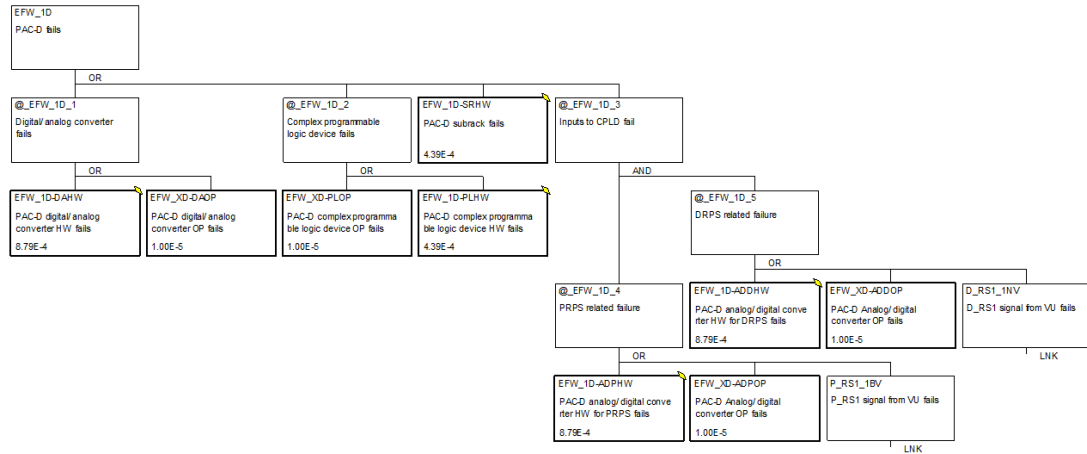


## RESEARCH REPORT

VTT-R-00897-23



# Preliminary probabilistic risk model for digital I&C architecture

Authors: Tero Tyrväinen

Confidentiality: VTT Public

Version: 8.2.2024



<b>Report's title</b> Preliminary probabilistic risk model for digital I&C architecture	
<b>Customer, contact person, address</b> VYR	<b>Order reference</b> SAFER 7/2023
<b>Project name</b> Probabilistic Risk Assessment Labour, Improvements and Extensions	<b>Project number/Short name</b> 135903/PRALINE
<b>Author(s)</b> Tero Tyrväinen	<b>Pages</b> 27/2
<b>Keywords</b> probabilistic risk assessment, instrumentation and control, software reliability	<b>Report identification code</b> VTT-R-00897-23
<p><b>Summary</b></p> <p>This report presents a preliminary probabilistic risk assessment (PRA) model for the OECD/NEA WGRISK DIGMORE reference case representing digital instrumentation and control (I&amp;C) systems in a simplified boiling water reactor plant. The reference case covers an I&amp;C architecture with several systems, such as the primary and diverse reactor protection system, operational I&amp;C system, hard-wired backup system, and prioritization and actuation control systems. The reference case has not been completed yet, and therefore, tentative modelling assumptions have been used in the PRA model. There are still several issues that need to be clarified, including the design of the operational I&amp;C, spurious signals, reliability parameters and common cause failure assumptions.</p> <p>In the preliminary results, certain priority and actuation control (PAC) units have a very high risk contribution. Even though the risk contribution is somewhat dependent on tentative parameter values, the logic of the model clearly implies that PAC is the most important part of the I&amp;C systems, because it has no diverse alternative. The risk contributions of the other I&amp;C system failures are small, because there are diverse solutions in each case.</p>	
<b>Confidentiality</b>	VTT Public
Espoo 9.2.2024	
<b>Written by</b> Tero Tyrväinen, Research Scientist	<b>Reviewed by</b> Kim Björkman, Research Scientist
<b>VTT's contact address</b> VTT Technical Research Centre of Finland Ltd, P.O. Box 1000, FI-02044 VTT, FINLAND	
<b>Distribution (customer and VTT)</b> SAFER2028 TAG1.1 members, VTT archive	
<p><i>The use of the name of "VTT" in advertising or publishing of a part of this report is only permissible with written authorisation from VTT Technical Research Centre of Finland Ltd.</i></p>	



## Approval

### VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD

Date: 09 February 2024

Signature:

DocuSigned by:  
*Teemu Kärkelä*  
E7B76042F134471...

Name: Teemu Kärkelä

Title: Research Team Leader



## Contents

---

List of acronyms .....	4
1. Introduction .....	6
2. Reference case description .....	6
2.1 Reference plant .....	7
2.2 Overall I&C architecture .....	7
2.3 Primary reactor protection system.....	9
2.4 Diverse reactor protection system.....	10
2.5 Hard-wired backup system.....	11
2.6 Priority and actuation control.....	11
3. PRA model .....	12
3.1 Event tree .....	12
3.2 Modelling approach and level of detail .....	13
3.3 Probabilities of hardware failure basic events .....	13
3.4 Common cause failures.....	16
3.5 Fault trees .....	17
4. Preliminary results .....	23
4.1 Main results .....	23
4.2 Sensitivity analysis .....	24
5. Conclusions .....	25
References .....	25
Appendix: Risk importance measures .....	27



## 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
ASC	Analog signal conditioning
CC	Calculation circuit
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
ECR	Emergency control room
EFW	Emergency feed-water system
ESF	Engineered safety features
HVA	Heating, venting and air conditioning system
HW	Hardware
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
PAC-A	Priority and actuation control – analog
PAC-D	Priority and actuation control – digital
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
RPS	Reactor protection 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
WD	Watchdog
WDT	Watchdog timer
WGRISK	Working group on risk assessment

## 1. Introduction

---

Reliability analysis of digital instrumentation and control (I&C) systems is a challenging topic because the systems are very complex, the field is evolving, and there is very little failure data available. Software failures are particularly challenging to model. 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 modelled in overly simplified and conservative manner in most PRAs currently if modelled at all.

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, 2021a; 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 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 will also contain a benchmark study with participants from several countries. In the DIGMORE project, the reference case is extended compared to DIGMAP to cover new modelling aspects, such as priority logic, back-up systems and spurious actuations. The work should achieve an in-depth understanding of PRA relevant impacts of interactions within the entire I&C architecture. The overall goal is to provide recommendations for the development of PRA models concerning digital I&C systems.

This report develops a preliminary PRA model for the DIGMORE reference case (OECD NEA CSNI, 2023). Some details of the model can be expected to change later, because the reference case has not been finalized yet. In this report, the modelling is performed based on the information that was available in December 2023. The operational I&C system, spurious signals, reactor trip system and manual commands have been excluded because those have not been fully defined yet in the reference case. The reliability parameters and CCF assumptions used in the analysis are tentative.

## 2. Reference case description

---

This chapter gives a brief description of the DIGMORE reference case (OECD NEA CSNI, 2023). Note that the reference case has not been finalized yet, and some details can still change.

## 2.1 Reference plant

The reference plant is the same as in the DIGMAP project (OECD NEA CSNI, 2021a). 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 reliability parameters of the components have been multiplied by 0.01 so that this simplification does not distort results.

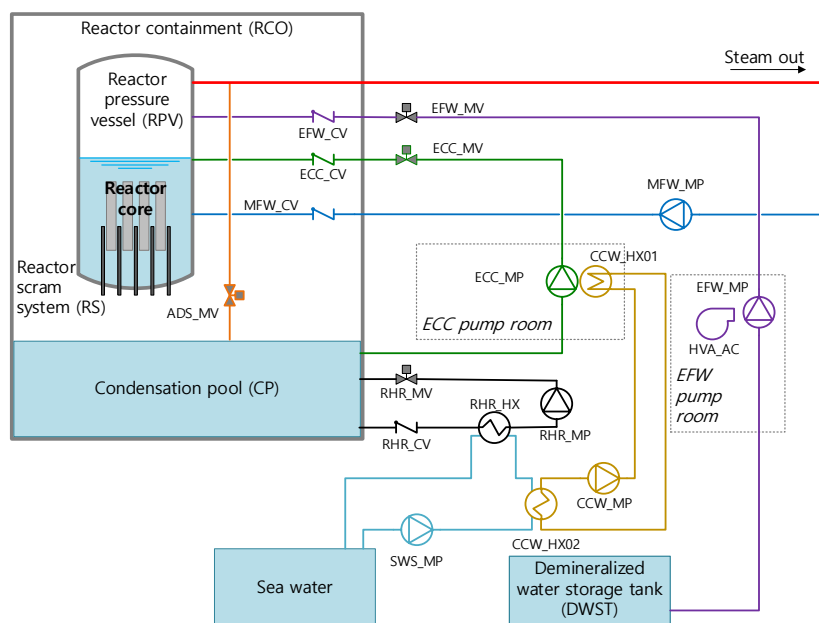


Figure 1. The layout of main safety systems (OECD NEA CSNI, 2023).

Table 1. Safety systems.

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

## 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, and priority and actuation control system (PAC). The architecture of I&C systems is presented in Figure 2. The safety I&C systems provide analog signals to the safety systems and the reactor trip system (RTS). The OIC system provides digital signals to the MFW system. Different I&C systems have human-machine



interfaces in the main control room (MCR) and emergency control room (ECR). 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 systems.

