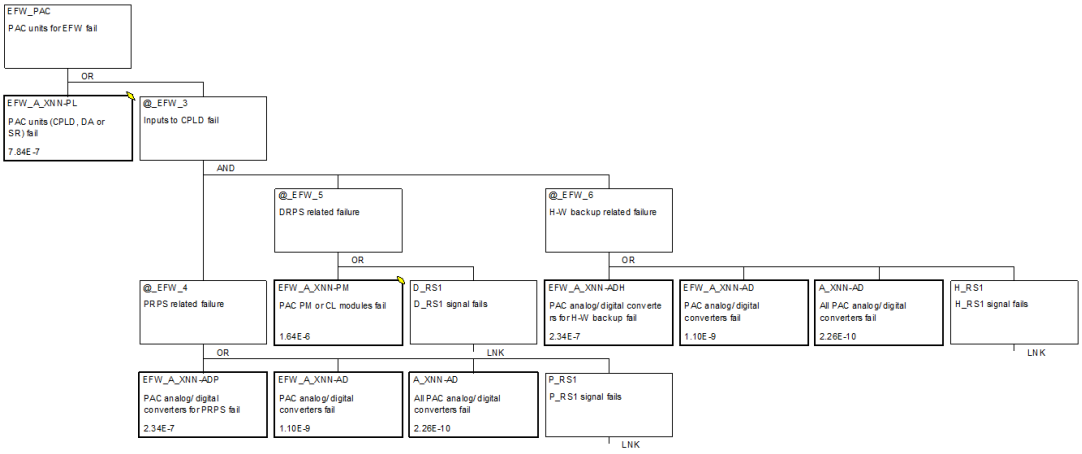
RESEARCH REPORT

VTT-R-00522-25



Probabilistic risk assessment of a digital I&C architecture

Authors: Tero Tyrväinen

Confidentiality: VTT Public

Version: 8.12.2025

Report's title Probabilistic risk assessment of a digital I&C architecture	
Customer, contact person, address VYR	**Order reference** SAFER 6/2025
Project name Probabilistic Risk Assessment Labour, Improvements and Extensions	**Project number/Short name** 141374/PRALINE
Author(s) Tero Tyrväinen	**Pages** 42/7
Keywords probabilistic risk assessment, instrumentation and control, common cause failure	**Report identification code** VTT-R-00522-25

Summary

This report presents a 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.

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.

When comparing the results with other DIGMORE participants, some interesting observations were made on CCF models. The beta-factor model is normally considered a conservative CCF model compared to the alpha-factor model. However, in certain situations, the beta-factor model is not conservative at all and can actually be optimistic. This is the case, e.g., when a failure criterion 2-out-of-N is modelled.

Variations made to the base case model demonstrated the importance of diversity. The PAC systems were much less reliable when no diversity was assumed, and the removal of the back-up systems increased the risk significantly. The significance of software failures is quite sensitive to the failure probabilities used in the model.

Confidentiality	VTT Public

Espoo 9.12.2025

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

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

Distribution (customer and VTT)

SAFER2028 TAG1.1 members, VTT archive

Approval

VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD

Date:	09 December 2025
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
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 overall goal is to provide recommendations for the development of PRA models concerning digital I&C systems.

This report presents VTT's PRA analyses performed the DIGMORE reference case (OECD NEA CSNI, 2025). The reference case is first briefly described in Section 2. The PRA model for the "base case" is presented in Section 3. The model is the same as the one already presented in the previous report (Tyrväinen & Björkman, 2024). Compared to the previous report, some new observations and conclusions have been added. Section 4, on the other hand, describes new analyses performed by varying configurations, assumptions and parameters compared to the base case. Section 5 concludes the study.

2. Reference case description

This chapter gives a brief description of the DIGMORE reference case (OECD NEA CSNI, 2025).

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.

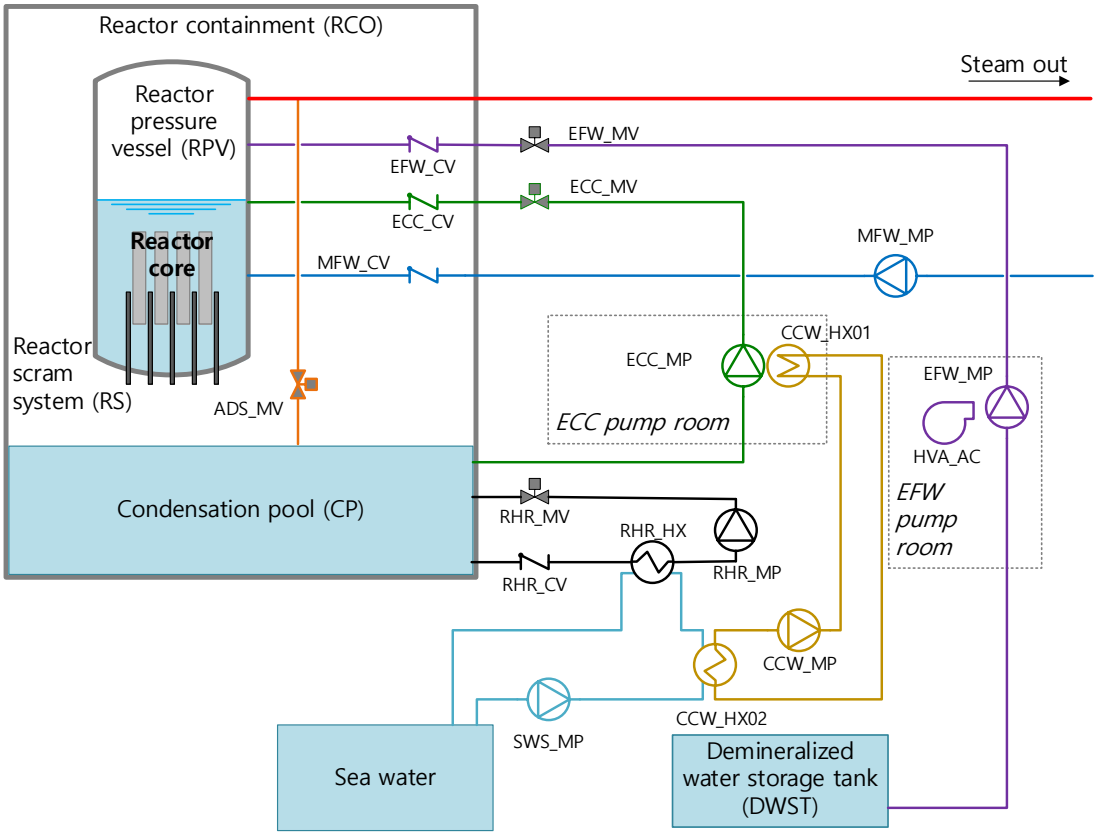


Figure 1. The layout of main safety systems (OECD NEA CSNI, 2025).

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 the I&C

systems is presented in Figure 2. When the measurement data indicates a need for a 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.

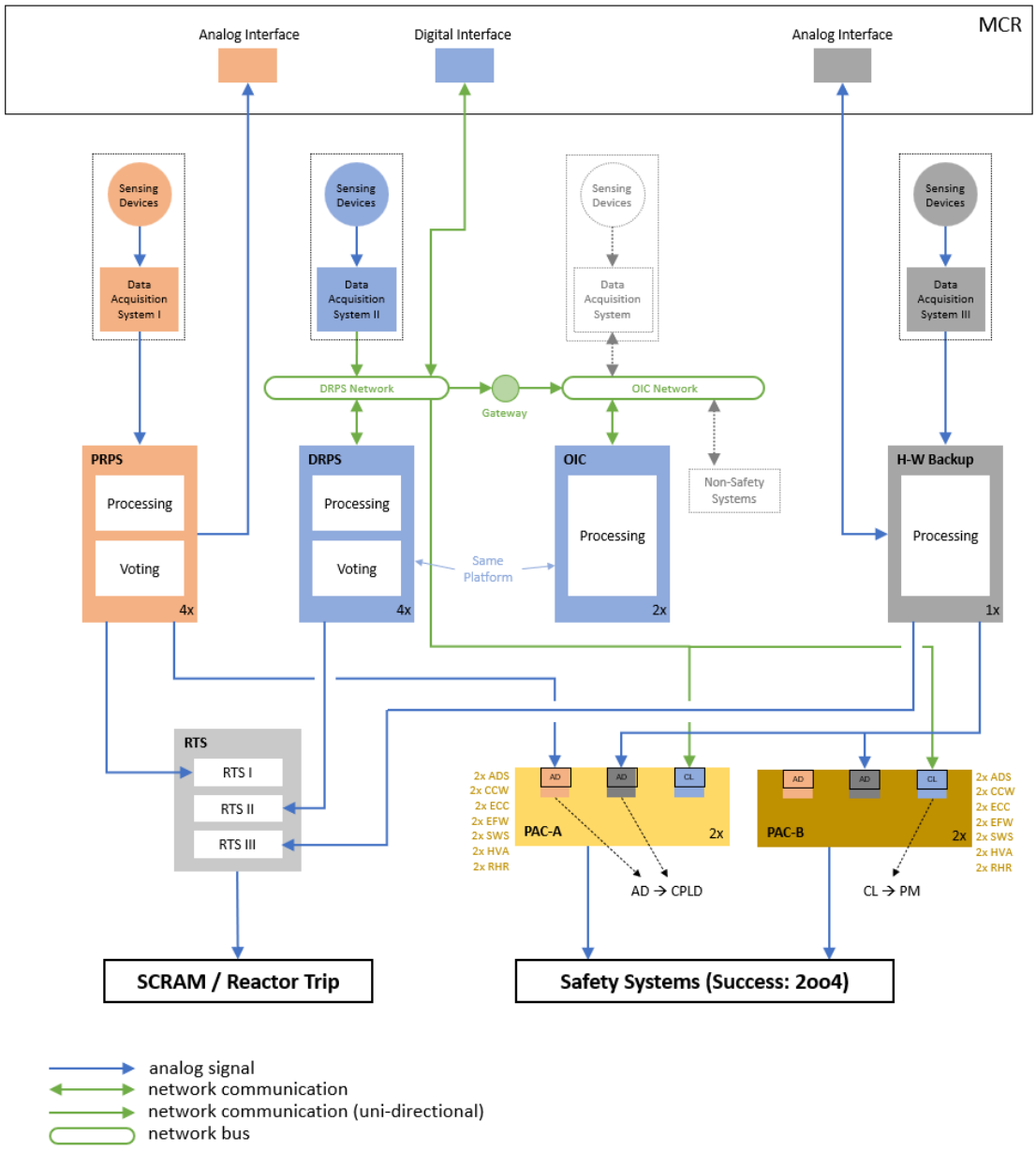


Figure 2. The architecture of I&C systems (OECD NEA CSNI, 2025).

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 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 and RTS. 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.

