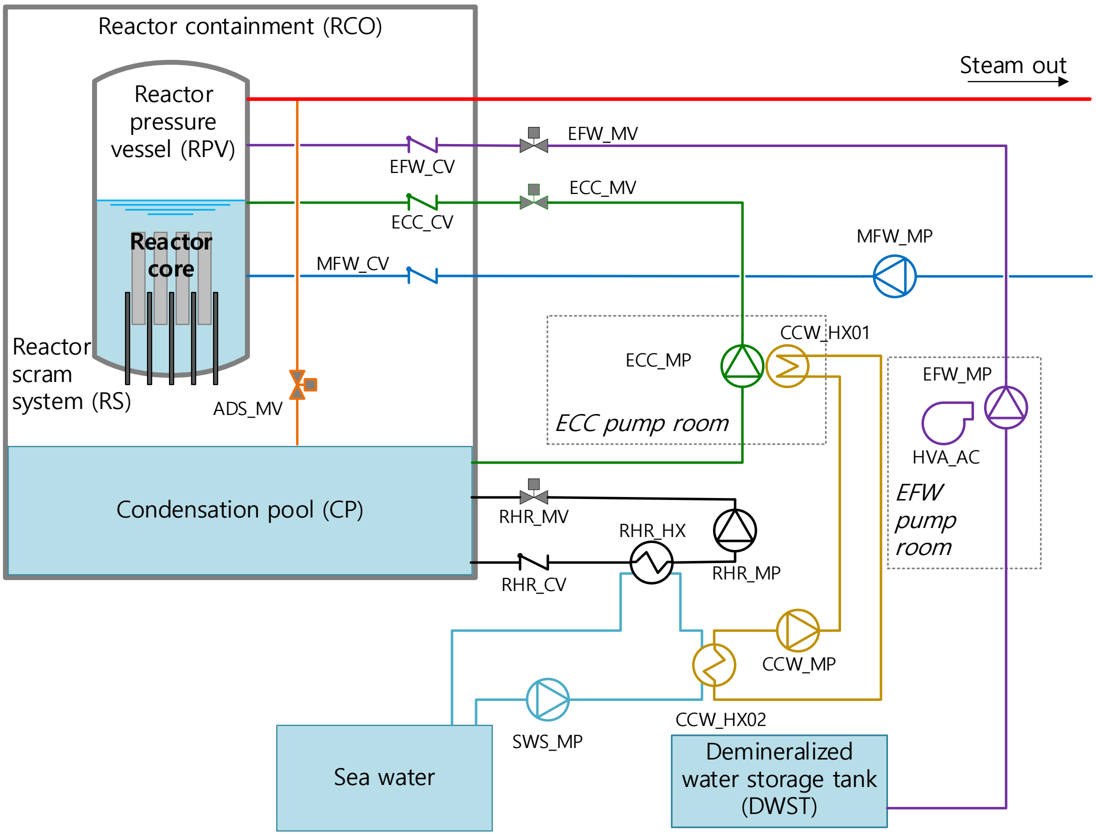


Figure 1. The layout of main safety systems (OECD NEA CSNI, 2024c).

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**
Heating, venting and air conditioning system	**HVA**
Main feed-water system	**MFW**
Residual heat removal system	**RHR**
Reactor scram system	**RS**
Service water system	**SWS**

2.2 Overall I&C architecture

The I&C systems of the reference case include the primary reactor protection system (PRPS), diverse reactor protection system (DRPS), operational I&C system (OIC), hard-wired (H-W) backup system (HWBS), and priority and actuation control systems (PAC-A and PAC-B). The architecture of I&C systems is presented in Figure 2. When the measurement data indicates a need for safety function actuation, the PRPS, DRPS and HWBS send actuation signals to the PAC systems and the reactor trip system (RTS). The PAC systems prioritize the input signals and send actuation signals to the safety systems (the systems in Table 1, except for MFW and RS). The OIC system provides digital signals to the MFW system. Different I&C systems have human-machine interfaces in the main control room (MCR). The number of divisions in each system is indicated in the lower right corner of the box representing the system (e.g. 4x for the PRPS). Safety systems are considered successfully actuated if actuation signals are received from two PAC units (2-out-of-4). Different safety systems have separate PAC units. The I&C systems are described in more detail in the following subsections.

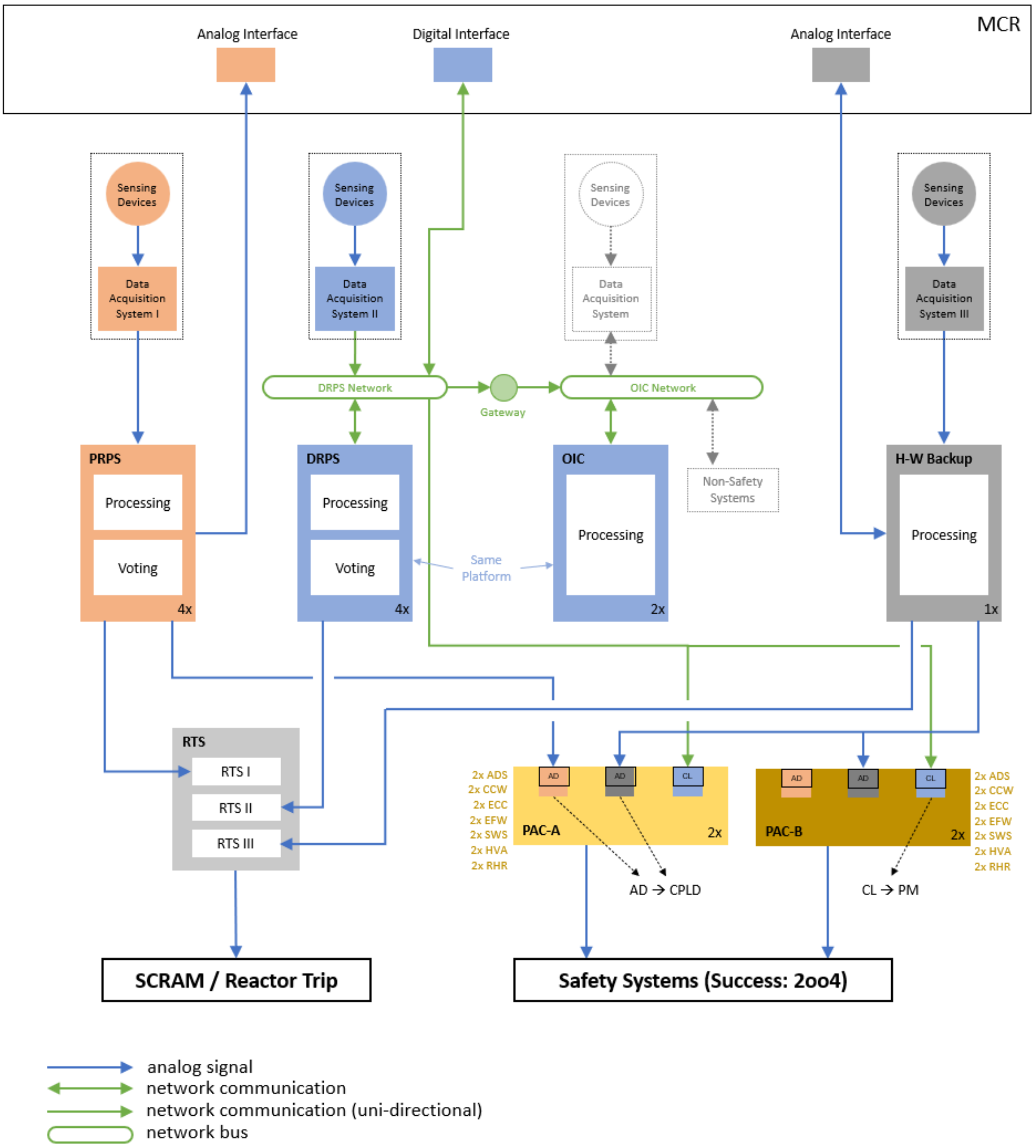


Figure 2. The architecture of I&C systems (OECD NEA CSNI, 2024c).

2.3 Primary reactor protection system

The PRPS is the same reactor protection system that was modelled in the DIGMAP project (OECD NEA CSNI, 2024a). It consists of two diverse subsystems, PRPS-A and PRPS-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 PAC systems. 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 PRPS is presented in Figure 3. The actuation signals of components are summarised in Table 2.

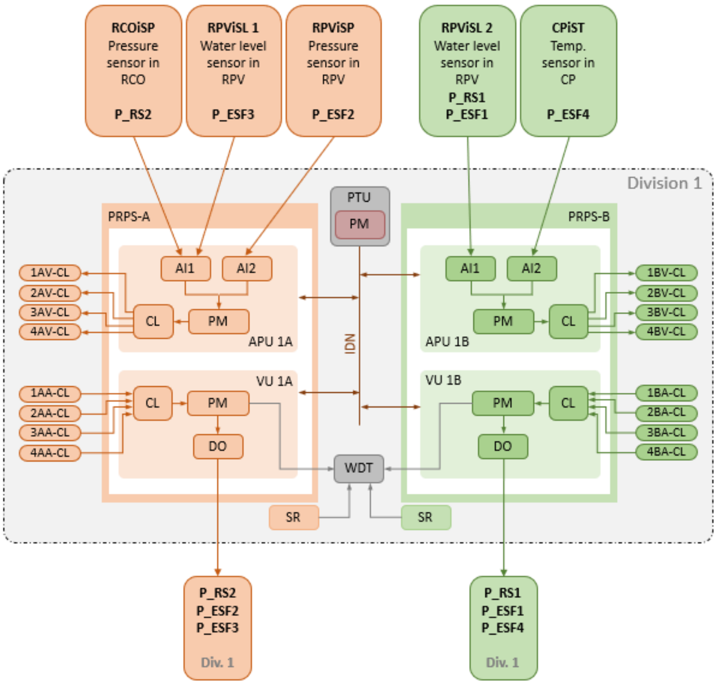


Figure 3. Primary reactor protection system layout (OECD NEA CSNI, 2024c).

Table 2. Actuation signals ('+' is the logical OR in the signal definitions).

System	Component	Control	Conditions	Signal
RS	Control rod breakers	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

System	Component	Control	Conditions	Signal
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	ESF3: low water level in reactor	ESF3
SWS	Pump	Start	RS2: high pressure in containment ESF3: low water level in reactor ESF4: high temperature in condensation pool	RS2+ESF3+ESF4

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 the 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.

Each processor module consists of HW, operating system (OS) and application software (AS). Other I&C modules consist of HW and operating system/platform software (OP). The reference case description (OECD NEA CSNI, 2024c) contains fictive reliability parameters for HW, OP and AS of each module. OP and AS failure probabilities are defined on demand basis, and they are assumed to be always undetected. For HW failures, failure rate is given, and it is 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.

2.4 Diverse reactor protection system

The DRPS is quite similar to the PRPS. It however contains only one subsystem that can actuate all safety systems. The sensors are connected to the system by a DRPS network, and each sensor has a CL module. The system also does not contain AI modules, but the signals from the sensors are received by CL modules. The system sends analog outputs to the RTS using the DO modules (it actually sends analog signals, but it is called a digital output module because the signals are binary) and digital outputs to the PAC units through the DRPS network using CL modules. There are no PTUs for failure detection, only WDTs. The layout of the system is presented in Figure 4.

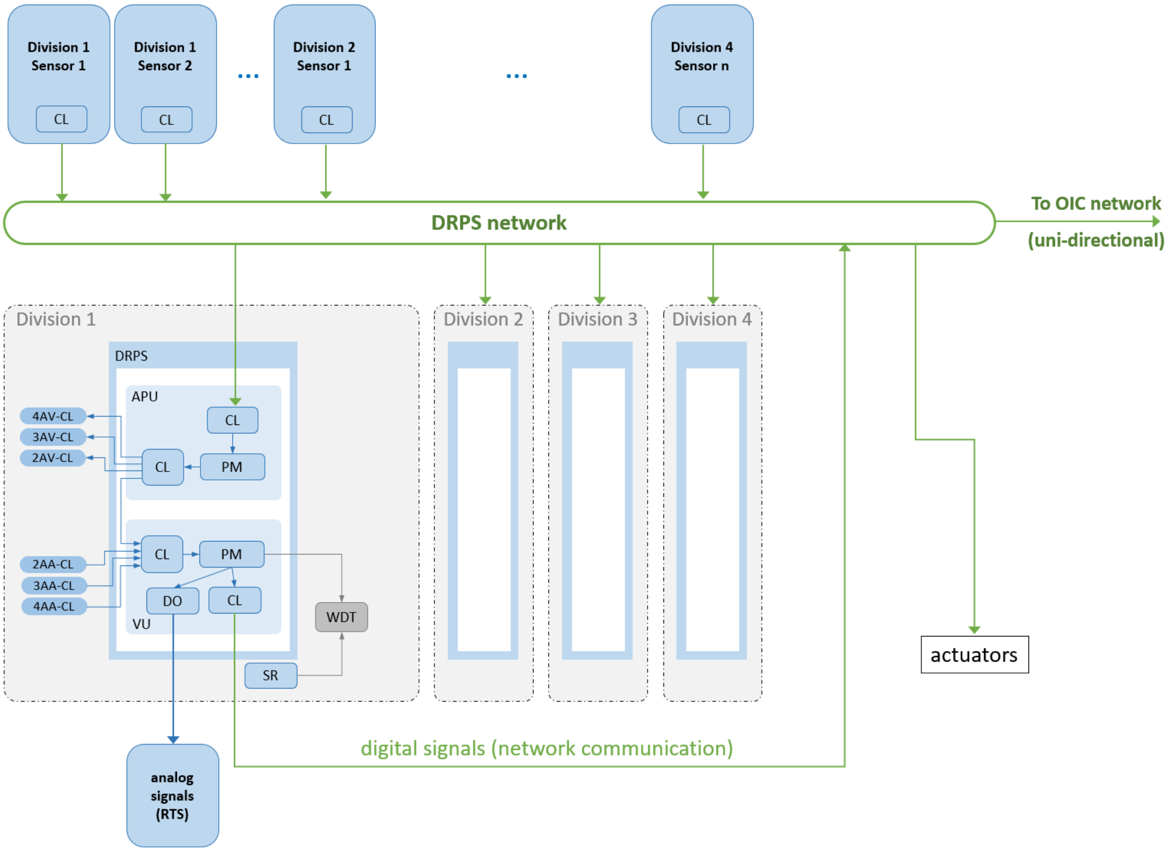


Figure 4. Diverse reactor protection system layout (OECD NEA CSNI, 2024c).

The DRPS has sensors for the same measurements as the PRPS, and the actuation signals of the DRPS are identical to the actuation signals of the PRPS.

2.5 Operational I&C system

The OIC system controls the MFW system in the reference case. It contains two divisions that are connected by a network. Both divisions include a PM that is connected to the network through a CL. One division has priority over the other in conflicting situations. Through the network, the system sends digital control signals to the MFW system. The layout of the system is presented in Figure 5.

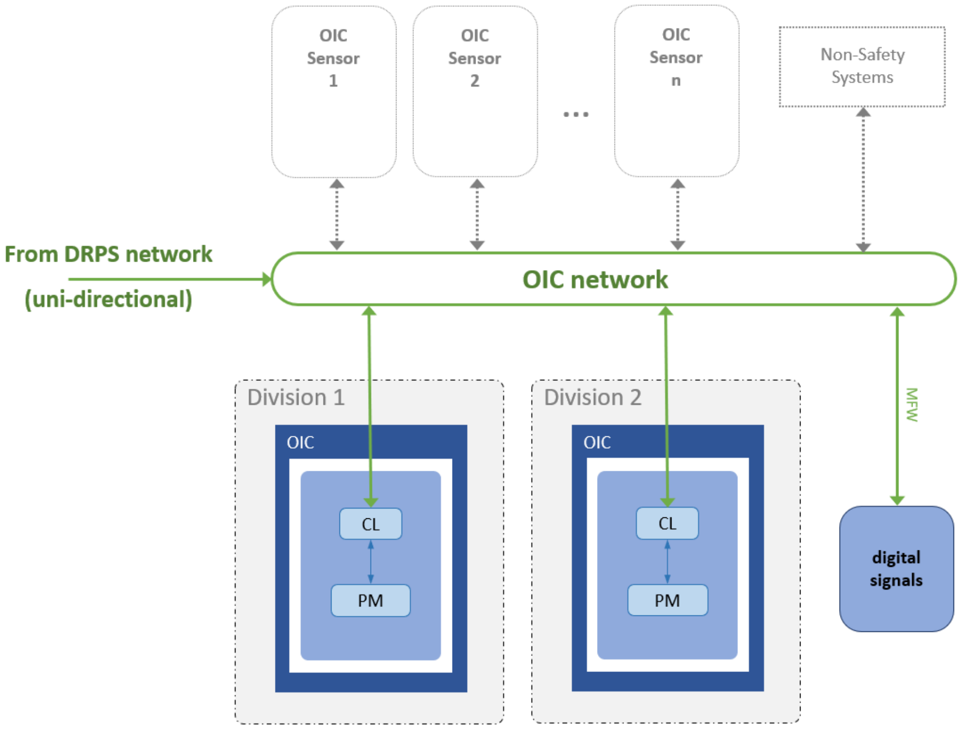


Figure 5. Operational I&C system layout (OECD NEA CSNI, 2024c).

The sensors of the OIC do not have relevance in the reference case. Instead, the OIC system uses the water level measurements from the DRPS. The OIC network is connected to the network of the DRPS. If two water level sensors in the reactor pressure vessel show high value, the MFW system is stopped.