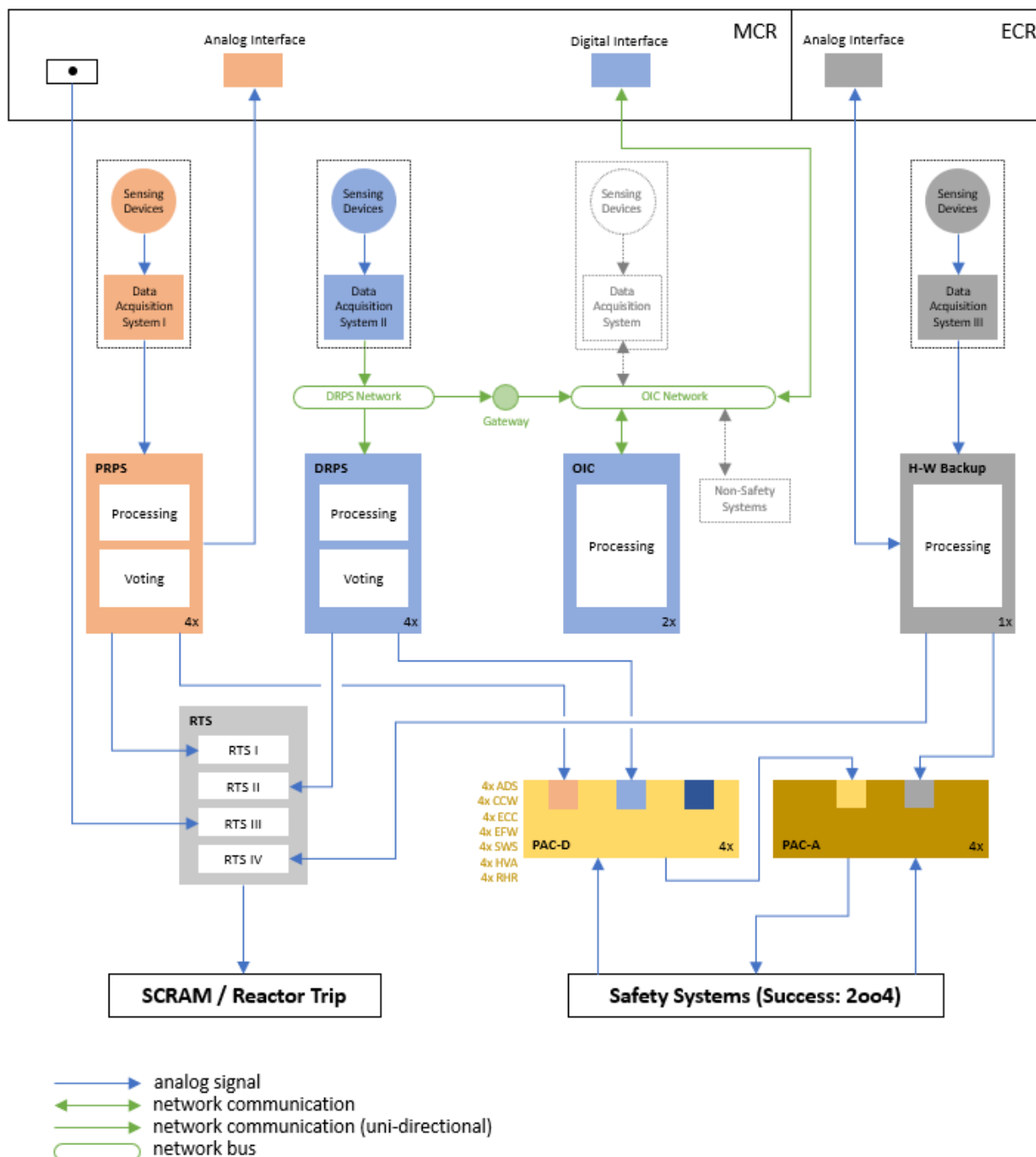


Figure 2. The architecture of I&C systems (OECD NEA CSNI, 2023).

It should be noted that different variations of the architecture will be analysed in the DIGMORE project, but only one configuration is modelled in this report.

## 2.3 Primary reactor protection system

The PRPS is the same reactor protection system that was modelled in the DIGMAP project (OECD NEA CSNI, 2021a). It consists of two diverse subsystems, PRPS-A and PRPS-B. Both subsystems contain four divisions. Each division contains its own measurement sensors, acquisition and processing unit (APU), voting unit (VU) and sub-rack (SR). Each unit contains a processor module (PM) and a communication link (CL) module. Each APU contains analog input (AI) modules for receiving signals from measurement sensors, and each VU contains a digital output (DO) module for sending signals to the PAC systems. In the PM of each VU, 2-out-of-4 voting is performed based on inputs from the APUs of all divisions. The layout of the reactor protection system is presented in Figure 3. The actuation signals of components are summarised in Table 2.

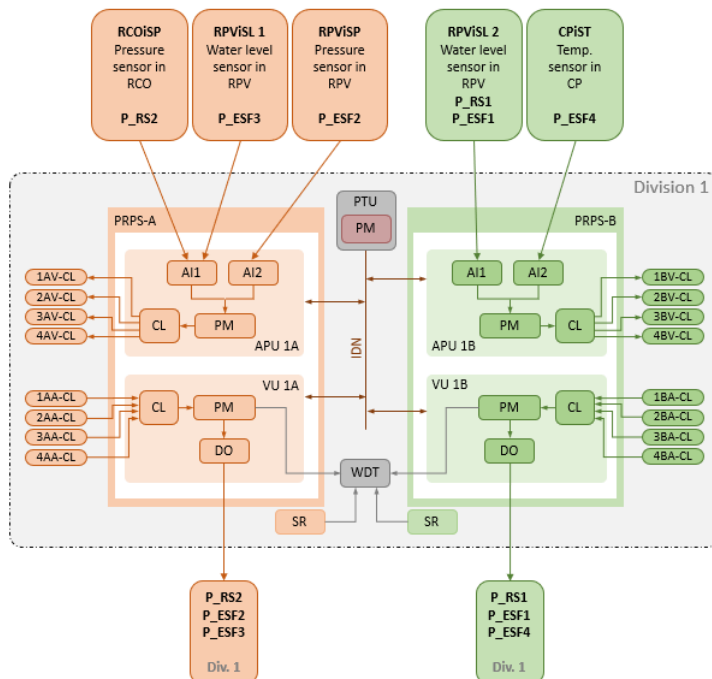


Figure 3. Primary reactor protection system layout (OECD NEA CSNI, 2023).

Table 2. Actuation signals.

System	Component	Control	Conditions	Signal
<b>RS</b>	Control rod breakers	Open	RS1: low water level in reactor RS2: high pressure in containment	RS1 + RS2
<b>EFW</b>	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
<b>HVA</b>	AC cooler	Start	RS1: low water level in reactor ESF1: extreme low water level in reactor	RS1 + ESF1
<b>ADS</b>	Pressure relief valve	Open	ESF2: high pressure in reactor	ESF2
<b>ECC</b>	Pump	Start	ESF3: low water level in reactor	ESF3
	Motor-operated valve	Open	ESF3: low water level in reactor	ESF3



System	Component	Control	Conditions	Signal
<b>RHR</b>	Pump	Start	RS2: high pressure in containment ESF4: high temperature in condensation pool	RS2+ESF4
	Motor-operated valve	Open	RS2: high pressure in containment ESF4: high temperature in condensation pool	RS2+ESF4
<b>CCW</b>	Pump	Start	ESF3: low water level in reactor	ESF3
<b>SWS</b>	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 model description (OECD NEA CSNI, 2023) contains fictive reliability parameters for HW, OP and AS of each module. OP and AS failure probabilities are defined on demand basis, and they are assumed to be always undetected. For HW failures, failure rate is given, and it is divided for failures detected by different fault tolerant features, which are automatic testing, periodic testing and full-scope testing. All HW failures are detected by full-scope testing performed every half a year if they are not detected earlier by other features.

## 2.4 Diverse reactor protection system

The DRPS is quite similar to the PRPS. It however contains only one subsystem that can actuate all safety systems. The sensors are connected to the system by a DRPS network, and each sensor has a CL module. The system also does not contain AI modules, but the signals from the sensors are received by CL modules. There are no PTUs for failure detection, only WDTs. The layout of the system is presented in Figure 4.

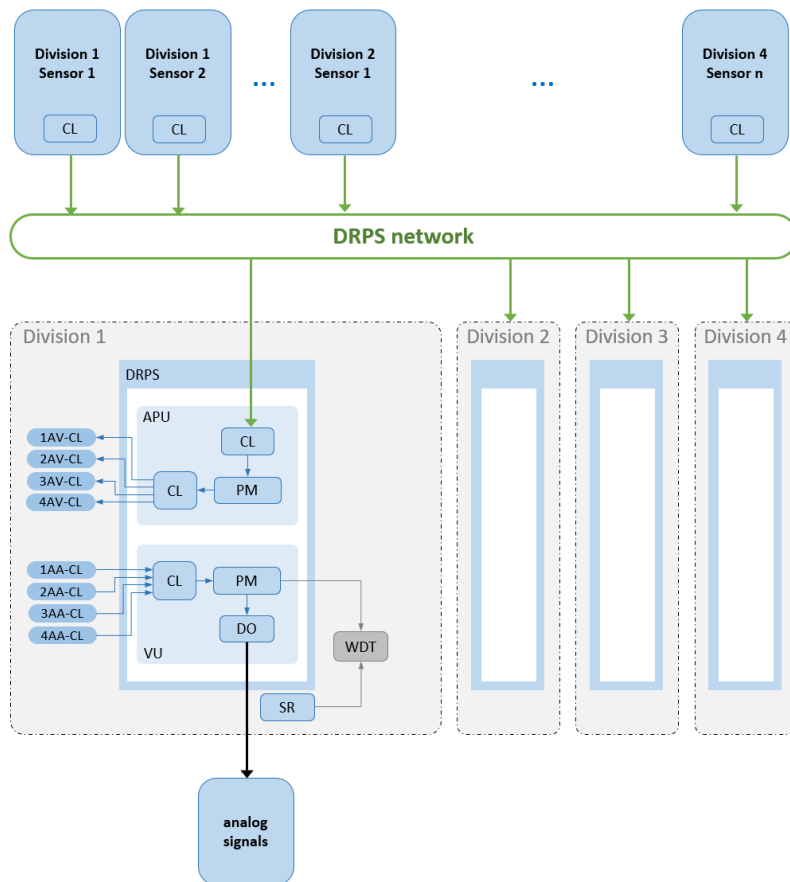


Figure 4. Diverse reactor protection system layout (OECD NEA CSNI, 2023).