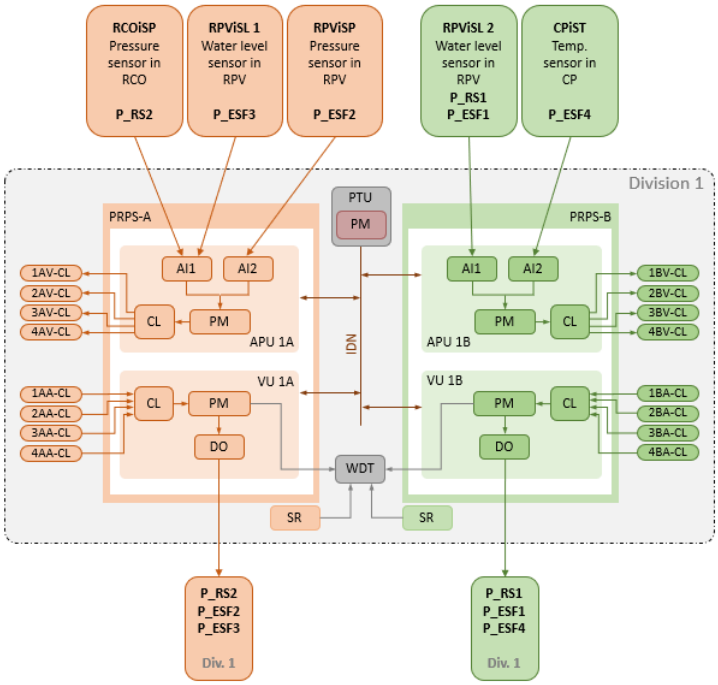


Figure 3. Primary reactor protection system layout (OECD NEA CSNI, 2025).

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
RHR	Pump	Start	RS2: high pressure in containment ESF4: high temperature in condensation pool	RS2 + ESF4

System	Component	Control	Conditions	Signal
	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, 2025) contains fictive reliability parameters for HW, OP and AS of each module. OP and AS failure probabilities are defined on demand basis. For HW failures, a 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 any AI modules, instead 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.

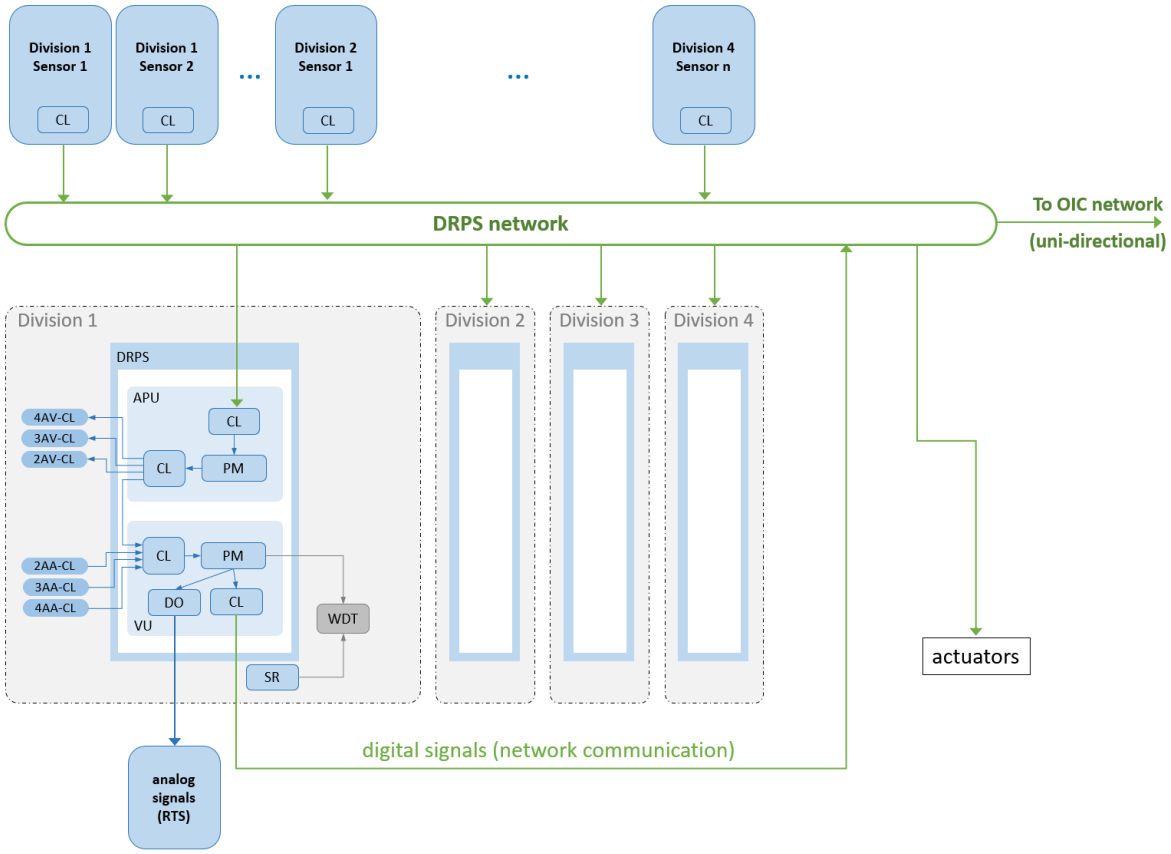


Figure 4. Diverse reactor protection system layout (OECD NEA CSNI, 2025).

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.

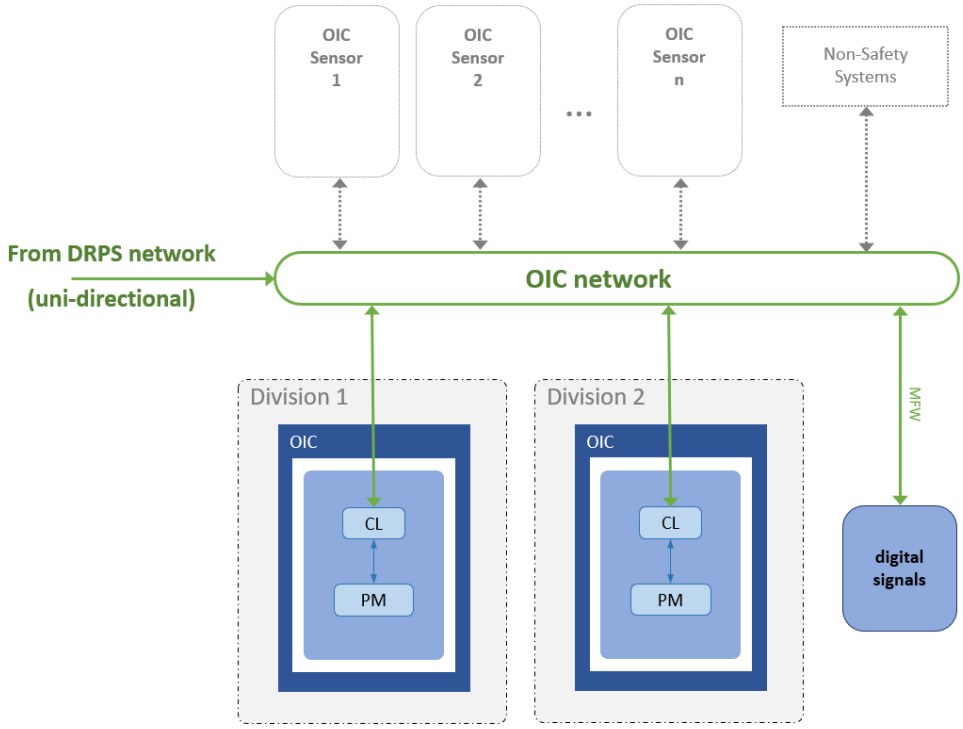


Figure 5. Operational I&C system layout (OECD NEA CSNI, 2025).

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.

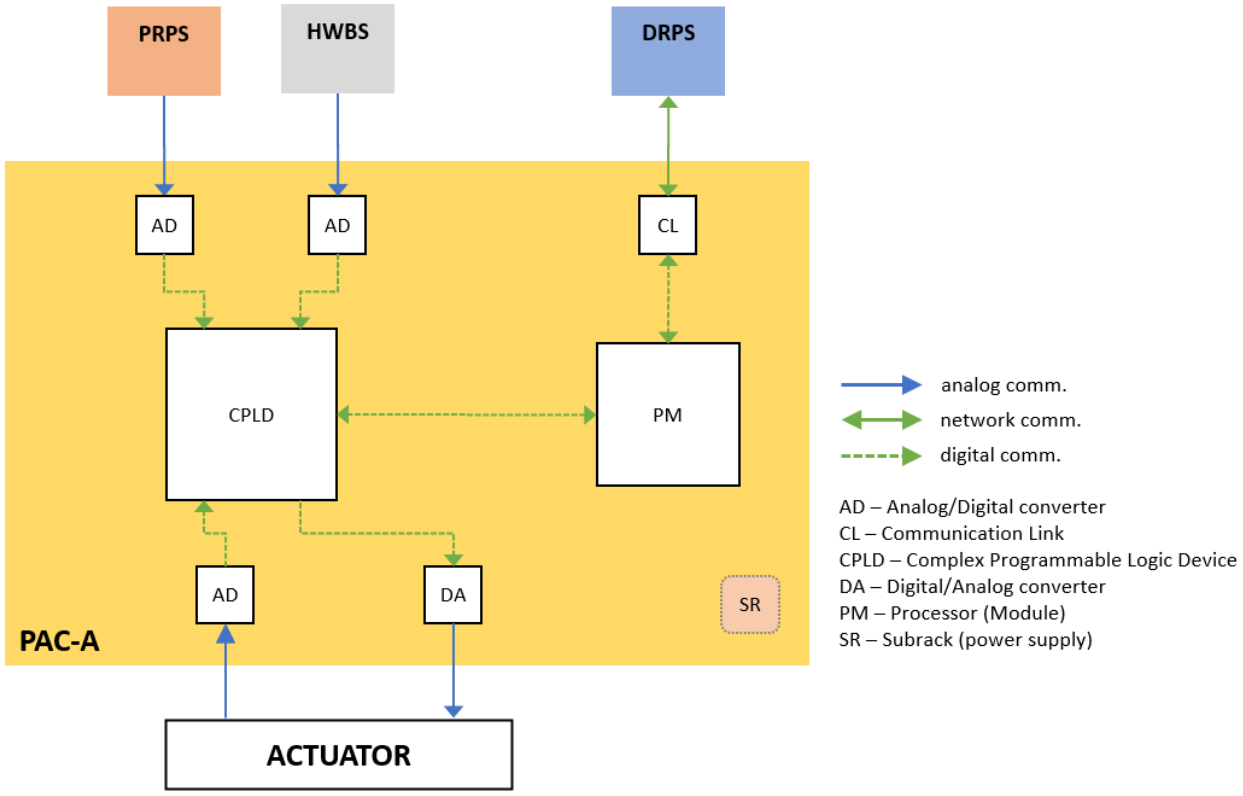


Figure 6. The layout of a PAC unit (OECD NEA CSNI, 2025).

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. The digital input signal from the DRPS is received by the CL and is transferred to the CPLD through the PM. 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, 2025) to the participants of the benchmark study.

