AnTeS-PRIO

Reliability and Safety Assessment of the Prioritization Between Safety and Operational I&C Systems in Nuclear Power Plants

GRS - 821

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

AnTeS-PRIO

Reliability and Safety Assessment of the Prioritization Between Safety and Operational I&C Systems in Nuclear Power Plants

Christian Müller
Ewgenij Piljugin
Jaroslaw Shvab

Juli 2025

Remark:

This report refers to the in-house research project 4722R01215 which has been funded by the German Federal Ministry for the Environment, Climate Action, Nature Conservation and Nuclear Safety (BMUKN).

The work was conducted by the Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH.

The authors are responsible for the content of the report.

GRS - 821
ISBN 978-3-911727-14-3

Keywords

Common-Cause Failures (CCF), Digital I&C, Fault Tree Analysis (FTA), Functional Diversity, Monte Carlo Simulation, Nuclear Safety Assessment, Operational I&C, Prioritization and Actuation Control, Redundancy, Safety I&C

Abstract

The increasing complexity of digital Instrumentation and Control (I&C) systems in nuclear power plants necessitates advanced methodologies for assessing their reliability and safety. This report presents the development, validation, and application of a comprehensive analytical framework for evaluating I&C architectures, with a particular focus on the prioritization between safety I&C (SIC) and operational I&C (OIC) systems. The study was conducted using the Analysis and Test System (AnTeS), a modular platform developed by GRS that combines real and simulated I&C systems with a comprehensive set of tools and methods for system analysis. Within the scope of this project, AnTeS was significantly extended to include additional operational I&C systems, prioritization and actuation control modules, and enhanced field system components, thereby expanding its capabilities for the detailed investigation of complex I&C architectures.

The inclusion of real and simulated OIC systems as well as prioritization and actuation control (PAC) modules in AnTeS enabled detailed reliability assessments under realistic conditions, particularly for architectures where multiple I&C systems interact. These real systems supported direct fault injection and response testing, ensuring that actual hardware behavior could be observed and analyzed. The corresponding simulation models, implemented in a high-fidelity simulation environment, allowed for extensive failure mode analyses, probabilistic safety assessments, and Monte Carlo simulations. This ensured a comprehensive evaluation of both the I&C systems and the prioritization mechanisms responsible for resolving command conflicts between SIC and OIC. The integration of these new real and simulated systems into AnTeS significantly expanded its analytical capabilities, enabling a more detailed examination of complex I&C architectures.

The simulation and analysis methodology used during the project was validated by comparing real-system behavior with simulation results, ensuring that the models accurately reflect real I&C system performance. The validation process demonstrated a high degree of consistency between different analytical approaches. Using the validated framework, a series of model systems with varying configurations of SIC, OIC, and PAC modules were analyzed to assess the impact of redundancy, functional diversity, and general diversity on system reliability. The results, summarized in this report, illustrate the influence of these design parameters on overall system availability and failure risk.

From a regulatory perspective, the findings are highly relevant for technical support organizations such as GRS and nuclear safety authorities. The ability to model, validate, and analyze complex I&C architectures is essential for licensing new reactors, evaluating modifications to existing plants, and ensuring compliance with international safety standards. The insights gained in this study contribute to risk-informed decision-making, e.g., by identifying the predominant failure modes, in particular common cause failures, through the systematic analysis of redundant and diverse I&C architectures. The analyses also provide a robust foundation for supporting regulatory reviews and technical safety analyses, and contribute to training and knowledge transfer by enabling GRS to strengthen its expertise in the field of I&C assessment through validated methodologies.

In conclusion, this study demonstrates that the applied methodology provides a systematic, reliable, and transparent approach for evaluating digital I&C architectures, particularly in the context of SIC-OIC prioritization. The successful development and testing of real and simulated SIC, OIC, and PAC systems significantly enhance the ability of GRS to perform detailed assessments of modern nuclear I&C architectures. The results establish a solid foundation for future research and regulatory developments, ensuring that nuclear power plants maintain the highest levels of safety and reliability in their I&C architectures.

Table of Contents

1 Introduction

Modern instrumentation and control (I&C) systems in nuclear power plants (NPPs) worldwide are very often based on digital technologies. As part of a GRS project, methods were therefore developed and tested with which the dynamic behavior of digital I&C (DIC) systems can be analyzed when system-internal failures occur /PIL 18/.

This work was continued in another GRS project. In particular, the GRS Analysis and Test System (AnTeS) was set up, tested, and used as a flexible tool for the investigation of DIC systems. At that stage, AnTeS comprised simulated and a real safety I&C system (based on components of the digital Teleperm XS (TXS) I&C platform of Framatome) as well as simulated and real controlled components /MUE 21/.

When the consideration of individual I&C systems is extended to complete I&C architectures, it becomes clear that many safety-relevant components in NPPs and other nuclear facilities are often controlled by both the safety I&C (SIC) system and the operational I&C (OIC) system. Wherever this is the case, a suitable, reliable prioritization of the corresponding signals from the SIC before those from the OIC must take place in order to guarantee the availability of the safety-relevant components at all times.

Although there are many qualitative and quantitative analysis methods[1] for evaluating the reliability of safety-relevant I&C, such as Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Monte Carlo (MC) simulation and Markov processes for example, to date, there are hardly any generally accepted approaches available for evaluating the reliability of prioritizations of signals from the SIC and OIC within complete I&C architectures, especially when digital equipment is involved.

The aim of this research project was therefore to develop a basis for evaluating complete I&C architectures including prioritization between SIC and OIC based on GRS methods. In particular, AnTeS has been expanded in this project to include prioritization and actuation control (PAC) modules, and OIC systems.

[1] These methods were and are used in different combinations or individually depending on the objective, the complexity of the object to be analyzed, and the availability of data and information. More information on the different methods can be found in /MUE 18/, /MUE 21/, /MUE 21a/, /MUE 23/, and /MUE 24/ as a starting point.

The following sections within this chapter provide a brief insight into the state of the art with regard to I&C architectures, OIC systems and PAC modules in NPPs.

1.1 I&C Architectures in NPPs

I&C architectures differ between almost all existing NPPs. In order to implement a more generic approach rather than a plant specific one it was decided to look at I&C architectures as laid out in conceptual schematic diagrams, as published for example by manufacturers or in other research projects.

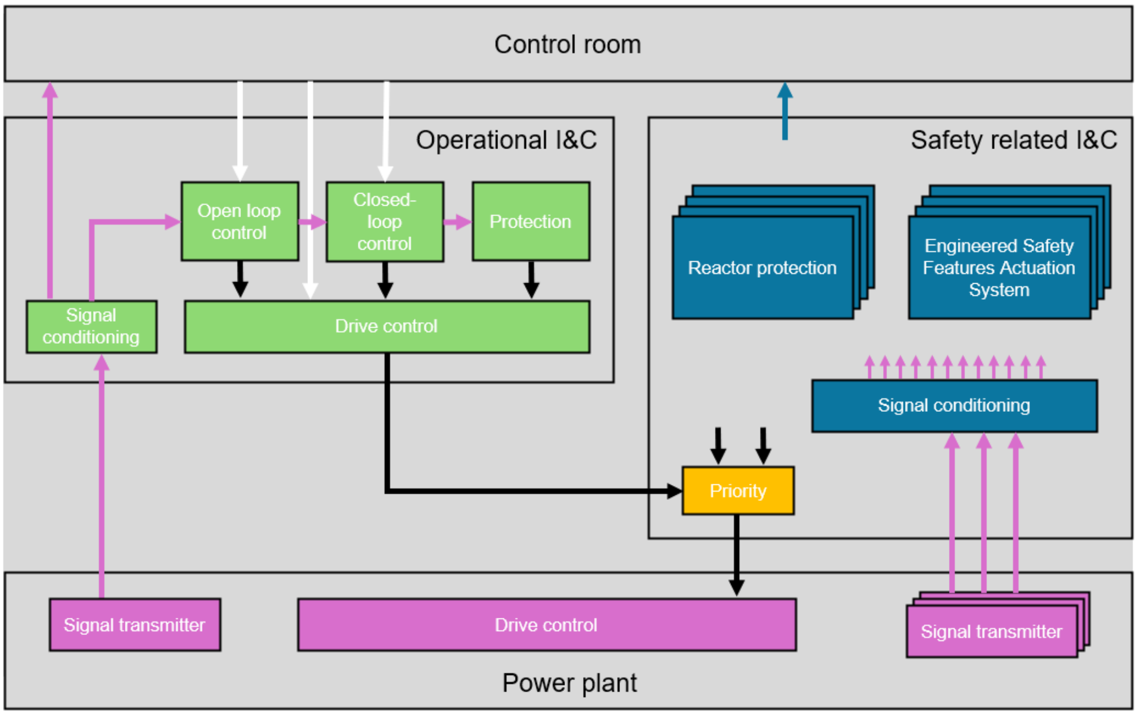


Figure 1.1 Schematic I&C concept for an NPP

Image has been created by GRS based on information from /SIE 07/.

Even if the concepts of different manufacturers differ in the details, many similarities can be found in the sense of a generic view, which can be transferred to a generic architecture. Figure 1.1, for example, shows a schematic concept from Siemens.

This figure shows conceptually how OIC and SIC interact in an I&C architecture. The SIC performs the I&C functions important to safety of the reactor protection system (in particular reactor shutdown), and the so-called Engineered Safety Features Actuation System (ESFAS) of the SIC ensures the control of safety-related systems. In normal operation, however, certain systems are controlled by the OIC, e.g., for regulation (open loop control) or control (closed loop control) purposes. The necessary prioritization between OIC and SIC commands is performed by PAC modules (“Priority” in the figure above).

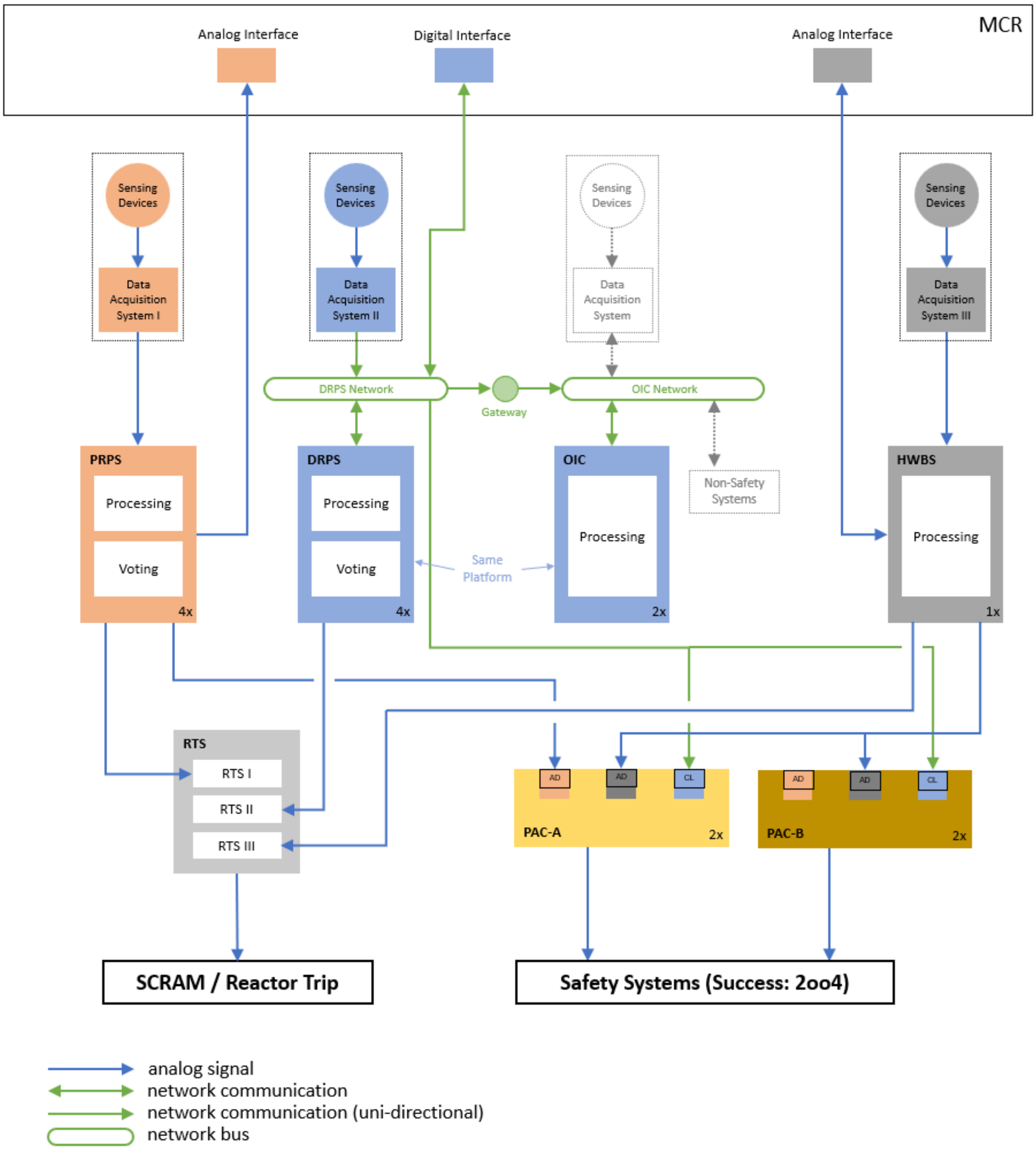


Figure 1.2 Generic I&C architecture

Image has been taken from /DIG 25/.

Another overview of an exemplary I&C architecture can be seen in Figure 1.2. This figure is part of the reference case in the DIGMORE project[2] /DIG 25/. As many experts from different countries work together in this project and developed this reference case together, this architecture can be considered a very good international reference for a generic I&C architecture.

Here, a total of even three different I&C systems (PRPS, DRPS and HWBS)[3] have access to the same safety systems, so that their actuation signals must be prioritized with the help of PAC modules. The comparatively high number of three different I&C systems performing the same functions and the additional diversity in the PAC modules (PAC-A and PAC-B) was a deliberate decision within the framework of DIGMORE. In this way other realistic I&C architectures can then be studied simply by omitting individual I&C systems or other parts of the architecture. In this sense, for example, the schematic concept (from Siemens) shown in Figure 1.1 could be represented quite well by omitting the diversity of the PAC modules and the HWBS.

1.2 Operational I&C (OIC) in NPPs

From a very basic point of view, OIC systems have a similar structure to SIC systems. However, important differences can be observed in detail, particularly when using digital OIC systems. Depending on the requirements, both qualified systems (i.e., systems that could also be used as SIC) and systems such as those used in conventional power plants can be used. In the latter case, technologies may be used that are not (yet) typically used in SIC systems.

Figure 1.3 shows a representative generic I&C architecture of a conventional power plant. Such architectures are often characterized by the extensive use of digital network technologies (in the figure: Ethernet, Profinet, Profibus[4], and even wireless networks in

[2] A task of the Working Group on Risk Assessment (WGRISK) of the Organisation for Economic Co-operation and Development (OECD) / Nuclear Energy Agency (NEA). GRS has taken over the leadership in this task.

[3] Primary reactor protection system (PRPS), diverse reactor protection system (DRPS), and hard-wired backup system (HWBS).

[4] Officially Siemens claims that Profibus is not a network technology but an extension of the backside bus of decentralized periphery. For the purpose of this project, Profibus is nevertheless treated as a network technology.

this case) and typically exhibit a low degree of redundancy. Even though some of these characteristics cannot easily be transferred to all OIC systems in NPPs (especially not to German NPPs), information from conventional plants can nevertheless serve as a source for developing models of generic OIC systems.

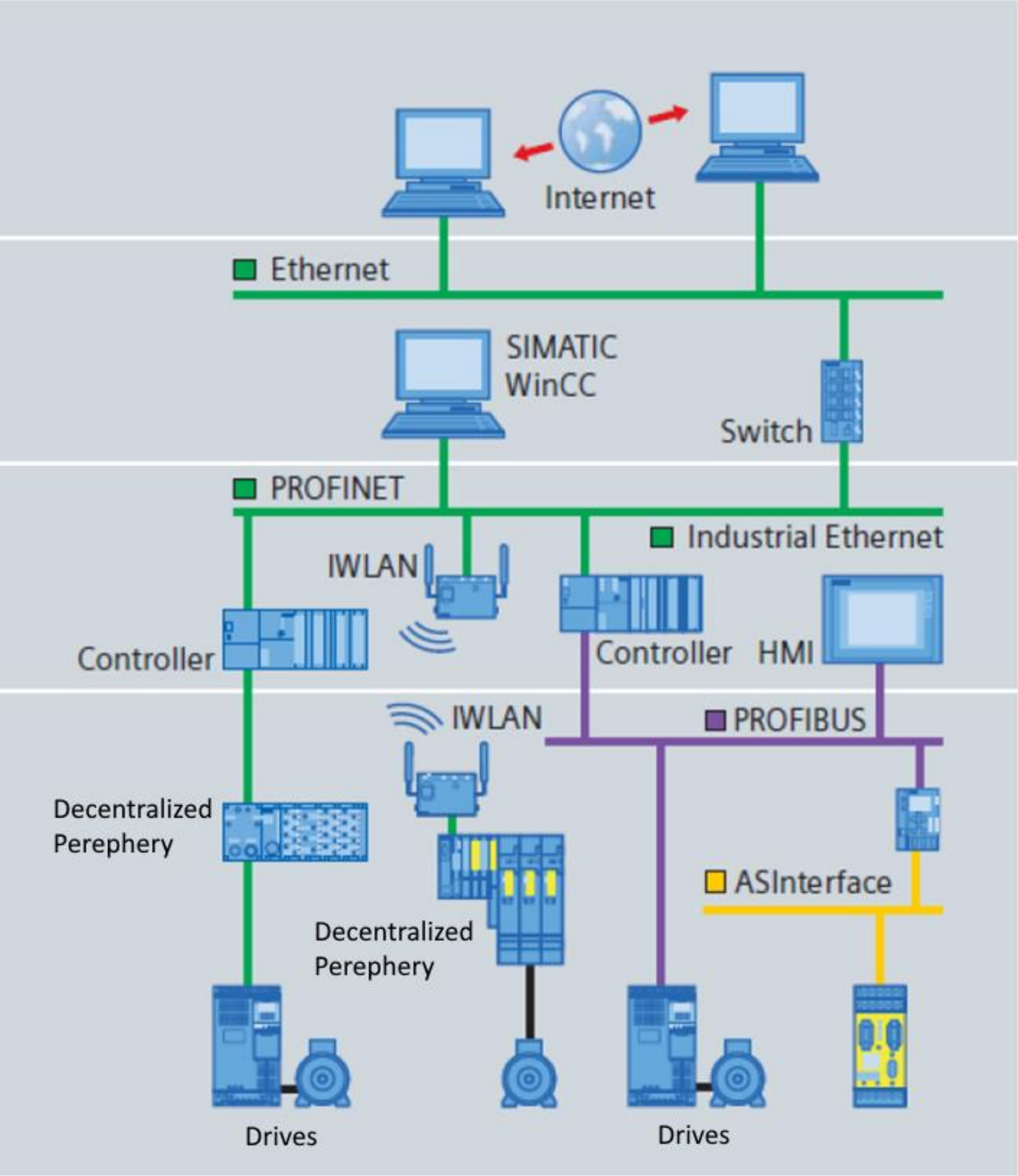


Figure 1.3 Example of an I&C architecture in a conventional power plant

This image has been taken from /ARI 15/, but subsequently modified. The modifications consisted solely of replacing some German terms with English terms (e.g., “Decentralized Periphery”).

While there is a similarly high degree of variety here as with SIC systems, many common, generic characteristics can still be consistently identified. Within the scope of this project, the models of OIC systems were primarily developed based on information about the Siemens Simatic S7 I&C platform, as this platform was also used for constructing the OIC system in the context of the expansion of AnTeS. Accordingly, in addition to the availability of extensive information, there was also direct experience with this platform. Further information on OIC systems can also be found elsewhere in this report (see Section 2.3 and Section A.2 in the appendix).

1.3 Prioritization and Actuation Control (PAC) in NPPs

In the hierarchical structure of I&C architectures of NPPs, prioritization and actuation control (PAC) modules are situated at the lowest level. PAC modules directly control the actuators via switchgears. Therefore, PAC modules are highly important interfaces between the command transmitters (e.g., manual control panels, SIC systems, and OIC systems) and command receivers (e.g., motor drives of pumps and valves). They perform all the necessary tasks of command processing and monitoring, whereby the input commands are linked according to the specified priority and permissibility and forwarded via the switchgears as control commands to the actuators being controlled (compare, e.g., Figure 1.4 or Figure 1.5).

In NPPs special PAC modules take over the task of prioritization, whereby the commands of the SIC system (e.g., reactor protection commands) are given priority over operational commands (e.g., manual commands, OIC commands) for safety-related motor and actuator drives.

As for OIC systems, extensive research was also carried out for PAC modules. As real AV42 modules and SPLM1-PC11 modules in particular are available at GRS (see Figure 2.11), the generic PAC modules of the model systems were based on these.