The DRPS has sensors for the same measurements as the PRPS. However, there is only one set of water level sensors in the reactor pressure vessel (RPV). The actuation signals of the DRPS are quite similar to the actuation signals of the PRPS. The only difference is that signals RS1 and ESF3 are merged together.

## 2.5 Hard-wired backup system

The H-W backup system works only based on manual commands executed from the ECR. It does not include any redundancy. It is modelled as a black box with only one basic event. The actuation signals of the H-W backup system are identical to the PRPS signals.

## 2.6 Priority and actuation control

PAC systems control safety-related actuators. There are two types of PAC systems: a digital PAC-D and an analog PAC-A. PAC-D receives signals from the PRPS and DRPS and sends an output signal to PAC-A. PAC-A also receives a signal from the H-W backup system and sends the actuation signal to the actuator. There are four pairs of PAC-D and PAC-A for each safety system, i.e. one pair for each PRPS and DRPS division per system. The layout of the PAC systems is presented in Figure 5. Note that signals from the OIC system are not considered in this report, even though OIC is included in the figure.

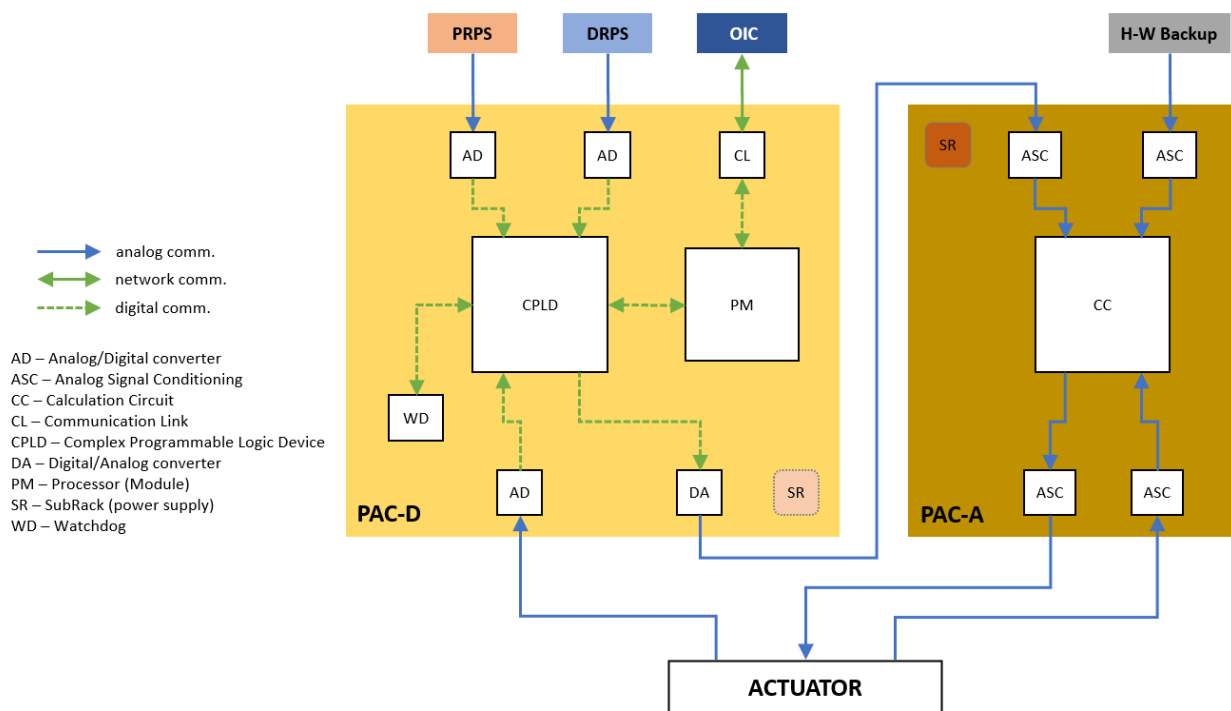


Figure 5. The layout of PAC systems (OECD NEA CSNI, 2023).

PAC-D contains analog/digital converters (AD) for input signals, a complex programmable logic device (CPLD), a digital/analog converter (DA) for the output signal, a PM, a CL, an SR and a watchdog (WD). The prioritization of signals is performed in the CPLD. The signals from the PRPS are prioritized over the signals from the DRPS.

PAC-A contains analog signal conditioning (ASC) modules for input and output signals, and calculation circuit (CC). The signals from the H-W backup systems are prioritized over the signals from the PRPS.

### 3. PRA model

#### 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 6 and it is also given in the model description (OECD NEA CSNI, 2023) to the participants of the benchmark study.

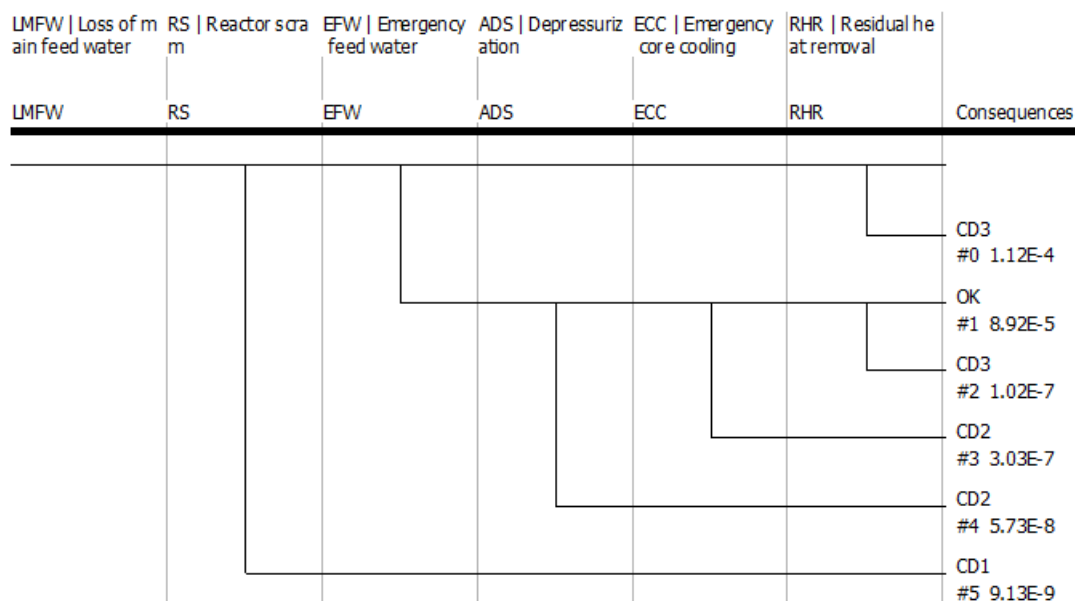


Figure 6. Event tree for loss of main feed-water.

### 3.2 Modelling approach and level of detail

In general, the modelling of the I&C systems is performed at module level using fault trees. The modelling approach used in this study is similar to the approach presented in (Tyrväinen, 2020), whereas it differs from VTT's final DIGMAP model (OECD NEA CSNI, 2021a & 2021b). In the final DIGMAP model, only CCFs were modelled, because FinPSA software did not enable automatic generation and calculation of CCF events for groups larger than four components at that time. Therefore, all the CCF calculations were performed in spreadsheets, and high level CCF events were used as basic events in the PRA model. After that, modelling of CCF groups containing up to eight components has been enabled in FinPSA. In this model, for CCF groups not exceeding eight components, the single failures are modelled explicitly, and the CCFs are generated automatically by FinPSA. CCF groups larger than eight components are treated in the same way as in the final DIGMAP model.

Modelling of HW failures is simplified as in VTT's DIGMAP models (OECD NEA CSNI, 2021a & 2021b; Tyrväinen, 2020). One basic event is used to represent all HW failures of a module. The probability of the basic event is calculated in background taking into account the fault-tolerant features. More detailed modelling would also be possible as seen in three other DIGMAP models (OECD NEA CSNI, 2021a & 2021b), but the simplification reduces modelling efforts and simplifies the interpretation of results.

### 3.3 Probabilities of hardware failure basic events

The failure data of HW failures is divided according to fault tolerant features (OECD NEA CSNI, 2023) 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 failure 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 parameters (OECD NEA CSNI, 2023).

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

For other systems, there are similar tables (OECD NEA CSNI, 2023), but those are simpler, because periodic testing is only considered for the PRPS. This means that the failures of 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  $\lambda$  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 7. In it, basic event APUC<sub>L</sub>\_F represents failures detected only by full-scope testing (case 1 above), and basic event APUC<sub>L</sub>\_P represents failures detected by periodic testing (case 2a above). The probabilities of these basic events are calculated as

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

where  $\lambda$  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:

- PTUPM\_F: HW failure of the PM in the PTU,
- PTUIDN\_F: HW failure of the IDN detected by full-scope testing,
- PTUIDN\_P: HW failure of the IDN detected by periodic testing,
- PTUPMOP\_N: OP failure of the PM in the PTU,
- PTUPMAS\_N: AS failure of the PM in the PTU,
- 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).