2.6 Hard-wired backup system

The HWBS works only based on manual commands executed from the MCR. It does not include any redundancy. It is modelled as a black box with only one basic event. It has one set of measurements that are identical to the measurements of the PRPS in one division. The actuation signals of the HWBS are identical to the PRPS signals.

2.7 Priority and actuation control

The PAC systems control safety-related actuators. A PAC unit receives input signals from the PRPS, DRPS and the HWBS, prioritizes the signals, and sends the calculated output signal to the actuator. There are four PAC units for each safety system, i.e. one for each PRPS and DRPS division per system. There are two diverse types of PAC units: PAC-A and PAC-B. For each system, there are two PAC-A units and two PAC-B units. The layout of a PAC unit is presented in Figure 6. The layouts and reliability data of PAC-A and PAC-B are identical.

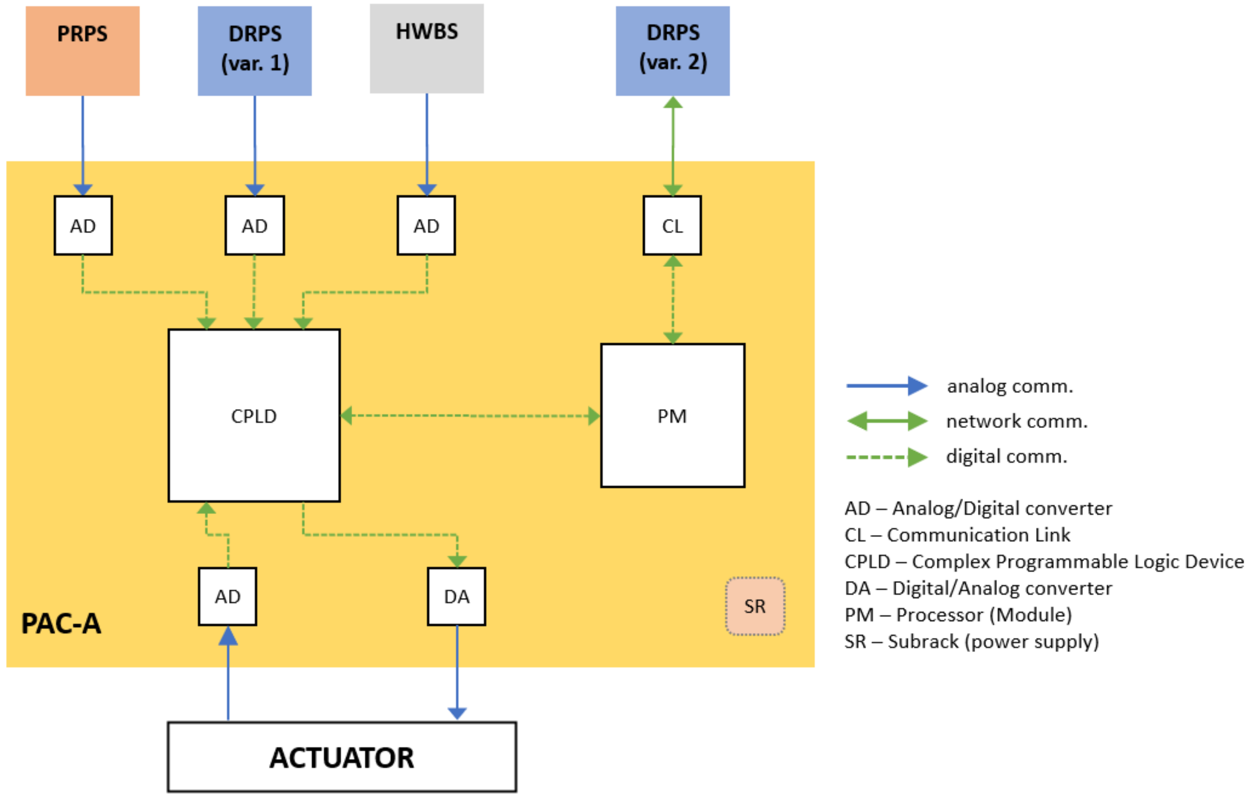


Figure 6. The layout of a PAC unit (OECD NEA CSNI, 2024c).

A PAC unit contains analog/digital converters (AD) for the input signals, a complex programmable logic device (CPLD), a digital/analog converter (DA) for the output signal, a PM, a CL, and an SR. Analog inputs from the PRPS and HWBS are handled using the AD modules. For handling the signal from the DRPS, there are two variants in the reference case: an AD module receives an analog signal from a DO module of the DRPS (var. 1) or a CL module receives a digital signal from a CL module of the DRPS (var. 2). Variant 2 is used in the base case of DIGMORE and modelled in this document. The prioritization of signals is performed in the CPLD. The priority order of the systems is (1) the PRPS, (2) the DRPS and (3) the HWBS.

Automatic testing of all other modules is performed by the PM. Automatic testing of the PM is performed by a watchdog, which is not included in the modelling case explicitly.

3. PRA model for DIGMORE base case

3.1 Event tree

Loss of main feed-water is the only accident scenario analysed in the benchmark study. The event tree is presented in Figure 7 and it is also given in the model description (OECD NEA CSNI, 2024c) to the participants of the benchmark study.

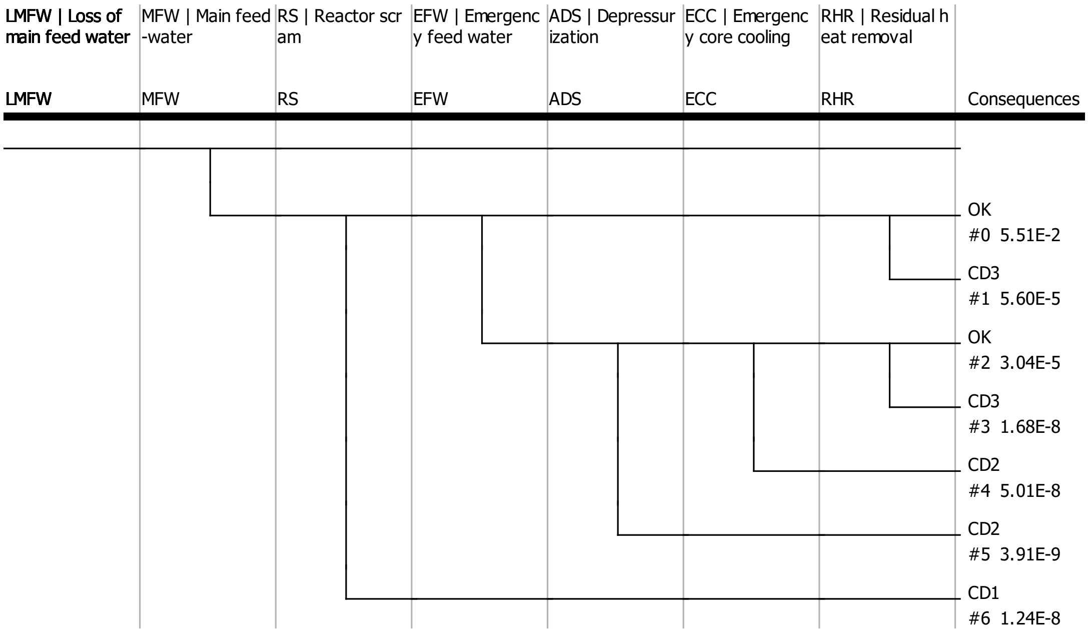


Figure 7. Event tree for loss of main feed-water.

The real initiating events are modelled in the MFW fault tree, and LMFW is a dummy event with probability 1.

3.2 Modelling approach and level of detail

For this study, a simplified modelling approach was selected due to challenges related to CCF modelling. Particularly, the reference case contains 28 PAC units that are divided into two CCF groups with 14 components. There is no way to perform such CCF calculations within the PRA model, if the alpha-factor model is applied as recommended in the reference case description (OECD NEA CSNI, 2024c). Therefore, the CCF calculations are performed in Excel, and only high-level CCF basic events are included in the PRA model. The approach is the same as used in VTT's final DIGMAP model (OECD NEA CSNI, 2024a & 2024b), though the modelling of PAC units differs to some extent from the modelling of the other systems.

All the basic events in the PRA model represent CCFs or high-level failure events (except for H-W backup system failures as there is only one redundancy), and the fault trees represent joint failures of redundant trains instead of only one train. CCFs are modelled separately for different modules and for AS, OP and HW. For each module, there is only one HW basic event (representing CCF) combining failures detected by different fault-tolerant techniques. Fault-tolerant techniques have been taken into account in background calculations only as described in Section 3.3.

3.3 Probabilities of hardware failure basic events

The failure data of HW failures is divided according to fault tolerant features (OECD NEA CSNI, 2024c) as presented in Table 3 for the PRPS. In the table, F refers to full-scope testing, A refers to automatic testing and P refers to periodic testing. The failure rates are divided for different fault tolerant techniques according to the fractions given in the table. Some failures can be detected only by full-scope test (the F column) and some failures can be detected by two or three fault tolerant techniques (AF, PF and APF columns). It is assumed that all HW failures are detected in full-scope testing if they are not detected by other means. For example, 60% (P(AF)+P(APF) = 0.4+0.2) of HW failures of an APU AI module are detected primarily by automatic testing (performed by the PM of the APU) and 20% primarily by periodic testing (performed by PTU). Failures that can be detected both by automatic testing and periodic testing (APF) are primarily detected by automatic testing because it is performed in real time. If automatic testing fails, one third (0.2/0.6) of failures that would have been detected by automatic testing are detected by periodic testing.

Table 3. PRPS hardware failure rates and failure detection coverages (OECD NEA CSNI, 2024c).

Module	Failure rate (/h)	F	AF	PF	APF
APU AI	2E-6	0.2	0.4	0.2	0.2
APU PM	2E-6	0.1	0.7	0.1	0.1
APU CL	5E-6	0.2		0.8	
VU DO	2E-6	0.2		0.8	
VU PM	2E-6	0.1	0.7	0.1	0.1
VU CL	5E-6	0.2		0.8	
PTU PM	2E-6	1			
PTU IDN	1E-6	0.8		0.2	
SR	2E-6		0.9	0.1	

For other systems, there are similar tables (OECD NEA CSNI, 2024c), but those are simpler, because periodic testing is only considered for the PRPS. This means that the failures of the other systems are only divided into F and AF categories.

The computation of HW failure probability can be divided into two parts: unavailability before detection and unavailability after detection. The unavailability after detection can simply be calculated as

$$P_d = \lambda T_r, \tag{1}$$

where λ is the failure rate and T_r is the mean time to repair (8 hours in each case). The total failure rate can be used here, because all failures are assumed to be detected sooner or later.

In the computation of unavailability before detection, the contributions of all failures not detected by automatic testing are combined. These failures can be classified as follows:

1. Failures that are detected by full-scope testing only
2. Failures that are primarily detected by periodic testing
    a. Failures detected by periodic testing
    b. Failures detected by full-scope testing because of a failure of a component needed in periodic testing
3. Failures that are not detected by automatic testing because of a failure of a component needed in automatic testing
    a. Failures detected by periodic testing
    b. Failures that cannot be detected by periodic testing and are detected by full-scope testing
    c. Failures detected by full-scope testing because of a failure of a component needed in periodic testing.

In the DIGMAP project, supporting fault trees (not appearing in the actual PRA model) were used to calculate the unavailability before detection for each module type. In this study, those calculations have been performed using spreadsheets, which was found a more compact and better structured approach. However, as the fault trees are more suitable for illustration, the supporting fault tree of an APU CL failure in the PRPS is presented in Figure 8. In it, basic event APUCL_F represents failures detected only by full-scope testing (case 1 above), and basic event APUCL_P represents failures detected by periodic testing (case 2a above). The probabilities of these basic events are calculated as

$$P_u = 1 - \frac{1}{\lambda T_t}\left(1 - e^{-\lambda T_t}\right), \tag{2}$$

where λ is the failure rate, and T_t is the testing interval. Here, the failure rate is not the total failure rate, but the failure rate related to the detection mechanism ($0.8 \cdot 5.0 \cdot 10^{-6} = 4.0 \cdot 10^{-6}$ for failures detected by periodic testing, and $0.2 \cdot 5.0 \cdot 10^{-6} = 1.0 \cdot 10^{-6}$ for failures detected by full-scope testing). The testing interval is 24 hours for periodic testing and half a year for full-scope testing. The AND gate in the fault tree is related to scenarios where periodic testing fails, and the failures can only be detected by full-scope testing (case 2b above). Basic event APUCL_PF represents failures that would have normally been detected by periodic testing, but are detected by full-scope testing in this scenario. There are six basic events causing the failure of periodic testing in the PTU:

1. PTUPM_F: HW failure of the PM in the PTU,
2. PTUIDN_F: HW failure of the IDN detected by full-scope testing,
3. PTUIDN_P: HW failure of the IDN detected by periodic testing,
4. PTUPMOP_N: OP failure of the PM in the PTU,
5. PTUPMAS_N: AS failure of the PM in the PTU,
6. PTUIDNOP_N: OP failure of the IDN.

The probability of APUCL_PF has been calculated according to equation (2). The testing interval is half a year. The probabilities of basic events PTUPM_F, PTUIDN_F and PTUIDN_P are sum values of values calculated using equations (1) and (2).

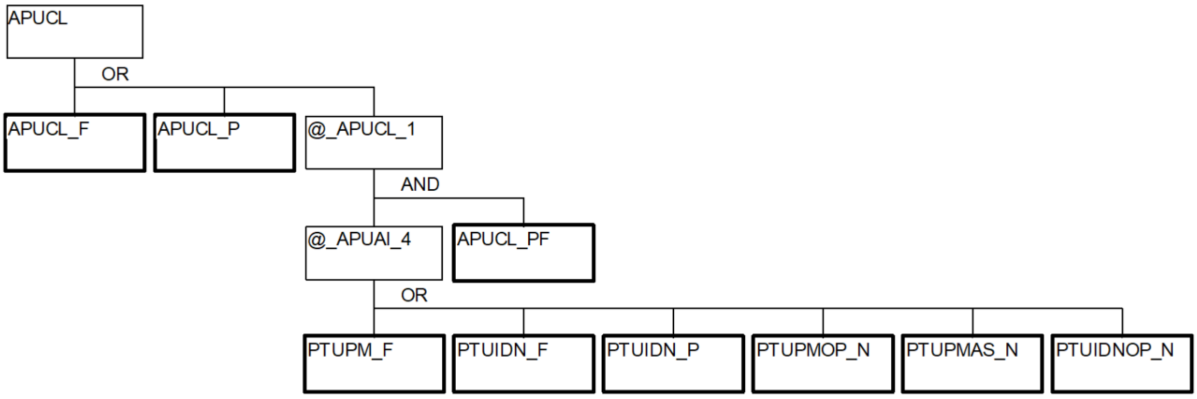


Figure 8. Fault tree of undetected APU CL failure.

The fault tree produces the following minimal cut sets:

S1-sum 2.29E-03

Num	Prob.	%	Cumul	Prob	Name
1	2.19E-03	95.53	95.53	2.19E-03	APUCL_F
2	4.80E-05	2.10	97.62	4.80E-05	APUCL_P
3	3.82E-05	1.67	99.29	8.71E-03 4.38E-03	APUCL_PF PTUPM_F
4	1.53E-05	0.67	99.96	8.71E-03 1.76E-03	APUCL_PF PTUIDN_F

5	8.71E-07	0.04	100.00	8.71E-03 APUCL_PF 1.00E-04 PTUPMAS_N
6	8.71E-08	0.00	100.00	8.71E-03 APUCL_PF 1.00E-05 PTUIDNOP_N
7	8.71E-08	0.00	100.01	8.71E-03 APUCL_PF 1.00E-05 PTUPMOP_N
8	3.48E-08	0.00	100.01	8.71E-03 APUCL_PF 4.00E-06 PTUIDN_P

The total unavailability before detection is 2.29E-3. It is conservative to multiply the probability of APUCL_PF directly with the probabilities of PTUPM_F, PTUIDN_F and PTUIDN_P, because the PTU failure needs to occur before the APU CL failure so that the CL failure is not detected, but this formula just multiplies the unavailabilities. In addition, PTUIDN_P is detected in 24 hours. A more accurate way to perform the calculations could be found, but it would require information about the test times, such as the difference between the full-scope test times of the CL and PTU. The approximation obtained by multiplying the unavailabilities is considered sufficient, because the CL failure probability is dominated by APUCL_F.

The unavailability before detection and unavailability after detection are summed to calculate the HW basic event probability to be used the main model. For APU CL, the probability is 2.29E-3 + 4.00E-5 = 2.33E-3.

The CL failure analysis was presented above, because it is among the simplest analysis scenarios from the PRPS. Analysis of processor modules and sub-racks is more complicated, because also the failure of the automatic testing needs to be included in the analysis. The analyses are not presented here, but the principles are the same as in the CL case. SR is the only case where failures of fault tolerant techniques contribute significantly to the total probability, because all failures are detected either by automatic testing or periodic testing when the WDT and PTU are working. Because of the same reason, the failure probability of a SR is quite small and larger portion of the total probability comes from the unavailability after detection. In most other cases, the unavailability after detection is significantly smaller than the unavailability before detection.

3.4 Common cause failures

In the DIGMORE project, the participants have freedom to choose their own assumptions for CCF modelling. However, there is a recommendation to use the alpha-factor model with parameters given in the reference case description (OECD NEA CSNI, 2024c) or the beta-factor model with beta-factor 1. The alpha-factor parameters are given for groups with up to 16 components. These parameter values are generic and originate from (Wierman et al., 2000). In the reference case, there are some CCF groups that include more than 16 components, which means that there is no clear recommendation for the modelling of those groups.