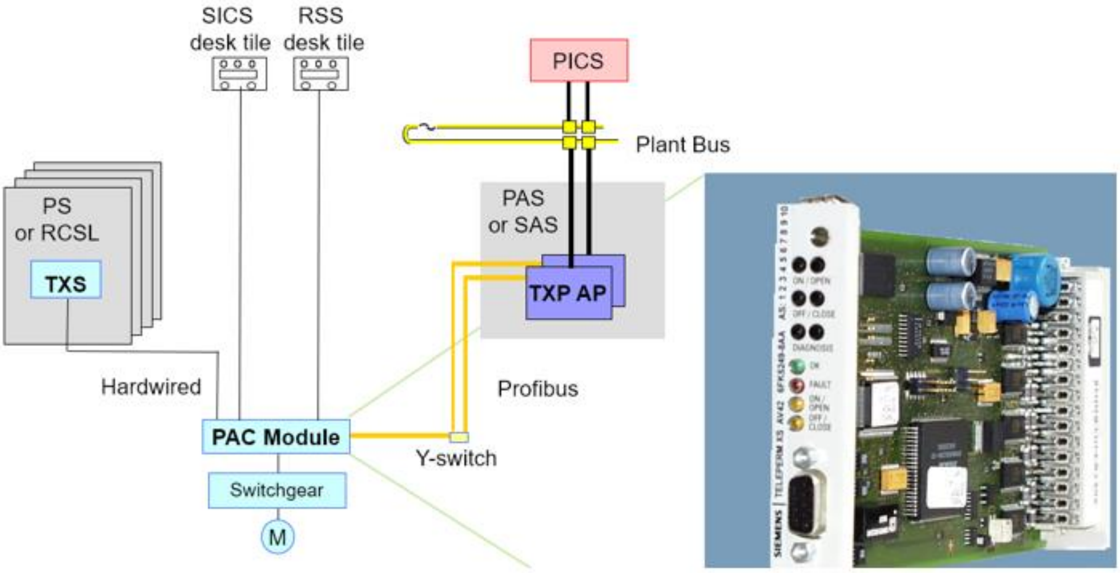


Figure 1.4 Priority control based on the AV42 module

This image has been taken from /GRA 06/. Note that the AV42 shown in the embedded photo is still labeled with “Siemens”. The AV42 was later manufactured by Areva, today Teleperm XS is manufactured and delivered by Framatome.

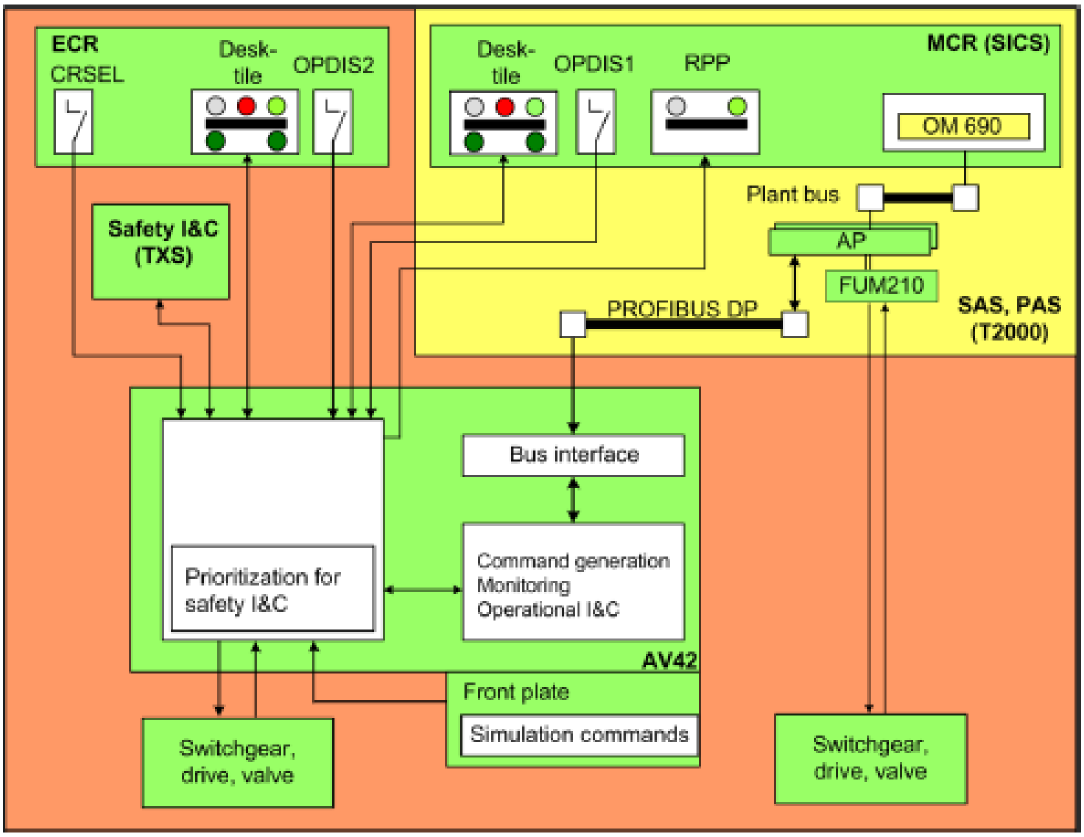


Figure 1.5 The tasks of the AV42 module in an NPP

This image has been taken from /ARE 17/.

2 The Analysis and Test System (AnTeS) of GRS

This chapter presents the Analysis and Test System (AnTeS) of GRS in detail. There is no specific differentiation in this chapter between parts that already existed and parts that were created during this project. In particular, however, the AnTeS-OIC and AnTeS-PAC modules were created from scratch as part of this project, as were significant further developments in the AnTeS-FIELD module. More detailed information on the work on these modules can be found in Appendix A "Details on the Extension of AnTeS".

2.1 Overview

AnTeS of GRS is a modular platform of different tools and methods for investigations into I&C technology. AnTeS basically has four modules (see also Figure 2.1):

AnTeS-SIC

- AnTeS-SIC-real: a real safety I&C system (SIC)
  - based on Teleperm XS hardware and software from Framatome
- AnTeS-SIC-sim: simulated safety I&C systems
  - based on Matlab/Simulink /MAT 25/

AnTeS-OIC[5]

- AnTeS-OIC-real: a real operational I&C system (OIC)
  - based on Simatic S7 hardware and software from Siemens
- AnTeS-OIC-sim: simulated I&C systems
  - based on Matlab/Simulink

AnTeS-PAC

- AnTeS-PAC-real: real priority (and actuation) modules (PAC)
  - AV42, SPLM1-PC11
  - Generic priority module (GRS in-house development for AnTeS)
- AnTeS-PRIO-sim: simulated priority modules
  - based on Matlab/Simulink

[5] In the context of this report, the term OIC is always used for this module of AnTeS. However, it should be noted that this system could also be understood as a (possibly less qualified) diverse backup system.

AnTeS-FIELD

- AnTeS-FIELD-real: real process engineering systems
  - vessels, drives, measuring devices/sensors, valves, pumps
- AnTeS-FIELD-sim: simulated process engineering systems
  - SimGen, see /MUE 21/ and Section 2.5

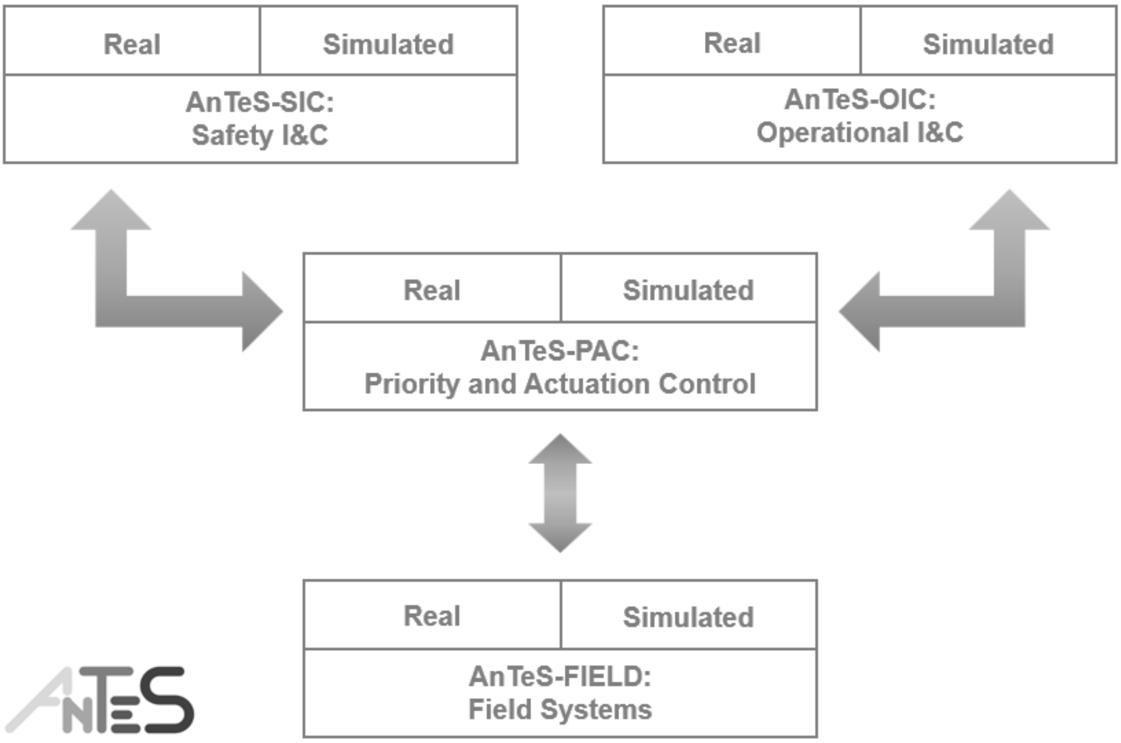


Figure 2.1 AnTeS: overview

In addition, various analysis methods are available that can be used in conjunction with the AnTeS modules for investigations relating to I&C:

- FMEA – Failure Mode and Effects Analysis
  - FMEA is a systematic method for identifying, evaluating, and prioritizing potential faults or weaknesses in a product, process, or system. By analyzing possible causes of failure and the effects of these failures, FMEA helps to identify risks at an early stage and develop suitable measures to prevent, minimize or eliminate failures. The method is used in various sectors, including the automotive industry, aviation, medical technology, and the energy industry, to increase the reliability and safety of products and processes (see for example /NAT 15/).

  - In the context of AnTeS and the methodology applied at GRS, FMEA is mainly used to determine the relevant failure modes (e.g., of components, subsystems) for further modeling. More detailed descriptions and further references can be found in /MUE 21/.

- Automatic impact analysis or failure effects analysis (“FMEA+”)

  - This is an extended FMEA procedure that was developed as part of a GRS project /MUE 21/. Here, a simulated or real system is used into which failures (e.g., of components or subsystems) can be injected with the aid of fault injection. By automatically varying all conceivable states (inputs as well as internal states) of all considered parts of the system ("has failed self-reporting", "has failed non-self-reporting", "is functioning correctly") and simultaneously recording the overall state of the system ("actuation of the safety function occurs as intended", "actuation of the safety function does not occur as intended"), all failure combinations can be determined in this way that are equivalent to an overall failure of the system.

  - In the context of AnTeS, the more comprehensive and less error-prone automatic impact analysis usually replaces a simple FMEA. The results of the automatic impact analysis in turn support the fault tree analysis. More detailed descriptions can be found in /MUE 21/.

- FTA - Fault tree analysis

  - Fault tree analysis is a systematic, top-down approach used to determine how combinations of lower-level failures and conditions can lead to a specified undesired event (the so-called top event) in complex systems. It visualizes the possible error paths in the form of a tree diagram, in which the top level represents the undesirable end state. By analyzing the failure paths step by step from the top of the tree to the root causes, critical weaknesses and potential combinations of events that could lead to an undesired event can be identified. Fault tree analysis is a powerful tool used in various industries to assess risks, develop safety measures, and improve the reliability of complex systems. By incorporating probabilities and data on individual events, fault tree analysis also enables the quantitative assessment of risks and the derivation of probabilities for the occurrence of undesirable events, which provides a sound basis for decision-making, for example for preventive measures (see for example /XIN 08/).

  - In the context of AnTeS, fault tree analyses provide the same qualitative results as automatic impact analyses (whereby the two methods check each other). In addition, fault tree analyses can also be used to obtain quantitative results on the analyzed systems. More detailed descriptions and further references can be found in /MUE 21/. Comparable quantitative results can also be obtained with Monte Carlo simulations.

- Monte Carlo simulation

  - Monte Carlo simulations are a computer-aided method used in various fields to analyze complex problems for which analytical solutions are difficult or impossible. This method is based on random sampling and repeats the analysis of a model or system thousands or even millions of times, each time taking into account random variations in the input parameters. The results of these simulations provide statistical distributions of possible outcomes and enable the estimation of probabilities, risks, and other quantitative information. Monte Carlo simulations are used in finance, engineering, natural sciences, risk analysis and many other disciplines to get a better idea of the possible outcomes of complex systems or models (see for example /RUB 16/).

  - In connection with AnTeS, simulated I&C systems are used for Monte Carlo simulations, into which statistical failures of certain components are fed by fault injection. Quantitative results comparable to fault tree analyses can be achieved. Thus, Monte Carlo simulations can completely replace fault tree analyses in individual cases or at least verify their results. More detailed descriptions and further references can be found in /MUE 21/.

By combining real and/or simulated modules into an overall system, different configurations and I&C architectures can be flexibly implemented depending on the requirements and investigated using the available methods (see Figure 2.1). The following Sections 2.2 to 2.5 present the individual modules (AnTeS-SIC, AnTeS-OIC, AnTeS-PAC, AnTeS-FIELD) in more detail.

2.2 AnTeS-SIC – Safety I&C

The AnTeS-SIC-real submodule is based on components of the I&C platform Teleperm XS (TXS) of Framatome (formerly Areva), which were acquired by GRS from the NPP Krümmel in May 2017. These components were originally intended for a modernization of the turbine control system but were never implemented. Following the final shutdown of the plant in 2011, the components were no longer needed by the NPP Krümmel and were sold to GRS.

After setting up the I&C cabinets in a server room at the GRS facility in Garching and connecting them to an appropriate power supply, two of the cabinets were completely gutted. The AnTeS-SIC-real submodule was then installed in these cabinets, commissioned, and tested for functionality /MUE 21/.

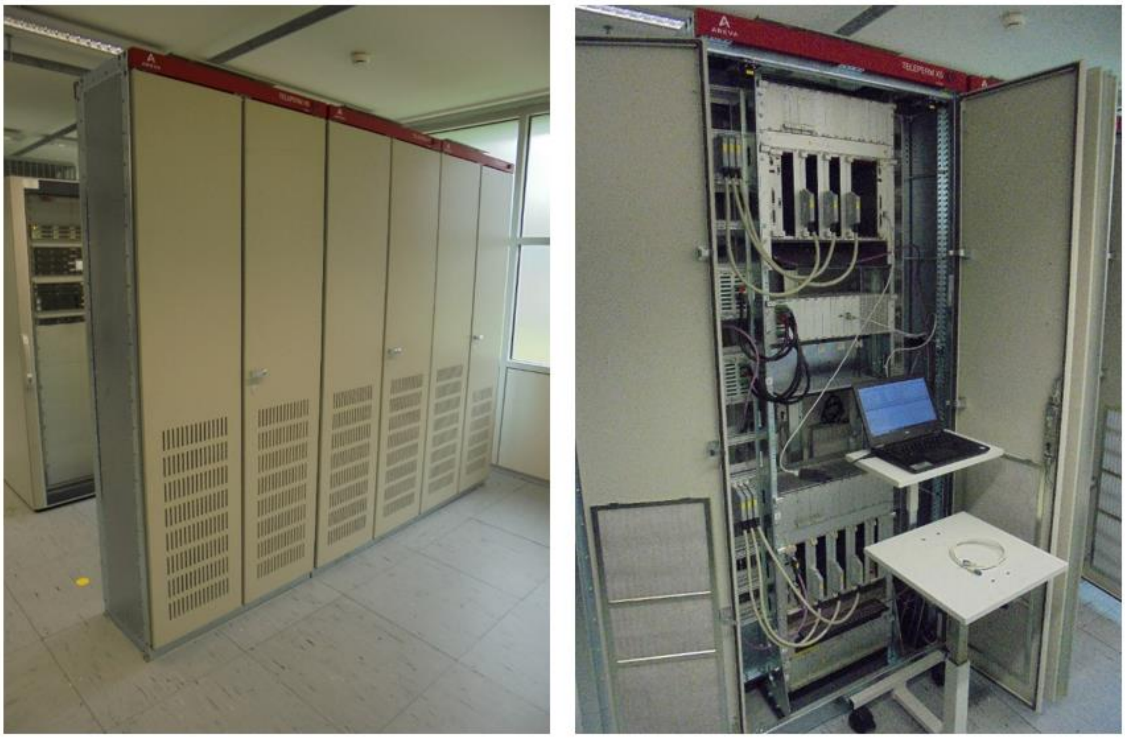


Figure 2.2 AnTeS-SIC-real: Teleperm XS (generation 2) cabinets

A typical configuration of AnTeS-SIC-real includes up to four redundant processing units (each consisting of a processor module as well as analog and digital input/output modules[6]) housed in two cabinets (see Figure 2.2). Each cabinet also contains dedicated communication processor modules that enable network connections to a service unit (computer). Figure 2.3 illustrates a possible configuration (network plan) within the TXS engineering environment SPACE (“specification and coding environment”). SPACE itself allows the flexible creation of different configurations and the programming of TXS (function block creation) on the service unit via a graphical interface. To achieve this, the service unit, also provided by the NPP Krümmel, was virtualized and is now operated as a virtual machine on a server in a separate cabinet within the same server room at GRS.

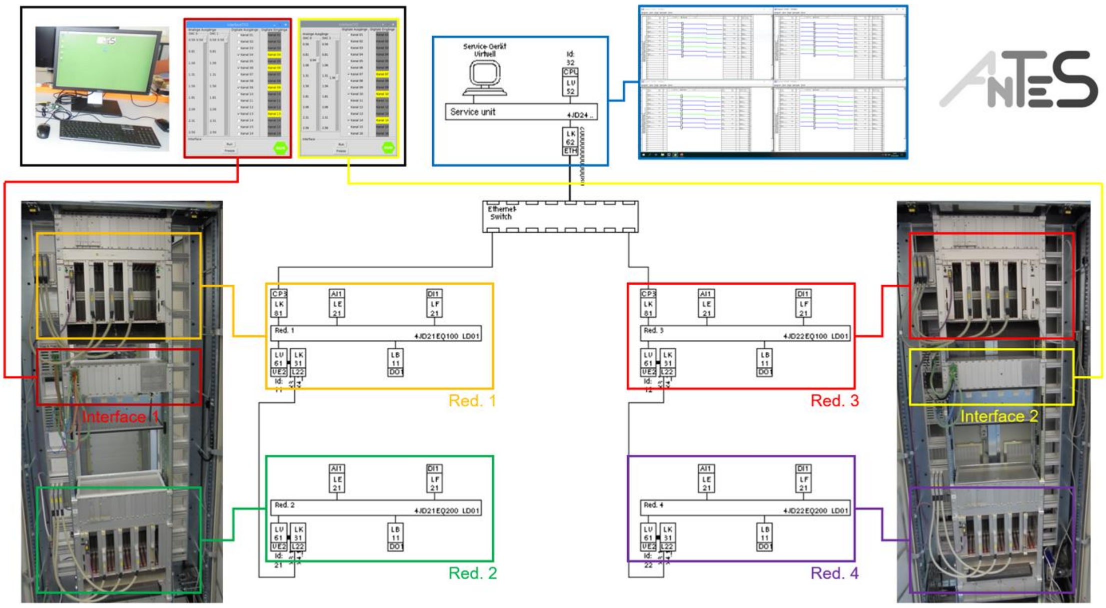


Figure 2.3 AnTeS-SIC-real: standard configuration

The middle part of the image is a screenshot of the network plan of the standard configuration (from the engineering environment SPACE of the system) in which the service unit (blue) and the four redundancies (orange, green, red, and purple) have been framed with boxes. Photos of the real cabinets have been added on the right and left, and the corresponding redundancies have also been marked with boxes in the respective colors. In addition, an operating station for the interfaces, which are used to exchange signals with the I&C system, is shown at the top left.

[6] In the field of I&C systems engineering, the terms "analog" and "digital" are often used somewhat imprecisely. Naturally, all signals within an actual digital I&C system (e.g., TXS) are purely digital. The terms "digital" and "analog" are frequently employed to differentiate between strictly binary signals (e.g., 0/1; 0 V/24 V) and signals that can represent more than just two states (e.g., floating-point numbers, 4...20 mA, etc.).

In addition to using a real I&C system (AnTeS-SIC-real), the AnTeS-SIC-sim submodule allows for the use of simulated I&C systems for analyses. These simulated systems can replicate the same functionalities as the real I&C system (TXS) as well as other real or generic I&C systems.