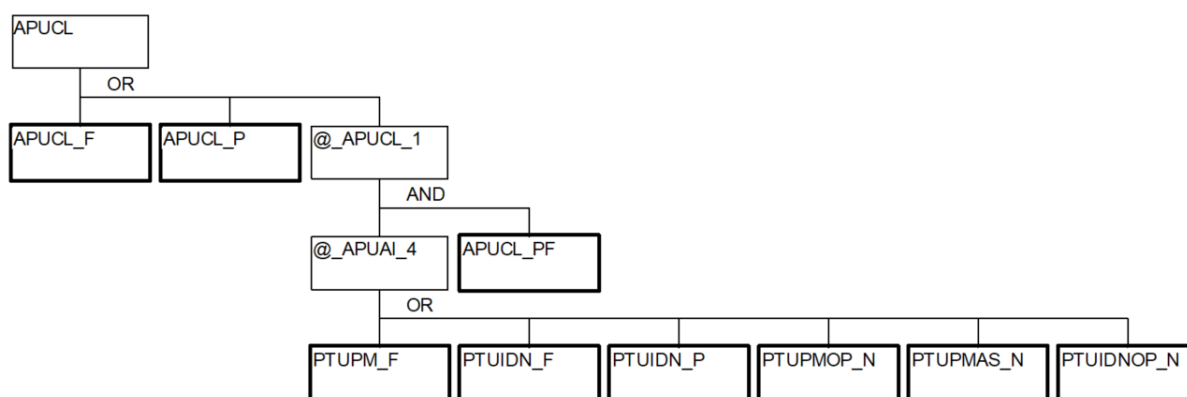


Figure 7. Fault tree of undetected APU CL failure.

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	APUCL_PF
				4.38E-03	PTUPM_F
4	1.53E-05	0.67	99.96	8.71E-03	APUCL_PF
				1.76E-03	PTUIDN_F





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

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

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

The CL failure analysis was presented above, because it is among the simplest analysis scenarios from the PRPS. Analysis of processor modules and sub-racks is more complicated, because also the failure of 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.

For PAC-D, failures of fault-tolerant techniques are not included in the calculations, because its watchdog failures have been defined automatically detected, which means that the watchdogs can be unavailable only eight hours on average. The probability of a failure of a component tested by the watchdog during that period is negligible. Furthermore, also the processor module of PAC-D is used for automatic detection, which means that it also should fail at the same time so that the PAC-D failure would be undetected. Therefore, only failures not detected by automatic testing are counted in the unavailability before detection. On the other hand, failures of the watchdogs in the other systems have not been assumed automatically detected. This inconsistency needs to be addressed later. The failure rates of the watchdogs in the other systems are also significantly smaller.

### 3.4 Common cause failures

At this point, there is no agreement on CCF groups to be modelled in the DIGMORE project. Therefore, tentative CCF assumptions are applied in this report.

For the PRPS, the same CCF groups are assumed as in the DIGMAP project (OECD NEA CSNI, 2021a). 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. For hardware CCFs, generic alpha-factors from (Wierman et al., 2000) were used (also presented in Appendix A of (OECD NEA CSNI, 2021a)). 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, similar CCF assumptions are used as for the PRPS. In this case, CCF groups however include only four components. The PRPS and DRPS are assumed to be independent of each other.

For PAC systems, only CCFs between units related to the same system are modelled. This means that, for example, CCFs between PACs serving the EFW and ECC systems are not modelled. This is only a tentative assumption that will be reconsidered at a later phase. In this case, the CCF groups include four or eight components. The same generic alpha-factors are applied to HW CCFs as for the other systems. Software CCFs are modelled assuming complete dependency (beta-factor 1). In total, there are 28 PAC-D units and 28 PAC-A units in the reference case. The modelling of CCFs between all of those would probably not be practical using the alpha-factor model, due to lack of parameter values and due to computational burden. Some other model, such as the modified beta-factor model (Bao et al., 2022), could be a better option if potential for CCFs is identified.

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 reliability provided by the DRPS and the H-W backup system. If there was a need to model the dependency, it would be best to apply detailed modelling of the fault-tolerant techniques instead of the simplified treatment used in this report.

### 3.5 Fault trees

The model employs small fault trees as building blocks. The fault trees related to the EFW and the top fault tree for reactor scram are presented in this section. With the comments visible in the gates and basic events, the fault trees are self-explanatory. The other safety functions have been modelled with similar types of fault trees. The model contains in total 245 fault trees.

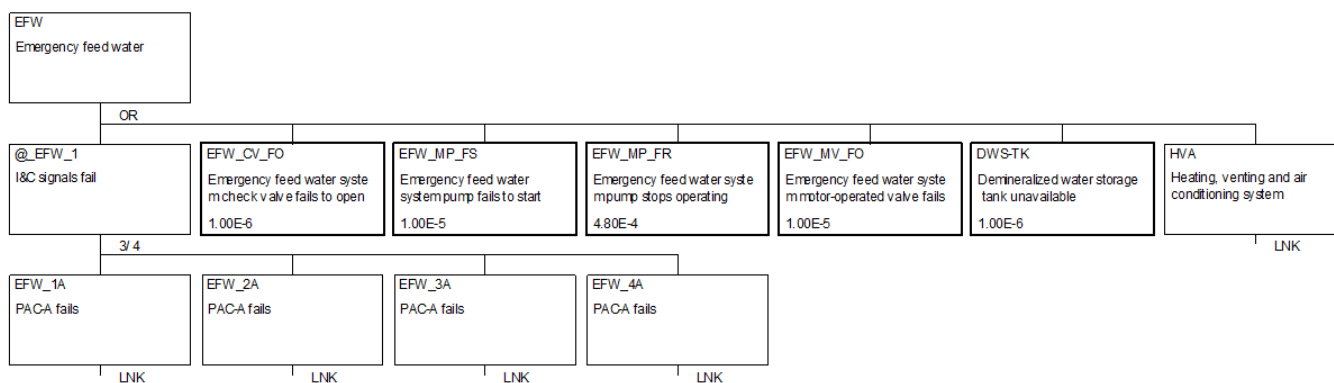


Figure 8. Fault tree for the emergency feedwater system.

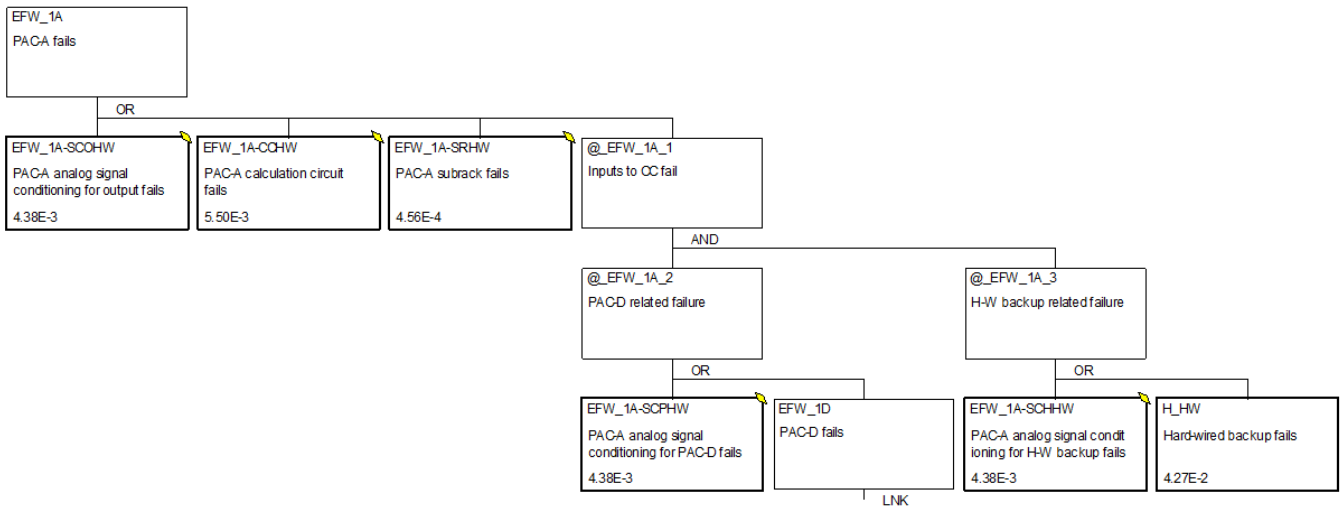


Figure 9. Fault tree for a PAC-A.

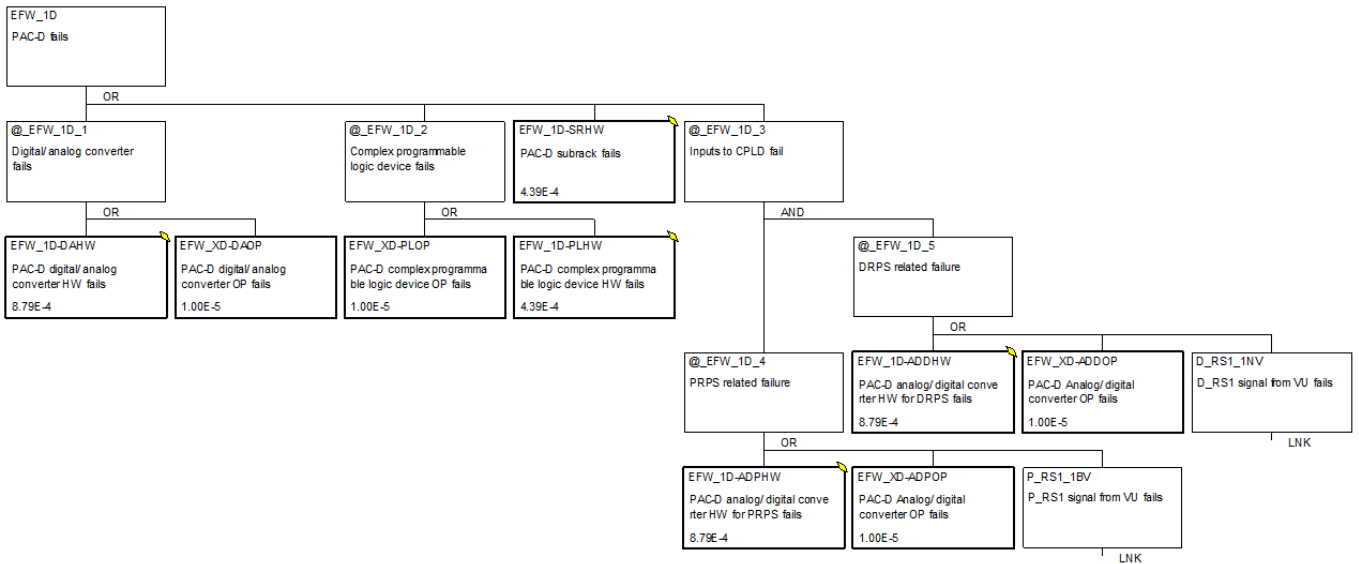


Figure 10. Fault tree for a PAC-D.