In general, we have applied the alpha-factor model and recommended parameters to HW CCF groups with 16 or less components. For groups with more than 16 components, the modified beta-factor model is applied, and the beta-factors are estimated using the partial beta-factor method (Bao et al., 2022). The only difference between the traditional beta-factor model and the modified beta-factor model is that in the modified beta-factor model, a component can belong to multiple CCF groups. This enables modelling of CCFs at different levels, e.g. between redundant divisions, between subsystems and between systems.

For the PRPS, the same CCF groups are assumed as in the DIGMAP project (OECD NEA CSNI, 2024a). In the main case of DIGMAP, only functional diversity was assumed between the PRPS subsystems, i.e. the components in different subsystems were assumed identical. Therefore, CCFs between subsystems were modelled in all cases, except for AS modules in APUs and sensors. The largest CCF group was the group of AI modules, which included 16 components, whereas most of the groups included eight components. Software CCFs were modelled assuming complete dependency (beta-factor 1). The probability of AS CCF was 1E-4, and the probability of OP CCF was 1E-5 in each case.

For the DRPS, mostly similar CCF assumptions are used as for the PRPS. Most of the CCF groups include only four components. However, there are 20 identical CL modules related to the sensors of the system. The probability of AS CCF is 1E-3, and the probability of OP CCF is 1E-4 in each case.

For PAC systems, there are two groups of 14 identical PAC units. This means that there are two groups of 28 AD modules, whereas for other modules, the group size is 14. HW CCFs are modelled using the alpha-factor model or the modified beta-factor model depending on the group size. The probability of OP CCF is 1E-5 for every relevant module type.

3.4.1 Alpha-factor calculations

Only CCFs that cause one or multiple safety functions to fail are included in the PRA model explicitly. The CCFs that have the same system level effect are merged into the same basic event. For example, all PRPS APU communication link HW CCFs with at least three failures in one specific subsystem are merged into one basic event, because the failure criterion is 3-out-of-4. However, those APU communication link HW CCFs with at least three failures in both subsystems are modelled with a separate basic event. In total there are three APU communication link HW CCFs that are modelled: CCF in PRPS-A (but not in B), CCF in PRPS-B (but not in A), and CCF in both subsystems. The CCF in both subsystems is modelled in FinPSA as a CCF of the subsystem specific events with the Q-factor model. All CCF groups in the RPS, and most CCF groups in the DRPS (with exception of the 20 CL modules related to the sensors) are handled in a similar manner.

The probabilities of the HW CCF basic events are calculated in Excel. In addition to normal alpha-factor computations, this requires quite complex combinatorial calculations to manage the CCF combinations with group sizes of 8 and 16. The numbers of combinations with difference failure effects are presented in Table 4 for group size of 8 and Table 5 for group size of 16. The CCF calculations are performed based on single failure probability calculations discussed in Section 3.3.

Table 4. Numbers of CCFs causing failure of one PRPS subsystem or both with 3-o-o-4 criterion.

Number of failures	Only PRPS-A fails	Both PRPS-A and PRPS-B fail
1		
2		
3	4	
4	17	
5	28	
6	6	16
7		8
8		1

Table 5. Numbers of CCFs causing failure of specific AI modules with 3-o-o-4 criterion.

Number of failures	Only AI1 in PRPS-A fails	Only AI1 fails in PRPS-A and PRPS-B	Only AI1 and AI2 fail in PRPS-A and AI1 fails in PRPS-B	AI1 and AI2 fail in PRPS-A and PRPS-B
1				
2				
3	4			
4	49			
5	276			
6	898	16		
7	1792	136		
8	2124	513		
9	1296	1000	64	
10	216	988	304	
11		336	588	
12		36	337	256
13			76	256
14			6	96
15				16
16				1

With this approach, an important question is how to ensure that the risk is not underestimated, because minimal cut sets with single failures or two or more CCFs are left out, e.g. minimal cut sets including CCF of two VU CLs and a single failure of a VU PM. Therefore, to make the estimates presumably conservative, the calculated CCF basic event probabilities are multiplied by 1.1, i.e. 10% is added to the probabilities. Based on the comparisons made in DIGMAP and other tests, this factor 1.1 has been observed to be sufficient. The contribution of those other combinations can well be several percents in some cases but unlikely over 10%. For some components with smaller failure probabilities, the contribution can be higher when a CCF/failure is combined with a CCF/failure of components with larger failure probabilities, but that can be considered to be covered by the CCF probability related to the CCF group with the larger failure probability in this simplified approach.

3.4.2 CCF calculations for PAC units

There are two diverse types of PAC units: PAC-A and PAC-B. In total, there are 14 units of both types. Therefore, for each PAC module type (except for AD modules), there are two CCF groups with 14 components.

Since for each system there are two PAC-A units and two PAC-B units, and the failure criterion is 3-out-of-4, a failure of a system due to PAC failures requires a combination of at least two CCFs, three single failures, or a CCF and a single failure. This makes the analysis much more complicated than in the cases where a single CCF can cause the failure of the system. A simple solution would, of course, be to use the modified beta-factor model, but we apply the alpha-factors for HW CCFs as those are recommended in the reference case description. As an alternative, the modified beta-factor model is applied in a comparison presented in Section 4.1.1.

A Visual Basic script has been developed to go through all the combinations with a CCF or single failure from both groups. In total, it makes 268402689 combinations. For each combination,

1. each system is gone through, and for each system it is checked, if the system fails due to the combination (i.e. at least three PAC units fail).
2. the number of failed systems is calculated.
3. the probability of the combination is calculated based on the alpha-factor formulas.
4. the probability is added to the results vector based on how many systems failed.

For this analysis, CPLD, DA and SR modules are merged together as their failures have the same system level impact. This is the most convenient way to handle combinations where different module types fail (e.g. CPLDs in PAC-As and DAs in PAC-Bs). The CCF calculations are performed based on the joint failure probability. Similarly, CL and PM modules are merged together for the calculations.

Software CCFs are also taken into account in the calculations, including combinations with

- a software CCF and a HW failure or HW CCF
- two software CCFs (which causes failure of all systems)

The first case is managed in the same way as the combinations that only include HW failures/CCFs, though the script is slightly simpler as there is only one software CCF to consider (the one in which all modules in the group fail).

The result of the analysis is the PAC (3-out-of-4) failure probability for one specific system, for two specific systems, for three specific systems, etc. The results are presented in Table 6, and those probabilities are used in the PRA model. Note that in the case of CL and PM failures, the whole system does not fail but only the connections of the PACs to the DRPS.

Table 6. System level failure probabilities based on PAC failures.

Number of failed systems	CPLD & DA & SR	CL & PM
1	7.84E-7	1.64E-6
2	6.69E-9	1.34E-8
3	1.06E-9	2.04E-9
4	4.11E-10	7.60E-10
5	3.09E-10	5.51E-10
6	4.36E-10	7.56E-10
7	2.31E-9	3.51E-9

It is again important to notice that these calculations are simplified. The calculations do not cover e.g. cases with three single failures or CCFs. Therefore, 10% extra has been added to the probabilities calculated by the script. It was checked that the total contribution of the cases with three single failures would be less than 3%.

The Visual Basic script can be found in Appendix A.

3.4.3 Partial beta-factor method

Bao et al. (2022) propose the partial beta-factor method for digital I&C CCF parameter estimation. It has been used widely in the United Kingdom for non-I&C CCF modelling as part of the unified partial method, though not much anymore.

In the partial beta-factor method, the analyst gives scores (A, B, C, etc.) to several subfactors that affect the CCF probability depending on how good the defense against CCFs is. After that, the beta-factor is calculated simply by summing table values related to the scores of the subfactors. The table values related to different scores and subfactors are presented in Table 7, and the beta-factor is calculated with the following formula:

$$\beta = \frac{\sum_{i=1}^{8} v_i}{51000},$$

where v_i is the table value of i:th subfactor. Rules for scoring the subfactors can be found from (Lindberg, 2007). For the redundancy (& diversity) subfactor, the rules are presented in Table 8.

Table 7. Beta-factor estimation table of the partial beta-factor method.

Subfactor	A	A+	B	B+	C	D	E
Redundancy (& diversity)	1800	882	433	212	104	25	6
Separation	2400		577		139	33	8
Understanding	1800		433		104	25	6
Analysis	1800		433		104	25	6
Man-machine interface	3000		721		173	42	10
Safety culture & training	1500		360		87	21	5
Control	1800		433		104	25	6
Tests	1200		288		69	17	4

Table 8. Rules for the scores of the redundancy (& diversity) subfactor (Lindberg, 2007).

Score	Rule
A	Minimum identical redundancy (e.g. 1oo2, 2oo3, 3oo4 for success).
A+	Enhanced identical redundancy (e.g. 1oo3, 2oo4 for success).
B	Robust identical redundancy (e.g. 1oo4, 1oo5, 2oo5 etc.).
B+	Unusually high identical redundancy (1oo≥8).
C	Enhanced identical redundancy (e.g. 1oo3) with functional diversity OR Robust identical redundancy (e.g. 1oo≥4) with operational diversity. OR Unusually high identical redundancy (1oo≥8) in a passive system.
D	Robust identical redundancy (1oo≥4) with functional diversity.
E	Two entirely diverse independent redundant sub-systems.

For the DIGMORE case, the beta-factor parameters for two specific HW CCF groups are estimated using the partial beta-factor method. Since the case is fictive, the scores of the subfactors are mostly assumed without deeper consideration. However, the redundancy (& diversity) subfactor is judged based on the rules presented in (Lindberg, 2007), even though the rules are not directly applicable to the asymmetric cases of DIGMORE.

The cases where the partial beta-factor method is used are:

1. Two CCF groups with 28 PAC AD modules. All subfactors, except redundancy (& diversity), are assumed to have score D. CCFs are modelled in three different levels:
   - 2 redundant AD modules that take input from the same system (PRPS or HWBS) and serve the same front-line safety system. The redundancy (& diversity) subfactor has score A. The resulting beta-factor is 0.0390.
   - 4 AD modules that serve the same front-line safety system. The redundancy (& diversity) subfactor has score A+. The resulting beta-factor is 0.0208. The redundancy score cannot be directly deduced from (Lindberg, 2007) for this asymmetric case, but A+ corresponds to 2-out-of-4 case. It could maybe be argued that there is some functional diversity, which could even lead to score C, but A+ is a conservative choice.
   - All 28 AD modules in the group. The redundancy (& diversity) subfactor has score C. The resulting beta-factor is 0.00565. Again, this asymmetric case cannot directly by judged by the rules in (Lindberg, 2007), but C is the most conservative choice as there is clearly functional diversity.
2. 20 CL modules related to DRPS sensors. All subfactors, except redundancy (& diversity), are assumed to have score C. CCFs are modelled in two different levels:
   - 4 redundant CL modules related to identical sensors. The redundancy (& diversity) subfactor has score A+. The resulting beta-factor is 0.0325.
   - All 20 CL modules in the group. The redundancy (& diversity) subfactor has score C. The resulting beta-factor is 0.0173. Again, this asymmetric case cannot directly by judged by the rules in (Lindberg, 2007), but C is the most conservative choice as there is clearly functional diversity.

For the AD modules in PAC, the modelling problem is somewhat similar to other PAC modules (see Section 3.4.2). There are two CCF groups, one for PAC-A and one for PAC-B. To have a 3-out-of-4 failure, two CCFs, a CCF and a single failure, or three single failures are required. Normally there would not be any problem in modelling the CCF events in fault trees. However, since in the other cases only 3-out-of-4 failures are modelled in the fault trees, the same level of detail in modelling is also applied to the AD modules. Probabilities are calculated for three cases:

1. 3-out-of-4 failure of AD modules that take input from the same system (PRPS or HWBS) and serve the same front-line safety system. The probability is calculated as $4SR + R^2 + 4S^3 + 2(P + A + M)(2S + R) \approx 2.34 \cdot 10^{-7}$, where S is the probability of a single failure, R is the probability of a CCF of two redundant modules, M is the probability of a CCF of four AD modules that serve the same front-line system, A is the probability of a HW CCF of all identical AD modules, and P is the probability of a CCF of a OP software CCF of all identical AD modules.
2. Two 3-out-of-4 failures of AD modules that serve the same front-line safety system (one corresponding to inputs from the PRPS and one corresponding to inputs from the HWBS). The probability is calculated as $M^2 + 2(M + A + P)(2S + R)^2 + 2(A + P)M \approx 1.10 \cdot 10^{-9}$.
3. Failure of all 56 AD modules. The probability is calculated as $(A + P)^2 \approx 2.26 \cdot 10^{-10}$.

3.4.4 Other dependencies

It can be noticed that the PRPS-A and PRPS-B are dependent through the common fault tolerant-techniques (PTUs and WDTs). This dependency is not modelled as it was earlier evaluated to be insignificant for the plant risk (Tyrväinen, 2020), and in the DIGMORE case, it is even more insignificant due to additional defence provided by the DRPS and the HWBS. If there was a need to model the dependency, some more complexity would need to be added to the model, i.e. failures of the PTUs and WDTs would need to be modelled explicitly and failures detected by the PTUs and WDTs would need to be modelled with separate basic events.

In addition, failure of a PAC PM means both that the input from the DRPS is lost and that the automatic failure detection of PAC AD modules is lost. If the PM fails, the AD modules have higher failure probability. This means that there is a dependency between the PAC inputs coming from different systems. However, it was evaluated that the probability of 3-out-of-4 failure in the PM modules and AD modules simultaneously is smaller than 1E-14. Therefore, this dependency was screened out from modelling.

3.5 Spurious signals

Spurious signals to stop the MFW system are modelled as initiating events. In the DIGMORE reference case, it is assumed that the spurious signals can be caused by failures in the PMs of the OIC system or VUs of the DRPS, or the water level sensors of the DRPS. The failure rate for a spurious signal from a PM is 4.6E-7/h (4.03E-3/year) and from a water level sensor 1.33E-7/h (1.17E-3/year). The failure rate of a PM is assumed to cover both HW and software failures. It is conservatively assumed that the safety signals processed by the PM fail at the same time. If a spurious signal comes from a water level sensor (the sensor shows high value spuriously), the signals triggered by a low water level naturally fail at the same time.

The following spurious signal cases are modelled:

1. Spurious signal from the primary PM of the OIC system
2. Two spurious signals due to a CCF of the PMs of the DRPS VUs (but not three)
3. Three spurious signals due to a CCF of the PMs of the DRPS VUs (all safety signals of the DRPS fail)
4. Two spurious signals from the DRPS because two water level sensors show high value (but not three)
5. Three spurious signals from the DRPS because three water level sensors show high value (the corresponding safety signals of the DRPS fail)

The CCF calculations of the PMs of the DRPS and the water level sensors have been performed in Excel in the same way as those that are presented in Section 3.4.1. The calculations are simple as the groups include only four components.

It can be noticed that if there are two spurious signals from the DRPS, only one more failure is required for safety function failure, which means that DRPS failure probability increases considerably. As failures of individual trains are not modelled in the main PRA model, this cannot be explicitly modelled in the PRA model. Instead, this is included in background calculations in a simplified way: the single failure probabilities of two trains are summed and multiplied by the frequency of two spurious signals. The resulting frequencies are added to the cases with three spurious signals because the consequence is the same (loss of main feed-water and failure of safety signals).

It is assumed that a normal failure of the OIC system does not cause the MFW system to stop. Instead, reactor scram is activated if a failure is detected. Failures of the network or CL modules are not modelled as initiating events. Detected failures in the DRPS also do not cause the MFW system to stop.

3.6 Fault trees

The fault trees related to the EFW, the top fault tree for reactor scram and the initiating event fault tree are presented in this section. The other safety functions have been modelled with similar types of fault trees. The model contains in total 59 fault trees.

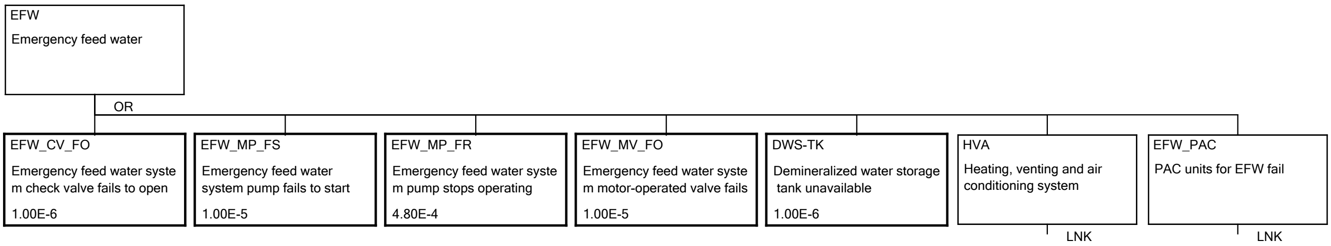

EFW
Emergency feed water
OR
EFW_CV_FO
Emergency feed water syste m check valve fails to open
1.00E-6
EFW_MP_FS
Emergency feed water system pump fails to start
1.00E-5
EFW_MP_FR
Emergency feed water syste m pump stops operating
4.80E-4
EFW_MV_FO
Emergency feed water syste m motor-operated valve fails
1.00E-5
DWS-TK
Demineralized water storage tank unavailable
1.00E-6
HVA
Heating, venting and air conditioning system
LNK
EFW_PAC
PAC units for EFW fail
LNK

Figure 9. Fault tree for the emergency feedwater system.