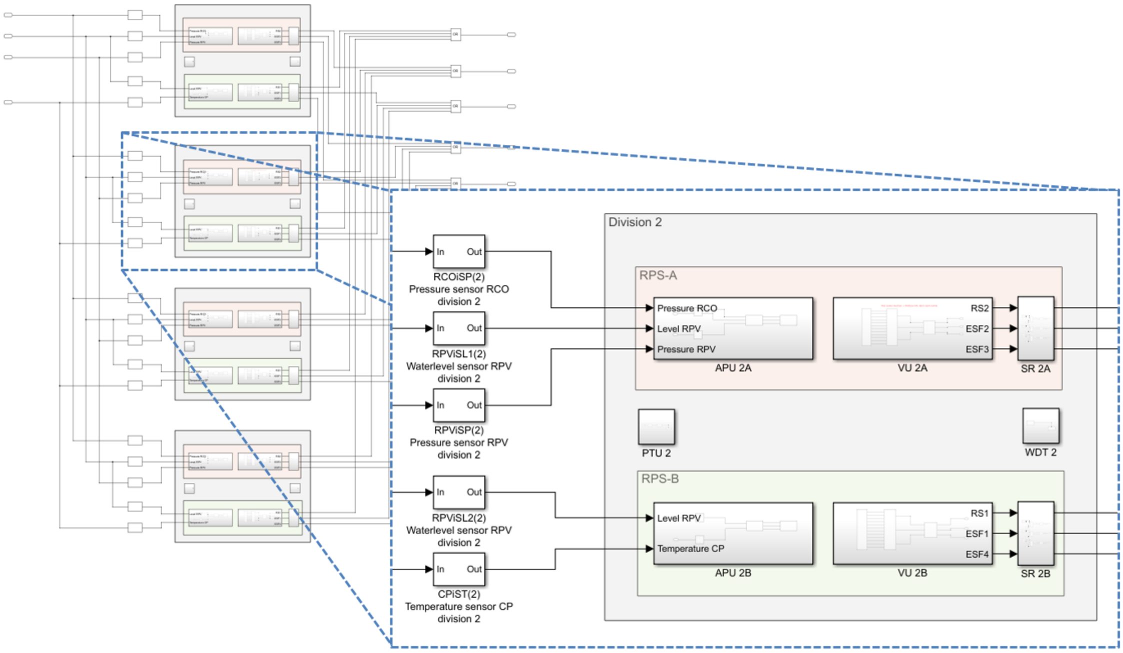


Figure 2.4 AnTeS-SIC-sim: example

AnTeS-SIC-sim is based on the Simulink software, which is generally used for system modeling and is an add-on product for Matlab /MAT 25/. Systems are modeled within a GUI using function blocks, the data flow between these blocks is represented by connecting lines (see Figure 2.4). A system modeled in this way can then be simulated within Simulink using various solution methods (solvers).

Additional Simulink software packages enable these simulations to be exported as dynamic link libraries (DLLs), which can then be used for further simulation by external programs or scripts (for details, see /MUE 21/). Alternatively, Simulink allows for direct export and execution of simulation models on external hardware (e.g., Raspberry Pi microcomputers), simplifying the integration of models with other systems.

Using Simulink to program I&C functions is similar in practice to using the SPACE engineering environment of the TXS system. Simulink offers a wide range of function blocks within the software interface. Using these blocks, a variety of model systems can be created.

Of particular importance is the ability to create custom function blocks within Simulink using so-called subsystems. When using Simulink as an engineering environment for virtual (simulated) I&C systems, custom function blocks can be created that behave identically to the corresponding function blocks of real I&C systems (Figure 2.5). To replicate TXS function plans using Simulink, a wide range of TXS function blocks (as Simulink subsystems) have been created. This has resulted in a dedicated Simulink library containing TXS function blocks, which already includes many of the most commonly used blocks, though it is not yet comprehensive. Missing blocks can be added as needed with relatively little effort. Furthermore, Simulink also allows the hardware functionalities of simulated I&C systems to be accounted for using existing Simulink function blocks or custom subsystems, as required.

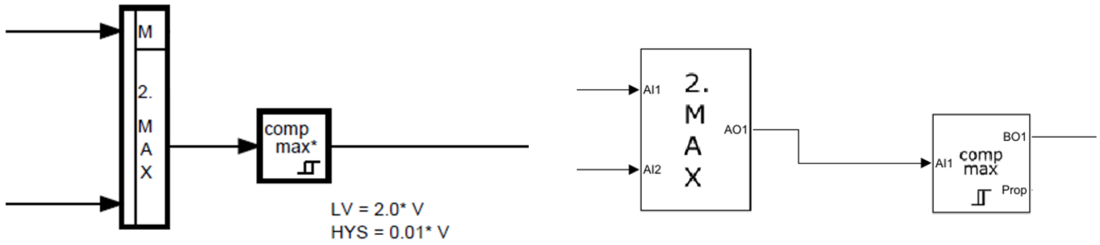


Figure 2.5 AnTeS: engineering with function blocks

On the left side: function blocks of AnTeS-SIC-real (within the engineering environment SPACE of TXS); on the right side: function blocks of AnTeS-SIC-sim (within Simulink).

An important element in the investigation of I&C systems with AnTeS is the possibility of fault injection. For this purpose, faulty behavior is implemented in special, additional functions directly during the engineering process (i.e., with SPACE for TXS), which can later be switched on or off during operation. The corresponding descriptions for SIC and OIC fault injection in Sections 4.2 and 4.3 provide more detailed insights on this way of fault injection.

With regard to fault injection specifically into the network communication (of any system), there is also a direct intervention option via network manipulators specially developed by GRS for this purpose /MUE 24/, see Figure 2.6.

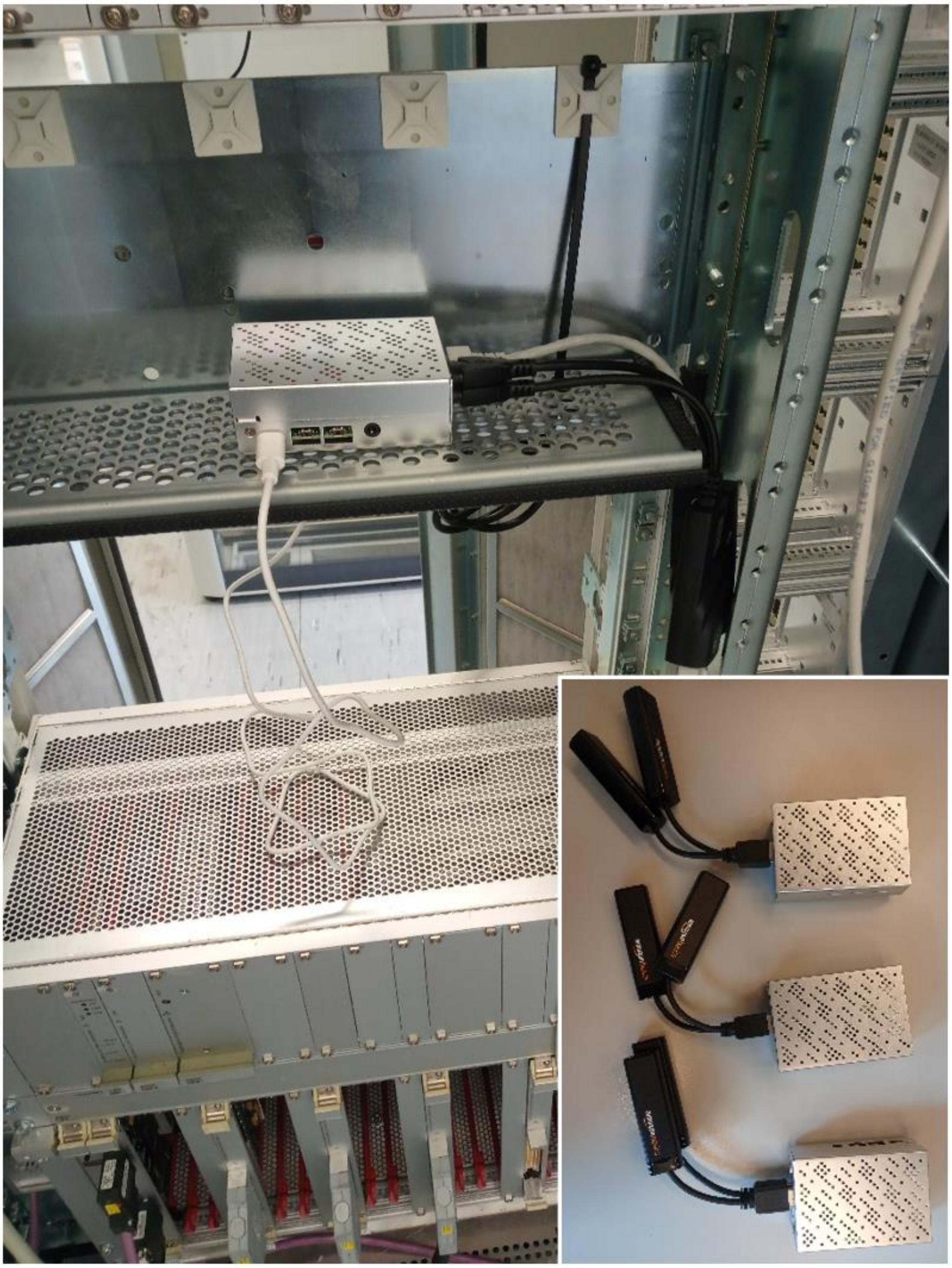
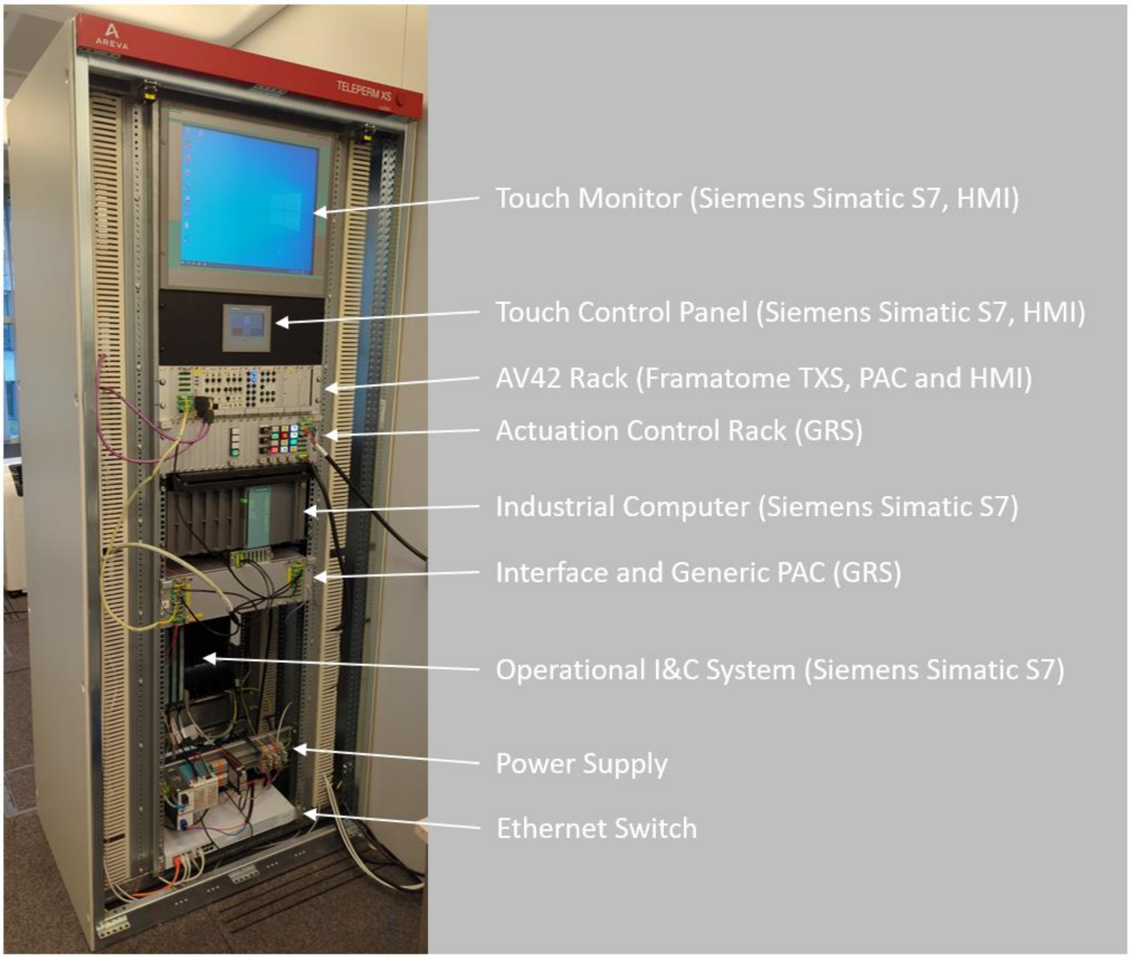


Figure 2.6 Fault injection modules for network communication

Network manipulators, which can be used as fault injection modules for (any) network communication, were developed as part of a GRS project (see /MUE 23/, /MUE 24/). These allow both targeted manipulation (in the sense of cyber-attacks) and the simulation of random failures. The figure shows one of these manipulators in use in one of AnTeS-SIC's cabinets and three others in the embedded photo. GRS has a total of five such self-developed manipulators, and more could be quickly replicated at any time if required.

2.3 AnTeS-OIC – Operational I&C

The AnTeS-OIC-real submodule is located together with other systems in an additional cabinet in the AnTeS laboratory of GRS (Figure 2.7).



AREVA
TELEPERM XS
Touch Monitor (Siemens Simatic S7, HMI)
Touch Control Panel (Siemens Simatic S7, HMI)
AV42 Rack (Framatome TXS, PAC and HMI)
Actuation Control Rack (GRS)
Industrial Computer (Siemens Simatic S7)
Interface and Generic PAC (GRS)
Operational I&C System (Siemens Simatic S7)
Power Supply
Ethernet Switch

Figure 2.7 AnTeS cabinet with OIC, PAC and HMI

The cabinet shown is located in the AnTeS laboratory in the immediate vicinity of the server room in which the cabinets for AnTeS-SIC are installed. This cabinet was delivered together with the other Teleperm XS cabinets and was originally intended as a place specifically for the service unit (and an additional gateway). Since the service unit for AnTeS-SIC was virtualized, this cabinet was available for free use. For this reason, the cabinet is still labeled Teleperm XS at the top. However, apart from a priority module (AV42), the parts installed in the cabinet are not TXS components.

This cabinet contains from top to bottom:

- Touch monitor
  - Siemens Simatic S7
  - part of human-machine interface (HMI) of AnTeS

- Touch control panel
    - Siemens Simatic S7
    - part of human-machine interface (HMI) of AnTeS
- AV42 rack
    - Framatome TXS
    - part of AnTeS-PAC
    - see also Section 2.4
- Actuation control rack
    - in-house development by GRS
    - part of AnTeS-FIELD
    - see also Section 2.5
- Industrial computer
    - Siemens Simatic S7
    - part of AnTeS-FIELD
- Interface and generic PAC
    - in-house development by GRS
    - part of AnTeS-PAC and AnTeS-OIC
- OIC system
    - Siemens Simatic S7-400
    - AnTeS-OIC
- Power supply
- Ethernet switch

A close-up of the OIC system mentioned above can be seen in Figure 2.8, which forms the AnTeS-OIC-real submodule within AnTeS. With this module, different OIC configurations can be realized flexibly. The I&C functions to be implemented for each configuration are programmed using the engineering environment TIA Portal (Totally Integrated Automation Portal – Software from Siemens)[7].

[7] Within TIA Portal, three options are available for programming I&C functions. In the context of AnTeS-OIC-real, programming the system with function blocks within function plan diagrams is usually preferred; this then essentially corresponds to the procedure in AnTeS-SIC-real with its engineering environment SPACE (compare Section 2.2).

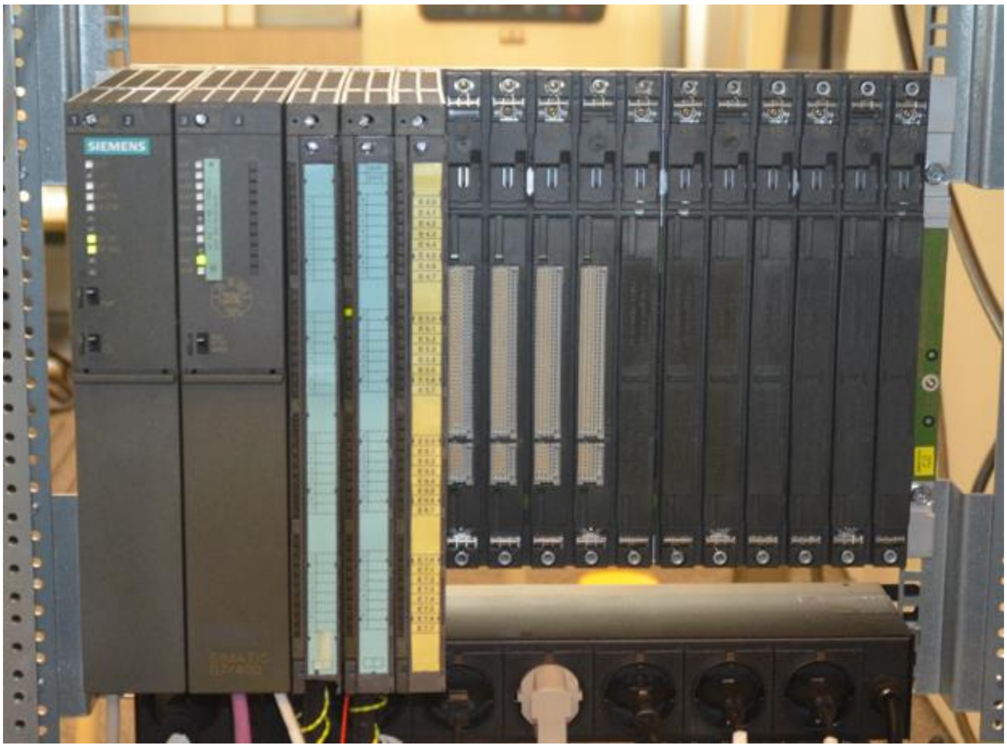


Figure 2.8 AnTeS-OIC-real: Simatic S7-400

Located in the cabinet shown in Figure 2.7 (position in cabinet marked with “Operational I&C System (Siemens Simatic S7)”).

Figure 2.9 shows the so-called device view within TIA Portal, the setup shown corresponds to the configuration in Figure 2.8. The plug-in cards used in this standard configuration of AnTeS-OIC-real can be easily identified in both figures (from left to right):

- Slot 1 (& 2): Power supply (PS) module
- Slot 3 (& 4): Programmable Logic Controller (PLC)[8]
- Slot 5: Digital Input (DI) module
- Slot 6: Digital Output (DO) module
- Slot 7: Analog Input (AI) module

As with the AnTeS-SIC-real module, the network configuration must also be defined within the engineering environment during engineering process (Figure 2.10). In this example, the PLC is connected to a touch panel (HMI_1) and the PC system on which

[8] Basically, a computer including processor and work memory. The naming was taken from the manufacturer, but for the purposes of this report it is a processor module (PM).

TIA Portal is installed via a Profinet connection (PN/IE_1). In addition, an AV42 is connected to the PLC via a Profibus connection.