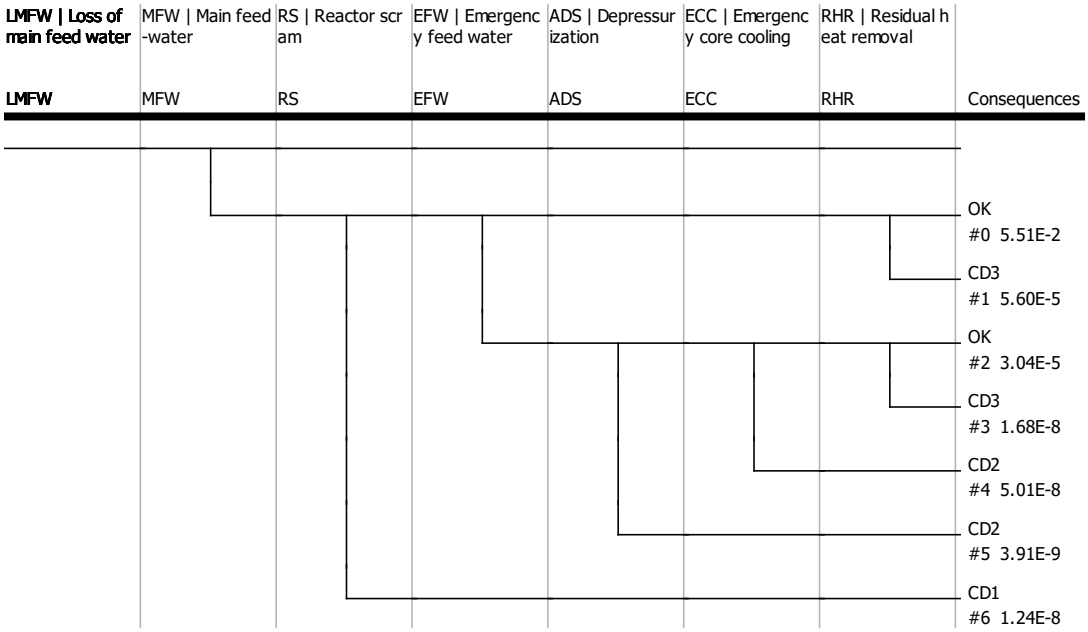


Figure 7. Event tree for loss of main feed-water.

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, 2025). 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 HWBS failures as there is only one redundancy), and the fault trees represent joint failures of redundant trains instead of only one train. For the PRPS and DRPS, 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, 2025) 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, 2025).

Module	Failure rate (/h)	F	AF	PF	APF	Automatic testing by
APU AI	2E-6	0.2	0.4	0.2	0.2	APU PM
APU PM	2E-6	0.1	0.7	0.1	0.1	VU PM
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	WDT
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		WDT

For other systems, there are similar tables (OECD NEA CSNI, 2025), 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

$$P_d = \lambda T_r, \quad (1)$$

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

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

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).

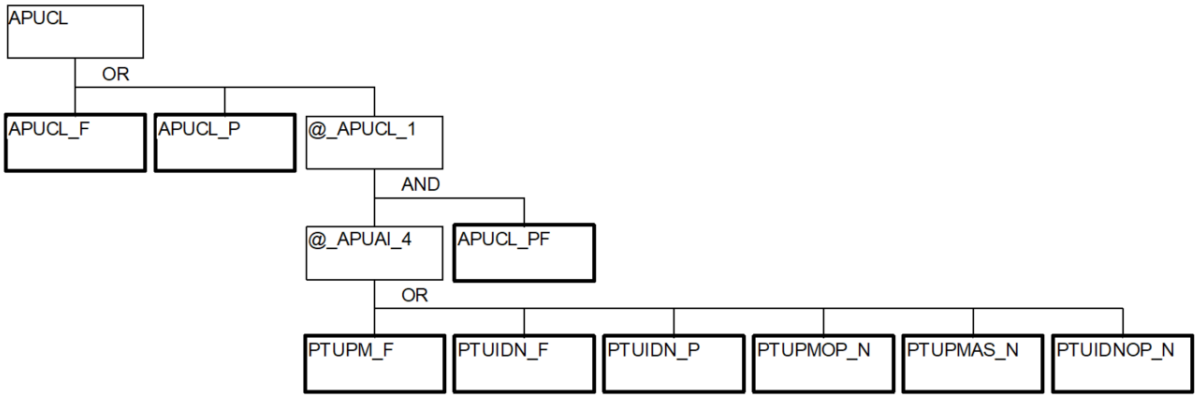


Figure 8. Fault tree of undetected APU CL failure.

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 1.00E-04	APUCL_PF PTUPMAS_N
6	8.71E-08	0.00	100.00	8.71E-03 1.00E-05	APUCL_PF PTUIDNOP_N
7	8.71E-08	0.00	100.01	8.71E-03 1.00E-05	APUCL_PF PTUPMOP_N
8	3.48E-08	0.00	100.01	8.71E-03 4.00E-06	APUCL_PF 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 in 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, 2025) 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. Therefore, the modified beta-factor model and partial beta-factor method are applied for that case. 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 CL 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 (Tyrväinen et al., 2023). All HW CCF groups in the PRPS, 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 numbers were calculated “manually” in Excel for this study, but a recently developed tool (Björkman, 2025) also calculated the same numbers. 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. A comparison of the alpha-factor model and the modified beta-factor model was performed in the previous report (Tyrväinen & Björkman, 2024).

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 be 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 be 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 OP 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 the inputs from the PRPS and one corresponding to the 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, the 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 the reactor scram and the initiating event fault tree are presented in this section (Figures 9-29). The other safety functions have been modelled with similar types of fault trees. The model contains in total 59 fault trees.

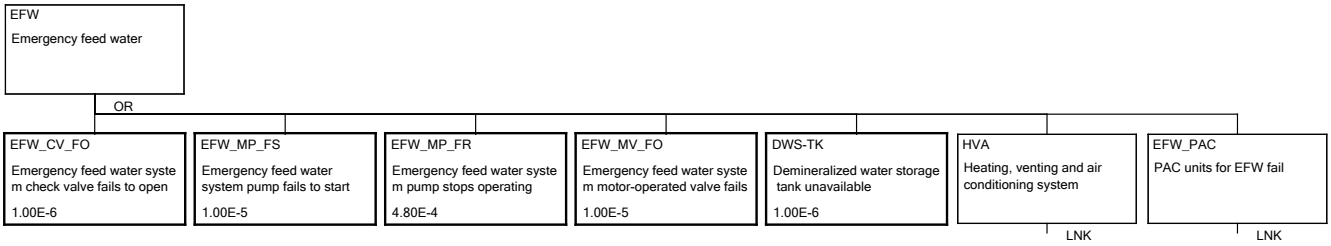


Figure 9. Fault tree for the emergency feed-water system.

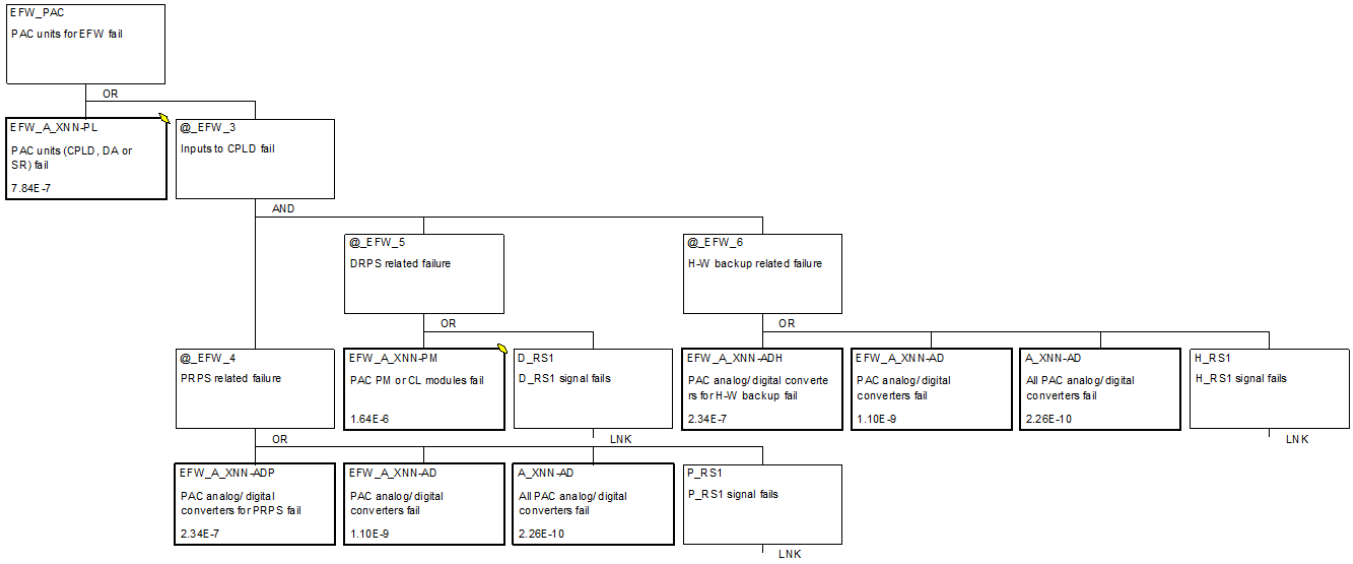


Figure 10. Fault tree for PAC (3-out-of-4 units fail).

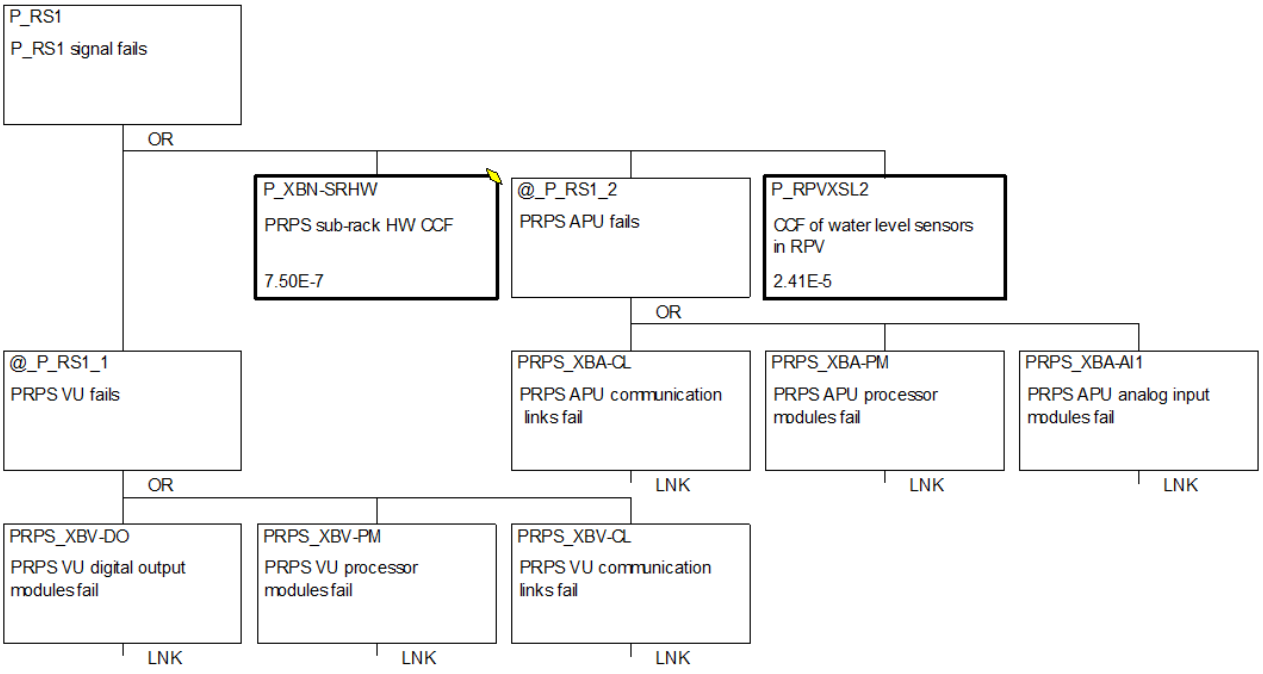


Figure 11. Fault tree for P_RS1 signal from PRPS-B (3-out-of-4 divisions fail).