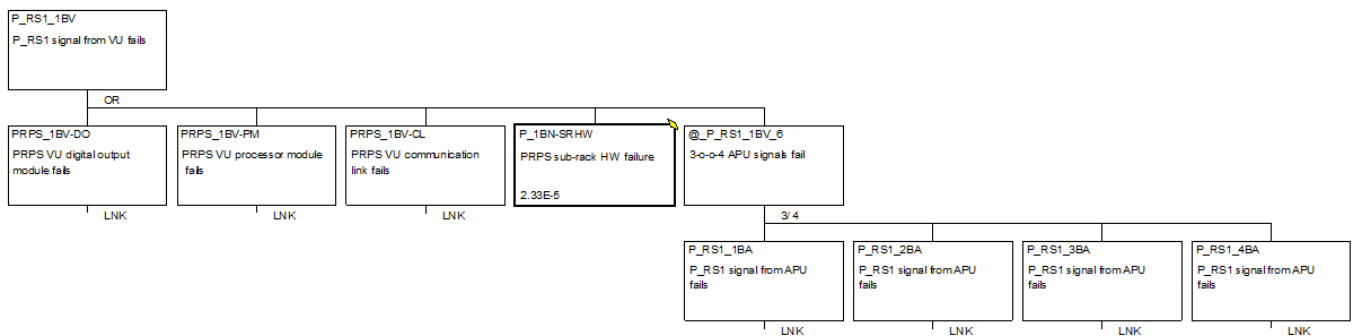


Figure 11. Fault tree for a PRPS voting unit.

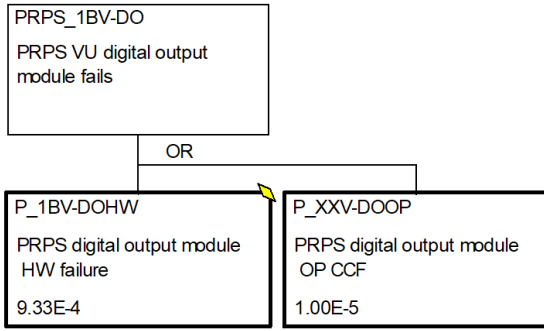


Figure 12. Fault tree for the digital output module in a PRPS voting unit.

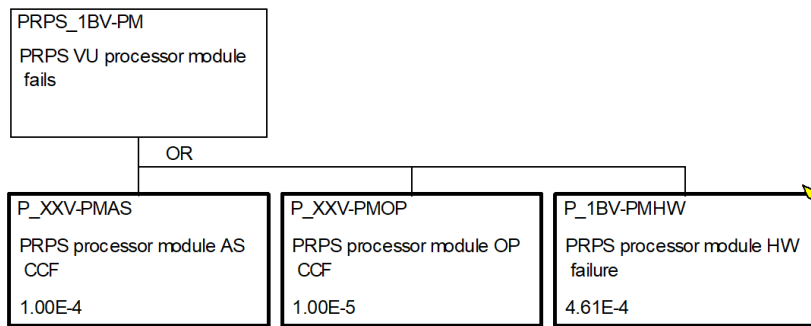


Figure 13. Fault tree for the processor module in a PRPS voting unit.

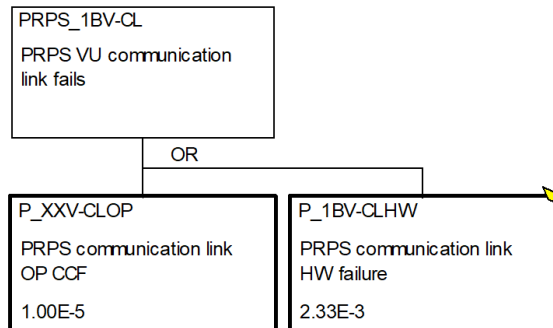


Figure 14. Fault tree for the communication link in a PRPS voting unit.

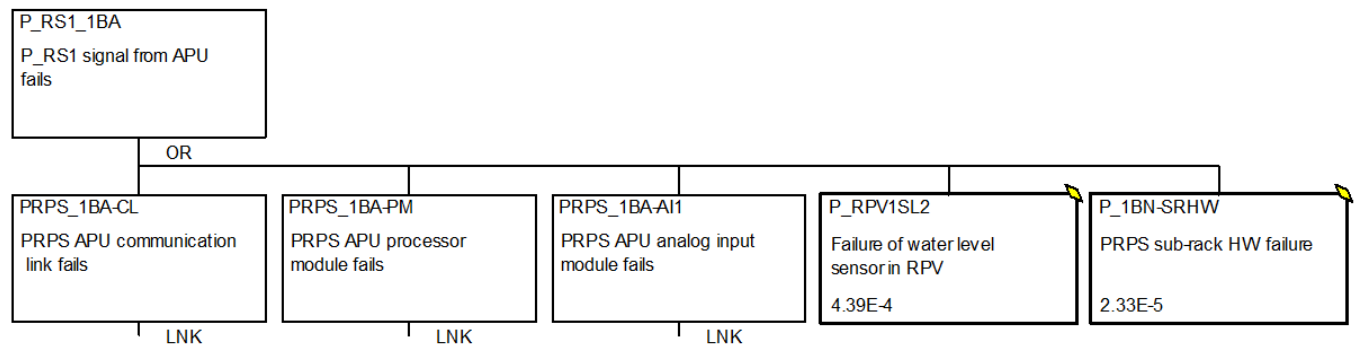


Figure 15. Fault tree for a PRPS APU.

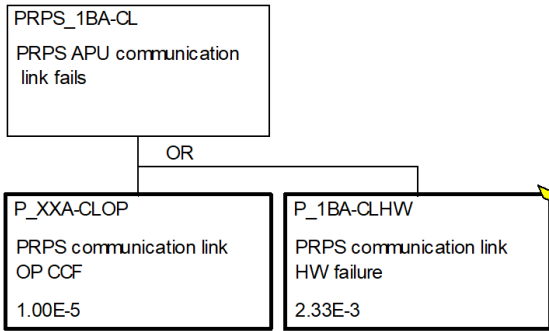


Figure 16. Fault tree for the communication link in a PRPS APU.

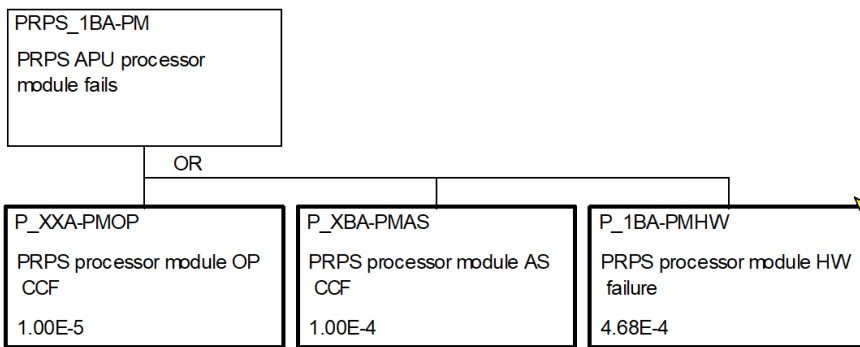


Figure 17. Fault tree for the processor module in a PRPS APU.

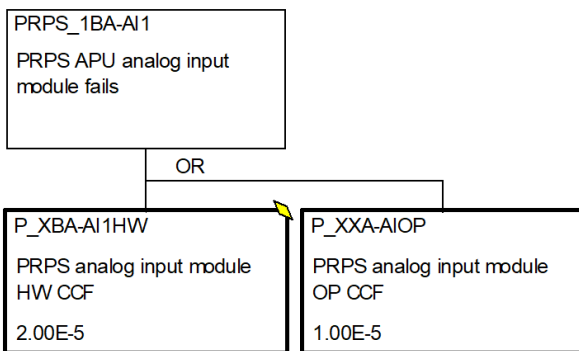


Figure 18. Fault tree for the analog input module in a PRPS APU.

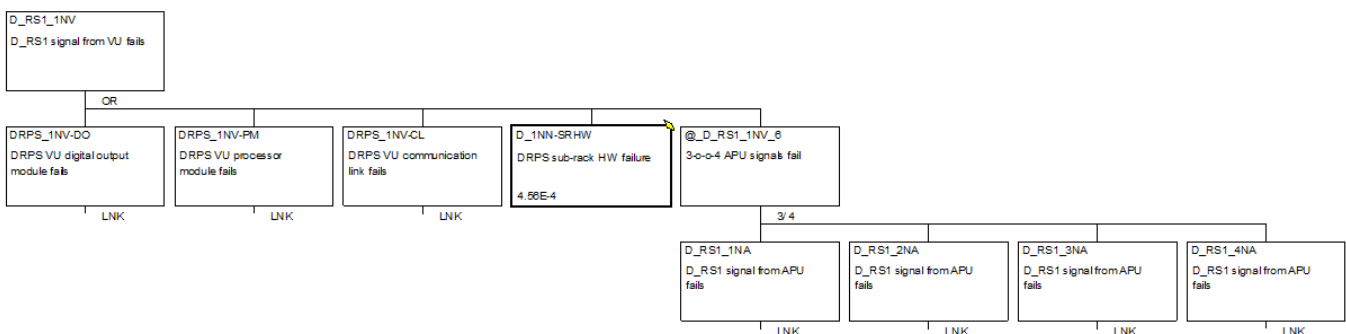


Figure 19. Fault tree for a DRPS voting unit.