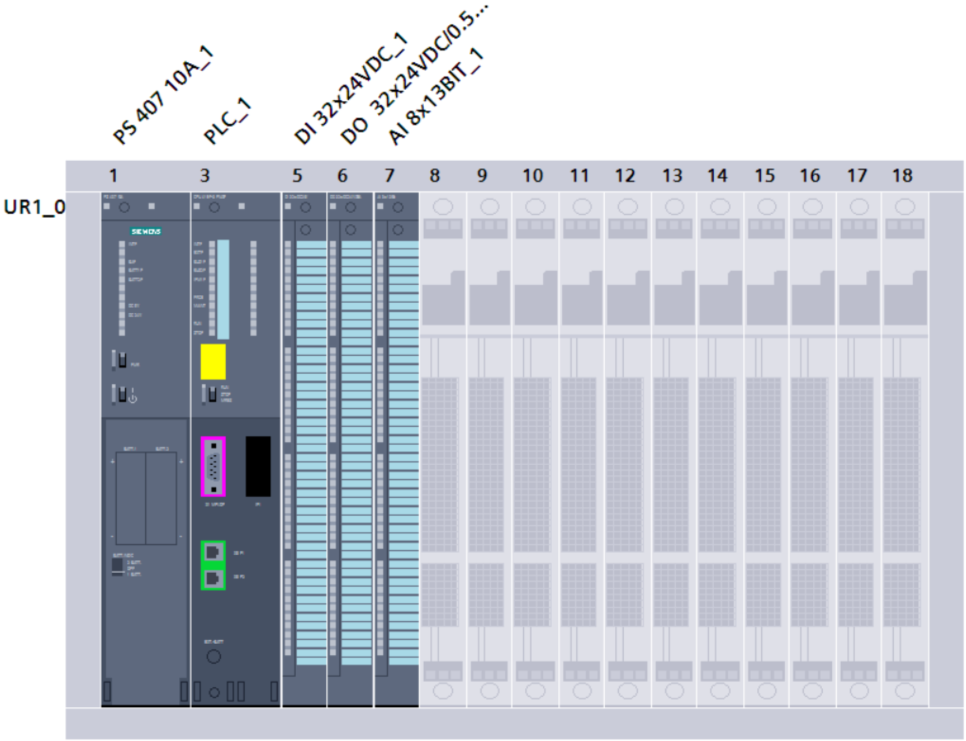


Figure 2.9 AnTeS-OIC-real: Siemens TIA Portal – device view

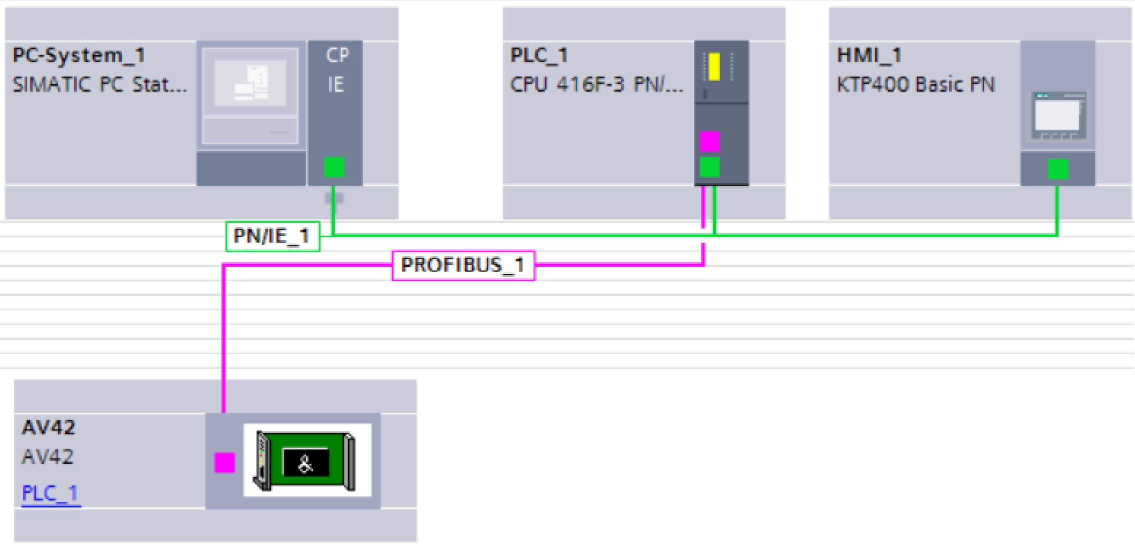


Figure 2.10 AnTeS-OIC-real: Siemens TIA Portal – network view

In addition to the Simatic S7 system in Figure 2.8, GRS has another subrack, another PLC and a number of additional input and output cards, so that an OIC system with at least double redundancy could also be implemented within AnTeS-OIC-real if required. More information on AnTeS-OIC-real can be found in Section A.2 of the annex.

The AnTeS-OIC-sim submodule can be used to simulate (in principle any) OIC systems. The creation, programming and use of these systems is completely analogous to simulated systems within AnTeS-SIC-sim (see Section 2.2).

2.4 AnTeS-PAC – Prioritization and Actuation Control

Prioritization and actuation control (PAC) modules of the types AV42 and SPLM1-PC11 from Framatome (formerly Areva) are available as real prioritization modules within AnTeS-PAC-real. Figure 2.11 shows four such PAC modules in a GRS test subrack during the commissioning and set-up phase of AnTeS-PAC-real.

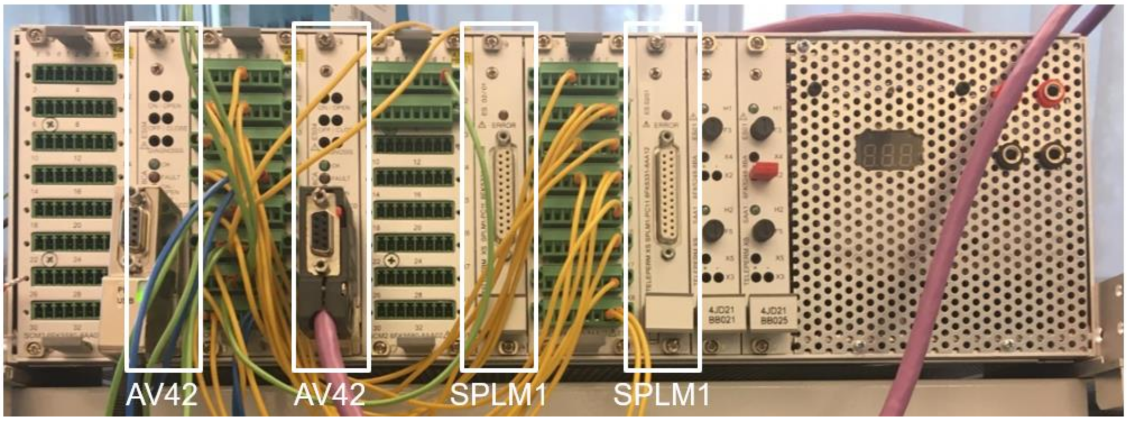


Figure 2.11 AnTeS-PAC-real: real priority modules in a test rack

The standard procedure for investigations with AnTeS-PAC-real, particularly in the context of this project, is to use an AV42 prioritization module in its own subrack (Figure 2.12). This subrack was kindly made available to GRS on permanent loan by the manufacturer Framatome and is located in the same cabinet as AnTeS-OIC-real (see Figure 2.7).

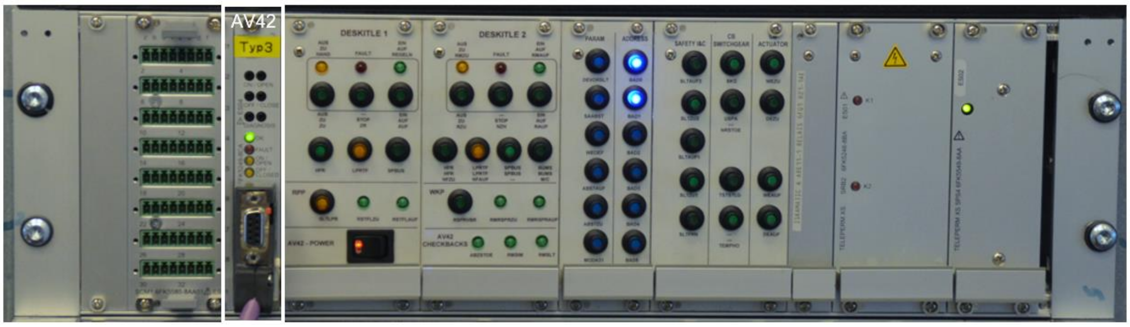


Figure 2.12 AnTeS-PAC-real: AV42 subrack

This subrack not only has a slot for an AV42, but also two connected control panels and allows a very convenient access to the rear pins of the AV42 via sockets (far left in the picture). In addition, input signals from I&C systems can be simulated and some parameterization of the AV42 can be carried out via buttons.

In order to be able to take other PAC modules into account as flexibly as possible and, among other things, to make it as easy as possible to use fault injection with PAC modules during analyses, a generic PAC module was also set up by GRS (Figure 2.13).

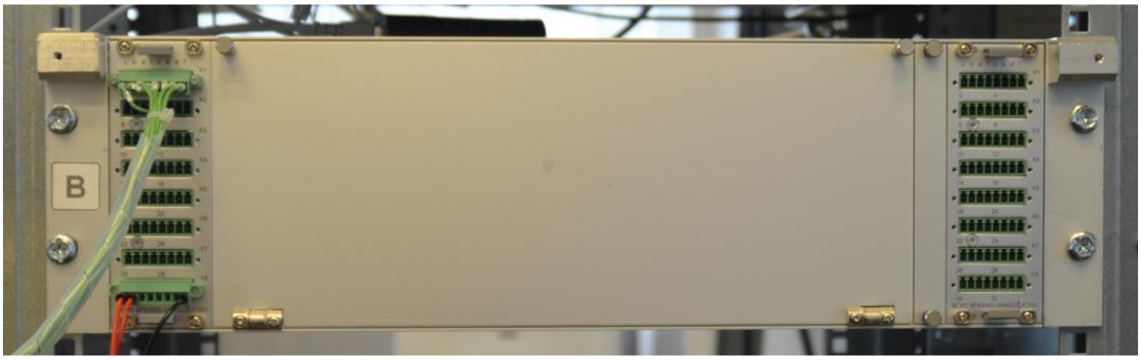


Figure 2.13 AnTeS-PAC-real: generic priority module (and AnTeS-OIC interface)

This generic PAC module is based on a mini-computer (Raspberry Pi 4) and two microcontroller cards (Arduino Due) installed in the corresponding subrack together with some optocoupler and relay cards. The behavior of this PAC module can be flexibly configured (e.g., adapted to the behavior of a PAC module from any manufacturer) with the help of software developed by GRS.

This subrack of AnTeS-PAC-real with a total of 32 binary inputs, 32 binary outputs, 8 analog inputs and 2 analog outputs also serves as a general interface to the OIC and is therefore also part of AnTeS-OIC-FIELD.

Pure simulation models of PAC modules, for example for use in Monte Carlo simulations, are created within AnTeS-PAC-sim using the Simulink software (add-on module for Matlab /MAT 25/). Figure 2.14 shows an example for this, where a Hardline-B.PRIO 11 module (Framatome) is functionally reproduced using Simulink.

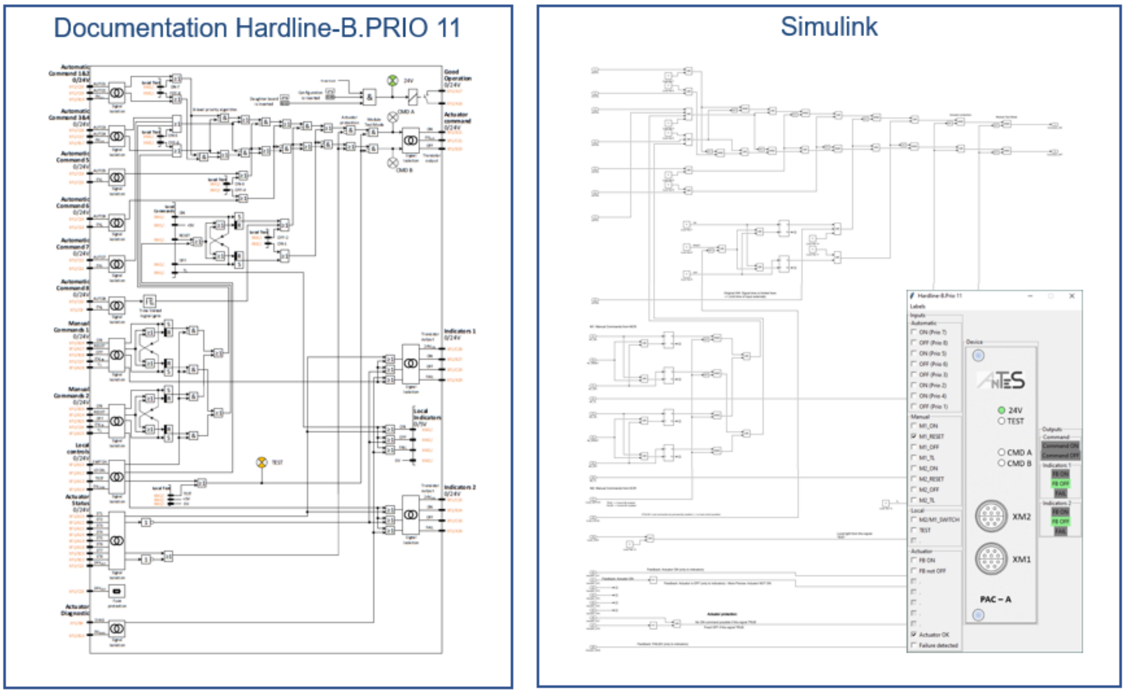


Figure 2.14 AnTeS-PAC-sim: simulated priority modules (example)

Even if the function blocks in this illustration are too small to be able to recognize details, the similar pattern of both illustrations (left side: functional representation in the documentation of the real PAC module; right side: reproduction using Simulink) makes it clear how Simulink can be used to reproduce the functionality of a real PAC module. The image embedded in the right-hand image shows software written by GRS that uses the model created with Simulink (as a DLL).

2.5 AnTeS-FIELD – Field Systems

AnTeS-FIELD includes all parts of AnTeS that can be controlled by the AnTeS I&C systems (AnTeS-SIC and AnTeS-OIC). In the simplest case, this can also just be software for exchanging signals with one of the I&C systems (Figure 2.15).

The software shown in Figure 2.15 was created by GRS and runs in the interfaces to AnTeS-SIC-real (see also Appendix A.1). Analog input signals can be generated into the AnTeS-SIC-real on the left-hand side using two sliders, and binary input signals (DI 1 to

DI 16) can be generated on the right-hand side using checkboxes. Binary signals coming from AnTeS-SIC (DO 01 to DO 16) are displayed in color (gray for a logical 0, yellow for a logical 1). A total of up to four analog and 32 binary different signals can currently be sent to AnTeS-SIC-real and 16 analog and 32 binary signals can be received from AnTeS-SIC-real via the two available SIC interfaces (note: the analog inputs of the interface are not visible in Figure 2.15).

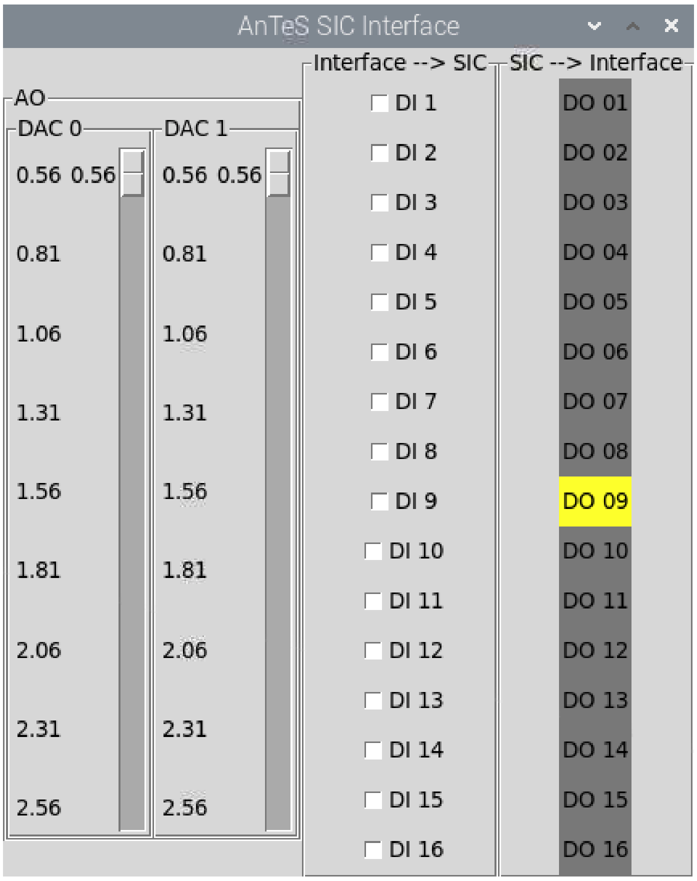


Figure 2.15 AnTeS interface software (example: SIC interface 1)

AnTeS-FIELD also includes all other parts of the human-machine interfaces that can be found at various points in AnTeS; examples of such HMIs are shown in Figure 2.16.

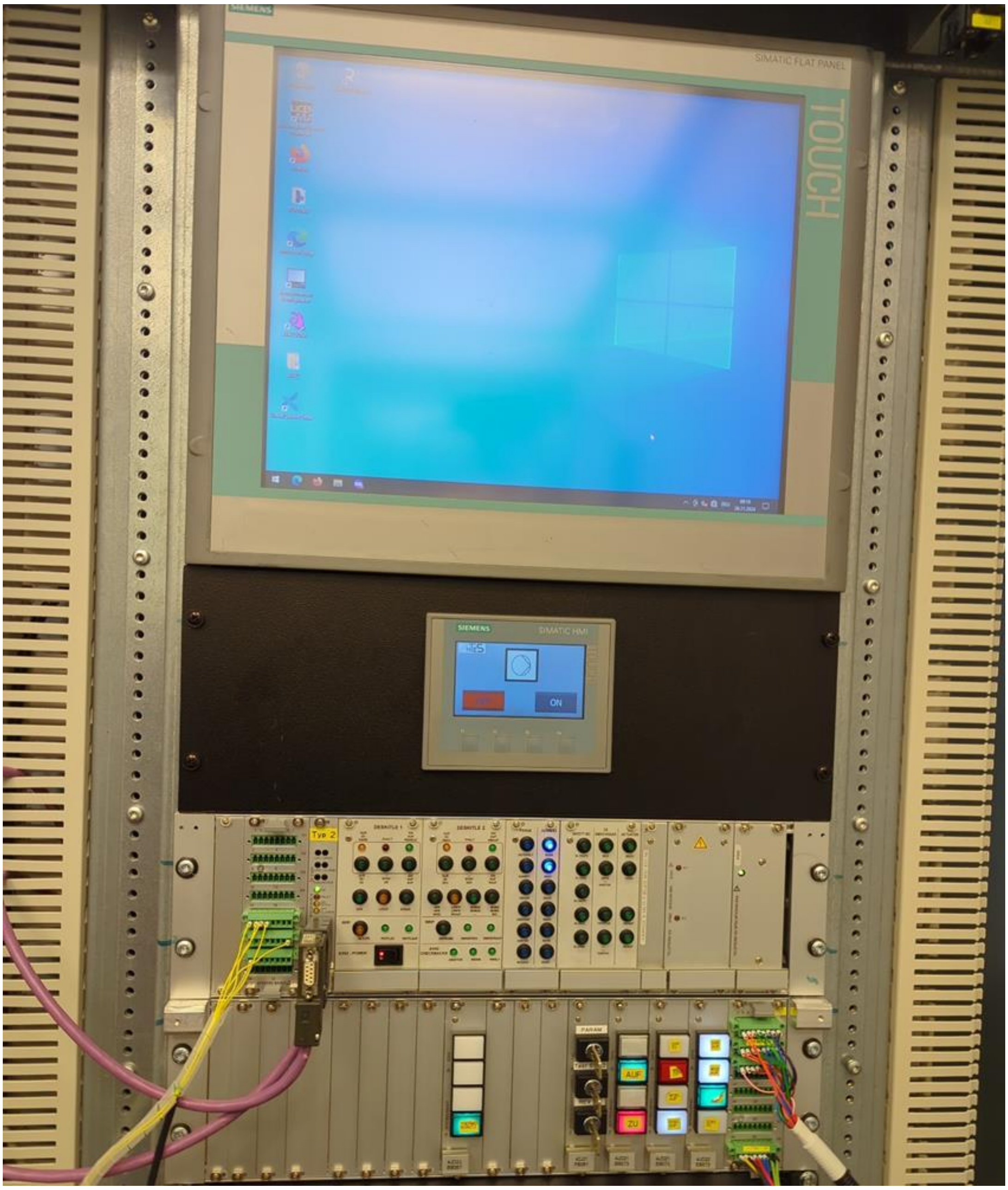


Figure 2.16 AnTeS: human-machine interfaces (HMIs)

This image shows a section of the cabinet in Figure 2.7. A touch monitor can be seen at the very top, which is connected to the industrial PC in the same cabinet and is available for the free creation of user interfaces. Directly below it is a small touch panel that can be freely programmed with the engineering environment of AnTeS-OIC (TIA Portal, Siemens) independently of the industrial PC. Below the touch panel is the AV42 subrack (see also Section 2.4), which also contains two control panels, such as those found in the main control room and the emergency control room of a nuclear power plant. This part of this subrack is therefore formally part of AnTeS-FIELD. At the bottom is another sub-rack with some control buttons, which can formally be considered part of AnTeS-FIELD, too. This subrack is used for the safe control of real drives (see below in the text).

The AnTeS-FIELD-real submodule provides real process engineering components that can be controlled by both AnTeS-SIC and AnTeS-OIC. In addition to vessels, pipes and a pump, the components of particular importance are the drives, valves and sensors qualified for use in nuclear power plants. The development of this part of AnTeS was started in an earlier GRS project under the name TeSys (for test system) /MUE 21/. Figure 2.17 provides an impression of the current status of this system, Figure 2.18 shows the corresponding switchgear.