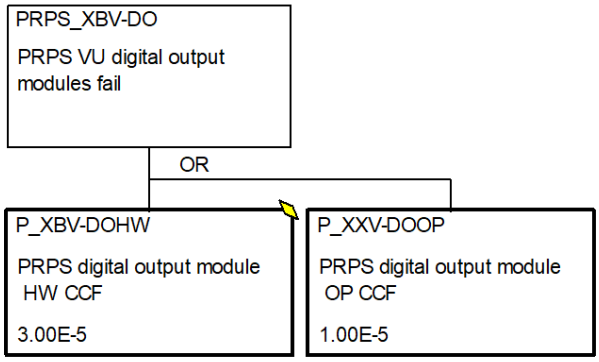


Figure 12. Fault tree for the digital output modules in PRPS voting units (3-out-of-4 divisions fail).

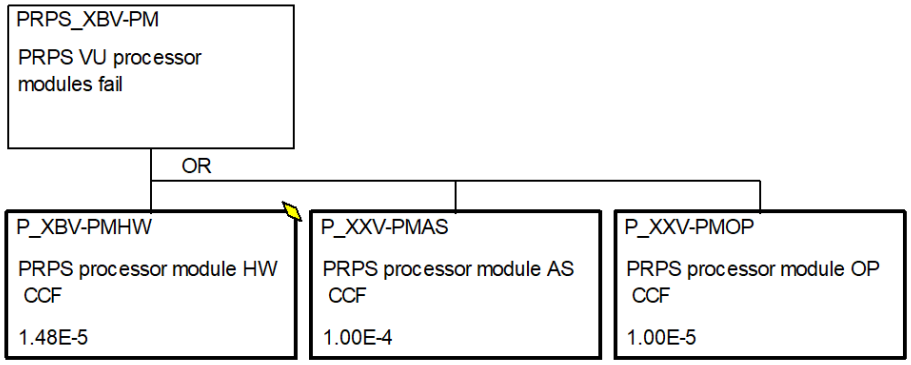


Figure 13. Fault tree for the processor modules in PRPS voting units (3-out-of-4 divisions fail).

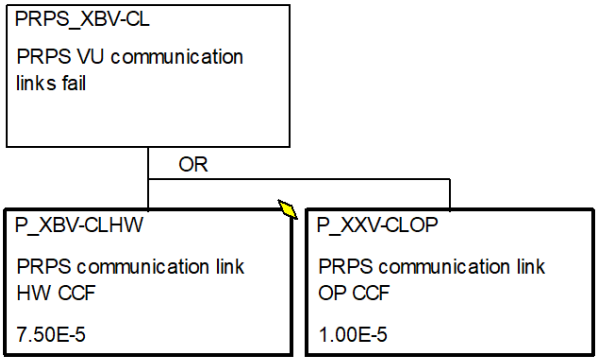


Figure 14. Fault tree for the communication links in PRPS voting units (3-out-of-4 divisions fail).

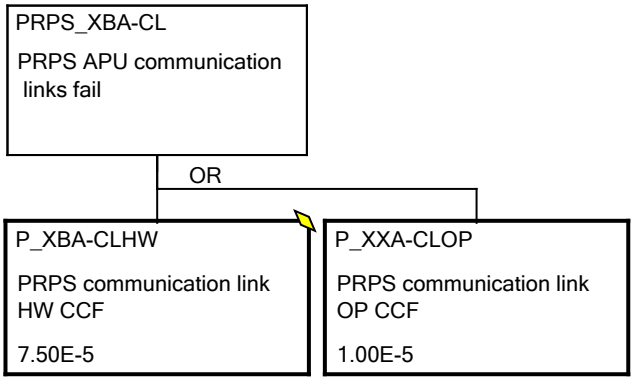


Figure 15. Fault tree for the communication links in PRPS APUs (3-out-of-4 divisions fail).

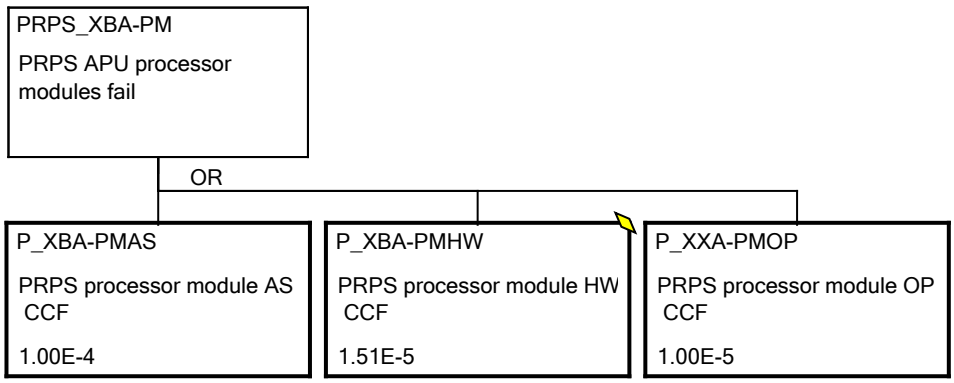


Figure 16. Fault tree for the processor modules in PRPS APUs (3-out-of-4 divisions fail).

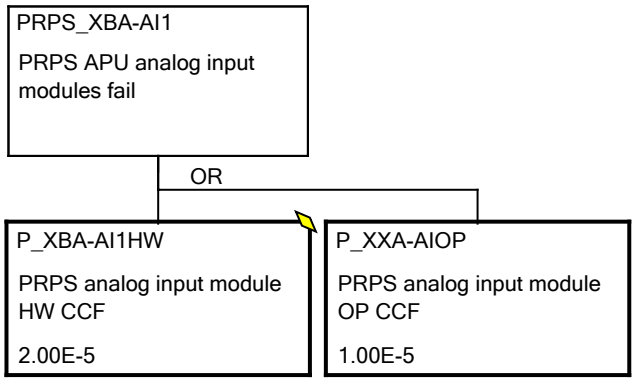


Figure 17. Fault tree for the analog input modules in PRPS APUs (3-out-of-4 divisions fail).

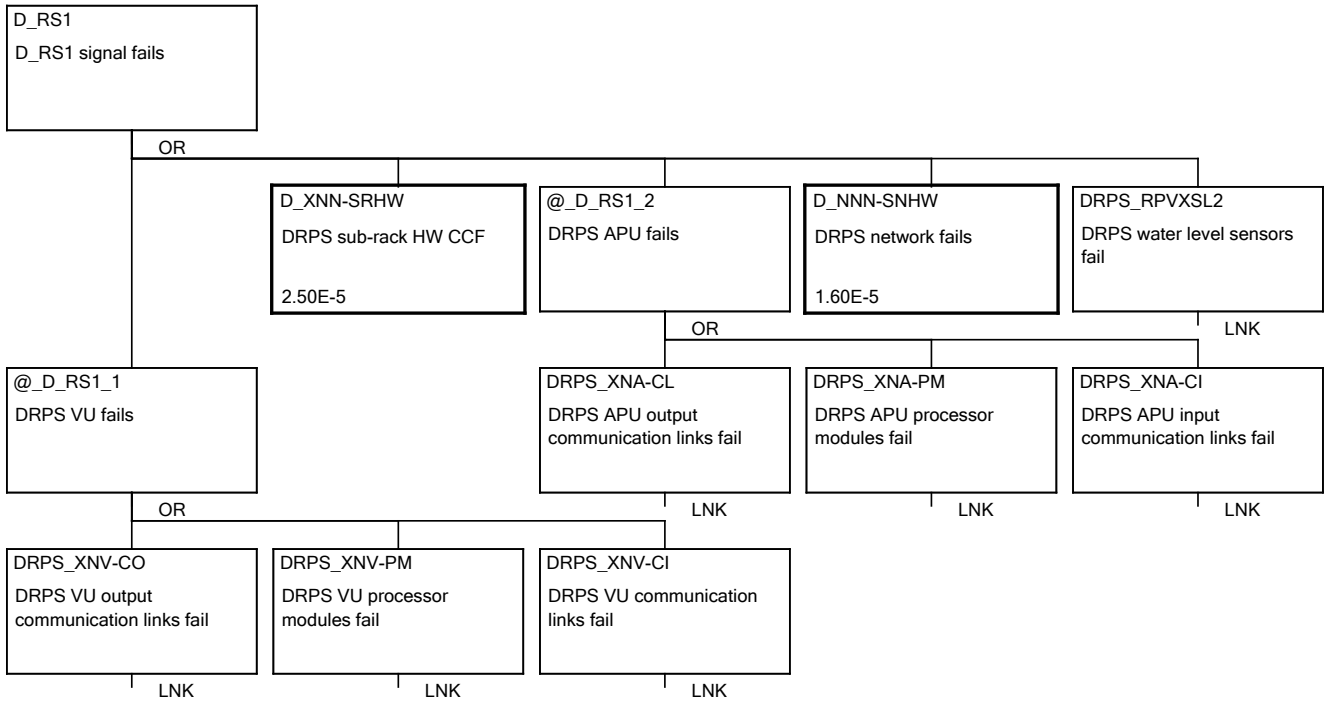


Figure 18. Fault tree for D_RS1 signal from the DRPS (3-out-of-4 divisions fail). There is another variant of this fault tree for reactor scram modelling, where the VU output CL is replaced by DO.

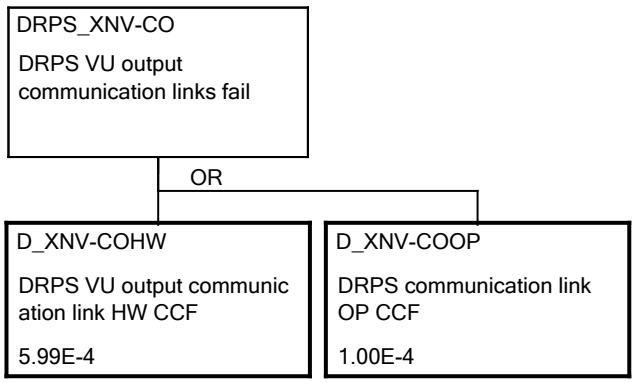


Figure 19. Fault tree for output communication links in DRPS voting units (3-out-of-4 divisions fail).