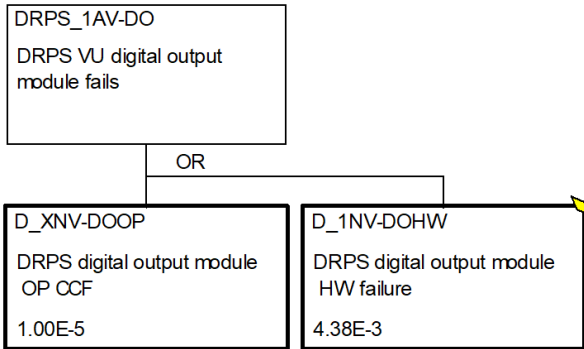


Figure 20. Fault tree for the digital output module in a DRPS voting unit.

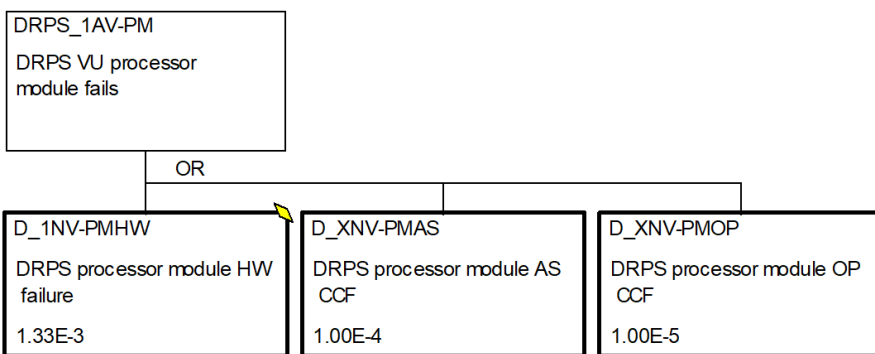


Figure 21. Fault tree for the processor module in a DRPS voting unit.

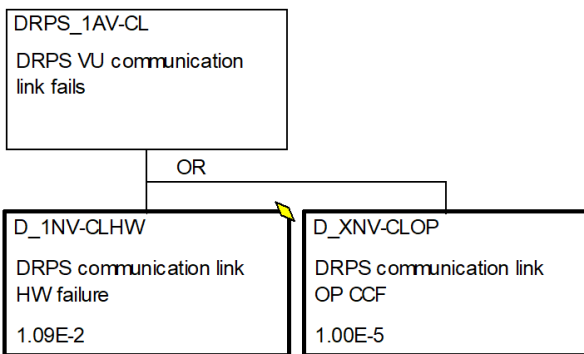


Figure 22. Fault tree for the communication link in a DRPS voting unit.

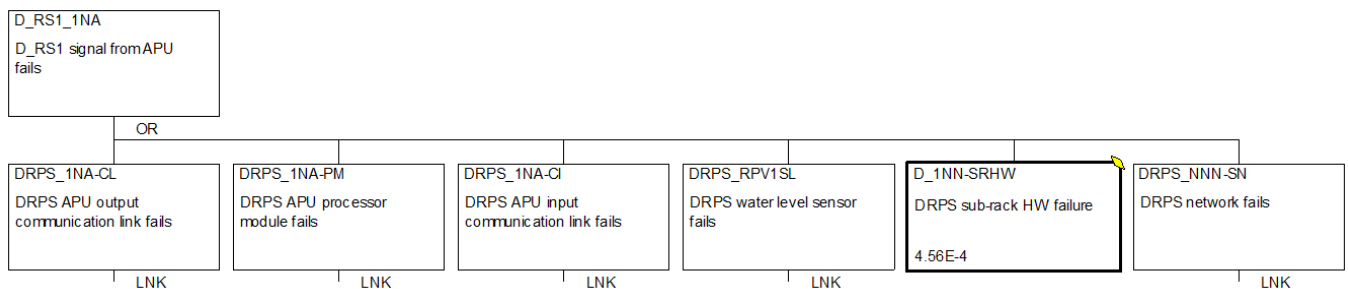


Figure 23. Fault tree for a DRPS APU.

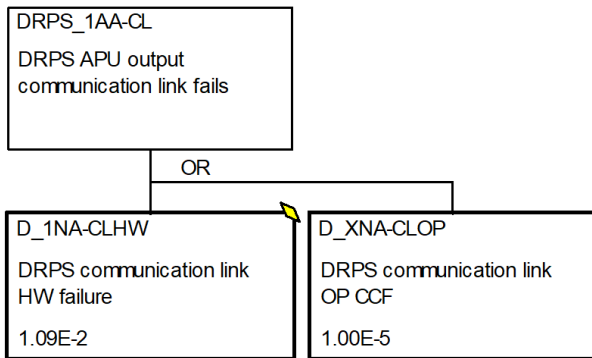


Figure 24. Fault tree for the output communication link in a DRPS APU.

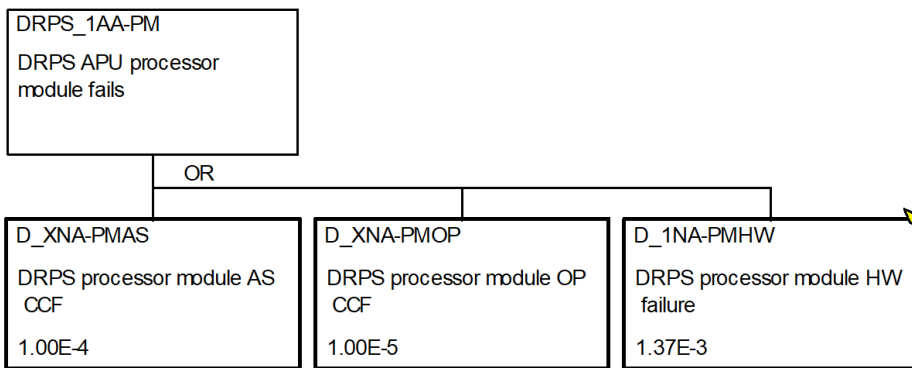


Figure 25. Fault tree for the processor module in a DRPS APU.

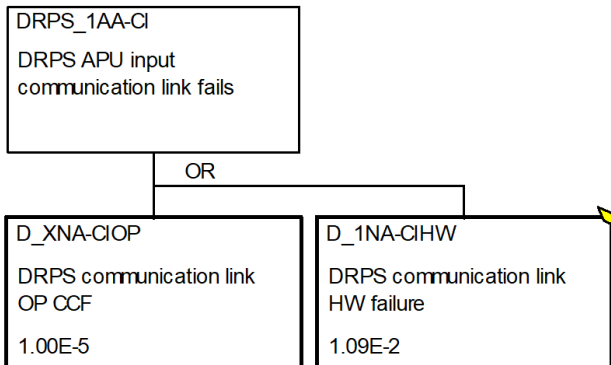


Figure 26. Fault tree for the input communication link in a DRPS APU.

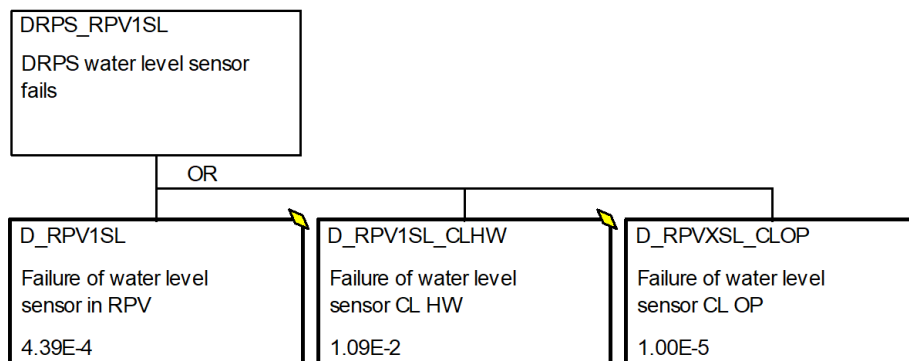


Figure 27. Fault tree for a DRPS water level sensor.

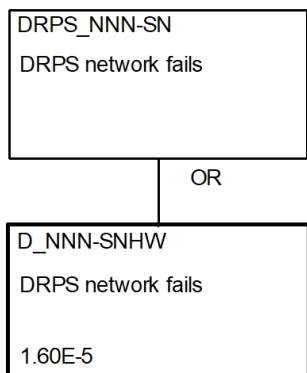


Figure 28. Fault tree for the DRPS network.