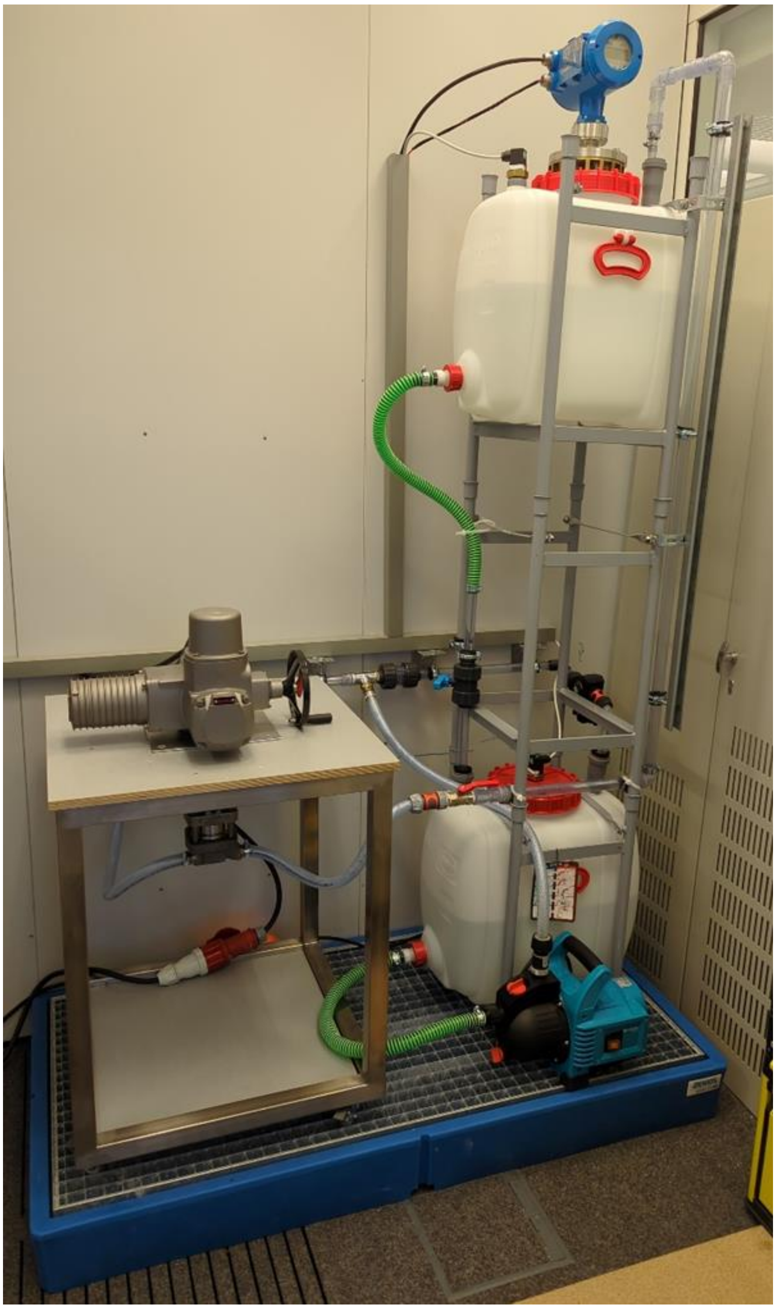


Figure 2.17 AnTeS-FIELD-real: real field components (test system TeSys)

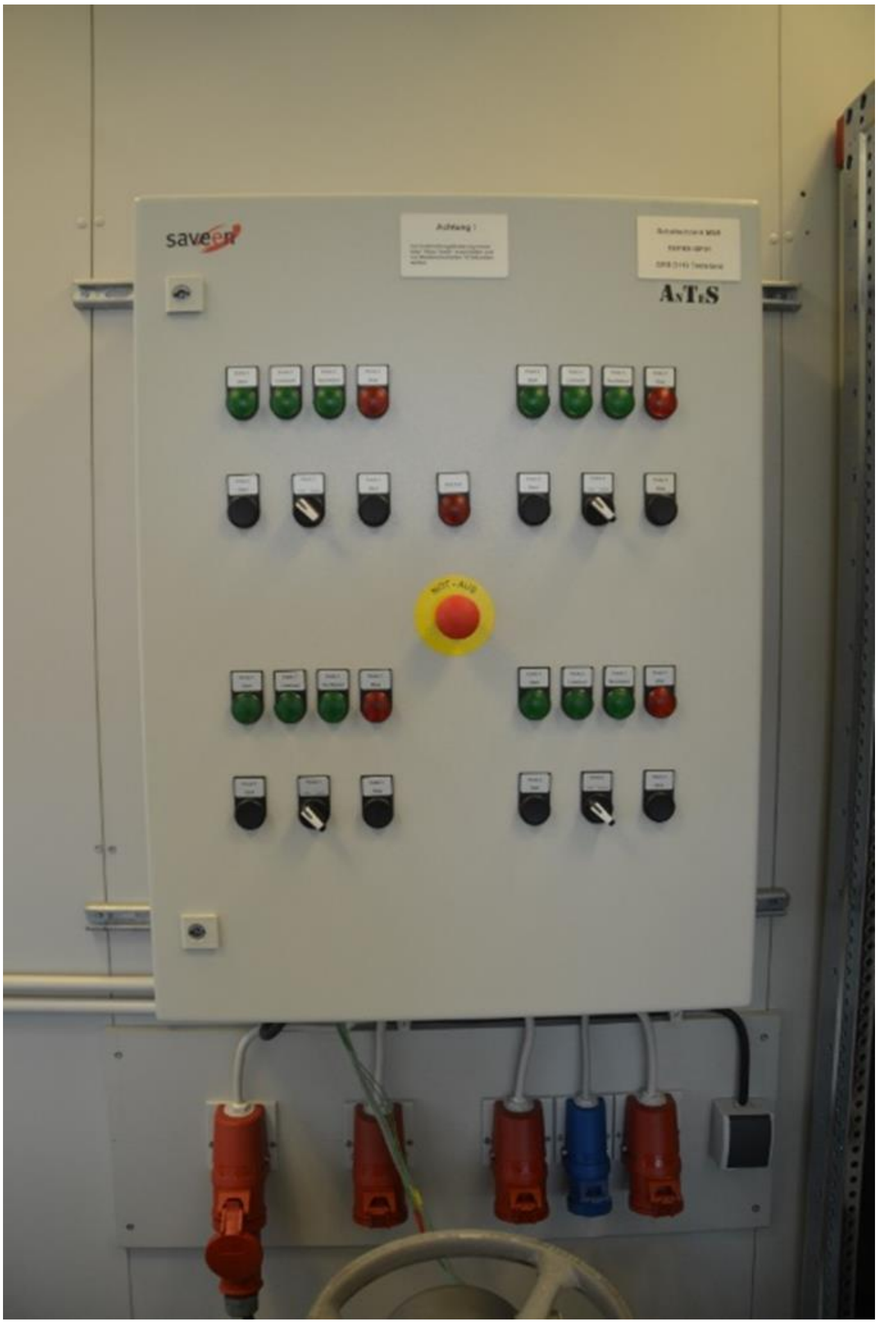


Figure 2.18 AnTeS-FIELD-real: switchgear

AnTeS-FIELD-sim provides additional simulated systems that can also be controlled by AnTeS-SIC and AnTeS-OIC. These are essentially simulations of hoisting gear (Figure 2.19) and freely configurable systems that can be created with the SimGen software (for Simulation Generator). Both options are in-house developments by GRS.

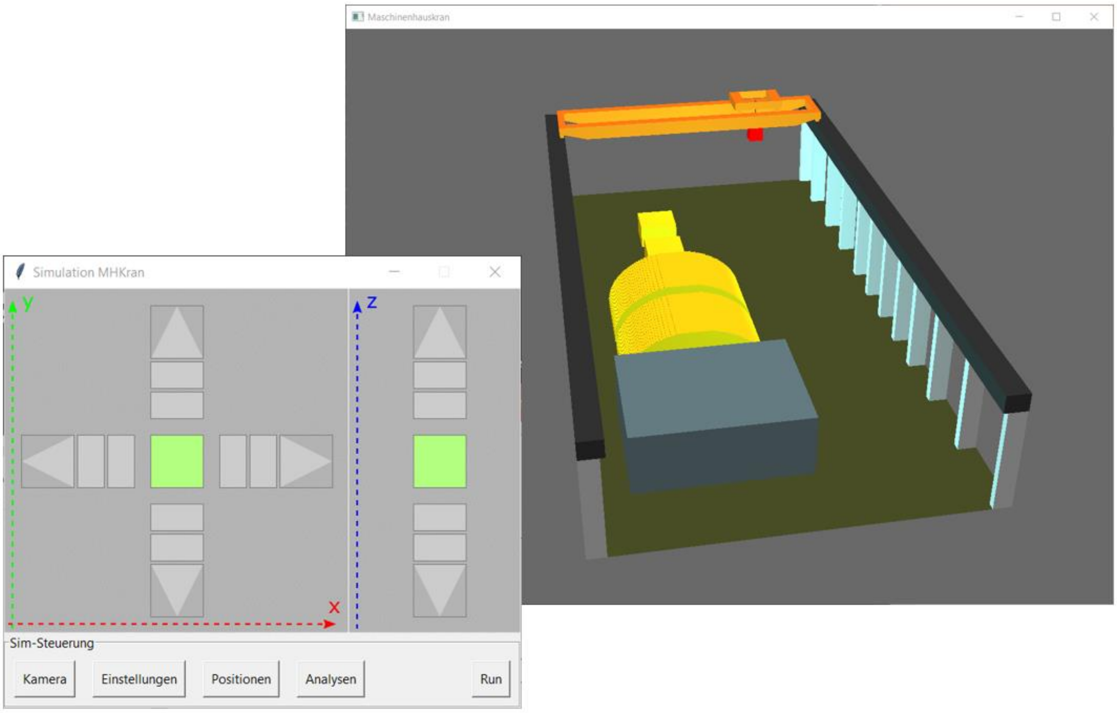


Figure 2.19 AnTeS-FIELD-sim: hoisting gear simulation

This figure shows a screenshot of the proof of concept for the simulation of hoisting gear, which was developed as part of a previous GRS project /MUE 21/. Sophisticated crane simulations are currently being developed in an ongoing GRS project /GRS 25/.

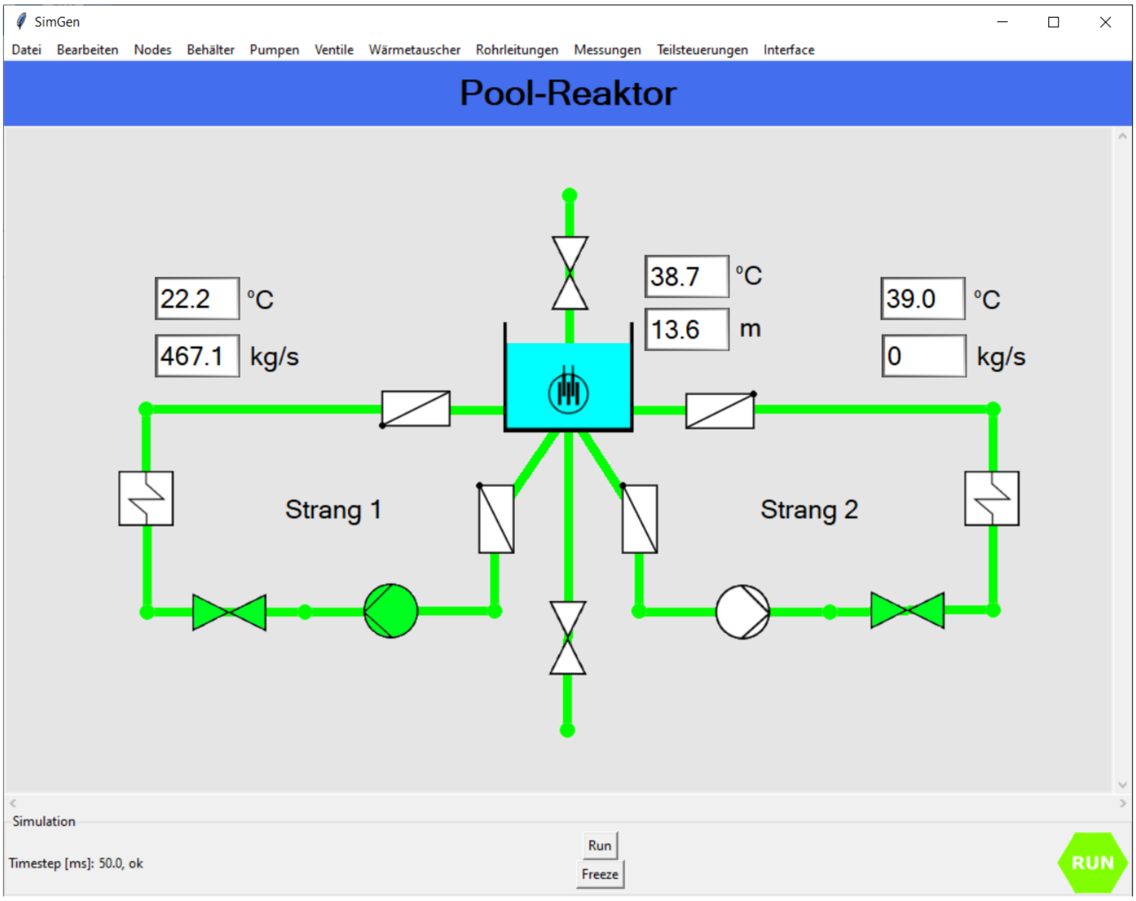


Figure 2.20 AnTeS-FIELD-sim: SimGen – simulation generator software

The software SimGen (for Simulation Generator) has been developed and tested in a previous GRS project /MUE 21/. It allows the creation (via drag and drop) and use of simulated process engineering systems with AnTeS-SIC and AnTeS-OIC. The example shown in the illustration is a pool reactor with two redundant cooling systems.

3 Model Systems

The model systems defined and used within this project were based on new research, the model systems of a previous GRS project /MUE 21/, and the reference case of the ongoing OECD DIGMORE project led by GRS /DIG 25/. These model systems were designed in such a way that effects of redundancy, functional diversity, and general diversity in particular could be analyzed within this project.

3.1 Base Case and Nomenclature

The base case for all model systems is shown in Figure 3.1. As the base case is a model system itself, it describes an I&C architecture with a SIC system and an OIC system. Both I&C systems in the base case each have no redundancies, although the SIC is divided internally into two subsystems (SIC-A and SIC-B).

The two subsystems of SIC receive diverse measurement signals from two sensors (sensor A and sensor B) whose measured physical variables differ in such a way that similar actuation signals (S_A and S_B) are generated in the subsystems on the basis of functionally diverse criteria. However, the hardware used in the two subsystems is based on the same I&C platform and uses the same hardware, which is why there is no general diversity between the two subsystems.

In both subsystems of SIC, the respective analog sensor data is read in and digitized by analog input (AI) modules of the acquisition and processing units (APUs). This digital information is then forwarded to processor modules (PM) within the APUs, where it is used to generate signals based on defined criteria (e.g., input value is greater or less than a predefined limit value). Any signals generated are then sent from the APUs to the assigned voting units (VUs) via communication link (CL) modules.

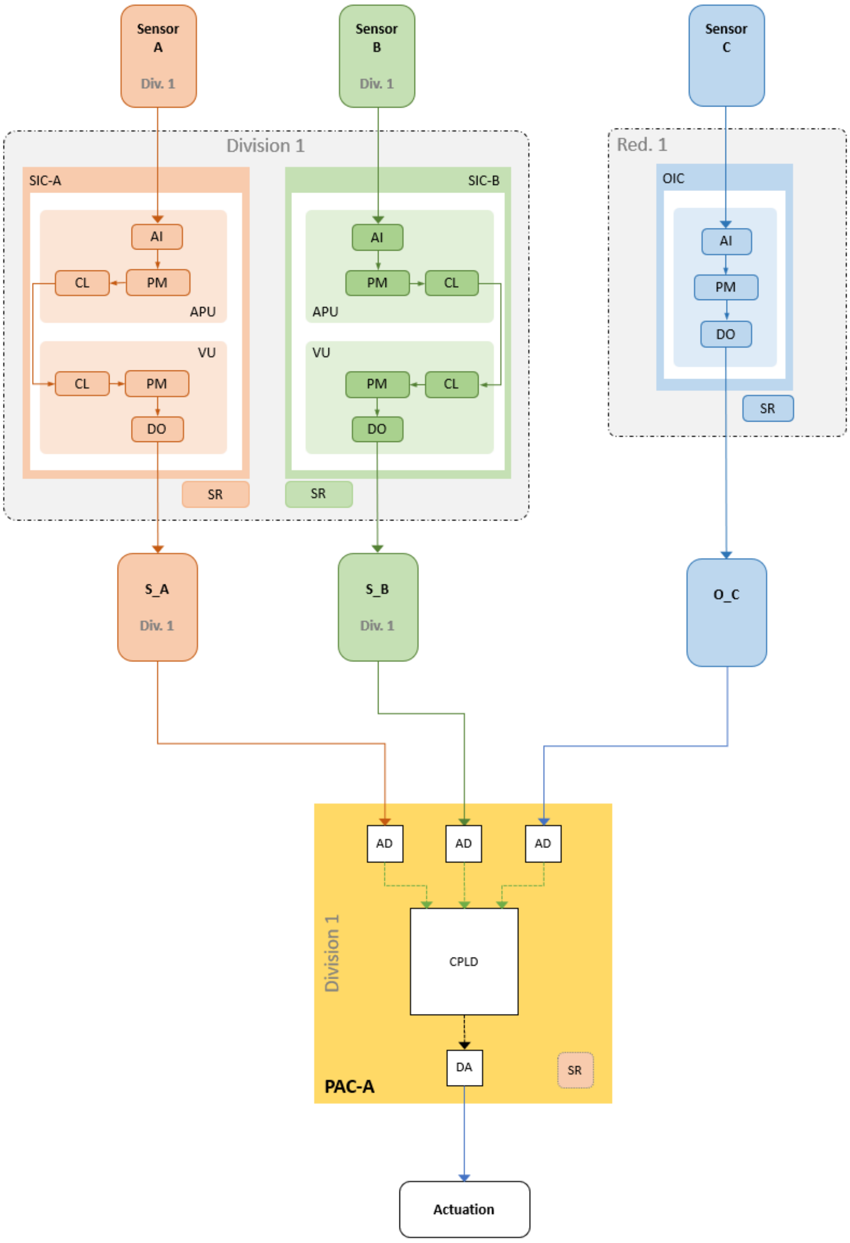


Figure 3.1 Base case architecture A1B1C1P1

The VUs receive their input signals from all assigned APUs via CL modules. The actual evaluation then takes place in the VUs' own PMs, and the signals generated there are finally output via digital output (DO)[9] modules. In the base case, the only possible input signal into each of the two subsystems comes from the only APU of the same subsystem, but in more complex configurations all signals from all APUs (of all

[9] This naming ("DO”), which is commonly used by I&C manufacturers and generally in the I&C community, is imprecise. The output signals are of course analog, but binary (e.g. 0/24 V).

redundancies/divisions) of the same subsystem. The PMs of the VUs then perform the evaluation, which is only the detection of an actuation signal (formally a 1-out-of-1 selection) in the base case. In more complex model systems, for example, 2-out-of-3 or 2-out-of-4 selections are made here for a triple or quadruple redundant subsystem.

A third diverse measurement (sensor C) is used to generate an additional, diverse actuation signal (O_C) within the OIC (formally referred to as system C within the model systems). In the OIC (system C), the analog sensor data is read in and digitized by an analog input (AI) module, afterwards forwarded to a processor module (PM). Based on defined criteria, a signal (O_C) is generated in this module (comparable to the PMs in the APUs of the SIC subsystems), which is output via the DO module of system C.

All generated signals from SIC and OIC (S_A, S_B, O_C) are sent to the subordinate prioritization and actuation control (PAC) modules. In the base case, this is a single PAC-A. In other model systems, diversified PACs (PAC-B) can also be used in addition to PAC-A. Both PAC-A and PAC-B read in all analog input signals from the I&C systems via analog-to-digital (AD) converters. Prioritization is then taken over by complex programmable logic devices (CPLDs), whose output signals are finally sent back to actuators via digital-to-analog (DA) converters.

For all individual systems of the base case and all other model systems, the respective subracks (SR) are also considered (SR failures lead to the complete unavailability of all components installed in them).

The nomenclature of the model systems directly reflects how many redundancies of the individual systems the respective model system contains. For example, the formal designation of the base case is A1B1C1P1:

- A1: there is one SIC-A subsystem in the model system
- B1: there is one SIC-B subsystem in the model system
- C1: OIC (C) is single redundant
- P1: there is one PAC in the model system

There is a further distinction in the nomenclature with regard to the PAC modules. For example, the model systems A4B0C1P4 and A4B0C1P2-2 both have a total of four SIC-A subsystems, no SIC-B subsystem, an OIC (C) system with no redundancy, and four

PAC modules. In the second case, “2-2” indicates that there are two PAC-As and two PAC-Bs, while in the first case the model system has four PAC-As.

3.2 Model Systems – Overview

In the following as complete list of the model system is given; illustrations of all model systems can be found in appendix 0:

- A1B1C1P1 (Base Case)
- A1B0C0P1
- A2B0C0P2
- A3B0C0P3
- A4B0C0P4
- A4B0C0P2-2
- A1B0C1P1
- A2B0C1P2
- A3B0C1P3
- A4B0C1P4
- A4B0C1P2-2
- A4B4C0P2-2
- A4B4C1P2-2

The model system A4B0C1P2-2 is considered in more detail here as a representative example (Figure 3.2). As explained in Section 3.1 on nomenclature, the composition of the model system can be interpreted as follows:

- A4: there are four redundant subsystems SIC-A[10]
- B0: there is no subsystem SIC-B

[10] This means that SIC-A is present in all four divisions.