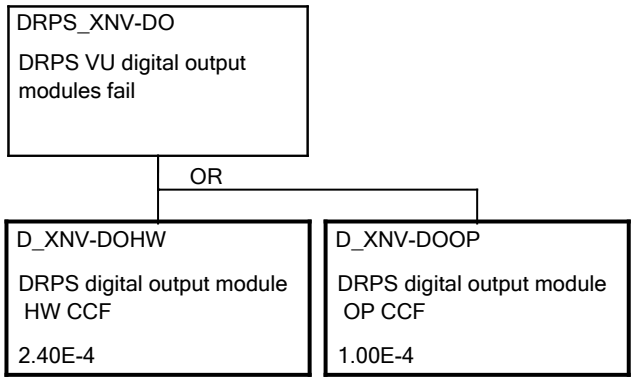


Figure 20. Fault tree for digital output modules in DRPS voting units (3-out-of-4 divisions fail).

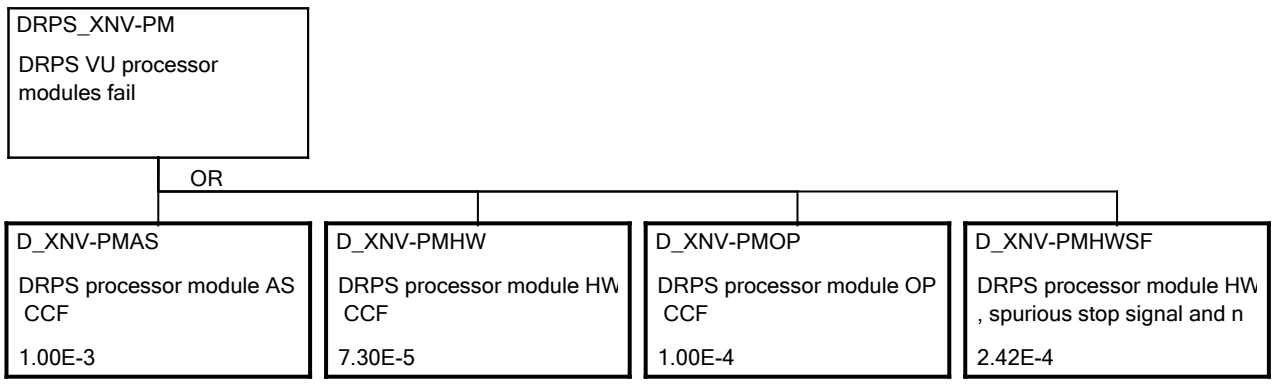


Figure 21. Fault tree for the processor modules in DRPS voting units (3-out-of-4 divisions fail). D_XNV-PMHWSF is an initiating event that is also assumed to cause failures of the safety function actuation signals in the PMs.

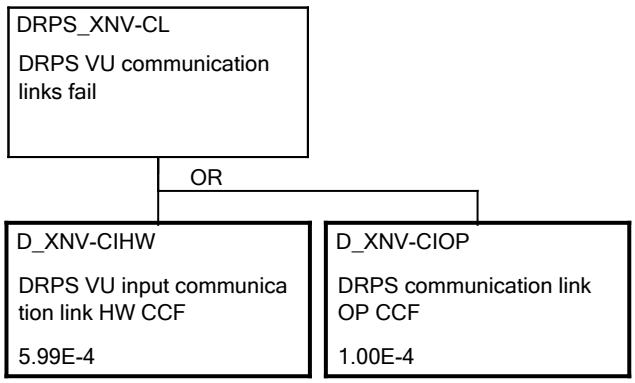


Figure 22. Fault tree for the input communication links in DRPS voting units (3-out-of-4 divisions fail).

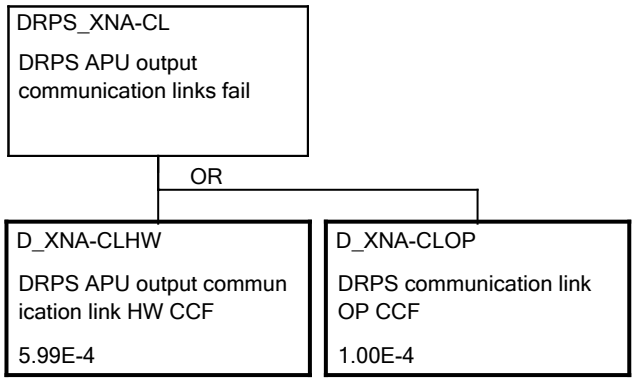


Figure 23. Fault tree for the output communication links in DRPS APUs (3-out-of-4 divisions fail).

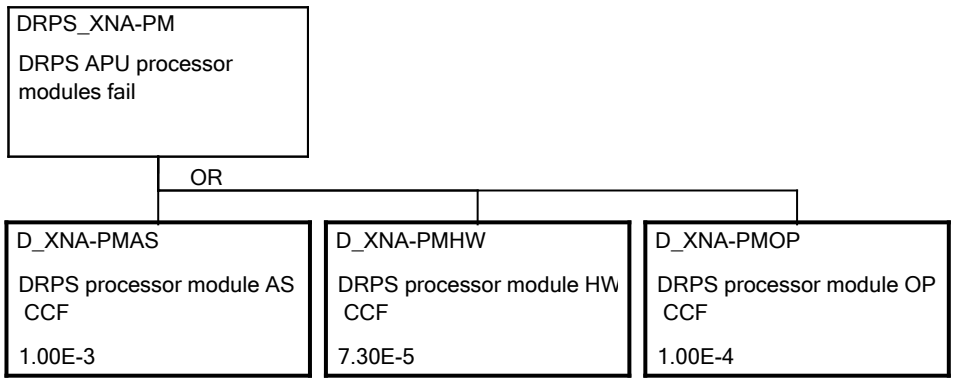


Figure 24. Fault tree for the processor modules in DRPS APUs (3-out-of-4 divisions fail).

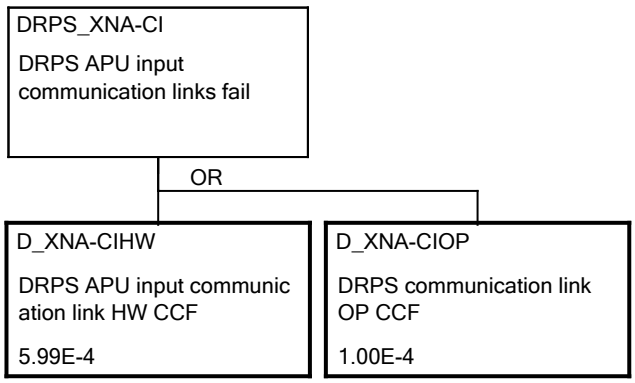


Figure 25. Fault tree for the input communication links in DRPS APUs (3-out-of-4 divisions fail).

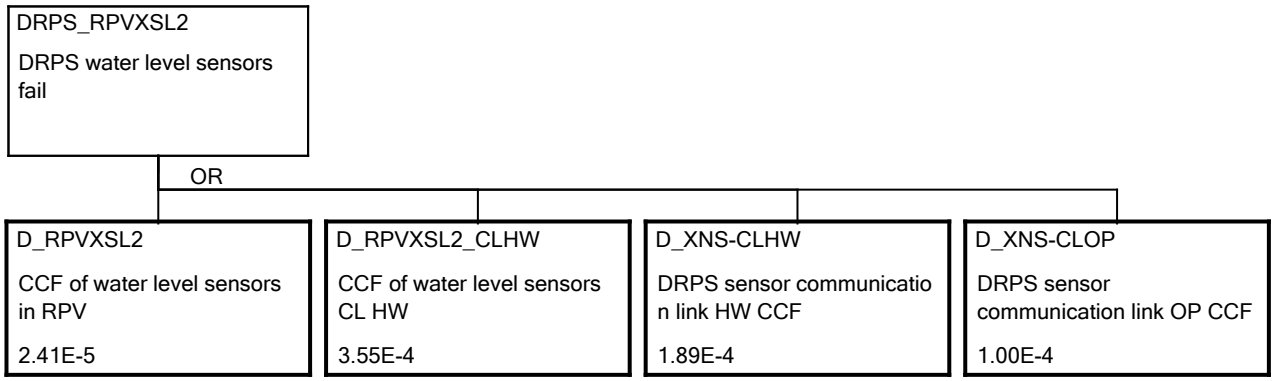


Figure 26. Fault tree for DRPS water level sensors (3-out-of-4 divisions fail).

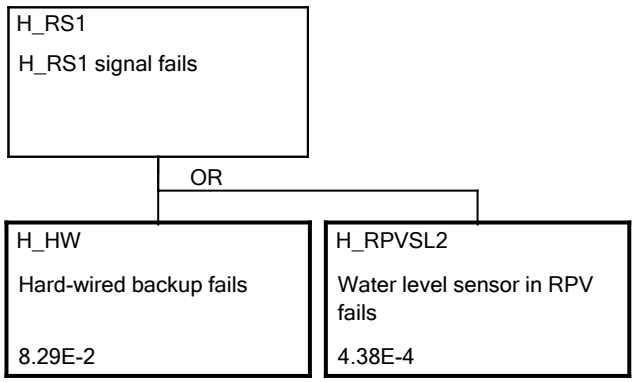


Figure 27. Fault tree for H_RS1 signal from the H-W backup system.