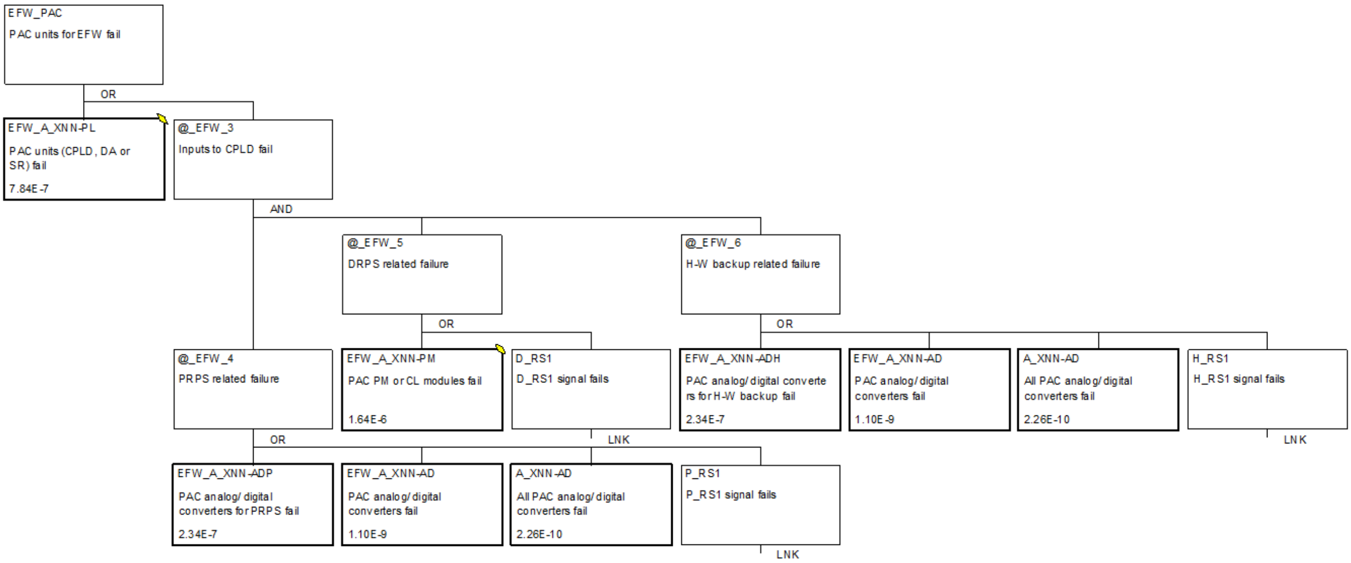


Figure 10. Fault tree for PAC (3-out-of-4 units fail).

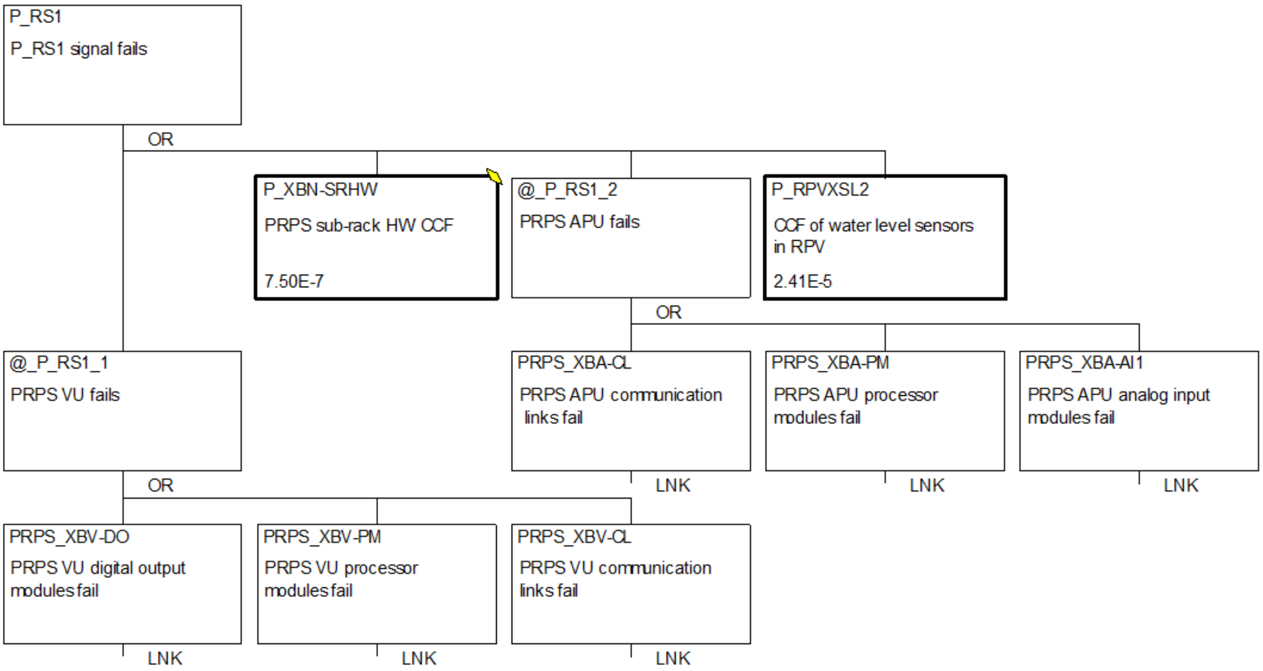

P_RS1
P_RS1 signal fails
OR
P_XBN-SRHW
PRPS sub-rack HW CCF
7.50E-7
@_P_RS1_2
PRPS APU fails
P_RPVXSL2
CCF of water level sensors in RPV
2.41E-5
OR
@_P_RS1_1
PRPS VU fails
PRPS_XBA-CL
PRPS APU communication links fail
LNK
PRPS_XBA-PM
PRPS APU processor modules fail
LNK
PRPS_XBA-AI1
PRPS APU analog input modules fail
LNK
OR
PRPS_XBV-DO
PRPS VU digital output modules fail
LNK
PRPS_XBV-PM
PRPS VU processor modules fail
LNK
PRPS_XBV-CL
PRPS VU communication links fail
LNK

Figure 11. Fault tree for P-RS1 signal from PRPS-B (3-out-of-4 divisions fail).

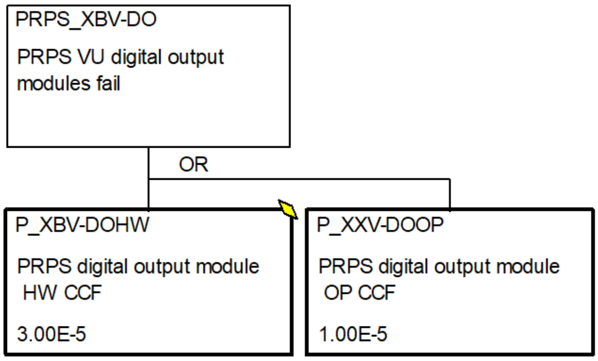

PRPS_XBV-DO
PRPS VU digital output modules fail
OR
P_XBV-DOHW
PRPS digital output module HW CCF
3.00E-5
P_XXV-DOOP
PRPS digital output module OP CCF
1.00E-5

Figure 12. Fault tree for the digital output modules in PRPS voting units (3-out-of-4 divisions fail).

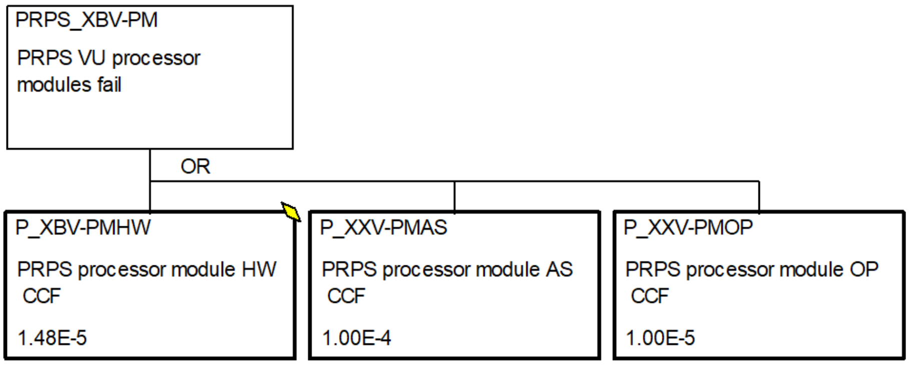

PRPS_XBV-PM
PRPS VU processor modules fail
OR
P_XBV-PMHW
PRPS processor module HW CCF
1.48E-5
P_XXV-PMAS
PRPS processor module AS CCF
1.00E-4
P_XXV-PMOP
PRPS processor module OP CCF
1.00E-5

Figure 13. Fault tree for the processor modules in PRPS voting units (3-out-of-4 divisions fail).

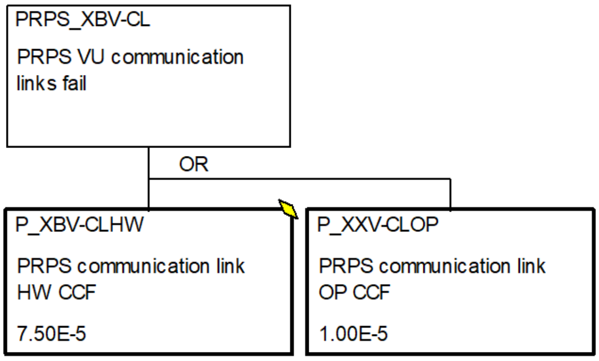

PRPS_XBV-CL
PRPS VU communication links fail
OR
P_XBV-CLHW
PRPS communication link HW CCF
7.50E-5
P_XXV-CLOP
PRPS communication link OP CCF
1.00E-5

Figure 14. Fault tree for the communication links in PRPS voting units (3-out-of-4 divisions fail).

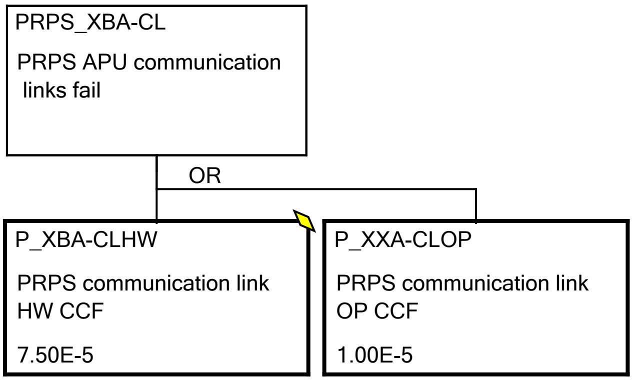

PRPS_XBA-CL
PRPS APU communication links fail
OR
P_XBA-CLHW
PRPS communication link HW CCF
7.50E-5
P_XXA-CLOP
PRPS communication link OP CCF
1.00E-5

Figure 15. Fault tree for the communication links in PRPS APUs (3-out-of-4 divisions fail).

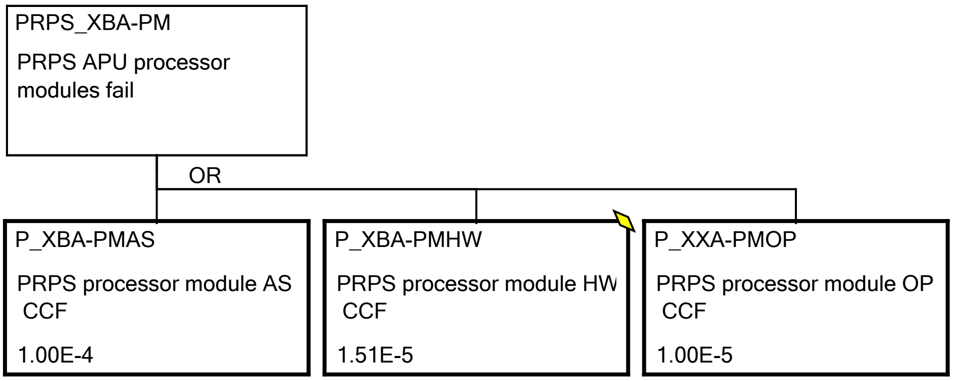

PRPS_XBA-PM
PRPS APU processor modules fail
OR
P_XBA-PMAS
PRPS processor module AS CCF
1.00E-4
P_XBA-PMHW
PRPS processor module HW CCF
1.51E-5
P_XXA-PMOP
PRPS processor module OP CCF
1.00E-5

Figure 16. Fault tree for the processor modules in PRPS APUs (3-out-of-4 divisions fail).

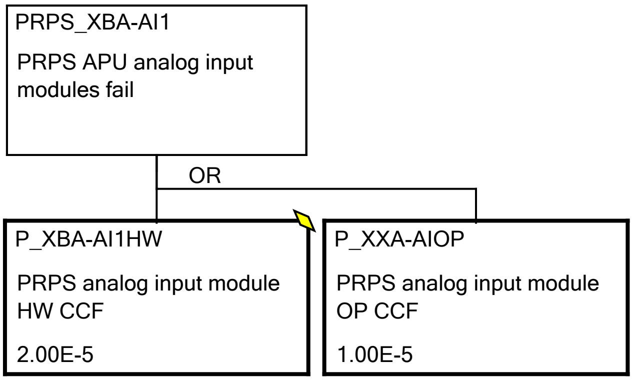

PRPS_XBA-AI1
PRPS APU analog input modules fail
OR
P_XBA-AI1HW
PRPS analog input module HW CCF
2.00E-5
P_XXA-AIOP
PRPS analog input module OP CCF
1.00E-5

Figure 17. Fault tree for the analog input modules in PRPS APUs (3-out-of-4 divisions fail).

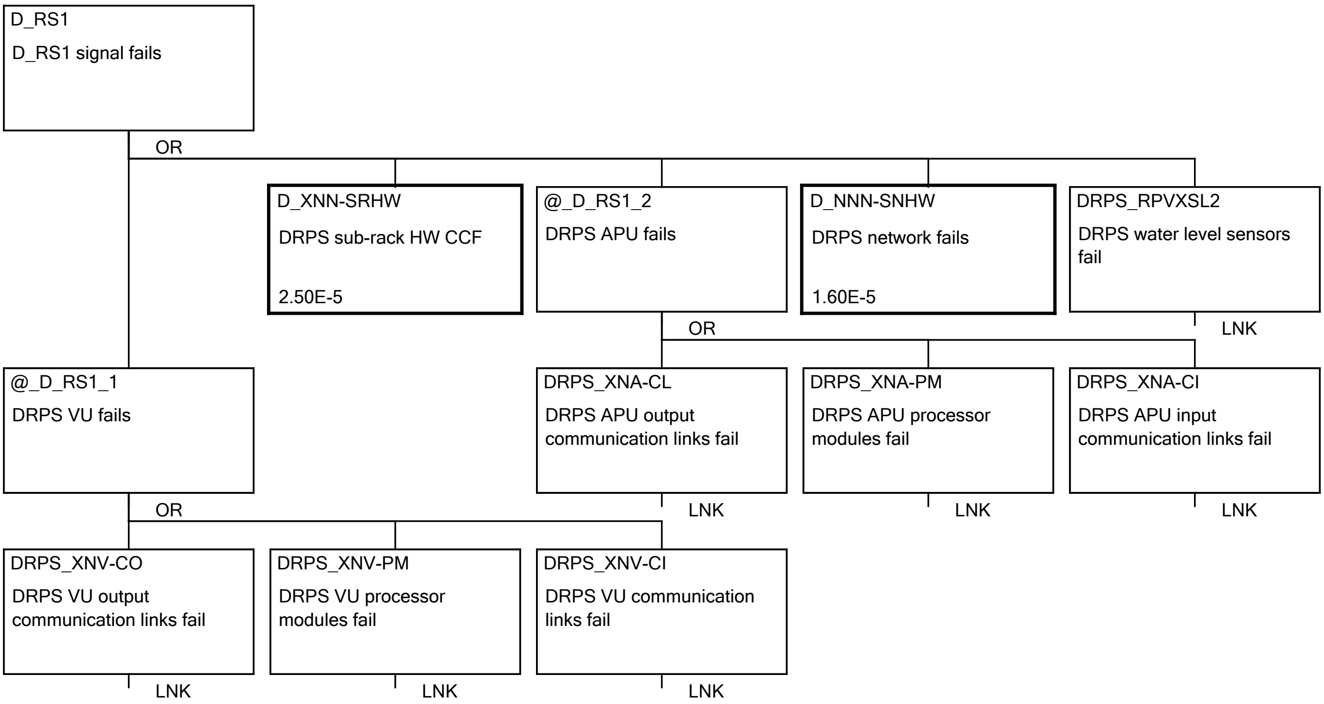


Figure 18. Fault tree for D_RS1 signal from the DRPS (3-out-of-4 divisions fail). There is another variant of this fault tree for reactor scram modelling, where the VU output CL is replaced by DO.

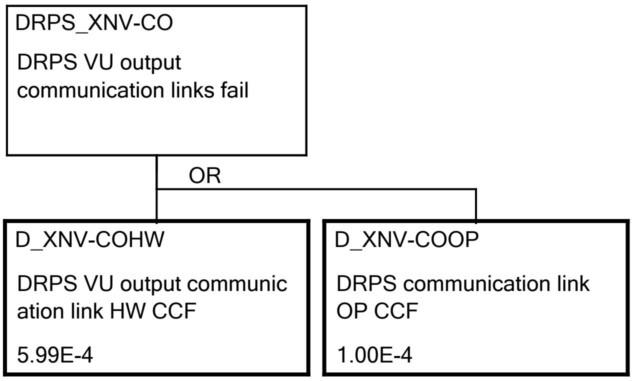

DRPS_XNV-CO
DRPS VU output communication links fail
OR
D_XNV-COHW
DRPS VU output communic ation link HW CCF
5.99E-4
D_XNV-COOP
DRPS communication link OP CCF
1.00E-4

Figure 19. Fault tree for output communication links in DRPS voting units (3-out-of-4 divisions fail).