- C1: the OIC (C) serves as a backup[11] and has no redundancy
- P2-2: the model system comprises four PAC modules, two of type PAC-A and two of type PAC-B (these are diverse to each other)

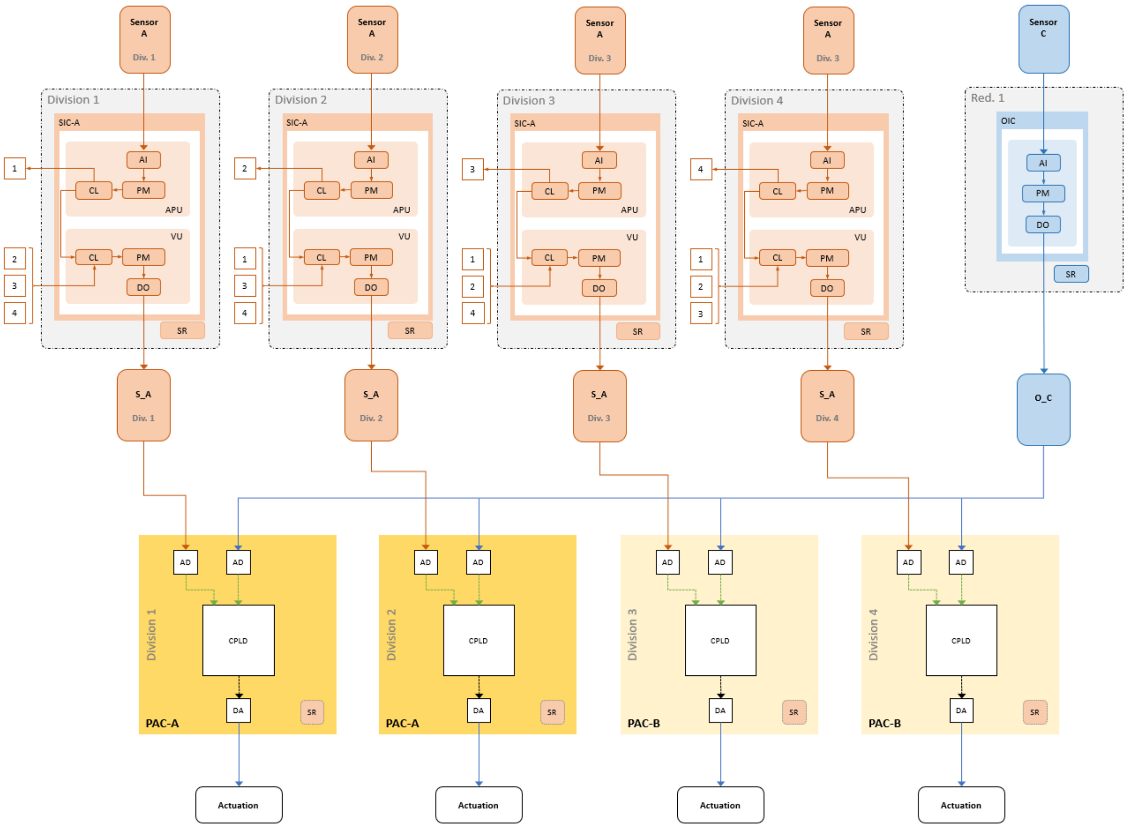


Figure 3.2 Model system A4B0C1P2-2

Each division of SIC-A has its own sensor A, whose signals are read in by AI modules in each division within the respective APU. These signals are then evaluated within a PM by comparing them with a defined limit value. The output signals of the PMs are sent to all VUs of SIC-A via CL modules. For example, the CL module of the APU of SIC-A in division 1 sends its output signal not only to the VU of the same division (direct arrow connection), but also to all VUs of the other divisions (indicated by the connectors (boxes with numbers)). The signals received via the CL module in each VU are then subjected to an 2oo4 (2-out-of-4) evaluation by the PM (of the respective VU) and corresponding

[11] In this case, since the OIC (C) controls the same components of the actuated system and performs the same I&C functions as the SIC-A subsystem, the operational I&C can be regarded as a diverse backup system.

signals are generated in turn. These are converted back into binary output signals by the DO[12] modules and forwarded to a separate PAC module within each division.

Signal generation by the OIC (C) works in the same way in principle. However, due to the fact that the OIC has no redundancy, the signals generated in the PM of the OIC are sent directly to all PAC modules via a DO module.

Each of the four PAC modules therefore receives its own input signal from the SIC-A of the same division. In addition, all PAC modules receive the same input signal from the OIC. In each PAC module, the input signals are read in via ADs (analogue-to-digital converters) and forwarded to a CPLD (complex programmable logic device), where the actual prioritization takes place. Actuation signals generated are finally output by the PAC modules via DAs (digital-to-analog converters).

In a real application, the output signals of the individual PAC modules would each control components (e.g., valves) of a (process engineering) safety system assigned to the same division. This means that each actuation signal in Figure 3.2 would control individual components. As the focus of this project is exclusively on the I&C and the actuated systems were not explicitly considered, this was replaced by success criteria. For this model system, for example, two out of four (2oo4) existing actuation signals to the controlled system are necessary for the overall actuation to be considered successful.

3.3 Failure Modes and Reliability Data

The reliability characteristics used in this project are mainly based on the corresponding data from the DIGMORE /DIG 25/ and DIGMAP /DIG 24/ projects (where the corresponding values were agreed with several international experts), but these were adapted to the needs within this project. The aim was to use reliability data as close to reality as reasonably possible for the (generic) model systems. However, these characteristics are only intended to be plausible in terms of order of magnitude and should therefore not be adopted uncritically for real applications.

[12] See footnote 9 on page 31!

Failures within this project were considered at module level (e.g., processor modules PMs). The failure modes (column "Description") and failure rates (column "FR") are shown in the following tables (3.1 to 3.3). For example, failures to "low" were assumed for all sensors, since (without limiting the generality) all limit values were assumed to be maximum limit values.

Common-cause failures (CCF) were considered in this project by means of separate basic events, each with a failure rate corresponding to 5% of the individual failure rates (which formally corresponds to the use of a beta factor model with a beta factor of 0.05 in FTA).

Table 3.1 Reliability data SIC

ID	Component	Description	FR	FR CCF
X_Sensor_A_Low	Division X Sensor A	Failure to low	1.8E-07 /h	9.0E-09 /h β = 0.05
X_Sensor_B_Low	Division X Sensor B	Failure to low	1.8E-07 /h	9.0E-09 /h β = 0.05
XY_APU_AI	Division X SIC-Y (Y=A/B) APU AI	Failure to 0	4.0E-07 /h	2.0E-08 /h β = 0.05
XY_APU_PM	Division X SIC-Y APU PM	Failure to 0 Includes failures of CL	3.0E-07 /h	1.5E-08 /h β = 0.05
XY_VU_PM	Division X SIC-Y VU PM	Failure to 0 Includes failures of CL	3.0E-07 /h	1.5E-08 /h β = 0.05
XY_VU_DO	Division X SIC-Y VU DO	Failure to 0 Includes failures of SR	4.0E-07 /h	2.0E-08 /h β = 0.05

All failures, which have been quantitatively considered for the individual modules of the model systems, are assumed to be detected (exclusively) by recurring tests (regular checks for PRPS, DRPS and PAC every six months and for HWBS every twelve months), which are then repaired within eight hours.

Table 3.2 Reliability data OIC

ID	Component	Description	FR	FR CCF
1_Sensor_C_Low	Red. 1 Sensor C	Failure to low	1.8E-06 /h	None
1O_AI	Red. 1 OIC AI	Failure to 0	1.2E-06 /h	None
1O_PM	Red. 1 OIC PM	Failure to 0	9.0E-07 /h	None
1O_DO	Red. 1 OIC DO	Failure to 0	2.0E-07 /h	None
1O_SR	Red. 1 OIC SR	Failure to low	1.8E-07 /h	None

.

Table 3.3 Reliability data PAC

ID	Component	Description	FR	FR CCF
XPY_AD	Division X PAC-Y (Y=A/B) AD	Failure to 0	4.0E-07 /h	2.0E-08 /h β = 0.05
XPY_CPLD	Division X PAC-Y CPLD	Failure to 0	2.0E-07 /h	1.0E-08 /h β = 0.05
XPY_DA	Division X PAC-Y DA	Failure to 0	4.0E-07 /h	2.0E-08 /h β = 0.05
XPY_SR	Division X PAC-Y SR	Failure to 0	2.0E-07 /h	1.0E-08 /h β = 0.05

Two special aspects are explicitly noted at this point: Firstly, no failures were explicitly considered for the subracks (SRs) of the SIC, as all failures here have been regarded as self-reporting and these are repaired immediately (i.e., have no relevance compared to undetected failures, in particular CCFs). On the other hand, the OIC has no redundancies in any of the model systems under consideration, which is why only individual failures must be considered for it (which is why no CCF parameters are specified in Table 3.2).

4 Validation

The first section of this chapter first provides an insight into the methodology and methods used by GRS to analyze I&C architectures and systems. Subsequently, Sections 4.2 and 4.3 show how the simulations of the SIC and the OIC of the model systems in particular were validated using AnTeS-SIC-real and AnTeS-OIC-real. Section 4.4 then shows how a real PAC (AV42), the generic PAC of GRS, and a simulated PAC were cross-checked with each other for validation. Finally, Section 4.5 is devoted to the representative comparison of a model system (base case) in fault tree analyses and Monte Carlo simulations.

4.1 Methodology and Methods

The approach to analyzing I&C architectures and systems at GRS, which has been expanded and applied afterwards to model systems as part of this project, stipulates that both qualitative and quantitative results are always obtained using at least two different methods and tools wherever possible. This safeguards the results of the analyses, particularly against user errors. AnTeS-SIC-real and AnTeS-OIC-real also have the task of ensuring that the observations in the analyses not only contain no user errors, but that the modeling (e.g., of the simulated model systems within AnTeS, or modelled by fault trees) correctly reflect the real behavior of real components. The fundamental approach used within this project can be explained using Figure 4.1.

A system described through text and images (“System / Architecture under Analysis”) is recreated functionally, both with real and simulated components (“AnTeS Real” and “AnTeS Simulated”). In both implementations, defined failures can be activated or deactivated (fault injection). By automatically configuring all conceivable failure combinations (via fault injection) and recording the overall system state in each case, a tabular listing of all possible system states is generated, with an evaluation of whether the state is to be considered a total failure or not (“FMEA+”).

The same result can also be achieved through a manual execution, i.e., by creating and populating the table in “FMEA+” in the figure manually by an expert based on the system description. All three approaches (“AnTeS Real” “AnTeS Simulated”, or manual creation) cross-verify each other since the same result (i.e., the same table) is obtained through any of the three methods (assuming error-free execution).

However, the analysis steps described so far only provide qualitative results and do not, for instance, indicate how likely an unfavorable state might be. To obtain these quantitative results, two different methods are available, which also cross-verify each other. These methods are fault tree analyses (“FTA”) and Monte Carlo (“MC”) simulations using simulated I&C systems. In addition to quantitative results, these two methods can also provide qualitative results. As indicated by the upper “Cross-Check” arrow in the figure, the so-called minimal cut sets (MCS)[13], obtained from the FTA, can be compared with the results of the FMEA+ analysis. This cross-verification helps to validate both the logical structure of the fault trees and the correctness of the underlying models.

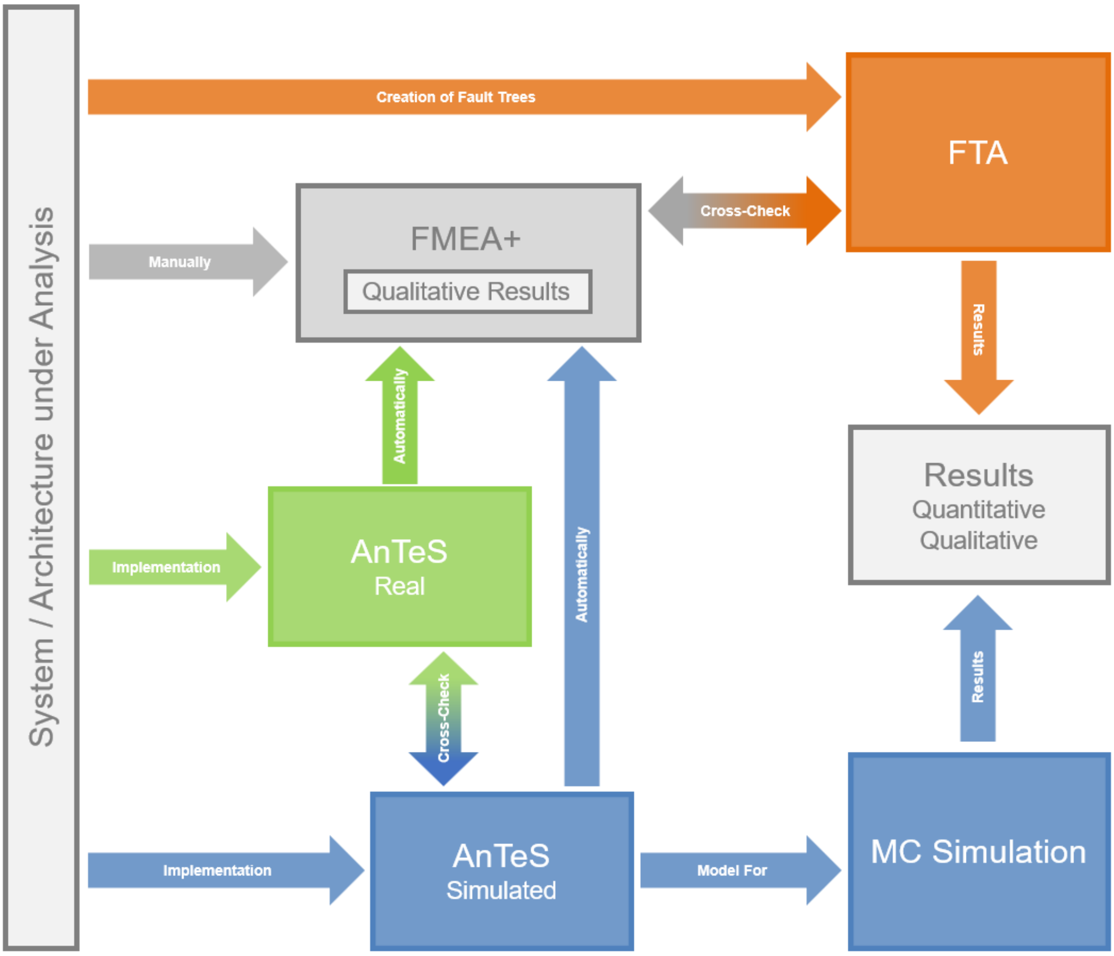


Figure 4.1 AnTeS methods and tools, and their interaction

[13] Minimal cut sets are the smallest combinations of basic events in a fault tree analysis that, if they all occur, would lead to the failure of the top event (system-level failure). Each minimal cut set represents a potential pathway to failure, and their identification is critical in assessing system reliability and identifying vulnerabilities.

Overall, the GRS methodology provides both qualitative and quantitative results, each derived from three or two different methods, respectively. This duplication makes implementation errors very unlikely (although errors, e.g., in the system description or its interpretation, cannot be ruled out).

More details of the GRS methodological approach can be found in /MUE 23/ and /MUE 24/.

4.2 AnTeS-SIC – Safety I&C

Figure 4.2 shows a single-division OIC model as described for the base case, for example (see Section 3.1).

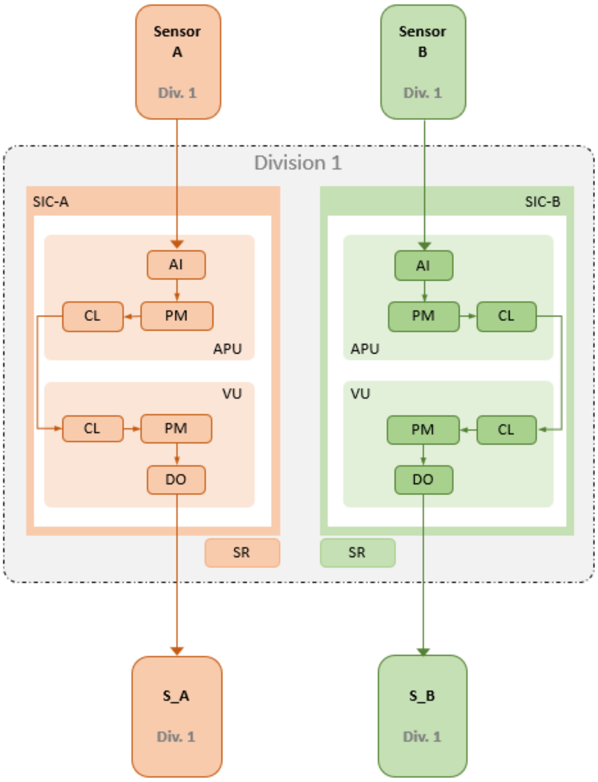


Figure 4.2 SIC (original naming of model systems)

APU – Acquisition and Processing Unit
AI – Analog In (Module)
CL – Communication Link (Module)
DO – Digital Out (Module) (binary output)
PM – Processor Module
SR – Subrack

If one changes the designations such as they are used for AnTeS-SIC-real (i.e., TXS) instead, the same system looks like in Figure 4.3.

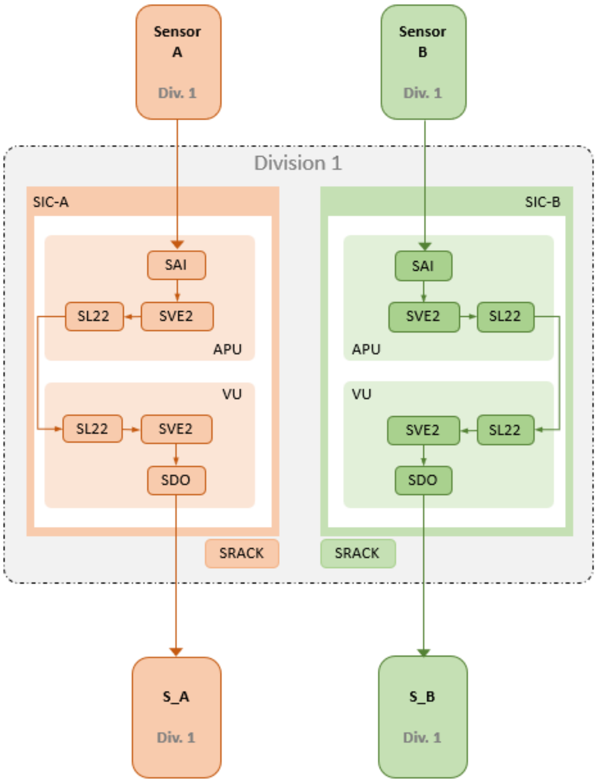


Figure 4.3 SIC (modules named as for TXS)

The implementation of this system with the real I&C components of AnTeS-SIC-real is straightforward. Figure 4.4 shows a screenshot of a network diagram in the SPACE engineering environment of TXS. In this image, the modules and connections have also been color-coded as in Figure 4.3, and the names have been added again in separate boxes.

The implemented I&C functions are kept simple and correspond to the descriptions for the model systems in Chapter 3. Essentially, the sensor data read into the PM of an APU is compared with a limit value and its output is forwarded to the respective VU.

In this simplified case, additional VUs in the subsystems (SIC-A and SIC-B) are basically superfluous but have been retained here to ensure similarity with the model systems. Accordingly, in this simple SIC model, only a 1-out-of-1 selection takes place in the PMs of the VUs.