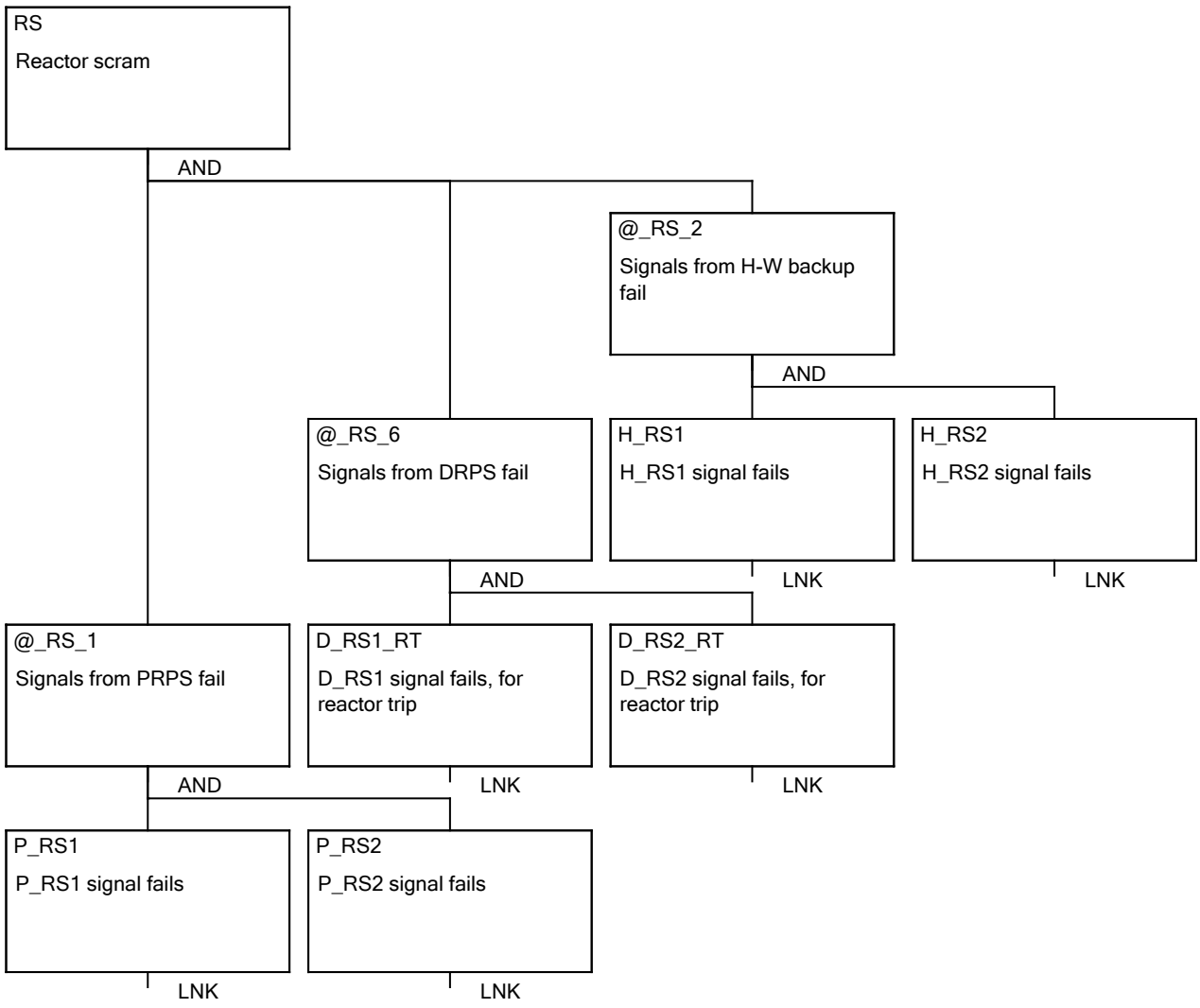


Figure 28. Fault tree for the reactor scram.

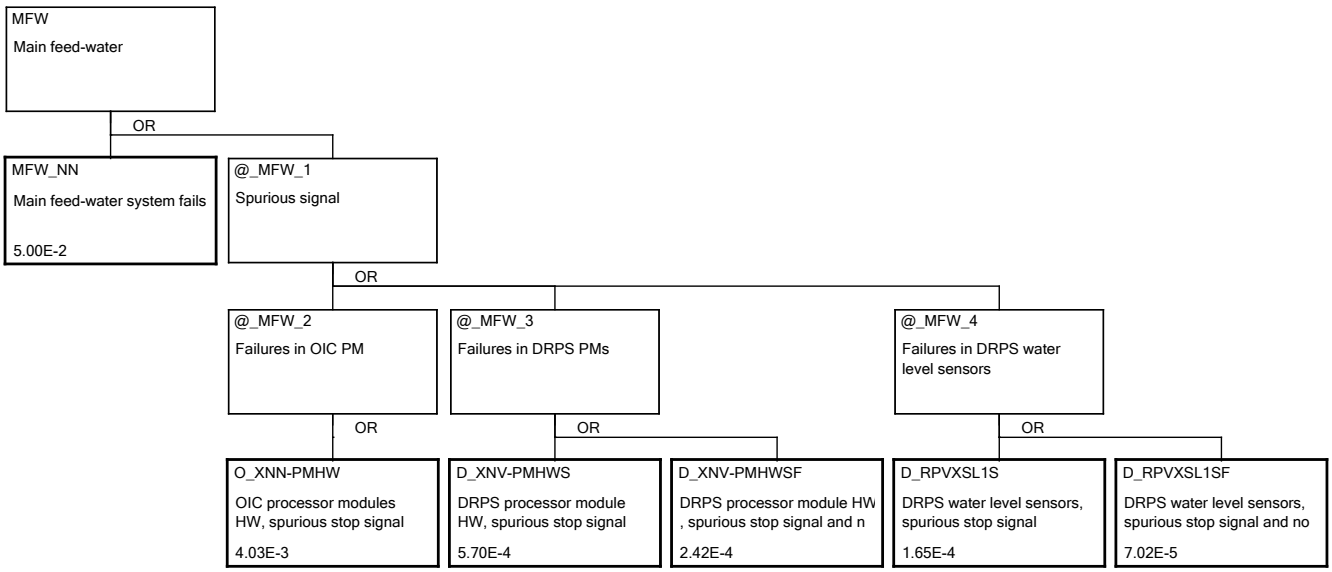


Figure 29. Fault tree for the initiating events.

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 (anticipated transient without scram (ATWS)). 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.

The Fussell-Vesely of software failures is approximately 5E-4, if spurious signals are not counted (spurious signals were not modelled separately for HW and software). The risk contribution of PAC is dominated by HW failures. The contribution of OP CCFs to the CDF related to PAC is approximately 18%. The Fussell-Vesely of AS CCFs in the PRPS and DRPS is 1.2E-4, and the Fussell-Vesely of OP CCFs in the PRPS and DRPS is 6.5E-5. The contributions of HW and software are in better balance for the PRPS.

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

3.8 Observations on common cause failure models

When comparing the results with different DIGMORE participants, it was noticed that VTT has a higher frequency for consequence CD2. Particularly, the risk contribution of PAC systems was significantly higher in VTT's model than in other models. VTT's CD2 frequency related to PAC failures was about 200% larger than with some of the participants that had applied the beta-factor model with relatively high beta parameters (e.g. 0.05) for the CCF of 14 identical PAC units. Detailed analysis revealed the following reasons for this surprising result:

- The beta-factor model is not necessarily conservative if the failure criterion is 2-out-of-N or similar but can actually be optimistic. This is explained below in detail.
- The alpha-factor parameters used by VTT result in higher total probability of CCFs than the beta parameters used by other participants. With the generic alpha-factor parameters used by VTT, the portion of CCFs of the failures of one unit is 0.206, which is significantly larger than beta parameter 0.05.
- VTT used a conservative factor adding 10% extra to the calculated PAC failure probabilities. Obviously, this had only a minor impact.

In the DIGMORE model, the occurrence of CD2 requires failure of two systems. To illustrate the difference between the alpha-factor model and beta-factor model, let us first consider a case with six identical components and failure criterion 2-out-of-6. The total failure probability for one component is 0.01. For the alpha-factor model, we use the parameters in Table 10 taken from the DIGMORE reference case description (OECD NEA CSNI, 2025). The CCF and single failure probabilities calculated using the alpha-factor model are presented in Table 11 (Q1 is the single failure probability, and Qi is the probability for a CCF event with i components). For comparison, we use the beta-factor model with the beta parameter 0.143. In that case, the single failure probabilities are the same with both models. Also, with the alpha-factor model, the sum of the probabilities of CCF events related to one specific component is the same as the CCF probability using the beta-factor model (1.43E-3).

Table 10. The parameters of the alpha-factor model.

α_1	α_2	α_3	α_4	α_5	α_6
0.938	0.041	0.0135	0.00426	0.00206	0.00118

Table 11. Common cause failure and single failure probabilities calculated using the alpha-factor model.

Q1	Q2	Q3	Q4	Q5	Q6
8.57E-3	1.50E-4	3.70E-5	1.56E-5	1.88E-5	6.47E-5

For failure criterion 2-out-of-6, the alpha-factor model gives total failure probability 4.50E-3, and the beta-factor model gives total failure probability 2.53E-3. The alpha-factor model gives 78% larger result. The reason for the difference is that the CCF probability with the beta-factor model only corresponds to the CCF combinations including one specific component while there are many more CCF combinations leading to 2-out-of-6 failure. The difference in the CCF combinations is shown in Table 12. For example, there are 15 different CCF combinations with two components (total probability 2.25E-3), while there are only 5 CCF combinations related to one specific component (total probability 7.49E-4).

Table 12. CCF combinations.

The number of components in CCF	The number of CCF combinations related to one specific component	The number of CCF combinations in total	The number of CCF combinations for failure criterion (C1 + C2) * (C3 + C4 + C5 + C6)
2	5	15	8
3	10	20	16
4	10	15	14
5	5	6	6
6	1	1	1

To make sure that the beta-factor model is not optimistic, the beta parameter could be selected so that it corresponds to all the possible combinations instead of the combinations related to one specific component. In that case, the beta parameter would be 0.340, the single failure probability would be 6.60E-3, and the CCF probability would be 3.4E-3. Even in this case, the beta-factor model would give smaller total probability (4.05E-3), because the single failure probabilities would be smaller than with the alpha-factor model.

In the DIGMORE case, the failure criterion for CD2 is (EFW + HVA) * (ADS + ECC + CWC + SWS), i.e. either EFW or HVA must fail and either ADS, ECC, CWC or SWS must fail. In the example case, a corresponding failure criterion would be (C1 + C2) * (C3 + C4 + C5 + C6), where Ci means failure of component i. With this failure criterion, the alpha-factor model gives total failure probability 2.80E-3, and the beta-factor model gives total failure probability 2.02E-3 (with beta parameter 0.143). The alpha-factor model gives 37% larger result. Again, this is explained by the fact that there are more CCF combinations satisfying the failure criterion than CCF combinations related to one specific component as presented in Table 12.

This example shows that the beta-factor model can actually be optimistic when the failure criterion is 2-out-of-N or similar. If the beta-factor model is used in that kind of case, the beta parameter should be selected carefully.

In the DIGMORE case, there are seven safety systems, one of which has no relevance for CD2. The failure probabilities for N specific systems are presented in Table 6 (N = 1,…,7). Let us consider only the values related CPLD, DA and SR modules as the other events have negligible risk contribution. The values in Table 6 are not CCF probabilities but involve two or more events as explained in Section 3.4.2. However, similar characteristics can be observed as with CCF probabilities. If we sum the probabilities of system failure combinations that include at least two systems failing and are related to one specific system, the result is 7.38E-8. Let us assume “conservatively” that this is the failure probability for all seven systems. This can be interpreted to correspond to the CCF probability with the beta-factor model in our previous example, while the probabilities in Table 6 correspond to the CCF probabilities calculated using the alpha-factor model. With the values from Table 6, the CD2 frequency is 5.89E-9/year (from PAC failures). With the “conservative” probability for the failure of the seven systems, the CD2 frequency is 4.29E-9/year (based on simplified calculation), i.e. 29% smaller. The reason for this is again that there are more system failure combinations than those involving one specific system. Therefore, in the DIGMORE case, we have similar effect as in the comparison of the alpha-factor model and the beta-factor model.