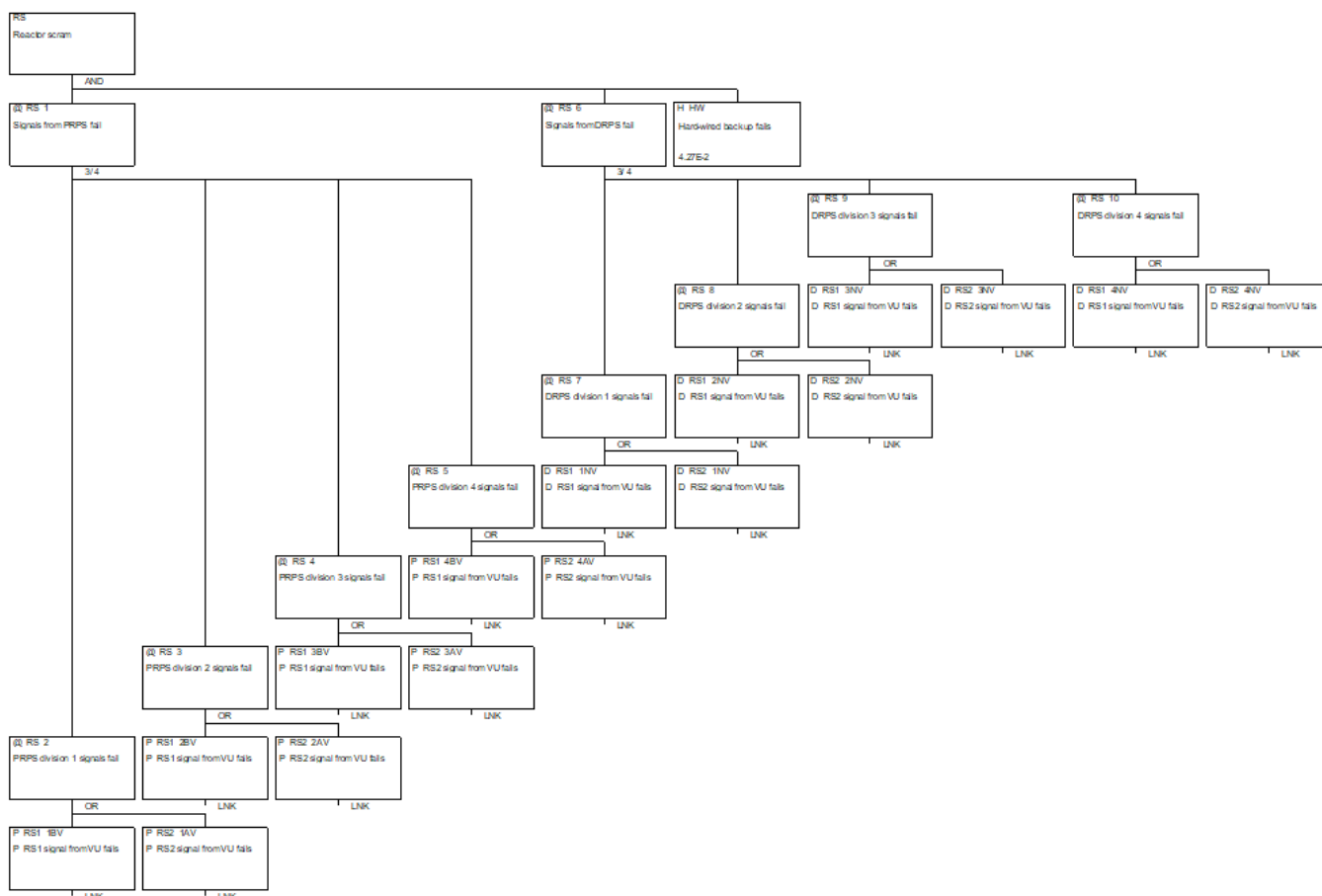


Figure 29. Fault tree for reactor scram.

## 4. Preliminary results

### 4.1 Main results

The core damage frequency (CDF) calculated from the model is 1.13E-4/year. It is totally dominated by sequence 0 (Figure 6), where the RHR system fails. The contribution of other sequences is only 0.41%. The reason for this is that failure of the RHR system alone causes a core damage after the initiating event, whereas in other cases, there is more defence-in-depth.





The risk contribution of I&C systems is around 55%. However, most of this contribution comes from failures of PAC-A units that serve the RHR system and its support system, SWS. In those cases, a CCF of three redundant PAC-A modules causes failure of the RHR, and therefore core damage. The risk contribution of all PAC-A units is 54.5%. The risk contributions of I&C systems are presented in Table 4. Other I&C systems have quite small risk contributions.

Table 4. Fussell-Vesely values of I&C systems with regard to different consequence categories.

System	CD	CD1	CD2	CD3
<b>PAC-A</b>	0.545	-	0.877	0.544
<b>H-W backup</b>	0.013	1	0.034	0.012
<b>PAC-D</b>	5.5E-3	-	0.016	5.5E-3
<b>DRPS</b>	1.1E-4	1	1.8E-4	2.5E-5
<b>PRPS</b>	8.7E-5	1	1.4E-4	5.2E-6

It is interesting that the DRPS has higher risk contribution than the PRPS. The reason for this is that the DRPS has no functional diversity that the PRPS has. The PRPS and DRPS always appear in the same minimal cut sets, except when failure of one system is combined with a CCF of PAC-D AD modules related to the other system.

The sequences of the event tree (Figure 6) have been divided into different core damage types (CD1-CD3). Table 4 presents also the risk contributions of I&C systems to those core damage types. The importance order of systems is the same in each consequence, except in CD1, which can occur only if the PRPS, DRPS and H-W backup system fail. The frequency of CD1 (anticipated transient without scram) is 9.1E-9/year, much lower than the frequencies of other sequences.

HW failures dominate I&C related risk as PAC-A units and H-W backup do not contain software. The risk contribution of OP failures is 0.077%, and the risk contribution of AS failures is 0.0025%.

Fussell-Vesely values for the most important basic events with regard to the CDF are presented in Appendix.

## 4.2 Sensitivity analysis

Since CCFs between PAC units serving different systems were excluded from the model, those are added for sensitivity analysis in a simplified way. In this sensitivity case, it is assumed that all PAC-A units fail with a probability of 1E-5, and all PAC-D units fail with a probability of 1E-5. These two CCF basic events are added to the fault trees of the PAC units.

The impact of the additional PAC CCFs on the results is relatively small, because the CDF was already very high due to the previously mentioned reasons. The frequency of the initiating event combined with the failure of all PAC-A units is now 5E-7/year. It stands out in sequence 4 of the event tree (Figure 6), but its overall Fussell-Vesely value is only 4.4E-3. For consequence category CD2, the CCF of PAC-A units is the most important basic event. If the reference case was changed so that there was a diverse option for the RHR system, this CCF would be among the most important basic events.

The CCF of PAC-D units has a smaller risk contribution, because the safety functions can be actuated by the H-W backup system without PAC-D units. It however has some significance with regard to consequence category CD2 (Fussell-Vesely 0.024).

## 5. Conclusions

---

This report has presented a preliminary 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 reference case has not yet been completed, and therefore, tentative modelling assumptions have been used in the PRA model.

In the preliminary results, certain PAC-A units have a very high risk contribution. Even though the risk contribution is somewhat dependent on tentative parameter values, the logic of the model clearly implies that PAC-A is the most important part of the I&C systems, because it has no diverse alternative. The risk contributions of the other I&C system failures are small, because there are diverse solutions in each case.

There are still several issues that need to be clarified in the reference case, including the design of the OIC system, spurious signals, reliability parameters and CCF assumptions. Sensitivity analyses are also planned for different I&C architecture options. Sensitivity analyses should also particularly be performed for the CCF assumptions and models.

## References

---

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

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

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

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

Liang, QZ, Guo, Y, Peng, CH. (2020). "A review on the research status of reliability analysis of the digital instrument and control system in NPPs", in: IOP Conference Series: Earth and Environmental Science 427.

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). (2021a). "Digital I&C PSA – Comparative Application of Digital I&C Modelling Approaches for PSA, Volume 1: Main Report and Appendix A", NEA/CSNI/R(2021)14, Paris, France. DRAFT.



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

Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI). (2023). "DIGMORE – a realistic comparative application of DI&C modelling approaches for PSA, Appendix A: Complete reference case descriptions". DRAFT.

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

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

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

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



## Appendix: Risk importance measures

The Fussell-Vesely values of the most important basic events with regard to the core damage frequency are listed in the following. Most of the top basic events are such that they alone form a minimal cut set with the initiating event (e.g. 2-23). In addition, the list contains some PAC-A failures that are combined with other PAC-A failures in minimal cut sets.

	Name	Fuss-Ves	Comment
1	LMFW	1.00E+00	Loss of main feed water
2	SWS_MP_FR	2.13E-01	Service water system pump stops operating
3	RHR_MP_FR	2.13E-01	Residual heat removal system pump stops operating
4	SWS_XA-CCHW-ABC	2.47E-02	3x CCF PAC-A calculation circuits fail
5	SWS_XA-CCHW-BCD	2.47E-02	3x CCF PAC-A calculation circuits fail
6	SWS_XA-CCHW-ACD	2.47E-02	3x CCF PAC-A calculation circuits fail
7	SWS_XA-CCHW-ABD	2.47E-02	3x CCF PAC-A calculation circuits fail
8	RHR_XA-CCHW-ABD	2.47E-02	3x CCF PAC-A calculation circuits fail
9	RHR_XA-CCHW-ACD	2.47E-02	3x CCF PAC-A calculation circuits fail
10	RHR_XA-CCHW-BCD	2.47E-02	3x CCF PAC-A calculation circuits fail
11	RHR_XA-CCHW-ABC	2.47E-02	3x CCF PAC-A calculation circuits fail
12	SWS_XA-CCHW-ABCD	2.28E-02	4x CCF PAC-A calculation circuits fail
13	RHR_XA-CCHW-ABCD	2.28E-02	4x CCF PAC-A calculation circuits fail
14	SWS_XA-SCOHW-ABD	1.97E-02	3x CCF PAC-A analog signal conditioning modules fail
15	SWS_XA-SCOHW-ACD	1.97E-02	3x CCF PAC-A analog signal conditioning modules fail
16	SWS_XA-SCOHW-BCD	1.97E-02	3x CCF PAC-A analog signal conditioning modules fail
17	SWS_XA-SCOHW-ABC	1.97E-02	3x CCF PAC-A analog signal conditioning modules fail
18	RHR_XA-SCOHW-ABD	1.97E-02	3x CCF PAC-A analog signal conditioning modules fail
19	RHR_XA-SCOHW-ACD	1.97E-02	3x CCF PAC-A analog signal conditioning modules fail
20	RHR_XA-SCOHW-BCD	1.97E-02	3x CCF PAC-A analog signal conditioning modules fail
21	RHR_XA-SCOHW-ABC	1.97E-02	3x CCF PAC-A analog signal conditioning modules fail
22	SWS_XA-SCOHW-ABCD	1.82E-02	4x CCF PAC-A analog signal conditioning modules fail
23	RHR_XA-SCOHW-ABCD	1.82E-02	4x CCF PAC-A analog signal conditioning modules fail
24	H_HW	1.25E-02	Hard-wired backup fails
25	RHR_HX	1.06E-02	Residual heat removal system heat exchanger fails
26	SWS_XA-SCIHW-ABCDEFGH	6.67E-03	8x CCF PAC-A analog signal conditioning modules fail
27	RHR_XA-SCIHW-ABCDEFGH	6.67E-03	8x CCF PAC-A analog signal conditioning modules fail
28	SWS_MP_FS	4.43E-03	Service water system pump fails to start
29	RHR_MP_FS	4.43E-03	Residual heat removal system pump fails to start
30	RHR_MV_FO	4.43E-03	Residual heat removal system motor-operated valve fails to open
31	SWS_3A-CCHW	2.78E-03	PAC-A calculation circuit fails
32	SWS_2A-CCHW	2.78E-03	PAC-A calculation circuit fails
33	RHR_3A-CCHW	2.78E-03	PAC-A calculation circuit fails
34	RHR_2A-CCHW	2.78E-03	PAC-A calculation circuit fails
35	SWS_4A-CCHW	2.78E-03	PAC-A calculation circuit fails
36	RHR_4A-CCHW	2.78E-03	PAC-A calculation circuit fails
37	SWS_1A-CCHW	2.78E-03	PAC-A calculation circuit fails
38	RHR_1A-CCHW	2.78E-03	PAC-A calculation circuit fails
39	SWS_3A-SCOHW	2.21E-03	PAC-A analog signal conditioning for output fails
40	SWS_2A-SCOHW	2.21E-03	PAC-A analog signal conditioning for output fails
41	RHR_2A-SCOHW	2.21E-03	PAC-A analog signal conditioning for output fails
42	RHR_3A-SCOHW	2.21E-03	PAC-A analog signal conditioning for output fails
43	SWS_4A-SCOHW	2.21E-03	PAC-A analog signal conditioning for output fails
44	RHR_4A-SCOHW	2.21E-03	PAC-A analog signal conditioning for output fails
45	SWS_1A-SCOHW	2.21E-03	PAC-A analog signal conditioning for output fails
46	RHR_1A-SCOHW	2.21E-03	PAC-A analog signal conditioning for output fails
47	SWS_XA-SRHW-ABD	2.05E-03	3x CCF PAC-A subracks fail