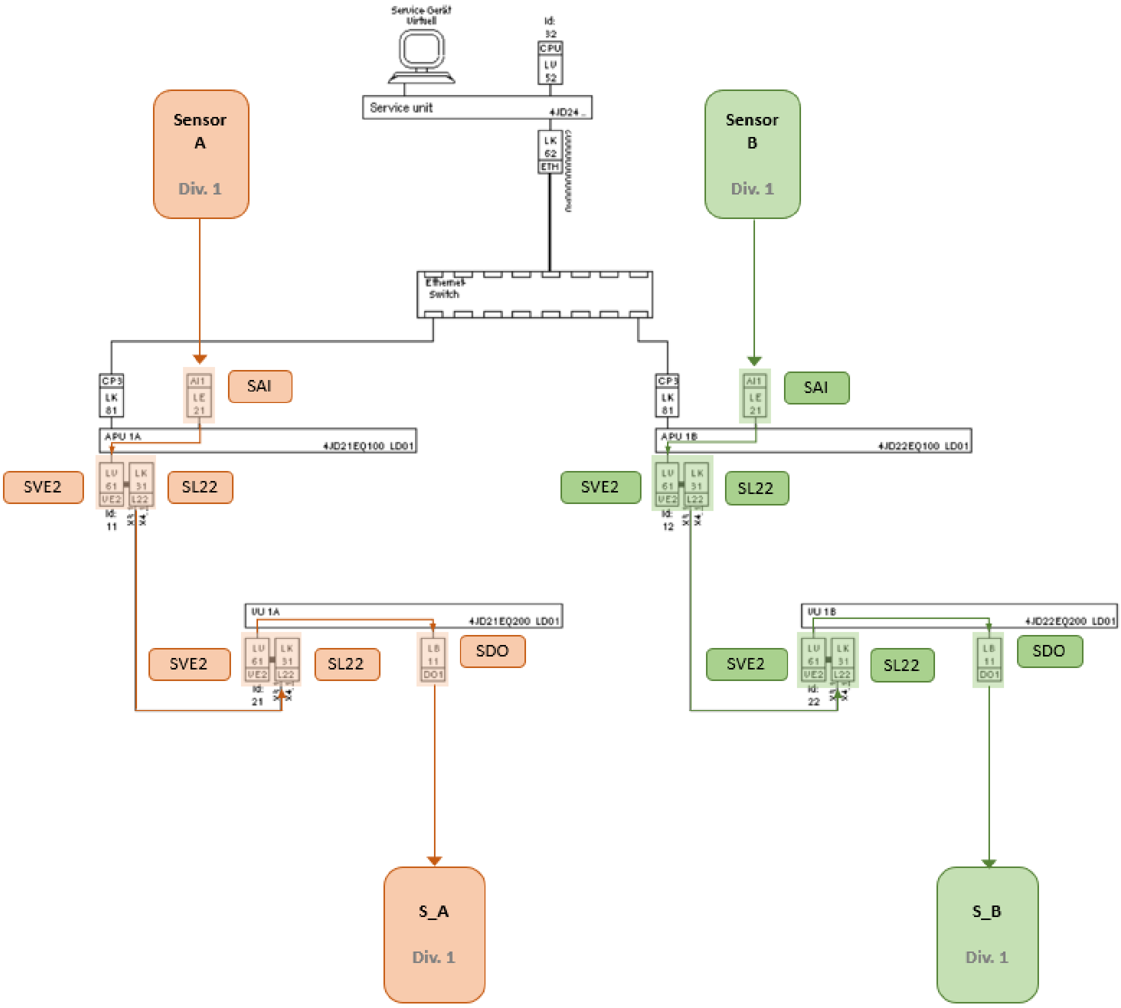


Figure 4.4 SIC (AnTeS, real SIC, network plan), colored boxes and arrows added

Additional functions were also implemented directly in the real I&C, which are used exclusively for fault injection. This is shown as an example for the AI module of SIC-B in Figure 4.5. The upper section shows the undisturbed (i.e., error-free) state. In this state, the green signal[14] ("1") coming from above is forwarded by a switch function block ("#") to the bottom right. If the signal "FI SIC-B APU AI"[15] is set (lower section), the switch function block forwards a fixed "0" instead of the correct signal.

[14] In the live visualization of SPACE, logical signal values are displayed as colors. A blue line stands for a logical 0, a green line for a logical 1.

[15] "FI SIC-B APU AI" – Fault Injection into the AI module of the APU of SIC-B

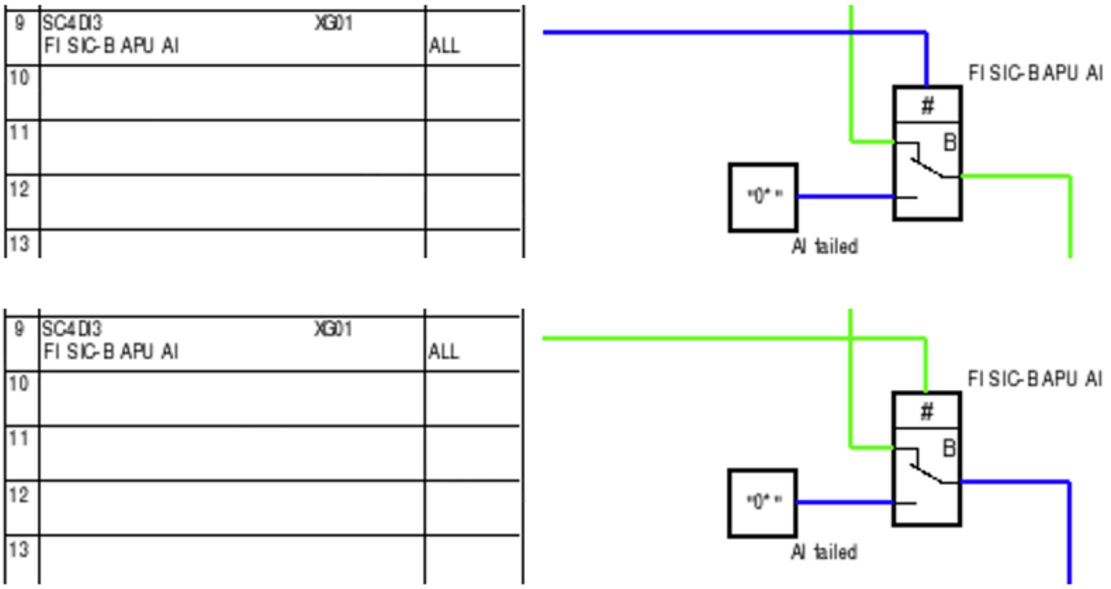


Figure 4.5 AnTeS-SIC-real: fault injection (example)

This means that the SIC system originally defined in Figure 4.2, including fault injection, has been completely set up using the existing real components of AnTeS-SIC-real.

In addition to this implementation with real components, the SIC model was also implemented as a simulation model using the Matlab/Simulink software within the AnTeS-SIC-sim module (Figure 4.6).

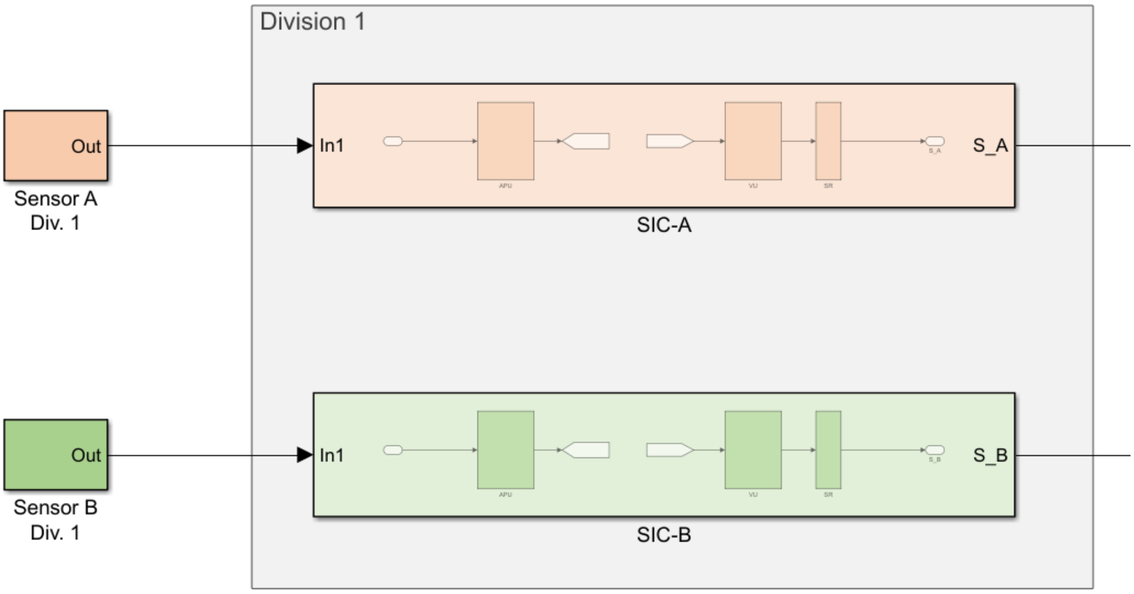


Figure 4.6 AnTeS-SIC-sim: SIC-A and SIC-B (of base case)

Within the graphical user interface of Simulink, the two subsystems SIC-A and SIC-B, or rather their APUs and VUs, can be examined in more detail, as shown in Figure 4.7 for the APU of SIC-A as an example. Like the real system, this APU contains an AI module, a PM, and a CL module.

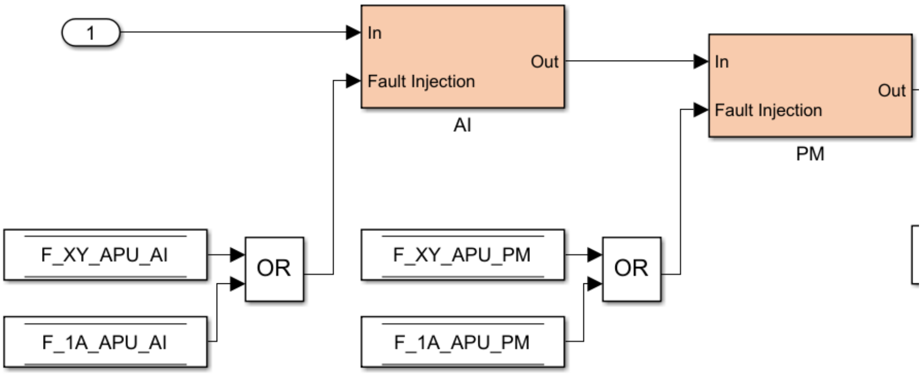


Figure 4.7 AnTeS-SIC-sim: fault injection (example: AI and PM of APU of SIC-A)

This figure also shows how fault injection in the individual modules (e.g., the AI module) of AnTeS-SIC-sim takes place. Special memory blocks within Simulink are used for this purpose, whose current values are routed from the memory blocks to the modules (AI, PM, CL in the lower area of the figure in this example). The values in the memory blocks can be changed externally for fault injection during the runtime of the simulation. Within the simulated modules (here: AI, PM, CL), whose internal structure is modeled in the colored function blocks, the possibly disturbed signals are used to switch to faulty signal values if necessary (just as in the example of fault injection into real components in Figure 4.5).

For both SIC-A and SIC-B eight possible single failures and all combinations of these failures had to be considered when validating the simulation models (AnTeS-SIC-sim) with the real components (AnTeS-SIC-real), as shown in Table 4.1.

Table 4.1 Comparison fault injection results for real and simulated SIC-A, excerpt

#	Fault Injection (FI) SIC-A								Output (Actuation)	
	Sensor A	APU			VU			SR	Real	Sim
		AI	PM	CL	CL	PM	DO			
1	0	0	0	0	0	0	0	0	1	1
2	0	0	0	0	0	0	0	1	0	0
3	0	0	0	0	0	0	1	0	0	0
…	…	…	…	…	…	…	…	…	…	…
254	1	1	1	1	1	1	0	1	0	0
255	1	1	1	1	1	1	1	0	0	0
256	1	1	1	1	1	1	1	1	0	0

The table shown can also be transferred 1:1 to SIC-B, as both systems are structured in the same way (see Figure 4.6).

This table contains all 256 possible fault combinations for the subsystem SIC-A (combinations of failures of the sensor, the modules AI, PM, CL of the APU as well as CL, PM, DO of the VU, and failures of the SR). All these combinations were tested automatically with both the real and the simulated system in order to perform an FMEA+ analysis (see Section 4.1). The last two columns of the table indicate which output signal was recorded for the real and the simulated system during this procedure, these match for each individual combination. The real system and the simulated system therefore behave in exactly the same way.

Since all combinations of failures in Table 4.1 except the combination in the first line lead to non-actuation for the real and the simulated systems, FMEA+ results are only of limited use here. However, the same simulation models (AnTeS-SIC-sim) were also used in Monte Carlo simulations for further validation (see Section 4.5).

4.3 AnTeS-OIC – Operational I&C

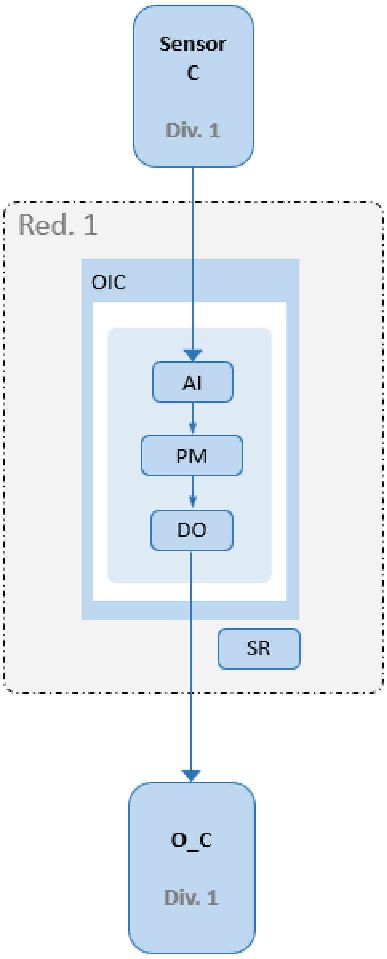


Figure 4.8 OIC (original naming)

The validation of the simulated OIC system (AnTeS-OIC-sim) using the real OIC system (AnTeS-OIC-real) was carried out in exactly the same way as the validation of the SIC system in the previous Section 4.2. Accordingly, Figure 4.8 shows the OIC model system under consideration with the names already used in the description of the model systems (see Section 3.1).

If the names of the modules are translated into the “language” of Simatic S7 (Figure 4.9), this model can also be transferred to the real hardware of AnTeS-OIC-real (Figure 4.10).

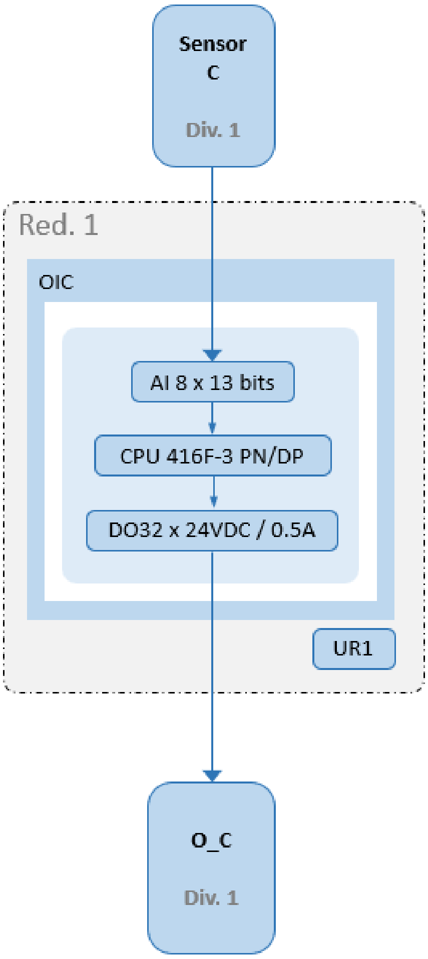


Figure 4.9 OIC (module named as for Simatic S7)

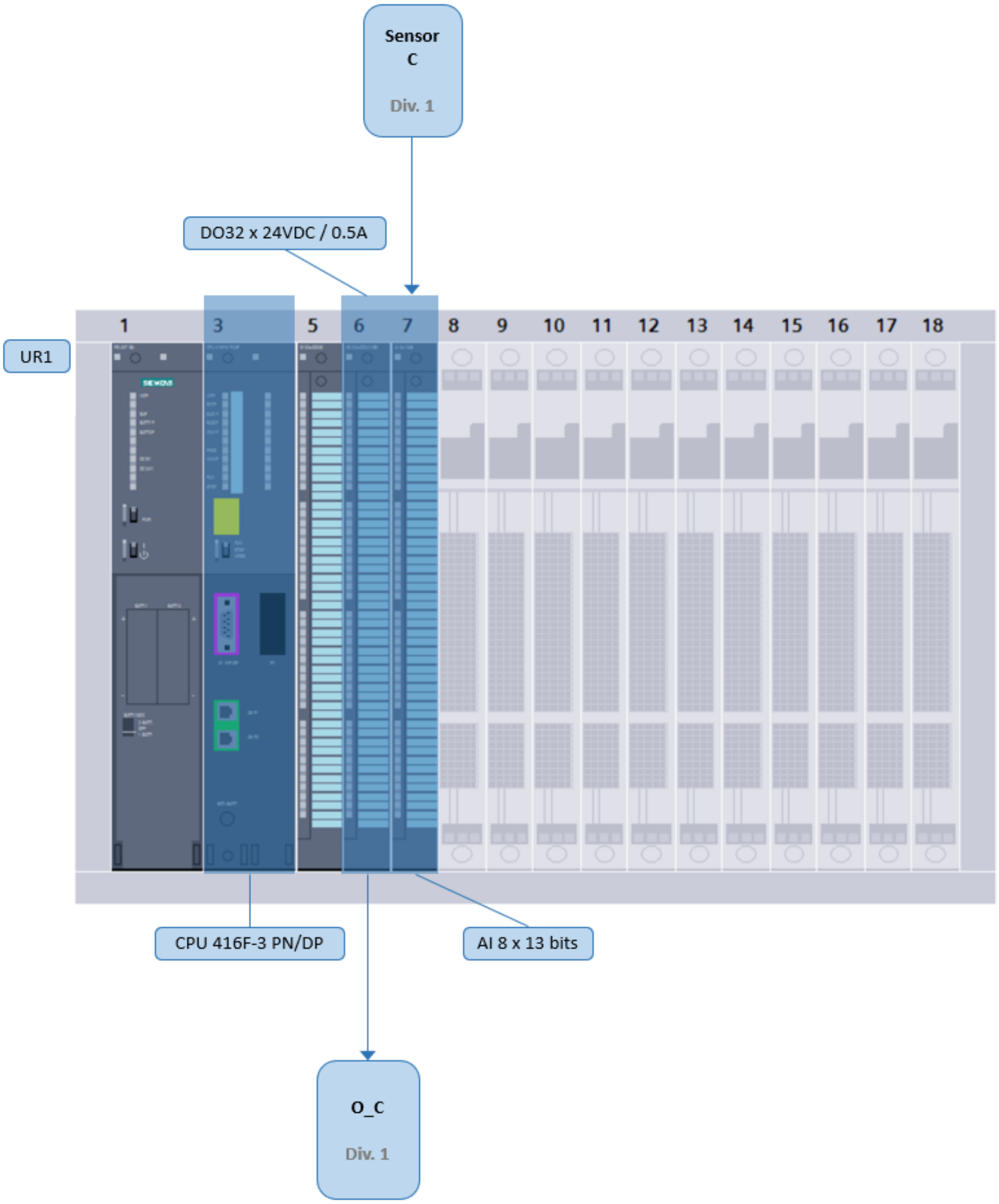


Figure 4.10 OIC (AnTeS, real OIC, device configuration), colored boxes and arrows added

The translation of the real system into a simulated system also corresponds in principle to the previously described procedure for AnTeS-SIC-sim; the simulation model for the OIC model in Figure 4.8 created with the Matlab/Simulink software is shown in Figure 4.12.

Fault injection into AnTeS-OIC-real (Figure 4.11) and AnTeS-OIC-sim (Figure 4.13) works in exactly the same way here as for AnTeS-SIC, except that the additional functions required to adapt to the engineering environment of AnTeS-OIC-real (TIA Portal) slightly changes the appearance like in Figure 4.11, since it is possible to define custom function blocks in the engineering environment of AnTeS-OIC-real.

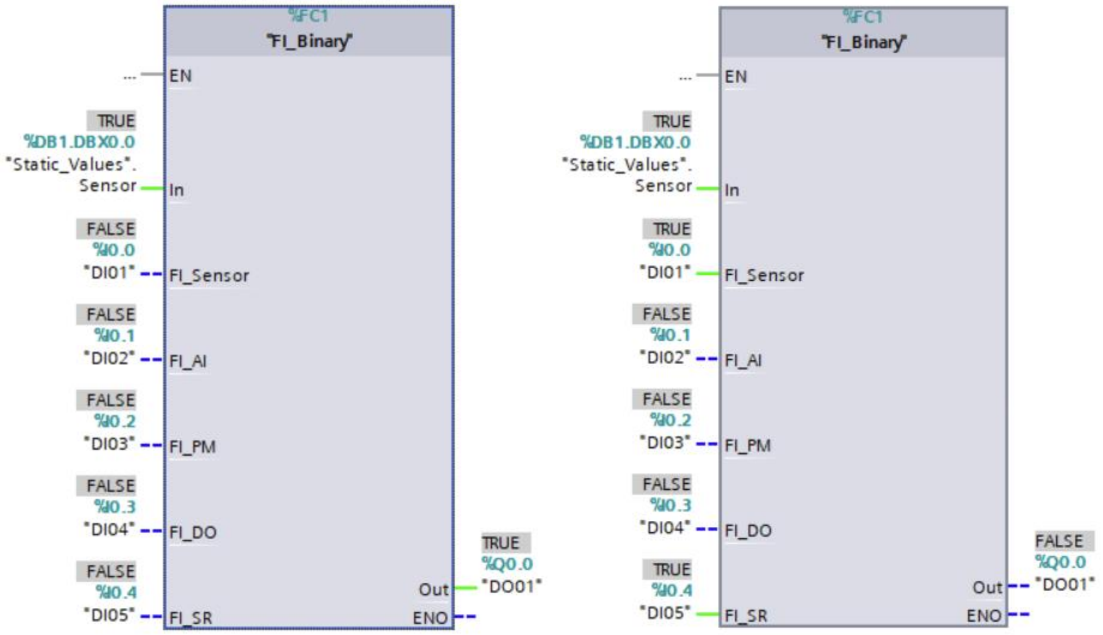


Figure 4.11 AnTeS-OIC-real: fault injection (example)

In the example shown here the output signal DO01 in the right-hand section has changed from “1” (green) to “0” (blue), as in contrast to the left-hand section two fault injection signals are active here (FI_Sensor and FI_SR).