One participant in the DIGMORE has applied beta parameter 0.05 to 14 identical PAC modules. With that assumption (taking into account also OP CCFs), the probabilities for 1, 2 and 7 specific systems failing are presented in Table 13, and VTT’s numbers are shown for comparison. The probabilities for 3, 4, 5 and 6 systems are so small with the beta-factor model that they are not calculated. The failure probability of all seven systems is 1.17E-8, i.e. much smaller than the probability 7.38E-8 in the previous paragraph, though also the failure probability of 2 systems has to be taken into account: 2.55E-9 * 8 ≈ 2.04E-8. With these inputs, VTT’s frequency for CD2 is 196% larger than the CD2 frequency of the other participant. The reasons for the difference are the ones given in the beginning of this section.

Table 13. Failure probability for N specific systems and CD2 frequency.

The number of systems	VTT	Other participant
1	7.84E-7	7.64E-7
2	6.69E-9	2.55E-9
3	1.06E-9	
4	4.11E-10	
5	3.09E-10	
6	4.36E-10	
7	2.31E-9	1.17E-8
CD2 Frequency (1/year)	**5.89E-9**	**1.99E-9**

4. Variations to the DIGMORE case

The impacts of different systems and design alternatives are studied in additional analysis cases. The idea is to start from a simple case that is close to the earlier DIGMAP case (OECD NEA CSNI, 2024a; Porthin et al., 2023) and then add more systems to produce the safety signals. The analysis cases are defined based on the systems that are included in the architecture and whether there are two diverse types of PAC unit:

1. PRPS and PAC systems (with diversity for PAC)
2. PRPS and PAC systems (with no diversity for PAC)
3. PRPS, HWBS and PAC systems (with diversity for PAC)
4. PRPS, HWBS and PAC systems (with no diversity for PAC)
5. PRPS, DRPS and PAC systems (with diversity for PAC)
6. PRPS, DRPS and PAC systems (with no diversity for PAC)
7. PRPS, DRPS, HWBS and PAC systems (with diversity for PAC)
8. PRPS, DRPS, HWBS and PAC systems (with no diversity for PAC)
9. PRPS, DRPS, OIC and PAC systems (with diversity for PAC)
10. PRPS, DRPS, OIC and PAC systems (with no diversity for PAC)
11. PRPS, DRPS, HWBS, OIC and PAC systems (with diversity for PAC)
12. PRPS, DRPS, HWBS, OIC and PAC systems (with no diversity for PAC)

Note that case 11 is the base case that has been modelled and analysed in Section 3.

In addition to the cases above, the following sensitivity cases will also be analysed:

13. Case 11 with the condition that failures causing spurious signals from DRPS do not cause safety signals to fail
14. Case 9 with the condition that failures causing spurious signals from DRPS do not cause safety signals to fail
15. Case 11 with all software CCF probabilities multiplied by 10

One should also notice that some variations on CCF probabilities and modelling of spurious signals were analysed in the previous report (Tyrväinen & Björkman, 2024).

The main results of different analysis cases are summarised in Table 14, and more results, including contributions of different systems, are presented in Appendix C. In addition, the analysis cases are discussed in the following subsections.

Table 14. Main results of analysis cases.

Case	Description	CDF	CD1 Freq	CD2 Freq	CD3 Freq
0	DIGMAP, PRPS with success criterion 1-o-o-4	6.32E-5	1.19E-5	3.39E-7	5.10E-5
1	PRPS and PAC systems (with diversity for PAC)	6.57E-5	1.43E-5	3.54E-7	5.11E-5
2	PRPS and PAC systems (with no diversity for PAC)	7.35E-5	1.43E-5	2.63E-6	5.66E-5
3	PRPS, HWBS and PAC systems (with diversity for PAC)	5.21E-5	1.18E-6	7.34E-8	5.08E-5
4	PRPS, HWBS and PAC systems (with no diversity for PAC)	5.82E-5	1.18E-6	2.34E-6	5.47E-5
5	PRPS, DRPS and PAC systems (with diversity for PAC)	5.09E-5	7.29E-8	5.97E-8	5.08E-5
6	PRPS, DRPS and PAC systems (with no diversity for PAC)	5.61E-5	7.29E-8	1.58E-6	5.45E-5
7	PRPS, DRPS, HWBS and PAC systems (with diversity for PAC)	5.09E-5	6.04E-9	4.90E-8	5.08E-5
8	PRPS, DRPS, HWBS and PAC systems (with no diversity for PAC)	5.60E-5	6.04E-9	1.57E-6	5.45E-5
9	PRPS, DRPS, OIC and PAC systems (with diversity for PAC)	5.62E-5	1.49E-7	6.72E-8	5.60E-5
10	PRPS, DRPS, OIC and PAC systems (with no diversity for PAC)	6.19E-5	1.49E-7	1.75E-6	6.00E-5
11	PRPS, DRPS, HWBS, OIC and PAC systems (with diversity for PAC)	5.60E-5	1.24E-8	5.40E-8	5.60E-5
12	PRPS, DRPS, HWBS, OIC and PAC systems (with no diversity for PAC)	6.18E-5	1.24E-8	1.73E-6	6.00E-5
13	Case 11 with the condition that failures causing spurious signals from DRPS do not cause safety signals to fail	5.60E-5	6.65E-9	5.39E-8	5.60E-5
14	Case 9 with the condition that failures causing spurious signals from DRPS do not cause safety signals to fail	5.61E-5	8.03E-8	6.58E-8	5.60E-5
15	Case 11 with all software CCF probabilities multiplied by 10	5.65E-5	2.63E-7	8.89E-8	5.61E-5

4.1 PRPS and PAC systems (with diversity for PAC)

In this case, the I&C architecture includes only the PRPS and PAC systems. The case is quite close to the DIGMAP case where the same PRPS was modelled without PAC systems (OECD NEA CSNI, 2024a; Porthin et al., 2023). In DIGMAP, the success criterion for each safety function was however 1-out-of-4, whereas it is 2-out-of-4 in DIGMORE.

The model for this case can easily be derived from the base case by setting the DRPS and HWBS failed and setting the probabilities of spurious signals to 0.

Compared to the DIGMAP case, the CDF increases from 6.32E-5/year to 6.57E-5/year. This is mainly due to the change in the PRPS success criteria. The addition of PAC failures has only a minor impact on the results because there are two diverse types of PAC, whereas there is only functional diversity in the PRPS.

4.2 PRPS and PAC systems (with no diversity for PAC)

In the base case, it has been assumed that there are two diverse types of PAC units. For each system, there are two PAC-A units and two PAC-B units. In this analysis case, we assume that all PAC units are identical. This is a challenge for modelling because there are 28 PAC units in total, and there are not enough alpha-factor parameters to model the CCFs between 28 components. Therefore, we model the

CCFs with the partial beta-factor method, which has already been used to model CCFs of the AD modules in the base case (see Section 3.4.3).

As for AD modules in Section 3.4.3, we select score D for every subfactor, except for the redundancy (& diversity). For the redundancy (& diversity) subfactor, we select score A+ when we model the HW CCF of four PAC units serving the same system, because the success criterion is 2-out-of-4. When we model the CCF of all PAC units, we select score C, because there is functional diversity (the same assumption as for the AD modules in Section 3.4.3). For OP CCFs between all PAC units, we apply beta-factor 1.

The new CCF probabilities are implemented in the model by changing the probabilities of existing basic events and CCFs, i.e. the fault trees are not changed. Besides the PAC CCF probabilities, the model is the same as in the previous case.

With the above-mentioned assumptions, the probability of failure of one front-line system due to PAC HW CCF is 5.61E-5 (including AD, CPLD, DA and SR CCFs). The probability of failure of all front-line safety systems is 1.52E-5 due to PAC HW CCFs and 3E-5 due to PAC OP CCFs.

Compared to case 1, the CDF increases from 6.57E-5/year to 7.35E-5/year, and the CDF related to PAC increases from 1.11E-7/year to 7.86E-6/year. The frequency of CD2 (which requires failures of two safety systems) increases from 3.54E-7/year to 2.63E-6/year, and PAC CCFs totally dominate that frequency. It is not a surprise that the diversity of PAC has a significant impact on the results.

4.3 PRPS, HWBS and PAC systems (with diversity for PAC)

This is the same case as case 1 except for that the HWBS is included, i.e., it is not set failed.

Compared to case 1, the CDF decreases from 6.57E-5/year to 5.21E-5/year. The frequency of CD1 (ATWS) decreases from 1.43E-5/year to 1.18E-6/year. This decrease approximately corresponds to the HWBS failure probability. It can be concluded that the I&C related risk can significantly be decreased by adding a back-up system in addition to the PRPS.

4.4 PRPS, HWBS and PAC systems (with no diversity for PAC)

This case is similar to case 2 except that the HWBS is included, i.e., it is not set failed. In this case, also PAC AD modules related to the HWBS need to be modelled. Two kinds of CCFs are modelled for AD modules:

- A CCF between four redundant AD modules (with inputs from either PRPS or HWBS) with probability 1.86E-5
- A CCF between all AD modules with probability 1.50E-5 (covering both HW and OP CCFs)

Concerning other PAC modules, the probability of failure of one front-line system due to HW CCF is 3.75E-5, the probability of failure of all front-line safety systems is 1.02E-5 due to PAC HW CCFs and 2E-5 due to PAC OP CCFs.

The results of this case are consistent with the results of cases 2 and 3. The risk related to the PRPS is practically the same as in case 3. The risk related to PAC systems is similar to case 2, but slightly smaller because a PAC unit now takes inputs from two systems meaning that failures of AD modules related to one system are not critical.

4.5 PRPS, DRPS and PAC systems (with diversity for PAC)

This is the same case as case 1 except for that the DRPS is included, i.e., it is not set failed.

Compared to case 3 where the HWBS was included instead of the DRPS, the CDF decreases from 5.21E-5/year to 5.09E-5/year. The frequency of CD1 (ATWS) decreases from 1.18E-6/year to 7.29E-8/year. The decrease in the ATWS frequency shows that the DRPS is much more reliable than the HWBS, and the reason for that is largely that the DRPS has redundancy, whereas the HWBS has not.

In this case, the risk contributions of different I&C systems are in good balance. Each system has almost the same risk contribution. The need for the HWBS can be questioned.

4.6 PRPS, DRPS and PAC systems (with no diversity for PAC)

This case is similar to case 2 except that the DRPS is included, i.e., it is not set failed. The modelling of PAC CCFs is similar to case 4. However, in this case, CCFs of PM and CL modules need to also be included. Similar assumptions are used as in cases 2 and 4. Two kinds of CCFs are modelled for PM and CL modules:

- A CCF between four redundant PM or CL modules with probability 5.58E-5
- A CCF between all PM or CL modules with probability 3.51E-5 (covering both HW and OP CCFs)

The results of this case are consistent with the results of cases 4 and 5. The risk contribution of PAC is only slightly smaller than in case 4 because the only differences are that the minimal cut sets related to PAC AD modules have changed and now there are minimal cut sets with PAC PM/CL module failures. The risk contributions of the PRPS and DRPS have increased only slightly compared to case 5 because the minimal cut sets where PRPS failures are combined with PAC PM/CL failures and minimal cut sets where DRPS failures are combined with PAC AD failures are more likely due to lack of diversity in PAC.