48	SWS_XA-SRHW-ACD	2.05E-03	3x CCF PAC-A subracks fail
49	SWS_XA-SRHW-BCD	2.05E-03	3x CCF PAC-A subracks fail
50	SWS_XA-SRHW-ABC	2.05E-03	3x CCF PAC-A subracks fail
51	RHR_XA-SRHW-ABC	2.05E-03	3x CCF PAC-A subracks fail
52	RHR_XA-SRHW-BCD	2.05E-03	3x CCF PAC-A subracks fail
53	RHR_XA-SRHW-ACD	2.05E-03	3x CCF PAC-A subracks fail
54	RHR_XA-SRHW-ABD	2.05E-03	3x CCF PAC-A subracks fail
55	SWS_XA-SRHW-ABCD	1.89E-03	4x CCF PAC-A subracks fail
56	RHR_XA-SRHW-ABCD	1.89E-03	4x CCF PAC-A subracks fail
57	SWS_XA-SCIHW-ABCDEFGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
58	SWS_XA-SCIHW-BCDEFGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
59	SWS_XA-SCIHW-ACDEFGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
60	SWS_XA-SCIHW-ABDEFGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
61	SWS_XA-SCIHW-ABCEFGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
62	SWS_XA-SCIHW-ABCDFGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
63	SWS_XA-SCIHW-ABCDEGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
64	SWS_XA-SCIHW-ABCDEFH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
65	RHR_XA-SCIHW-ABCDEFGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
66	RHR_XA-SCIHW-BCDEFGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
67	RHR_XA-SCIHW-ACDEFGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
68	RHR_XA-SCIHW-ABDEFGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
69	RHR_XA-SCIHW-ABCEFGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
70	RHR_XA-SCIHW-ABCDFGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
71	RHR_XA-SCIHW-ABCDEGH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
72	RHR_XA-SCIHW-ABCDEFH	1.57E-03	7x CCF PAC-A analog signal conditioning modules fail
73	SWS_XA-CCHW-CD	1.31E-03	2x CCF PAC-A calculation circuits fail
74	SWS_XA-CCHW-BD	1.31E-03	2x CCF PAC-A calculation circuits fail
75	SWS_XA-CCHW-AD	1.31E-03	2x CCF PAC-A calculation circuits fail
76	RHR_XA-CCHW-CD	1.31E-03	2x CCF PAC-A calculation circuits fail
77	RHR_XA-CCHW-BD	1.31E-03	2x CCF PAC-A calculation circuits fail
78	RHR_XA-CCHW-BC	1.31E-03	2x CCF PAC-A calculation circuits fail
79	RHR_XA-CCHW-AD	1.31E-03	2x CCF PAC-A calculation circuits fail
80	RHR_XA-CCHW-AC	1.31E-03	2x CCF PAC-A calculation circuits fail
81	RHR_XA-CCHW-AB	1.31E-03	2x CCF PAC-A calculation circuits fail
82	SWS_XA-CCHW-BC	1.31E-03	2x CCF PAC-A calculation circuits fail
83	SWS_XA-CCHW-AC	1.31E-03	2x CCF PAC-A calculation circuits fail
84	SWS_XA-CCHW-AB	1.31E-03	2x CCF PAC-A calculation circuits fail
85	SWS_XA-SCOHW-CD	1.05E-03	2x CCF PAC-A analog signal conditioning modules fail
86	SWS_XA-SCOHW-BD	1.05E-03	2x CCF PAC-A analog signal conditioning modules fail
87	SWS_XA-SCOHW-AD	1.05E-03	2x CCF PAC-A analog signal conditioning modules fail
88	RHR_XA-SCOHW-CD	1.05E-03	2x CCF PAC-A analog signal conditioning modules fail
89	RHR_XA-SCOHW-BD	1.05E-03	2x CCF PAC-A analog signal conditioning modules fail
90	RHR_XA-SCOHW-BC	1.05E-03	2x CCF PAC-A analog signal conditioning modules fail
91	RHR_XA-SCOHW-AD	1.05E-03	2x CCF PAC-A analog signal conditioning modules fail
92	RHR_XA-SCOHW-AC	1.05E-03	2x CCF PAC-A analog signal conditioning modules fail
93	RHR_XA-SCOHW-AB	1.05E-03	2x CCF PAC-A analog signal conditioning modules fail
94	SWS_XA-SCOHW-BC	1.05E-03	2x CCF PAC-A analog signal conditioning modules fail
95	SWS_XA-SCOHW-AC	1.05E-03	2x CCF PAC-A analog signal conditioning modules fail
96	SWS_XA-SCOHW-AB	1.05E-03	2x CCF PAC-A analog signal conditioning modules fail
97	SWS_XA-SCIHW-ABDEFH	6.57E-04	6x CCF PAC-A analog signal conditioning modules fail
98	SWS_XA-SCIHW-ACDEGH	6.57E-04	6x CCF PAC-A analog signal conditioning modules fail
99	SWS_XA-SCIHW-BCDFGH	6.57E-04	6x CCF PAC-A analog signal conditioning modules fail
100	SWS_XA-SCIHW-ABCEFG	6.57E-04	6x CCF PAC-A analog signal conditioning modules fail

**Certificate Of Completion**

Envelope Id: C17707E47EF24AE89791546481E40811	Status: Completed
Subject: Complete with DocuSign: VTT-R-00897-23	
Source Envelope:	
Document Pages: 29	Signatures: 1
Certificate Pages: 1	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelopeld Stamping: Enabled	Christina Vähävaara
Time Zone: (UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	Tekniikantie 21, Espoo
	.., . P.O Box1000, FI-0204
	Christina.Vahavaara@vtt.fi
	IP Address: 178.55.94.226

**Record Tracking**

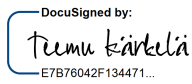
Status: Original	Holder: Christina Vähävaara	Location: DocuSign
09 February 2024   07:40	Christina.Vahavaara@vtt.fi	

**Signer Events**

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

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

**Signature**

DocuSigned by:  
  
E7B76042F134471...

Signature Adoption: Pre-selected Style  
Using IP Address: 130.188.156.70

**Timestamp**

Sent: 09 February 2024 | 07:41  
Viewed: 09 February 2024 | 12:16  
Signed: 09 February 2024 | 12:16

**Authentication Details**

SMS Auth:  
Transaction: 4922dc8c-b839-47fa-b240-4c755527a2b9  
Result: passed  
Vendor ID: TeleSign  
Type: SMSAuth  
Performed: 09 February 2024 | 12:16  
Phone: +358 40 7614199

**Electronic Record and Signature Disclosure:**  
Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp
<b>Editor Delivery Events</b>	<b>Status</b>	<b>Timestamp</b>
<b>Agent Delivery Events</b>	<b>Status</b>	<b>Timestamp</b>
<b>Intermediary Delivery Events</b>	<b>Status</b>	<b>Timestamp</b>
<b>Certified Delivery Events</b>	<b>Status</b>	<b>Timestamp</b>
<b>Carbon Copy Events</b>	<b>Status</b>	<b>Timestamp</b>
<b>Witness Events</b>	<b>Signature</b>	<b>Timestamp</b>
<b>Notary Events</b>	<b>Signature</b>	<b>Timestamp</b>
<b>Envelope Summary Events</b>	<b>Status</b>	<b>Timestamps</b>
Envelope Sent	Hashed/Encrypted	09 February 2024   07:41
Certified Delivered	Security Checked	09 February 2024   12:16
Signing Complete	Security Checked	09 February 2024   12:16
Completed	Security Checked	09 February 2024   12:16
<b>Payment Events</b>	<b>Status</b>	<b>Timestamps</b>