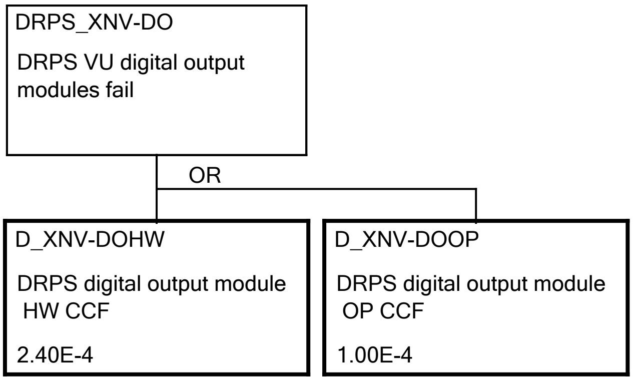

DRPS_XNV-DO
DRPS VU digital output modules fail
OR
D_XNV-DOHW
DRPS digital output module HW CCF
2.40E-4
D_XNV-DOOP
DRPS digital output module OP CCF
1.00E-4

Figure 20. Fault tree for digital output modules in DRPS voting units (3-out-of-4 divisions fail).

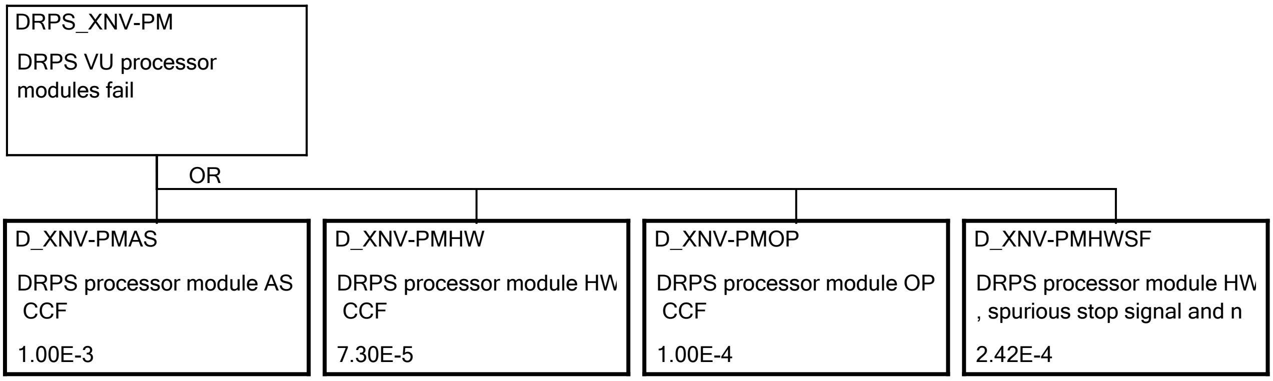

DRPS_XNV-PM
DRPS VU processor modules fail
OR
D_XNV-PMAS
DRPS processor module AS CCF
1.00E-3
D_XNV-PMHW
DRPS processor module HW CCF
7.30E-5
D_XNV-PMOP
DRPS processor module OP CCF
1.00E-4
D_XNV-PMHWSF
DRPS processor module HW, spurious stop signal and n
2.42E-4

Figure 21. Fault tree for the processor modules in DRPS voting units (3-out-of-4 divisions fail). D_XNV-PMHWSF is an initiating event that is also assumed to cause failures of the safety function actuation signals in the PMs.

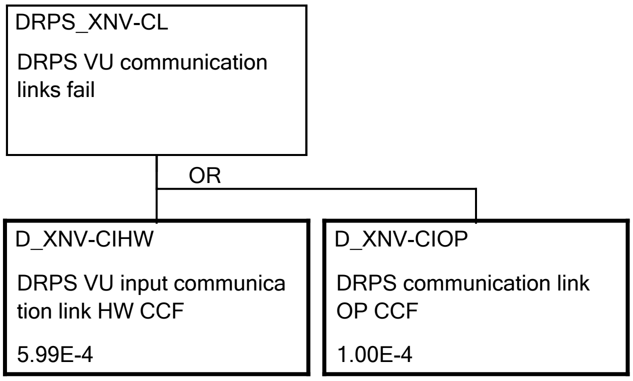

DRPS_XNV-CL
DRPS VU communication links fail
OR
D_XNV-CIHW
DRPS VU input communication link HW CCF
5.99E-4
D_XNV-CIOP
DRPS communication link OP CCF
1.00E-4

Figure 22. Fault tree for the input communication links in DRPS voting units (3-out-of-4 divisions fail).

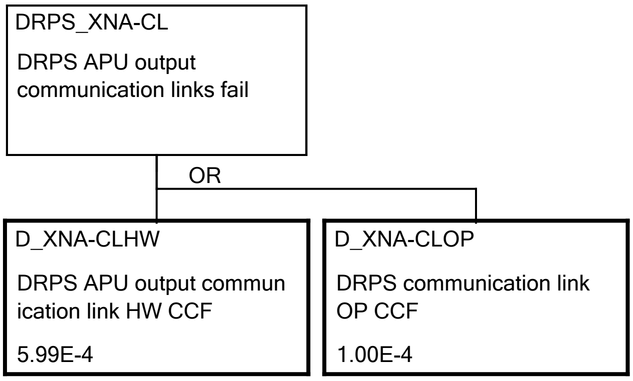

DRPS_XNA-CL
DRPS APU output communication links fail
OR
D_XNA-CLHW
DRPS APU output commun ication link HW CCF
5.99E-4
D_XNA-CLOP
DRPS communication link OP CCF
1.00E-4

Figure 23. Fault tree for the output communication links in DRPS APUs (3-out-of-4 divisions fail).

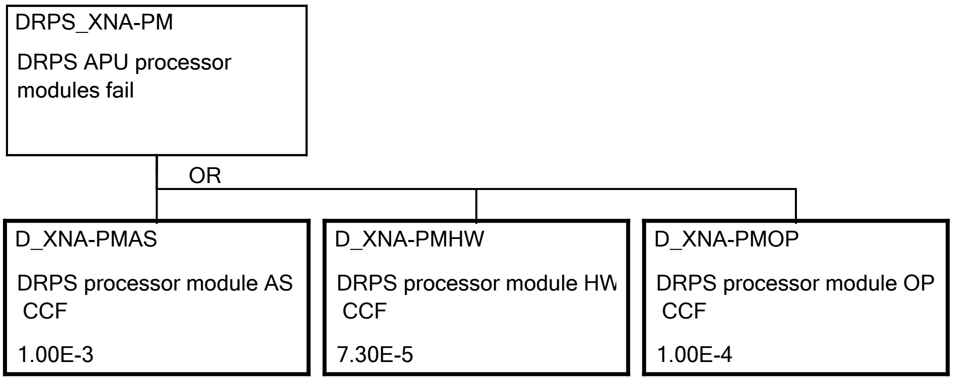

DRPS_XNA-PM
DRPS APU processor modules fail
OR
D_XNA-PMAS
DRPS processor module AS CCF
1.00E-3
D_XNA-PMHW
DRPS processor module HW CCF
7.30E-5
D_XNA-PMOP
DRPS processor module OP CCF
1.00E-4

Figure 24. Fault tree for the processor modules in DRPS APUs (3-out-of-4 divisions fail).

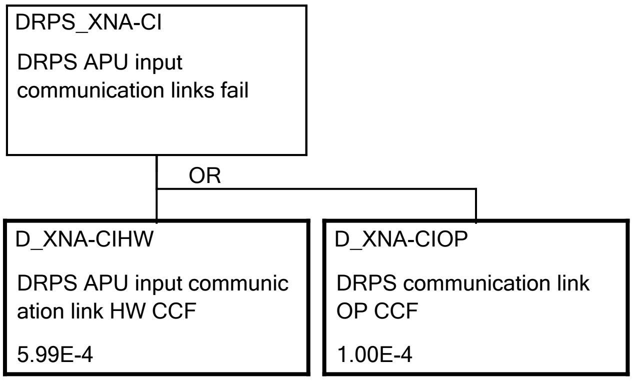

DRPS_XNA-CI
DRPS APU input communication links fail
OR
D_XNA-CIHW
DRPS APU input communic ation link HW CCF
5.99E-4
D_XNA-CIOP
DRPS communication link OP CCF
1.00E-4

Figure 25. Fault tree for the input communication links in DRPS APUs (3-out-of-4 divisions fail).

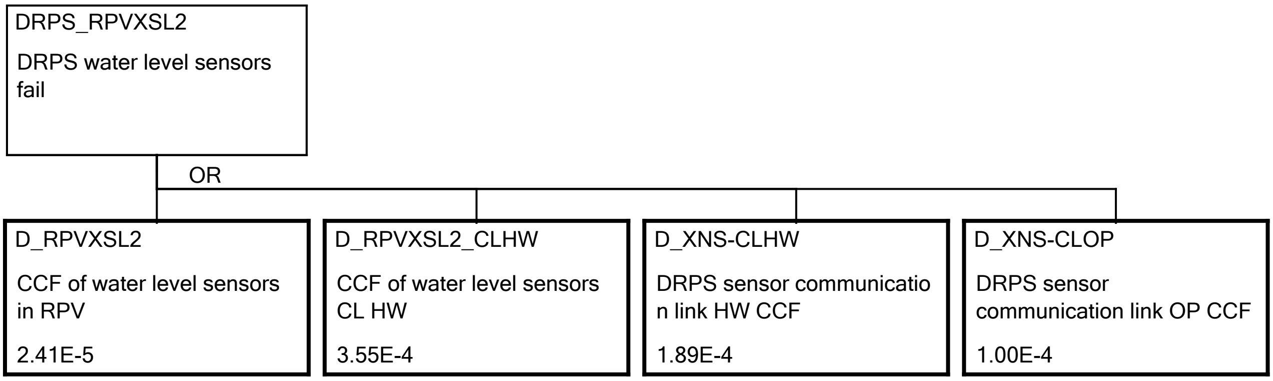

DRPS_RPVXSL2
DRPS water level sensors fail
OR
D_RPVXSL2
CCF of water level sensors in RPV
2.41E-5
D_RPVXSL2_CLHW
CCF of water level sensors CL HW
3.55E-4
D_XNS-CLHW
DRPS sensor communicatio n link HW CCF
1.89E-4
D_XNS-CLOP
DRPS sensor communication link OP CCF
1.00E-4

Figure 26. Fault tree for DRPS water level sensors (3-out-of-4 divisions fail).

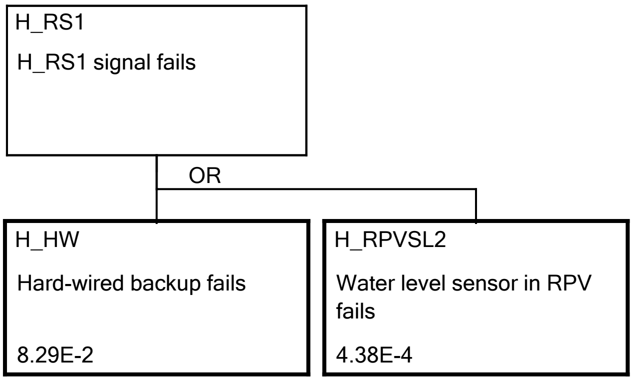


Figure 27. Fault tree for H_RS1 signal from the H-W backup system.

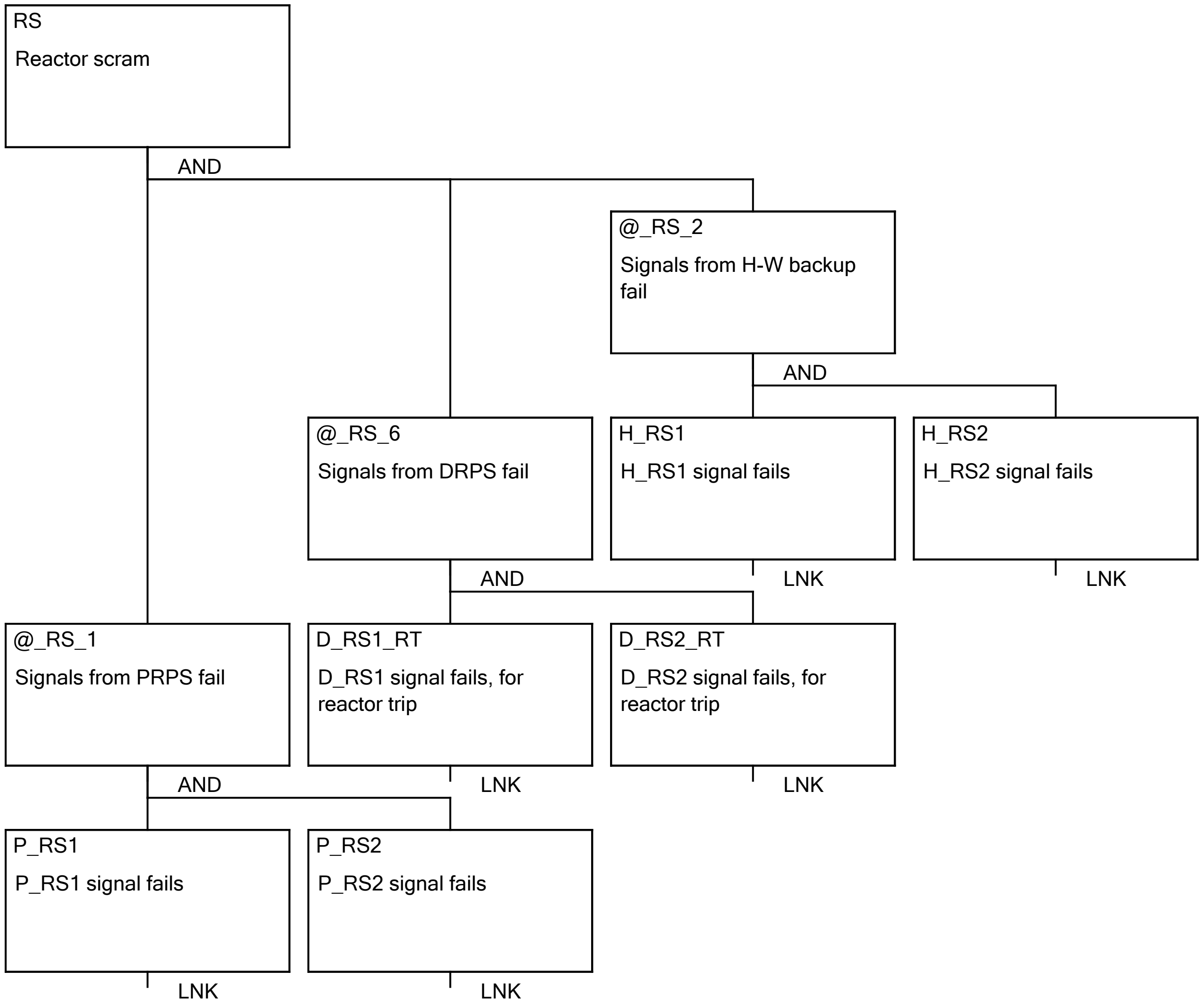


Figure 28. Fault tree for reactor scram.

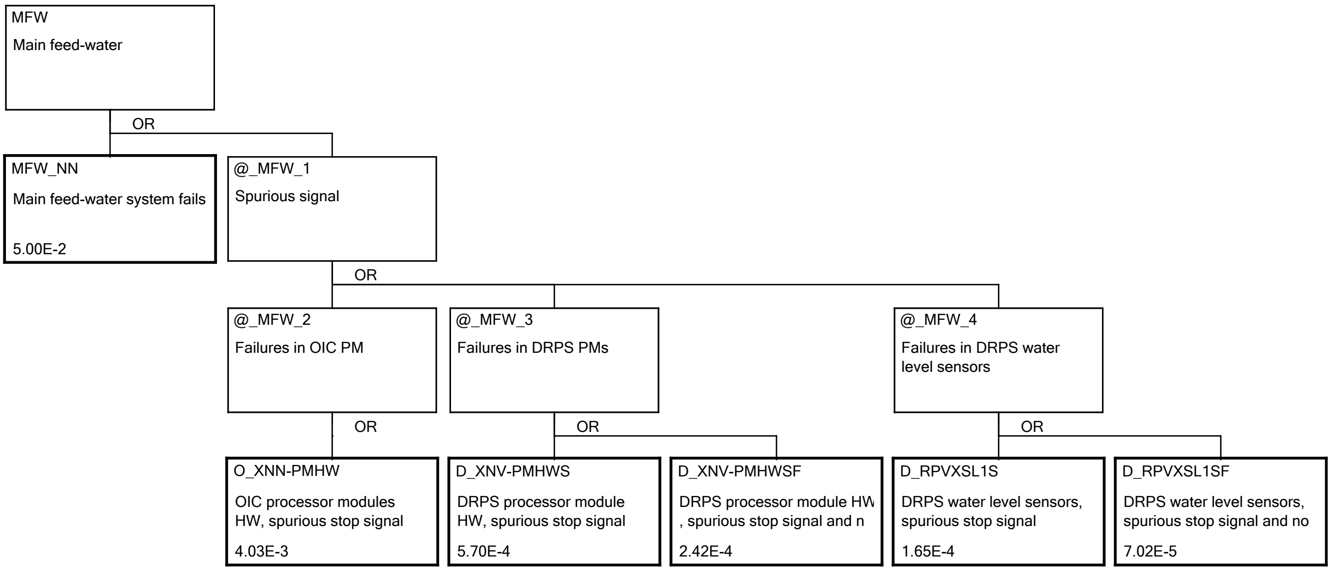

MFW
Main feed-water
OR
MFW_NN
Main feed-water system fails
5.00E-2
@_MFW_1
Spurious signal
OR
@_MFW_2
Failures in OIC PM
OR
@_MFW_3
Failures in DRPS PMs
OR
@_MFW_4
Failures in DRPS water level sensors
OR
O_XNN-PMHW
OIC processor modules HW, spurious stop signal
4.03E-3
D_XNV-PMHWS
DRPS processor module HW, spurious stop signal
5.70E-4
D_XNV-PMHWSF
DRPS processor module HW , spurious stop signal and n
2.42E-4
D_RPVXSL1S
DRPS water level sensors, spurious stop signal
1.65E-4
D_RPVXSL1SF
DRPS water level sensors, spurious stop signal and no
7.02E-5

Figure 29. Fault tree for the initiating events.