4.7 PRPS, DRPS, HWBS and PAC systems (with diversity for PAC)

This case is a mix of cases 3 and 5. In this case, both the DRPS and HWBS are included, i.e., they are not set failed.

Compared to case 5, the addition of the HWBS does not decrease the CDF anymore because PRPS and DRPS failures did not contribute significantly to the CDF in case 5 and the addition of the HWBS only decreases that contribution. The addition of the HWBS mainly decreases CD1 (ATWS) frequency significantly and also CD2 frequency moderately.

4.8 PRPS, DRPS, HWBS and PAC systems (with no diversity for PAC)

This case is a mix of cases 4 and 6. In this case, both the DRPS and HWBS are included, i.e., they are not set failed. The modelling of PAC AD modules is similar to case 4, and the modelling of PAC PM and CL modules is similar to case 6.

The results of this case are consistent with the results of cases 6 and 7. Compared to case 6, the CDF decreased only slightly due to the addition of the HWBS. The risk contribution of the PAC systems is almost the same as in case 6. The risk contributions of the PRPS, DRPS and HWBS are only slightly larger than in case 7 due to the lack of diversity for PAC AD, PM and CL modules (the same effect as observed in case 6 compared to case 5).

4.9 PRPS, DRPS, OIC and PAC systems (with diversity for PAC)

This case is similar to case 5 except for that spurious signals from the OIC and DRPS are added to the model.

The results are mostly similar to case 5 except for that the contribution of the spurious signals has been added to the risk metrics. The total risk contribution of the spurious signals is practically the CDF related to the OIC and DRPS.

4.10 PRPS, DRPS, OIC and PAC systems (with no diversity for PAC)

This case is similar to case 6 except for that spurious signals from the OIC and DRPS are added to the model.

The results are mostly similar to case 6 except for that the contribution of the spurious signals has been added to the risk metrics. The total risk contribution of the spurious signals is practically the CDF related to the OIC and DRPS.

4.11 PRPS, DRPS, HWBS, OIC and PAC systems (with diversity for PAC)

This is the DIGMORE base case. Its results have been presented and discussed in Section 3.

The results are mostly similar to case 7 except for that the contribution of the spurious signals has been added to the risk metrics. The total risk contribution of the spurious signals is practically the CDF related to the OIC and DRPS.

Compared to case 9, the addition of the HWBS does not decrease the CDF much because PRPS and DRPS failures did not contribute much to the CDF in case 9 and the addition of the HWBS only decreases that contribution. The addition of the HWBS mainly decreases CD1 (ATWS) frequency significantly and also CD2 frequency moderately.

4.12 PRPS, DRPS, HWBS, OIC and PAC systems (with no diversity for PAC)

This case is similar to case 10 except for that the HWBS is included, i.e., it is not set failed.

The results of this case are consistent with the results of cases 10 and 11. The CDF is almost the same as in case 10 because the addition of the HWBS mainly decreases the ATWS risk which was already small in case 10. The risk contribution of PAC systems is almost the same as in case 10. Compared to case 11, the risk contributions of the PRPS, DRPS and HWBS are only slightly larger because PAC diversity has only minor impact on those. However, the removal of diversity from the PAC systems does increase the CDF significantly.

4.13 Case 11 with the condition that failures causing spurious signals from DRPS do not cause safety signals to fail

This case is similar to case 11 (the base case) except for that basic events representing spurious signals have been removed from the DRPS fault trees meaning that spurious signals do not act as common cause initiators but are just initiating events.

The CDF is the same as in case 11. Only the frequency of CD1 (ATWS) decreases significantly. It can be concluded that the assumption related to failure of the DRPS in the case of spurious signals does not have

significance for the overall results but could have some significance if the RHR would not dominate so much.

4.14 Case 9 with the condition that failures causing spurious signals from DRPS do not cause safety signals to fail

This case is similar to case 9 except for that basic events representing spurious signals have been removed from the DRPS fault trees meaning that spurious signals do not act as common cause initiators but are just initiating events. On the other hand, this case is similar to case 13 except for that the HWBS has been removed from the model.

Compared to case 9, the CDF decreases only slightly. The assumption related to failure of the DRPS in the case of spurious signals does not make big difference in this case either, but the impact is one order of magnitude larger than in case 13.

4.15 Case 11 with all software CCF probabilities multiplied by 10

In the base case, software failures do not play a very important role. In this case, the probabilities of all AS and OP CCF basic events are simply multiplied by 10 compared to the base case (case 11). This increase is also taken into account in the computation of PAC failure probabilities using the computation script described in Section 3.4.2 and using formulas presented in Section 3.4.3.

The CDF increases from 5.60E-5/year to 5.65E-5/year, i.e., not very much. However, the frequency of CD1 (ATWS) increases over a decade from 1.24E-8/year to 2.63E-7/year. The increase comes from minimal cut sets including AS CCFs in the PRPS and/or DRPS. The total risk contribution of PAC systems also increases significantly but not as much. In general, larger software CCF probabilities can lead to much larger risk contribution of software failures. If spurious signals are not counted, the significance of software failures is at the same level as of HW failures in this sensitivity case.

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.

When comparing the results with other DIGMORE participants, some interesting observations were made on CCF models. The beta-factor model is normally considered a conservative CCF model compared to the alpha-factor model. However, in certain situations, the beta-factor model is not conservative at all and can actually be optimistic. This is the case, e.g., when a failure criterion 2-out-of-N is modelled.

Variations made to the base case model demonstrated the importance of diversity. The PAC systems were much less reliable when no diversity was assumed, and the removal of the back-up systems increased the risk significantly. On the other hand, the removal of the HWBS alone did not change the results much, and the risks related to different I&C systems were actually in better balance in that case. From the risk point of view, it is not necessary to have two diverse back-up systems in the DIGMORE case. In addition, it did not make much difference whether spurious signals from the DRPS were modelled as common cause initiators or as initiating events only.

Software failures did not play very important role in the results of the base case. However, the results related to the PRPS, DRPS and PAC systems are somewhat sensitive to the software failure probabilities, i.e., the importance of software failures increases significantly if the probabilities are increased significantly.

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.

Björkman, K. (2025). “Performing computations for digital I&C related CCFs in PRA”, VTT-R-00422-25, 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, 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, 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). (2025). “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 task 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.

Tyrväinen, T, Björkman, K. (2024). “Probabilistic risk model for digital I&C architecture”, VTT-R-00646-24, VTT Technical Research Centre of Finland Ltd, Espoo, Finland.

Tyrväinen, T, Mätäsniemi, T, Björkman, K. (2023). “FinPSA user guide, Release 2.3.0.x”, VTT Technical Research Centre of Finland Ltd.

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: Results of analysis cases

Case	Description	CDF	CD1 Freq	CD2 Freq	CD3 Freq	PAC CDF	PRPS CDF	DRPS CDF	HWBS CDF	OIC CDF	PAC CD2 Freq
0	DIGMAP, PRPS with success criterion 1-o-o-4	6.32E-5	1.19E-5	3.39E-7	5.10E-5	-	1.25E-5	-	-	-	-
1	PRPS and PAC systems (with diversity for PAC)	6.57E-5	1.43E-5	3.54E-7	5.11E-5	1.11E-7	1.48E-5	-	-	-	5.52E-9
2	PRPS and PAC systems (with no diversity for PAC)	7.35E-5	1.43E-5	2.63E-6	5.66E-5	7.86E-6	1.48E-5	-	-	-	2.28E-6
3	PRPS, HWBS and PAC systems (with diversity for PAC)	5.21E-5	1.18E-6	7.34E-8	5.08E-5	8.96E-8	1.23E-6	-	1.23E-6	-	5.38E-9
4	PRPS, HWBS and PAC systems (with no diversity for PAC)	5.82E-5	1.18E-6	2.34E-6	5.47E-5	6.17E-6	1.23E-6	-	1.39E-6	-	2.27E-6
5	PRPS, DRPS and PAC systems (with diversity for PAC)	5.09E-5	7.29E-8	5.97E-8	5.08E-5	8.75E-8	8.60E-8	8.60E-8	-	-	5.36E-9
6	PRPS, DRPS and PAC systems (with no diversity for PAC)	5.61E-5	7.29E-8	1.58E-6	5.45E-5	5.28E-6	8.81E-8	1.00E-7	-	-	1.53E-6
7	PRPS, DRPS, HWBS and PAC systems (with diversity for PAC)	5.09E-5	6.04E-9	4.90E-8	5.08E-5	8.75E-8	7.13E-9	7.13E-9	7.13E-9	-	5.34E-9
8	PRPS, DRPS, HWBS and PAC systems (with no diversity for PAC)	5.60E-5	6.04E-9	1.57E-6	5.45E-5	5.26E-6	7.28E-9	1.20E-8	8.18E-9	-	1.53E-6
9	PRPS, DRPS, OIC and PAC systems (with diversity for PAC)	5.62E-5	1.49E-7	6.72E-8	5.60E-5	9.67E-8	1.66E-7	1.23E-6	-	4.11E-6	5.90E-9
10	PRPS, DRPS, OIC and PAC systems (with no diversity for PAC)	6.19E-5	1.49E-7	1.75E-6	6.00E-5	5.83E-6	1.68E-7	1.37E-6	-	4.52E-6	1.69E-6
11	PRPS, DRPS, HWBS, OIC and PAC systems (with diversity for PAC)	5.60E-5	1.24E-8	5.40E-8	5.60E-5	9.63E-8	1.38E-8	1.08E-6	1.38E-8	4.10E-6	5.89E-9
12	PRPS, DRPS, HWBS, OIC and PAC systems (with no diversity for PAC)	6.18E-5	1.24E-8	1.73E-6	6.00E-5	5.82E-6	1.40E-8	1.20E-6	1.57E-8	4.52E-6	1.68E-6
13	Case 11 with the condition that failures causing spurious signals from DRPS do not cause safety signals to fail	5.60E-5	6.65E-9	5.39E-8	5.60E-5	9.63E-8	7.84E-9	1.08E-6	7.84E-9	4.10E-6	5.88E-9
14	Case 9 with the condition that failures causing spurious signals from DRPS do not cause safety signals to fail	5.61E-5	8.03E-8	6.58E-8	5.60E-5	9.65E-8	9.48E-8	1.16E-6	-	4.11E-6	5.91E-9
15	Case 11 with all software CCF probabilities multiplied by 10	5.65E-5	2.63E-7	8.89E-8	5.61E-5	2.55E-7	2.78E-7	1.34E-6	2.78E-7	4.13E-6	2.82E-8

In the table, e.g. PAC CDF means the CDF related to PAC failures (Fussell-Vesely of PAC multiplied by the CDF).