3.7 Results

The core damage frequency (CDF) calculated from the model is 5.60E-5/year. It is totally dominated by sequence 1 (Figure 7), where the RHR system fails. The contribution of other sequences is only 0.16%. The reason for this is that failure of the RHR system alone causes a core damage after the initiating event, whereas in the other cases, there is more defence-in-depth.

The risk contribution of I&C systems is 9.3%. The initiating event from the OIC system is the largest contributor, but also DRPS initiating events have significant contribution. The risk contributions of the PAC systems, PRPS, DRPS (excluding the initiating events) and HWBS are small. The risk contributions of I&C systems are presented in Table 9.

Table 9. Fussell-Vesely values of I&C systems with regard to different consequence categories.

System	CD	CD1	CD2	CD3
OIC	7.32E-2	3.94E-2	7.30E-2	7.32E-2
DRPS	1.93E-2	1	4.06E-2	1.90E-2
PAC	1.72E-3	-	0.109	1.61E-3
HWBS	2.46E-4	1	2.20E-2	4.74E-6
PRPS	2.46E-4	1	2.20E-2	4.36E-6

The reason for the small risk contribution of the PRPS and HWBS is clearly that there are three diverse systems to provide the same signals. PAC systems have also small failure probabilities due to their diversification, but still PAC systems are more important than the systems that provide the inputs as there is less redundancy and diversity.

The sequences of the event tree (Figure 7) have been divided into different core damage types (CD1-CD3). Table 9 presents also the risk contributions of the I&C systems to those core damage types. CD1 has quite different risk contributions as it represents the sequence where the reactor scram fails. The PRPS, DRPS and HWBS necessarily fail in this sequence. In CD2, PAC systems have relatively high risk contribution. CD2 requires failures of two front-line systems, which means that the dependencies related to I&C systems are more important, and failures of front-line systems do not dominate in the same way as in the overall results. All I&C systems have higher risk contributions in CD2, except for the OIC system. In CD3, some of the I&C systems have very small risk contribution, because the major minimal cut sets related to those systems go to other sequences.

It can be observed in the results that the risk contribution of the initiating events that also cause the DRPS to fail comes mainly from the loss of the MFW system. The contribution of the minimal cut sets where the DRPS failure actually matters is marginal. For example, spurious signals from the DRPS VU PM combined with DRPS failure have Fussell-Vesely of 4.50E-3, and their share of the total initiating event frequency is 4.39E-3. The Birnbaum value of this initiating event is 1.04E-3, while the Birnbaum of normal initiating events is 1.02E-3. The main reason for this is that failures of front-line systems dominate the risk. For CD1, the Fussell-Vesely value is 0.464 meaning that the failure of DRPS significantly increases the risk of CD1 (ATWS). For CD2, the Fussell-Vesely value is 6.58E-3, i.e. a bit higher than in the overall results.

Fussell-Vesely values for the most important basic events with regard to the CDF and the frequency of CD2 are presented in Appendix B.

4. Complementary analyses

4.1 Comparison of CCF models

4.1.1 Hardware CCFs with the modified beta-factor model and partial beta-factor method

In this section, all HW CCFs of the reference case are modelled using the modified beta-factor model and the partial beta-factor method. The new HW CCFs to be modelled with the partial beta-factor method are presented in Table 10. The selected “redundancy (& diversity)” subfactor scores are also presented in the table. Based on the rules in Table 8, 4-redundant cases with 2-out-of-4 success criterion get score A+. For two redundant PAC modules, score A is selected. For complex asymmetric configurations, there are no rules. Score C is selected for the functionally diverse cases, because it corresponds to 2-out-of-4 success criterion with functional diversity. For the CCFs between the PRPS and DRPS as well as the CCF between diverse PAC units, the best score, E, is selected.

Since the systems are fictive, there is no information based on which the other subfactors could be evaluated. For simplicity, the same score is selected for each subfactor at a time for a specific CCF case, but three different sensitivity cases are created. The selected scores are presented in Table 11. For the DRPS, worse scores are selected because it belongs to a lower safety class.

The estimated beta-factor values for different cases are presented in Table 12. It can be seen that for some CCFs, there is much more variation between the sensitivity cases than for others. When the redundancy score is A or A+, the other scores have relatively small impact, but when the redundancy score is E, the other scores have large impact. This is a general property of the method. When one subfactor has a poor score, the other subfactors do not matter much, unless they also have poor scores. The subfactor with the worst score is always the largest contributor to the beta-factor.

Table 10. Hardware CCF cases and their redundancy scores.

CCF case	Redundancy (& diversity) score
CCFs between two identical modules in redundant PAC units serving the same front-line system	**A**
CCFs between four PAC AD modules serving the same front-line system	**A+**
CCFs between identical modules in all PAC units	**C**
CCFs between identical modules in a PRPS subsystem	**A+**
CCFs between identical modules in different PRPS subsystems	**C**
CCFs between identical modules in the DRPS (except for sensor CL modules)	**A+**
CCF between all DRPS sensor CL modules	**C**
CCFs between similar modules in the PRPS and DRPS	**E**
CCFs between similar modules in PAC-A and PAC-B	**E**

Table 11. Scores for other subfactors than redundancy for different CCF and sensitivity cases.

CCF case	Scores in case 1	Scores in case 2	Scores in case 3
PAC CCFs	**E**	**D**	**C**
PRPS CCFs	**E**	**D**	**C**
DRPS CCFs	**D**	**C**	**B**

Table 12. Beta-factor values in different sensitivity cases.

CCF case	Case 1	Case 2	Case 3
CCFs between two identical modules in redundant PAC units serving the same front-line system	0.0362	0.0390	0.0506
CCFs between four PAC AD modules serving the same front-line system	0.0180	0.0208	0.0325
CCFs between identical modules in all PAC units	0.00284	0.00565	0.0173
CCFs between identical modules in a PRPS subsystem	0.0180	0.0208	0.0325
CCFs between identical modules in different PRPS subsystems	0.00284	0.00565	0.0173
CCFs between identical modules in the DRPS (except for sensor CL modules)	0.0208	0.0325	0.0808
CCF between all DRPS sensor CL modules	0.00565	0.0173	0.0656

We have developed two additional sensitivity analysis cases. In the first case (case 4), we model CCFs between similar modules in the PRPS and DRPS. We extend the reference case with CCFs between PRPS and DRPS. The scores for other subfactors (not redundancy (& diversity) score) are assumed to be D. The Beta-factor value for the CCF is 0.0038.

In the second case (case 5), we model CCFs between all PAC units. We extend the reference case with CCFs between similar modules PAC-A and PAC-B using the partial beta-factor method. The scores for other subfactors (not redundancy (& diversity) score) are assumed to be D. The Beta-factor value for the CCF is 0.0038.

Failure probabilities for CCFs between similar modules in PRPS and DRPS are shown in Table 13

Table 13. Failure probabilities for CCFs between similar modules in PRPS and DRPS

CCF	Probability
APU CL	8.86E-6
APU PM	1.78E-6
VU PM	1.75E-6
VU DO	3.55E-6
VU CL	8.86E-6
Sub rack	8.86E-8

Table 14. Failure probabilities for CCFs between similar modules in PAC-A and PAC-B.

CCF	Probability
PAC AD	3.39E-06
PAC CL	8.46E-06
PAC CPLD	1.73E-06
PAC DA	3.39E-06
PAC PM	1.72E-06
PAC Sub rack	1.73E-06

4.1.1.1 Results

The relation of CCF case probabilities of the PRPS and DRPS to the reference case are shown in Table 15 for the different sensitivity cases. All CCF event probabilities for the different cases are presented in Appendix C. The CCF probabilities are mostly smaller for cases 1 and 2 with respect to the reference case and larger for case 3. However, they are mostly within the same order of magnitude. The results indicate that with a lower subfactor score the beta-factor value is proportionally higher. In the reference case, DRPS sensor CL CCFs were modelled with the beta-factor model that represented case 2 (therefore the relative result is 100% in case 2). It can also be noted that the cases with two spurious signals from the DRPS are removed from the model when the modified beta-factor model is applied meaning that the initiating event frequencies decrease overall.

Table 15. The relation of PRPS and DRPS CCF case probabilities to the reference case.

CCF case	Case 1	Case 2	Case 3
CCFs between identical modules in a PRPS subsystem (not AI module)	56%	65%	101%
CCFs between AI modules in a PRPS subsystem	81%	94%	147%
CCFs between identical modules in different PRPS subsystems (not AI module)	17%	34%	103%
CCFs between AI modules in different PRPS subsystems	32%	64%	195%
CCFs between sensors in a PRPS subsystem	33%	38%	59%
CCFs between identical modules in the DRPS	38%	59%	147%
CCF between all DRPS sensor CL modules (1 sensor group)	64%	100%	249%
CCF between all DRPS sensor CL modules (all sensors)	33%	100%	379%
Three/four spurious signals due to a CCF of the PMs of the DRPS VUs	35%	54%	135%
Three/four spurious signals from the DRPS because water level sensors show high value	35%	54%	134%

In the main PRA model, only high-level failure events were modelled for PAC. The computation of the probabilities for those events is presented in Sections 3.4.2 and 3.4.3. In Table 16, the relative results using the partial beta-factor method are presented. Note that AD CCF probabilities were estimated using the partial beta-factor method already in the main analysis case corresponding to the scores of case 2 (therefore the relative result is 100% in case 2). Note also that different system failure combinations were analysed in the main PRA model (failure 2 systems, 3 systems, etc.). In Table 16, only failure of one front-line system and failure of all seven front-line systems are evaluated as the other combinations are not relevant with the beta-factor model. The values used in the main PRA model covered also software CCFs, but in this comparison, only HW CCFs are included. The probabilities estimated using the beta-factor model seem to be in line with the probabilities calculated using the alpha-factor model. For failure of one front-line system, the values are very similar. For PM and CL failures, the results are very similar to the CPLD/DA/SR case and are not separately presented here.

Table 16. The relation of PAC failure probabilities to the reference case.

CCF case	Case 1	Case 2	Case 3
3-o-o-4 failure of PAC units serving the same front-line system (CPLD, DA and SR failures)	87%	98%	144%
3-o-o-4 failure for all front-line systems due to PAC CCFs (CPLD, DA and SR CCFs)	7%	29%	270%
3-o-o-4 failure of AD modules that take input from the same system and serve the same front-line safety system	88%	100%	148%
Two 3-o-o-4 failures of AD modules that serve the same front-line safety system (one corresponding to inputs from the PRPS and one corresponding to inputs from the H-W backup)	67%	100%	296%
Failure of all 56 AD modules	25%	100%	938%

The CDF, I&C contribution and I&C contribution without initiating events for cases 1-5 and the reference case are shown in Table 17.

Table 17. CDF, I&C contribution with and without initiating event contribution for the different cases.

Case	CDF	I&C	I&C without IE
Reference	5.60E-5	0.093	1.82E-3
Case 1	5.50E-5	0.078	1.39E-3
Case 2	5.51E-5	0.079	1.55E-3
Case 3	5.54E-5	0.084	2.22E-3
Case 4	5.61E-5	0.095	3.96E-3
Case 5	5.64E-5	0.10	8.67E-3

The CDF for cases 1-3 is lower than for the reference case. This could be expected for cases 1 and 2 since the probabilities of the CCF events are lower than in the reference case. The initiating events affect the results the most and, thus, their frequencies have a large impact. This can be seen from the results when the I&C contribution is computed excluding the initiating events. Even though the overall I&C contribution decreases in case 3 due to initiating event frequencies, the I&C contribution without initiating events increases because the CCF probabilities are mostly larger in that case.

In case 4, the CCFs between the PRPS and DRPS have only a minor impact to the overall results. However, the new CCFs increase the most the frequency of sequence 6 (by a factor of 10) where the reactor scram fails. In this case, if both the PRPS and DRPS fail due to the same CCF event, only a failure of the HWBS is additionally needed for reactor scram failure (and consequently core damage). The contribution of these CCFs is 2.01E-3 in total results, which is significantly larger than the contribution of the PRPS specific CCFs.

Of the new PAC CCFs in case 5, the CCF of CPLD, DA, or SR modules has the largest impact on the results. The CCF fails all PACs and, thus, all PAC related safety functions fail. It has the highest Fussell-Vesely value (6,69E-3) of the I&C basic events (that are not initiating events). The other new CCF events (related to AD, PM, and CL modules) have at least two orders of magnitude smaller contributions. In the overall results, the CPLD, DA, or SR CCF contributes only to sequence 5 (see Figure 7) and, thus, core damage type CD2. In CD2, PAC systems had a relatively high risk contribution already in the reference case. In case 5, the CDF for CD2 is 4.34E-7 that is almost one order of magnitude higher than in the reference case. It can be concluded that PAC CCFs do not stand out in the overall results only because sequence 1 requires failure of only one front-line system.

4.1.2 Partial beta-factor method for software CCFs

Bao et al. (2022) have developed variants of the partial beta-factor method specifically to estimate beta-factors for software CCFs in non-diverse and diverse configurations. For software CCFs, the method is the same as for HW (presented in Section 3.4.3), but the subfactors and the table values are partly different. The table values for software CCFs in non-diverse configurations are presented in Table 18. The table for diverse configurations is the same except that it does not contain the “Redundancy (& diversity)” subfactor. The denominator in the computation formula is 100000 for non-diverse configurations and 76000 for diverse configurations. Rules for scoring the subfactors are presented in (Bao et al., 2022).

Table 18. Beta-factor estimation table for software in non-diverse configurations.

Subfactor	A	A+	B	B+	C	D	E
Redundancy (& diversity)	23976	10112	4265	1799	759	135	24
Input similarity	23976	10112	4265		759	135	24
Understanding	7992		1422		253	45	8
Analysis	7992		1422		253	45	8
Man-machine interface	11988		2132		379	67	12
Safety culture	6993		1244		221	39	7
Control	4995		888		158	28	5
Tests	11988		2132		379	67	12

In the case of diverse configurations, the CCF computation differs slightly. The parameter is not called beta and it is denoted as ϕ_n (and named defense factor). When $\phi_n = 1$, the defense level is the worst possible. The CCF probability is calculated as $\phi_n Q_{CC_n}$, where Q_{CC_n} is the theoretical CCF probability based on the similarity between the software components. The determination of Q_{CC_n} seems to involve expert judgment based on the discussion and examples in (Bao et al., 2022).

In the reference case, beta-factor value 1 has been applied to all software CCFs that have been modelled. Here, the impact of the partial beta-factor method on the results will be studied.

Software CCFs to be modelled with the partial beta-factor model are presented in Table 19. The same scores and beta-factors are assumed for OP and AS, even though there would probably be differences in reality. The selected “redundancy (& diversity)” and “input similarity” subfactors scores are also presented in the table. The CCF between similar modules in the PRPS and DRPS is analyzed by the formula for diverse configurations, which does not include the redundancy subfactor. Otherwise, the redundancy scores are the same as for the hardware CCFs. The scores for the other subfactors are assumed to be D for PRPS and PAC, and C for DRPS.

Table 19. Software CCFs and their redundancy and input similarity scores, and beta-factor values.

CCF case	Redundancy (& diversity) score	Input similarity score	Beta-factor
CCFs between two identical modules in redundant PAC units serving the same front-line system	A	D	0.244
CCFs between four PAC AD modules serving the same front-line system	A+	D	0.105
CCFs between identical modules in all PAC units	C	D	0.0119
CCFs between identical modules in a PRPS subsystem, except for VU CL	A+	D	0.105
CCFs between VU CL modules in a PRPS subsystem	A+	A	0.344
CCFs between identical modules in different PRPS subsystems	C	D	0.0119
CCFs between identical modules in the DRPS, except for VU CL	A+	D	0.119
CCFs between VU CL modules in the DRPS	A+	A	0.357
CCF between all DRPS sensor CL modules	C	D	0.0254
CCFs between similar modules in the PRPS and DRPS		E	0.00415

The rules to estimate the input similarity in (Bao et al., 2022) are not very clear. We assume that when the inputs are not same for the modules in the CCF group, the score is D. Even if the inputs are of the same type/identical for redundant modules, they are not the same, except for the VU CL modules. This seems to be the logic in the examples given in (Bao et al., 2022). For the CCFs between VU CL modules in a PRPS subsystem (or in the DRPS), the score is A, because the inputs are completely the same. For the CCFs between VU CL modules in different PRPS subsystems, the score should be A+ if the rules were followed precisely, because most of the inputs are same. However, this seems a bit questionable, because different subsystems have different inputs, meaning that there is good protection against CCFs between the subsystems, while not against CCFs inside a subsystem. Therefore, score D is used instead of A+. For CCFs between similar modules in the PRPS and DRPS, score E is selected, because the diversity is complete.

When either the redundancy or the input similarity subfactor score is poor (A or A+), i.e. there is no functional diversity, the beta-factor is over 0.1. The beta-factor is almost one order of magnitude higher than with better scores. When there is functional diversity, the beta-factor is 0.01-0.03. For the case with complete diversity, the beta-factor is 0.00415, i.e. smaller but still quite significant. As can be seen in Table 18, redundancy and input similarity subfactors have the highest impact to the beta factor.

In addition to the CCFs modelled in the main DIGMORE case, we model a CCF between application software of APU processor modules of the different PRPS sub-systems and software CCFs between the PRPS and DRPS. When we model the CCFs between similar modules in the PRPS and DRPS, we assume that the theoretical CCF probability (Q_{CC_n}) is the probability used for the PRPS CCFs in the DIGMORE case (1E-4 for AS and 1E-5 for OP).

4.1.2.1 Results

The contribution of software failures to the CDF is 1.02E-4 (without PAC basic events) and 1.65E-3 with PAC basic events included (PAC basic events include both software and hardware failures). The contribution of software in the reference case are 1.64E-4 and 1.88E-3 respectively. A large part of the contribution comes from the software CCFs between PRPS and DRPS that are not included in the reference case. The CCFs between PRPS and DRPS PM application software have the highest Fussell-Vesely values (3.38E-5) (of not PAC related software CCFs).

The use of the partial beta-factor method to model software failures decrease the contribution of software failures as was expected, even though new software CCFs were included. The CCF probabilities decrease when compared to the reference case (see Table 19). However, to the overall results the use of the partial beta-factor method had a very limited impact since already in the reference case software failures have a rather small contribution.

4.1.3 Hybrid approach

In some cases, a PRA analyst may prefer more detailed modelling than presented in this report and include single failure events explicitly in the PRA model. This can be the case, for example, when a risk monitor is used. To a point, the alpha-factor model works well with the detailed modelling because all the CCF combinations can be automatically mapped to the fault trees. The alpha-factor model is often preferred over the beta-factor model because all CCF combinations are included and because the alpha-factors are usually based on real CCF data (while the partial beta-factor method has mainly been developed by expert judgment). A drawback with the alpha-factor model is, on the other hand, that the calculations get complex when the number of components in a group is large. If a CCF group has eight components, there are 247 CCF combinations related to the group. If there are many groups with eight components, the generation of minimal cut sets can become computationally quite demanding, the number of minimal cut sets can become very large, and the interpretation of the results can become complex. Groups with more than eight components are even more demanding and usually not (fully) supported by PRA software tools.

One option to overcome the above-mentioned challenges is to use a hybrid approach where the smaller CCF combinations are modelled using the alpha-factor model and the larger CCF combinations are modelled using the beta-factor model. In our proposed hybrid approach, we use multiple CCF groups to model CCF events with more than four components. For example, the CCFs between components within one PRPS subsystem are modelled with one alpha-factor CCF group and the CCF between all components in different subsystems with another beta-factor CCF group. To estimate the beta-factor, there are different options. It could be calculated from alpha-factors as done in the main DIGMORE PRA model (or the CCF probability can be directly calculated from the alpha-factors) or estimated using the partial beta-factor method. To be consistent with the data, the alpha-factor model may be preferred, though it adds complexity to background calculations.

To test the applicability of the hybrid approach, we model the CCFs of the PRPS VU PMs with the approach. We model the CCFs within a subsystem with an alpha-factor model with four components and the CCF between the subsystems with an alpha-factor model with eight components. In this case, we include the single failure basic events in the model explicitly within one subsystem. The CCF between the subsystems is modelled in the PRA model in a simplified manner identically to the reference case. The CCF event probabilities are presented in Table 20.

Table 20. CCF probabilities with the hybrid approach and in the reference case.

CCF Probabilities	Reference	Hybrid
2x CCF between VU PM in a PRPS subsystem	-	1.09E-5
3x CCF between VU PM in a PRPS subsystem	1.48E-5	4.66E-6
4x CCF between VU PM in a PRPS subsystem		4.32E-6
CCF between VU PMs in different PRPS subsystems (at least 3 components fail in both subsystems)	7.76E-6	7.76E-6

The probability of three or four VU PMs failing is 2.30E-5 with the hybrid approach, which is a bit higher than in the reference case. Thus, the results are conservative, even more so than in the reference case. It can be noticed that in the reference case, the probability that at least three components fail in a subsystem is 1.48E-5 + 7.76E-6 = 2.26E-5 (calculated using an alpha-factor model with eight components), which is almost the same value. When two alpha-factor models are used in combination, some extra is added to the CCF probabilities in total, but the order of magnitude does not change.

To avoid conservatism, one option would also be to estimate the probabilities of smaller order CCF events with the alpha-factor model of eight components (counting also higher order combinations that do not cause failure of both subsystems), but it would require complex background calculations, which would reduce the usability of the approach.

4.2 Spurious signals

4.2.1 Spurious PRPS stop signals for safety functions

In the reference case, spurious signals caused by failures in the OIC system and DRPS were modelled. In this sensitivity case, we model spurious stop signals also from the PRPS. The reference case does not define stop/close signals for the safety systems. However, typically I&C systems generate also stop/close signals for the actuators of the safety systems. Similarly to the DRPS (see Section 3.5), we model the following spurious signal cases for the PRPS:

- Three spurious stop signals due to a CCF of the PMs of the PRPS VUs (all safety signals processed by those PMs of the PRPS fail)
- Three spurious stop signals from the PRPS because three sensors show incorrect value (the corresponding safety signals of the PRPS fail)

The failure rates are assumed to be the same as for the DRPS in the reference case, i.e. for a spurious signal from a PM the failure rate is 4.6E-7/h and from a sensor 1.33E-7/h. It is conservatively assumed that spurious signals can impact a safety system during the whole mission time (24h). This is conservative because, for example, in some systems the start signal will be set for a specified time. During that time a stop signal will not have any impact. The failure rate of a PM is assumed to cover both HW and software failures. It is conservatively assumed that the safety signals processed by the PM fail at the same time. If a spurious signal comes from a sensor (the sensor shows incorrect value spuriously), the start signals naturally fail at the same time. PRPS signals have the highest priority in PAC units and, thus, signals from the DRPS or HWBS will be ignored in the PACs when PRPS signals are set.

The CCFs are modelled in a simplified manner as described in section 3.4.1. The CCF probabilities are shown in Table 21. The probabilities are computed similarly to the DRPS case (see section 3.5).

Table 21. Spurious signal failure cases and their probabilities.

Failure case	Probability
Three spurious signals from VU PMs in one subsystem	3.34E-7
Three spurious signals from VU PMs in both subsystem	1.86E-7
Three spurious signals from PRPS sensors	1.67E-7

The spurious signal failure cases have only a minor impact to the overall results. Mainly the frequency of CD2 increases slightly (6.44E-8) when compared to the reference case (5.40E-8). The increase comes from sequence 5.

The Fussell-Vesely value for the CCF affecting both subsystems is 1.83E-4. The contribution of the other CCFs is several orders of magnitude lower. The contribution of the spurious signals affecting both subsystems is somewhat high when compared to other I&C failures, because a CCF of spurious signals will fail a whole safety system. For comparison, Fussell-Vesely of the whole PRPS is 2.46E-4 in the reference case. It can be concluded that these kinds of spurious signals could have significance in the total results if failure of the RHR did not dominate the results due to simplifications in the reference case. However, the assumptions made in the modelling are conservative, and more realistic analysis might produce a different result.

4.2.2 Spurious signals due to CCF between DRPS and OIC

Since, the OIC system and the DRPS are assumed to be based on identical platforms, we place in this complementary analysis case all PMs of those systems in the same CCF group (this CCF grouping was actually used in an earlier version of the main DIGMORE model). The secondary PM of the OIC system is excluded from the CCF group as it is not considered relevant for spurious signals. This CCF group includes nine PMs, and the alpha-factor model is applied. The assumptions are the same as in the reference case, i.e. if there are three this type of failures in the DRPS VUs or APUs, the safety signals of the DRPS also fail.

Because of the new CCF group the modelled spurious signal cases are modified a bit:

1. Spurious signal from the primary PM of the OIC system (and no failure of the DRPS)
2. Spurious signal due to a CCF of the primary PM of the OIC system and three PMs in DRPS VUs or APUs (all safety signals of the DRPS fail)
3. Two spurious signals due to a CCF of the PMs of the DRPS VUs (but not three; also, no three failures in the DRPS APUs)
4. Three spurious signals due to a CCF of the PMs of the DRPS VUs (all safety signals of the DRPS fail)
5. Two spurious signals due to a CCF of two PMs of the DRPS VUs and three PMs of the DRPS APUs (all safety signals of the DRPS fail) [this is combined with the previous case in the PRA model]

The CCF calculations have been performed in Excel in the same way as those that are presented in Section 3.4.1. The numbers of CCF combinations for the different cases are presented in Table 22. The cases are mutually exclusive.

Table 22. CCF combinations allocated to different spurious signal cases, their frequencies, and frequencies of the corresponding reference case initiating events.

Number of failures	Case 1	Case 2	Case 3	Case 4	Case 5
1	1				
2	8		6		
3	28		24	4	
4	48	8	36	17	
5	36	34		28	24
6		56		22	6
7		28		8	
8		8		1	
9		1			
Frequency (1/year)	3.92E-3	1.14E-4	4.27E-4	9.28E-5	2.24E-5
Ref Case frequencies[1)]	4.03E-3	--	5.70E-4	2.01E-4	

[1)] The reference case initiating events are not identical with the different spurious signal cases, but there is a clear correspondence between some of the cases.

The initiating event frequencies are quite similar with different CCF grouping options. The initiating event frequencies are a bit higher in the reference case for cases 1 and 3, but for the case where loss of main feed-water occurs and the safety signals in the DRPS fail the frequency is smaller in the reference case. Here, the total frequency of that case is 1.14E-4 + 9.28E-5 + 2.24E-5 = 2.29E-4.

The core damage frequency is 5.58E-5/year. The core damage frequency decreases due to the lower initiating event frequencies, even though the frequency of DRPS failure increases. Surprisingly, the CCF grouping used in the reference case is more conservative than this grouping option, and therefore, seems more sensible alternative also due to its simplicity.

5. Conclusions

This report has presented a PRA model for the OECD/NEA WGRISK DIGMORE reference case. The reference case covers an I&C architecture with several systems, such as the primary and diverse reactor protection system, operational I&C system, hard-wired backup system, and prioritization and actuation control systems. The modelling approach selected in this study is to develop a simplified PRA model with only CCFs and high-level failure events and to perform complex calculations in background. The approach was selected due to challenges related to CCF calculations, particularly concerning the PAC systems. The calculations related to PAC systems are very complex and required development of a computation script.

In the overall results of the PRA model, the I&C systems do not play a very important role. This is however partly because of the simplifications made in the reference case (failure of one front-line system is enough to cause core damage after initiating event). Spurious signals causing the main feed-water system to stop (initiating event) are the most important I&C failure events in the results. Concerning failures of safety functions, PAC systems are the most important I&C systems, because they have less redundancy and diversity than the other systems.

In the main PRA analysis, the aim was to follow the reference case description as closely as possible meaning e.g. that the alpha-factor model was applied to hardware CCFs in every case where it was possible. However, some of the CCF calculations were very complex with the alpha-factor model, particularly for PAC systems. Therefore, use of the modified beta-factor model was studied in the complementary analyses. It makes the modelling of CCFs much simpler. The beta-factor parameters were estimated using the partial beta-factor method. The partial beta-factor method produced mostly a bit smaller CCF probabilities than the alpha-factor model, but it depended on the assumptions used in the analysis. In general, the results were at the same order of magnitude. Benefits of the partial beta-factor method are that it takes into account case-specific defences against CCFs and is applicable to any CCF group size. However, it is an expert judgment -based method rather than based on CCF data. A hybrid approach applying the alpha-factor model to smaller CCF combinations and the beta-factor model to larger CCF combinations was also considered in the report.

A complementary analysis case was also developed for spurious stop signals of safety functions. Spurious stop signals coming from the PRPS were assumed to override the start signals coming from the other I&C systems, and therefore, such an event alone led to safety function failure. These spurious signals were more important in the results than other PRPS failures. However, the assumptions used in the modelling were conservative, and the aim was mainly to evaluate the maximal impact of this type of failure.

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, Denmark.

Bao, H, Zhang, S, Youngblood, R, Shorthill, T, Pandit, P, Chen, E, Park, J, Ban, H, Diaconeasa, M, Dinh, N, Lawrence, S. (2022). “Risk analysis of various design architectures for high safety-significant safety-related digital instrumentation and control systems of nuclear power plants during accident scenarios”, INL/RPT-22-70056, Idaho National Laboratory, Idaho Falls.

Björkman, K. (2023). “I&C system architecture PRA – Literature review”, VTT-R-00677-23, VTT Technical Research Centre of Finland Ltd, Espoo, Finland.

Chu, TL, Yue, M, Martinez-Guridi, M, Lehner, J. (2010). “Review of quantitative software reliability methods”, BNL-94047-2010, Brookhaven National Lab.

Liang, QZ, Guo, Y, Peng, CH. (2020). “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 427.

Lindberg, S. (2007). “Common cause failure analysis, Methodology evaluation using Nordic experience data”, Uppsala University, Uppsala, Sweden.

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). (2024a). “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.

Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI). (2024b). “Digital I&C PSA – Comparative Application of Digital I&C Modelling Approaches for PSA, Volume 2: Appendices B0 – B6”, NEA/CSNI/R(2021)14, Paris, France.

Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI). (2024c). “DIGMORE – a realistic comparative application of DI&C modelling approaches for PSA, Appendix A: Complete reference case descriptions”. DRAFT.

Porthin, M, Shin, S-M, Quatrain, R, Tyrväinen, T, Sedlak, J, Brinkman, H, Müller, C, Picca, P, Jaros, M, Natarajan, V, Piljugin, E, Demgne, J. (2023). “International case study comparing PSA modelling approaches for nuclear digital I&C – OECD/NEA tank DIGMAP”, Nuclear Engineering and Technology 55 (12), 4367-4381.

Wierman, TE, Beck, ST, Calley, MB, Eide, SA, Gentillon, CD, Kohn, WE. (2000). “Reliability study: Combustion engineering reactor protection system – Appendices D-E, 1984-1998”, NUREG/CR-5500, Vol. 10, U.S. Nuclear Regulatory Commission, Washington D.C.

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, Finland.

Tyrväinen, T. (2021). “Probabilistic modelling of common cause failures in digital I&C systems – Literature review”, VTT-R-00728-21, VTT Technical Research Centre of Finland Ltd, Espoo, Finland.

Appendix A: Scripts to calculate PAC failure probabilities

```
Sub CCFCombs()
    Dim I As Integer
    Dim J As Integer
    Dim K As Integer
    Dim N As Integer
    Dim S As Integer
    Dim Failures As Integer
    Dim Comp As Integer
    Dim Results(1 To 7, 1 To 2) As Double
    Dim SF As Integer
    Dim FI As Integer
    Dim FJ As Integer
    Dim R As Double
    Dim M As Integer
    Dim WrongComb As Boolean
    Dim Contributions(1 To 15, 1 To 15) As Double
    Dim C As Integer

    N = 16383  ' Number of combinations in one group
    S = 7      ' Number of safety systems
    C = 2      ' Number of calculation cases

    K = 1
    Do While K < S
        M = 1
        Do While M <= C
            Results(K, M) = 0
            M = M + 1
        Loop
        K = K + 1
    Loop

    ' Software CCFs are calculated first
    M = 1
    Do While M <= C
        Results(S, M) = Worksheets("Sheet1").Cells(M + 19, 3).Value ^ 2
        If M = 1 Then
            Contributions(15, 15) = Results(S, M)
        End If
        M = M + 1
    Loop

    I = 1
    Do While I <= N  ' Go through combinations in the first group
        J = 1
        Do While J <= N  ' Go through combinations in the second group
            SF = 0
            WrongComb = False
            K = 1
            Do While (K <= S) And (WrongComb = False)  ' Go through the safety systems
                Failures = 0

                ' Check which of the 4 components are failed in these two CCFs
                Comp = (K - 1) * 2 + 1
                If CompInComb(Comp, I) Then
                    Failures = Failures + 1
                End If
                If CompInComb(Comp, J) Then
                    Failures = Failures + 1
                End If

                Comp = (K - 1) * 2 + 2
                If CompInComb(Comp, I) Then
                    Failures = Failures + 1
                End If
                If CompInComb(Comp, J) Then
                    Failures = Failures + 1
                End If

                If Failures >= 3 Then  ' Are there at least 3 failures?
                    SF = SF + 1
                    ' Only the combinations where only the first system fails, only the first 2 systems fail, only the first 3 systems fail, etc. are calculated.
                    ' Other combinations do not need to be calculated, because the case is symmetric.
                    If SF < K Then
                        WrongComb = True
                    End If
                ElseIf K = 1 Then
                    WrongComb = True  ' If the first system does not fail, the combination is not counted.
                End If

                K = K + 1
            Loop

            ' If this combination is relevant, its probability is calculated
            If (SF > 0) And (WrongComb = False) Then
                FI = FailuresInComb(I)
                FJ = FailuresInComb(J)
                M = 1
                Do While M <= C  ' Calculations for 2 module combinations
                    R = Worksheets("Sheet1").Cells(FI + 1, 6 + M).Value * Worksheets("Sheet1").Cells(FJ + 1, 6 + M).Value
                    Results(SF, M) = Results(SF, M) + R

                    If M = 1 Then
                        Contributions(FI, FJ) = Contributions(FI, FJ) + R
                    End If

                    M = M + 1
                Loop
            End If

            J = J + 1
        Loop

        ' Go through cases where the other group fails due to software CCF
        SF = 0
        WrongComb = False
        K = 1
        Do While (K <= S) And (WrongComb = False)  ' Go through the safety systems
            Failures = 0

            ' Check if the 2 components are failed in this CCFs
            Comp = (K - 1) * 2 + 1
            If CompInComb(Comp, I) Then
                Failures = Failures + 1
            End If

            Comp = (K - 1) * 2 + 2
            If CompInComb(Comp, I) Then
                Failures = Failures + 1
            End If

            If Failures >= 1 Then  ' Is there at least 1 failure?
                SF = SF + 1

                ' Only the combinations where only the first system fails, only the first 2 systems fail, only the first 3 systems fail, etc. are calculated.
                ' Other combinations do not need to be calculated, because the case is symmetric.
                If SF < K Then
                    WrongComb = True
                End If
            ElseIf K = 1 Then
                WrongComb = True  ' If the first system does not fail, the combination is not counted.
            End If

            K = K + 1
        Loop

        ' If this combination is relevant, its probability is calculated
        If (SF > 0) And (WrongComb = False) Then
            FI = FailuresInComb(I)
            M = 1
            Do While M <= C  ' Calculations for 2 module combinations
                R = Worksheets("Sheet1").Cells(FI + 1, 6 + M).Value * Worksheets("Sheet1").Cells(M + 19, 3).Value
                Results(SF, M) = Results(SF, M) + 2 * R

                If M = 1 Then
                    Contributions(FI, 15) = Contributions(FI, 15) + R
                    Contributions(15, FI) = Contributions(15, FI) + R
                End If
```

```
                M = M + 1
            Loop
        End If

        If (I Mod 100) = 0 Then  ' Show the progress
            Worksheets("Sheet1").Cells(21, 13).Value = I / N * 100
        End If
        I = I + 1
    Loop

    K = 1
    Do While K <= S  ' Results are written for different cases
        M = 1
        Do While M <= C
            Worksheets("Sheet1").Cells(K + 1, 12 + M).Value = Results(K, M)
            M = M + 1
        Loop
        K = K + 1
    Loop

    I = 1
    Do While I <= 15
        J = 1
        Do While J <= 15
            Worksheets("Sheet1").Cells(1 + I, 17 + J).Value = Contributions(I, J)
            J = J + 1
        Loop
        I = I + 1
    Loop

    Worksheets("Sheet1").Cells(21, 13).Value = 100
End Sub


' Does the given component fail in the given combination?
Function CompInComb(Comp As Integer, Comb As Integer) As Boolean
    Dim T As Integer
    Dim L As Integer
    Dim C As Integer
    Dim A As Integer
    Dim Result As Boolean

    Result = False
    T = 14
    C = Comb
    L = T
    Do While L > Comp
        A = 2 ^ (L - 1)
        C = C Mod A
        L = L - 1
    Loop

    A = 2 ^ (Comp - 1)
    C = C \ A
    If C = 1 Then
        Result = True
    End If

    CompInComb = Result
End Function


' How many failures are included in the given combination?
Function FailuresInComb(Comb As Integer) As Integer
    Dim L As Integer
    Dim T As Integer
    Dim C As Integer
    Dim A As Integer
    Dim Num As Integer

    Num = 0
    T = 14
    C = Comb
    L = T
    Do While L > 0
        A = 2 ^ (L - 1)
        If C \ A = 1 Then
            Num = Num + 1
        End If

        C = C Mod A
        L = L - 1
    Loop

    FailuresInComb = Num
End Function
```

Appendix B: Risk importance measures

The Fussell-Vesely values of most important basic events with regard to the CDF are listed below.

	Name	Fuss-Ves	Comment
1	LMFW	1.00E+00	Loss of main feed water
2	MFW_NN	9.08E-01	Main feed-water system fails
3	SWS_MP_FR	4.72E-01	Service water system pump stops operating
4	RHR_MP_FR	4.72E-01	Residual heat removal system pump stops operating
5	O_XNN-PMHW	7.32E-02	OIC processor modules HW, spurious stop signal
6	RHR_HX	2.36E-02	Residual heat removal system heat exchanger fails
7	D_XNV-PMHWS	1.03E-02	DRPS processor module HW, spurious stop signal
8	SWS_MP_FS	9.82E-03	Service water system pump fails to start
9	RHR_MP_FS	9.82E-03	Residual heat removal system pump fails to start
10	RHR_MV_FO	9.82E-03	Residual heat removal system motor-operated valve fails to open
11	D_XNV-PMHWSF	4.50E-03	DRPS processor module HW, spurious stop signal and no actuations
12	D_RPVXSL1S	3.00E-03	DRPS water level sensors, spurious stop signal
13	D_RPVXSL1SF	1.27E-03	DRPS water level sensors, spurious stop signal and no actuation
14	RHR_CV_FO	9.82E-04	Residual heat removal system check valve fails to open
15	SWS_A_XNN-PL	7.70E-04	PAC units (CPLD, DA or SR) fail
16	RHR_A_XNN-PL	7.70E-04	PAC units (CPLD, DA or SR) fail
17	EFW_MP_FR	5.01E-04	Emergency feed water system pump stops operating
18	ECC_MP_FR	2.61E-04	Emergency core cooling system pump stops operating
19	CCW_MP_FR	2.61E-04	Component cooling water system pump stops operating
20	H_HW	2.46E-04	Hard-wired backup fails
21	CPO-TK	9.82E-05	Condensation pool failure
22	P_XXV-PMAS	8.29E-05	PRPS processor module AS CCF
23	HVA_AC_FR	5.00E-05	Air cooler 1 stops operating
24	P_XXA-CLHW-AB	3.25E-05	2x CCF Communication links HW
25	P_XXV-CLHW-AB	3.25E-05	2x CCF Communication links HW
26	D_XNA-PMAS	2.40E-05	DRPS processor module AS CCF
27	D_XNV-PMAS	2.40E-05	DRPS processor module AS CCF
28	D_XNV-COHW	1.45E-05	DRPS VU output communication link HW CCF
29	D_XNV-CIHW	1.44E-05	DRPS VU input communication link HW CCF
30	D_XNA-CIHW	1.44E-05	DRPS APU input communication link HW CCF
31	D_XNA-CLHW	1.44E-05	DRPS APU output communication link HW CCF
32	CCW_HX1	1.30E-05	Component cooling water system heat exchanger fails
33	CCW_HX2	1.30E-05	Component cooling water system heat exchanger fails
34	P_XXV-DOHW-AB	1.30E-05	2x CCF Digital output modules HW
35	ADS_MV_FO	1.09E-05	Pressure relief valve fails to open
36	EFW_MP_FS	1.04E-05	Emergency feed water system pump fails to start
37	EFW_MV_FO	1.04E-05	Emergency feed water system motor-operated valve fails to open

The Fussell-Vesely values of most important basic events with regard to the frequency of CD2 are listed below.

	Name	Fuss-Ves	Comment
1	LMFW	1.00E+00	Loss of main feed water
2	MFW_NN	9.06E-01	Main feed-water system fails
3	EFW_MP_FR	7.59E-01	Emergency feed water system pump stops operating
4	ECC_MP_FR	2.70E-01	Emergency core cooling system pump stops operating
5	SWS_MP_FR	2.70E-01	Service water system pump stops operating
6	CCW_MP_FR	2.70E-01	Component cooling water system pump stops operating
7	HVA_AC_FR	7.59E-02	Air cooler 1 stops operating
8	O_XNN-PMHW	7.30E-02	OIC processor modules HW, spurious stop signal
9	H_HW	2.20E-02	Hard-wired backup fails
10	EFW_MV_FO	1.58E-02	Emergency feed water system motor-operated valve fails to open
11	EFW_MP_FS	1.58E-02	Emergency feed water system pump fails to start
12	D_XNV-COHW	1.47E-02	DRPS VU output communication link HW CCF
13	CCW_HX2	1.35E-02	Component cooling water system heat exchanger fails
14	CCW_HX1	1.35E-02	Component cooling water system heat exchanger fails
15	ADS_MV_FO	1.13E-02	Pressure relief valve fails to open
16	D_XNV-PMHWS	1.03E-02	DRPS processor module HW, spurious stop signal

17	A_XNN-PL-AD	6.82E-03	2x CCF PAC unis (CPLD, DA or SR) fail
18	A_XNN-PL-AE	6.82E-03	2x CCF PAC unis (CPLD, DA or SR) fail
19	A_XNN-PL-CE	6.82E-03	2x CCF PAC unis (CPLD, DA or SR) fail
20	A_XNN-PL-CD	6.82E-03	2x CCF PAC unis (CPLD, DA or SR) fail
21	A_XNN-PL-EG	6.82E-03	2x CCF PAC unis (CPLD, DA or SR) fail
22	A_XNN-PL-DG	6.82E-03	2x CCF PAC unis (CPLD, DA or SR) fail
23	A_XNN-PL-BD	6.82E-03	2x CCF PAC unis (CPLD, DA or SR) fail
24	A_XNN-PL-BE	6.82E-03	2x CCF PAC unis (CPLD, DA or SR) fail
25	D_XNV-PMHWSF	6.58E-03	DRPS processor module HW, spurious stop signal and no actuations
26	P_XXV-PMAS	5.90E-03	PRPS processor module AS CCF
27	ECC_MP_FS	5.62E-03	Emergency core cooling system pump fails to start
28	ECC_MV_FO	5.62E-03	Emergency core cooling system motor-operated valve fails to open
29	SWS_MP_FS	5.62E-03	Service water system pump fails to start
30	CCW_MP_FS	5.62E-03	Component cooling water system pump fails to start
31	D_RPVXSL1S	2.99E-03	DRPS water level sensors, spurious stop signal
32	P_XXA-AIHW-BC	2.53E-03	2x CCF Analog input modules HW (RPS-A and -B)
33	D_XNV-COOP	2.45E-03	DRPS communication link OP CCF
34	A_XNN-PL-ABCDEFG	2.35E-03	7x CCF PAC unis (CPLD, DA or SR) fail
35	P_XXA-CLHW-AB	2.31E-03	2x CCF Communication links HW
36	P_XXV-CLHW-AB	2.31E-03	2x CCF Communication links HW
37	P_XXA-AIHW-BCD	1.88E-03	3x CCF Analog input modules HW (RPS-A and -B)
38	EFW_CV_FO	1.58E-03	Emergency feed water system check valve fails to open
39	DWS-TK	1.58E-03	Demineralized water storage tank unavailable
40	HVA_AC_FS	1.58E-03	Air cooler 1 fails to start
41	D_RPVXSL1SF	1.32E-03	DRPS water level sensors, spurious stop signal and no actuation
42	HVA_A_XNN-PL	1.24E-03	PAC units (CPLD, DA or SR) fail
43	EFW_A_XNN-PL	1.24E-03	PAC units (CPLD, DA or SR) fail
44	A_XNN-PL-CEG	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
45	A_XNN-PL-CDG	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
46	A_XNN-PL-CEF	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
47	A_XNN-PL-CDF	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
48	A_XNN-PL-CDE	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
49	A_XNN-PL-BCE	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
50	A_XNN-PL-BCD	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
51	A_XNN-PL-EFG	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
52	A_XNN-PL-DFG	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
53	A_XNN-PL-DEG	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
54	A_XNN-PL-BDE	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
55	A_XNN-PL-BDF	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
56	A_XNN-PL-BEF	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
57	A_XNN-PL-BDG	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
58	A_XNN-PL-BEG	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
59	A_XNN-PL-AEG	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
60	A_XNN-PL-ADG	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
61	A_XNN-PL-AEF	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
62	A_XNN-PL-ADF	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
63	A_XNN-PL-ADE	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
64	A_XNN-PL-ACE	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
65	A_XNN-PL-ABE	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
66	A_XNN-PL-ACD	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail
67	A_XNN-PL-ABD	1.08E-03	3x CCF PAC unis (CPLD, DA or SR) fail

Appendix C: Hardware CCF values for complementary analyses

The CCF probabilities for the DRPS are listed in Table 23 and DRPS spurious signal cases in Table 24.

Table 23. Hardware CCF probabilities for DRPS components.

Unit	Module	Reference Alpha	Case 1 Beta	Case 2 Beta	Case 3 Beta
APU	PM	7.30E-05	2.76E-05	4.32E-05	1.07E-04
APU	CL	5.99E-04	2.27E-04	3.55E-04	8.82E-04
VU	DO	2.40E-04	9.12E-05	1.42E-04	3.54E-04
VU	PM	7.30E-05	2.77E-05	4.32E-05	1.08E-04
VU	CL	5.99E-04	2.27E-04	3.55E-04	8.82E-04
	SR	2.50E-05	9.49E-06	1.48E-05	3.68E-05
RCOiSP	Sensor	2.41E-05	9.14E-06	1.43E-05	3.55E-05
RPViSL	Sensor	2.41E-05	9.14E-06	1.43E-05	3.55E-05
RPViSP	Sensor	2.41E-05	9.14E-06	1.43E-05	3.55E-05
CPiST	Sensor	2.41E-05	9.14E-06	1.43E-05	3.55E-05

Table 24. DRPS CCFs leading to spurious signals.

DRPS spurious signal cases	Reference Alpha	Case 1 Beta	Case 2 Beta	Case 3 Beta
Two spurious signals due to a CCF of the PMs of the DRPS VUs (but not three)	1.65E-04	0.00E+00	0.00E+00	0.00E+00
Three spurious signals due to a CCF of the PMs of the DRPS VUs (all safety signals of the DRPS fail)	7.02E-05	2.43E-05	3.80E-05	9.44E-05
Two spurious signals from the DRPS because two water level sensors show high value	5.70E-04	0.00E+00	0.00E+00	0.00E+00
Three spurious signals from the DRPS because three water level sensors show high value (the corresponding safety signals of the DRPS fail)	2.42E-04	8.38E-05	1.31E-04	3.26E-04

The CCF probabilities for the PRPS are listed in Table 25. In the table, probabilities of CCFs causing failure of one and two subsystems are presented (1 sub and 2 subs).

Table 25. Hardware CCF probabilities for PRPS components.

		Ref alpha		Case 1		Case 2		Case 3	
Unit	Module	1 sub	2 subs	1 sub	2 subs	1 sub	2 subs	1 sub	2 subs
APU	AI	2.00E-05	8.00E-06	1.62E-05	2.56E-06	1.88E-05	5.10E-06	2.93E-05	1.56E-05
APU	PM	1.51E-05	7.88E-06	8.42E-06	1.33E-06	9.73E-06	2.64E-06	1.52E-05	8.09E-06
APU	CL	7.50E-05	3.92E-05	4.19E-05	6.62E-06	4.85E-05	1.32E-05	7.57E-05	4.03E-05
VU	DO	3.00E-05	1.57E-05	1.68E-05	2.65E-06	1.94E-05	5.27E-06	3.03E-05	1.61E-05
VU	PM	1.48E-05	7.76E-06	8.29E-06	1.31E-06	9.58E-06	2.60E-06	1.50E-05	7.97E-06
VU	CL	7.50E-05	3.92E-05	4.19E-05	6.62E-06	4.85E-05	1.32E-05	7.57E-05	4.03E-05
	SR	7.50E-07	3.92E-07	4.19E-07	6.62E-08	4.85E-07	1.32E-07	7.57E-07	4.03E-07
RCOiSP	Sensor	2.41E-05		7.91E-06		9.14E-06		1.43E-05	
RPViSL	Sensor	2.41E-05		7.91E-06		9.14E-06		1.43E-05	
RPViSP	Sensor	2.41E-05		7.91E-06		9.14E-06		1.43E-05	
CPiST	Sensor	2.41E-05		7.91E-06		9.14E-06		1.43E-05	

The failure probabilities for the PAC are listed in Table 26.

Table 26. Hardware failure probabilities for PAC failure cases.

CCF case	Ref	Case 1	Case 2	Case 3
3-o-o-4 failure of PAC units serving the same front-line system (CPLD, DA and SR failures)	5.98E-07	5.14E-07	5.82E-07	8.57E-07
3-o-o-4 failure for all front-line systems due to PAC CCFs (CPLD, DA and SR CCFs)	3.61E-10	2.63E-11	1.04E-10	9.75E-10
3-o-o-4 PM/CL failures in PAC units serving the same front-line system	1.32E-06	1.16E-06	1.31E-06	1.91E-06
3-o-o-4 PM/CL failures in all front-line systems due to CCFs	7.98E-10	5.80E-11	2.29E-10	2.15E-09
3-o-o-4 failure of AD modules that take input from the same system and serve the same front-line safety system	2.00E-07	1.76E-07	2.00E-07	2.96E-07
Two 3-o-o-4 failures of AD modules that serve the same front-line safety system (one corresponding to inputs from the PRPS and one corresponding to inputs from the H-W backup)	6.70E-10	4.50E-10	6.70E-10	1.98E-09
Failure of all 56 AD modules	2.55E-11	6.43E-12	2.55E-11	2.39E-10