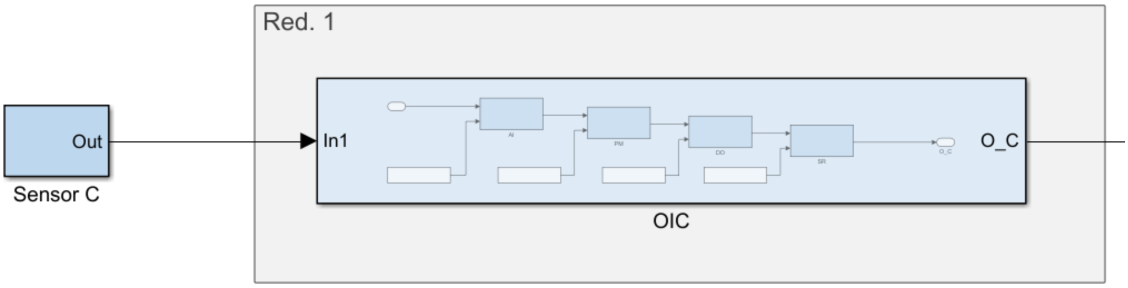


Figure 4.12 AnTeS-OIC-sim: OIC

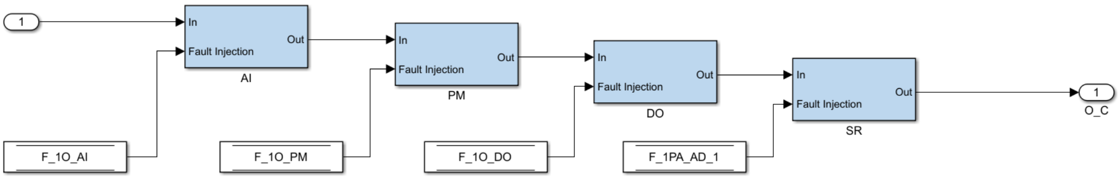


Figure 4.13 AnTeS-OIC-sim: fault injection (example)

Just as for the SIC system in the previous section, all fault combinations for the OIC system were automatically tested with both the real (AnTeS-OIC-real) and the simulated I&C system (AnTeS-OIC-sim), and the output signals were recorded (Table 4.2). The behavior of the real system matches that of the simulated system, although the same limitations apply here as for AnTeS-SIC (see previous section).

Table 4.2 Comparison fault injection results for real and simulated OIC, excerpt

#	Fault Injection (FI) OIC					Output (Actuation)	
	Sensor C	**AI**	**PM**	**DO**	**SR**	**Real**	**Sim**
1	0	0	0	0	0	1	1
2	0	0	0	0	1	0	0
3	0	0	0	1	0	0	0
…	…	…	…	…	…	…	…
30	1	1	1	0	1	0	0
31	1	1	1	1	0	0	0
32	1	1	1	1	1	0	0

Further important validation steps were therefore also carried out for the OIC system as part of the analysis of the base case (see Section 4.5).

4.4 AnTeS-PAC - Prioritization and Actuation Control

Figure 4.14 shows the basic structure of PAC-A[16] modules as defined for the model systems (see Chapter 3). In contrast to SIC and OIC systems, PAC modules are not subracks with plug-in cards, but plug-in cards themselves. This means that the individual “modules” (AD, CPLD, DA) within the commercial real PAC modules available at GRS are not accessible directly (e.g., for fault injection). For this reason, not only simulated PAC modules were created in AnTeS-PAC-sim, but also an additional generic PAC module in AnTeS-PAC-real.

[16] Even if PAC-B modules are formally assumed to be diverse from these modules within the model systems, these PAC-B modules are nevertheless structured in the same way. All explanations in this section therefore also apply to PAC-B modules.

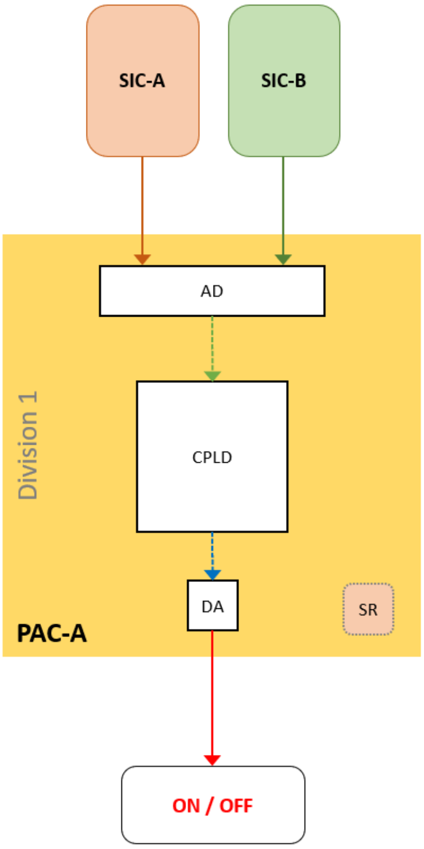


Figure 4.14 PAC (original naming)

As can be seen in Figure 4.15, the PAC modules of the model systems largely correspond to the basic structure of AV42 modules of AnTeS-PAC-real, as long as the additional processor available in AV42 modules is not used[17], for example.

In total, up to four pairs of ON and OFF signals from different sources (e.g., I&C systems or manual control panels in control rooms) can be read into AV42 modules via analog-to-digital converters (ADs). Based on the prioritization within the CPLDs, ON or OFF signals (e.g., for actuators) are then output via digital-to-analog converters (DAs).

[17] Note: The processor of an AV42 can be switched off by parameterization. However, the processor plays no role for the (in particular temporal) behavior of the PAC module at this point, as prioritization is carried out solely by the CPLD and no input signals through the processor were used in the tests described here.

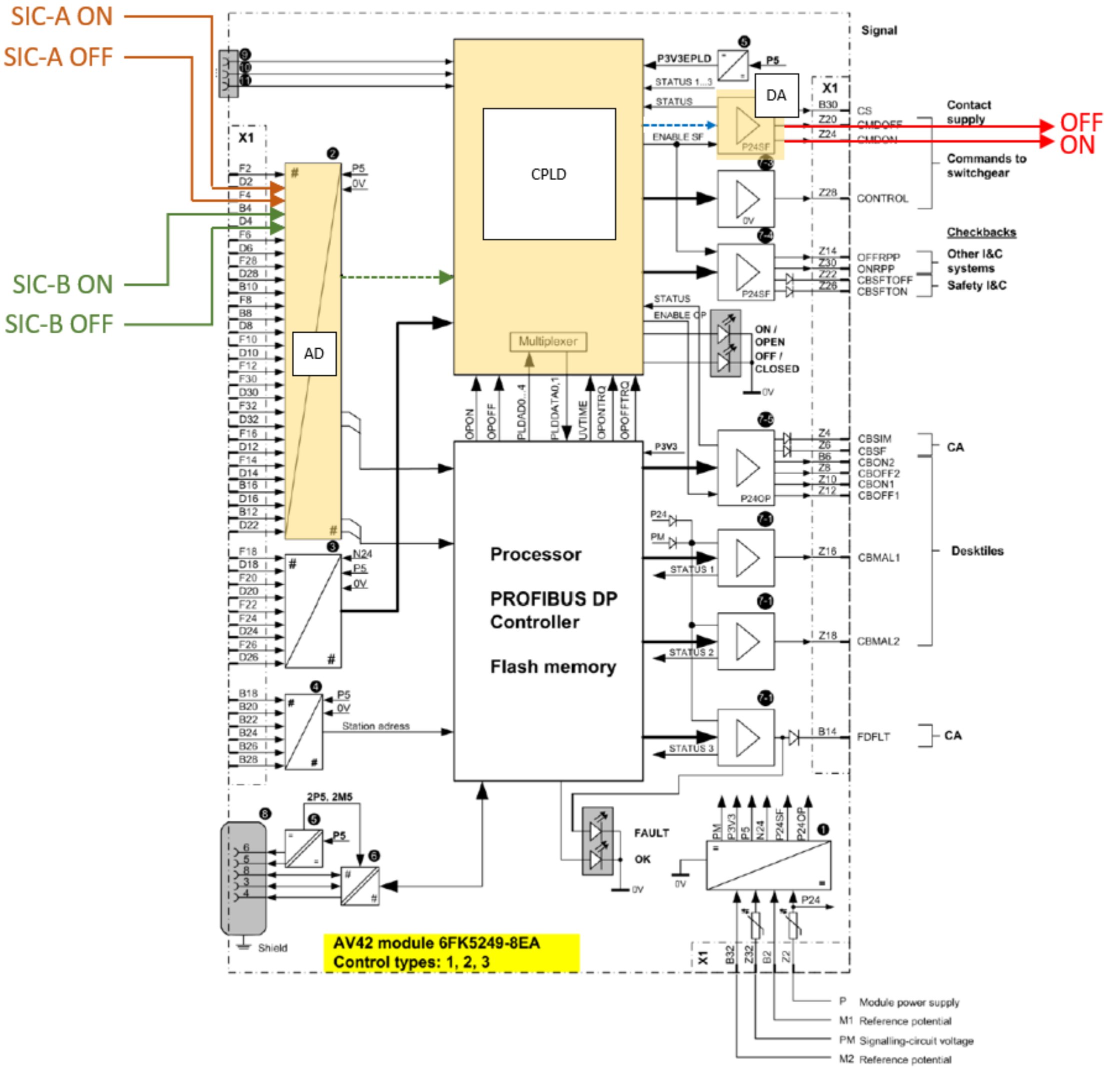
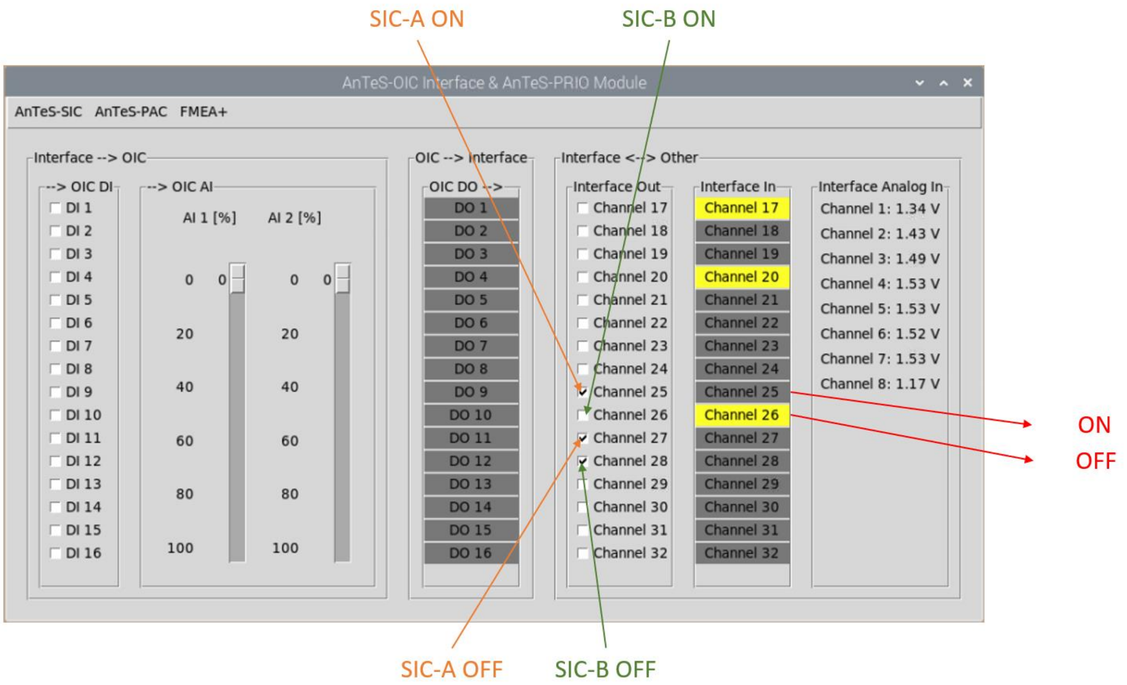


Figure 4.15 AnTeS-PAC-real: AV42, schematic

This schematic image was taken from /ARE 17/. However, additional boxes with the designations AD, CPLD and DA have been added to the illustration and the main parts have been color-coded (as in Figure 4.14) for this report. Furthermore, input and output signals have also been added here as colored arrows, as they were used for comparison with a simulated PAC module, and the generic PAC module of GRS.

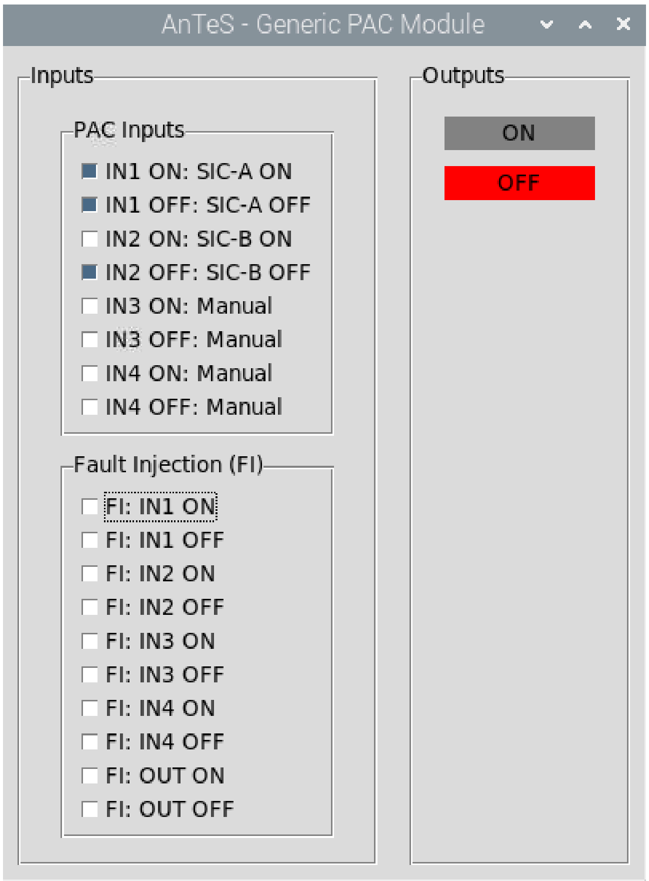
Real PAC modules of AnTeS-PAC-real can be controlled via the AnTeS-OIC interface (see also Section 2.4), for example. Figure 4.16 shows the GUI of this interface when connected to an AV42. In this example, the input signals shown in the illustration (SIC-A ON, SIC-B ON, SIC-A OFF, SIC-A ON) were fed into the AV42 from the output channels 25, 26, 27 and 28 and the outputs of the AV42 were simultaneously read into the input channels 25 and 26.



Channel 1: 1.34 V
Channel 2: 1.43 V
Channel 3: 1.49 V
Channel 4: 1.53 V
Channel 5: 1.53 V
Channel 6: 1.52 V
Channel 7: 1.53 V
Channel 8: 1.17 V

Figure 4.16 AnTeS-PAC-real: Controlling an AV42 PAC module with the OIC interface, example

To develop a generic PAC module for AnTeS-PAC-real, the behavior and general structure of real PAC modules were replicated by software developed by GRS. An example GUI of this software is shown in Figure 4.17. This software was implemented into the AnTeS-OIC interface shown in Figure 2.13, which therefore can also serve as a generic PAC module. The software for the generic PAC module allows the emulation of the behavior of any PAC module within AnTeS-PAC-real on dedicated hardware, including fault injection, which is much more flexible than only using AV42 or SPLM1-PC11 modules available in AnTeS-PAC-real.



AnTeS - Generic PAC Module

Inputs

PAC Inputs

- ☑ IN1 ON: SIC-A ON
- ☑ IN1 OFF: SIC-A OFF
- □ IN2 ON: SIC-B ON
- ☑ IN2 OFF: SIC-B OFF
- □ IN3 ON: Manual
- □ IN3 OFF: Manual
- □ IN4 ON: Manual
- □ IN4 OFF: Manual

Fault Injection (FI)

- □ FI: IN1 ON
- □ FI: IN1 OFF
- □ FI: IN2 ON
- □ FI: IN2 OFF
- □ FI: IN3 ON
- □ FI: IN3 OFF
- □ FI: IN4 ON
- □ FI: IN4 OFF
- □ FI: OUT ON
- □ FI: OUT OFF

Outputs

Figure 4.17 AnTeS-PAC-real: generic PAC module, example

The signal combination shown for this example configuration of the generic PAC module corresponds to the example in Figure 4.16 for an AV42. The input signals SIC-A ON, SIC-A OFF, and SIC-B OFF are 1 in both cases (all other input signals are 0), both then output an OFF signal.

The pure simulation of PAC modules (e.g., in Monte Carlo simulations) is carried out in AnTeS-PAC-sim with the help of Matlab/Simulink. The simulation of the PAC module in Figure 4.14 then looks like Figure 4.18 in Simulink, for example.

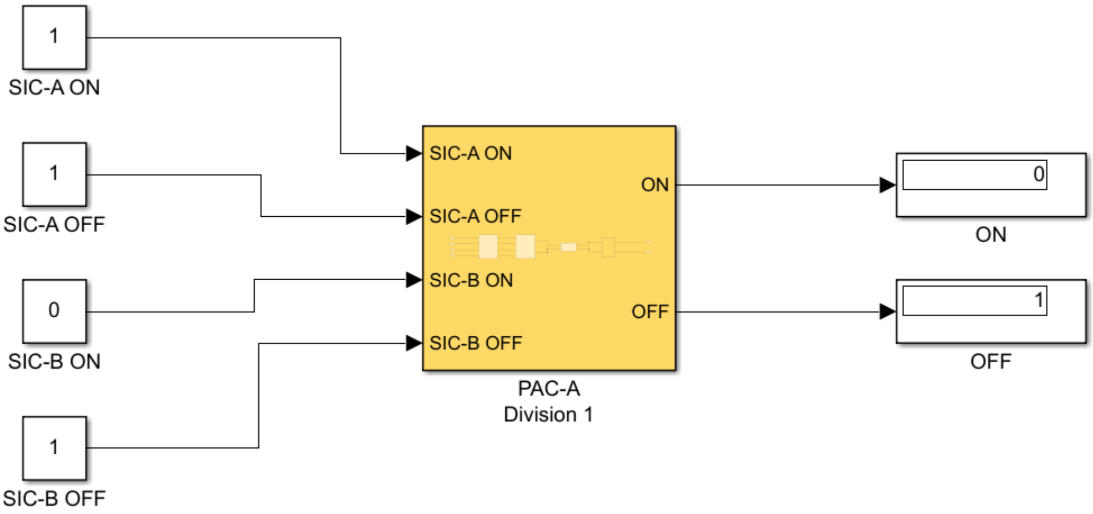


Figure 4.18 AnTeS-PAC-sim: simulated PAC (Simulink), example

For demonstration purposes, the same input signals are set in this example as in Figure 4.16 and Figure 4.17, so that an OFF signal is also output here.

The three PAC modules described above, in particular their response behavior to different input signal combinations, are compared in Table 4.3. In this table the input signals of two I&C systems (SIC-A and SIC-B) are shown in relation to the respective output signals of the AV24 (Figure 4.15), the generic PAC module (Figure 4.17), and the simulated PAC (Figure 4.18).

As expected, all three modules behave in the same way. All three modules prioritize OFF signals over ON signals, whereby in the example SIC-A is also correctly given a higher priority than SIC-B.

Table 4.3 Comparison AV42, generic PAC module, and simulated PAC module

#	Input				Output					
	SIC-A		SIC-B		AV42		Generic		Simulated	
	ON	OFF	ON	OFF	ON	OFF	ON	OFF	ON	OFF
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	1	0	1	0	1	0	1
3	0	0	1	0	1	0	1	0	1	0
4	0	0	1	1	0	1	0	1	0	1
5	0	1	0	0	0	1	0	1	0	1
6	0	1	0	1	0	1	0	1	0	1
7	0	1	1	0	0	1	0	1	0	1
8	0	1	1	1	0	1	0	1	0	1
9	1	0	0	0	1	0	1	0	1	0
10	1	0	0	1	1	0	1	0	1	0
11	1	0	1	0	1	0	1	0	1	0
12	1	0	1	1	1	0	1	0	1	0
13	1	1	0	0	0	1	0	1	0	1
14	1	1	0	1	0	1	0	1	0	1
15	1	1	1	0	0	1	0	1	0	1
16	1	1	1	1	0	1	0	1	0	1

More details on the PAC modules can be found in Annex A.3.

4.5 Model Systems – Base Case

This section explains the representative validation of the conducted fault tree analyses for the base case (model system A1B1C1P1, Figure 4.19) using Monte Carlo simulations. The simulation model used for this purpose is presented in Figure 4.20. The individual components of this simulation model are the simulation models of the SIC (Section 4.2), OIC (Section 4.3), and PAC (Section 4.4), which were previously validated through comparison with real systems.

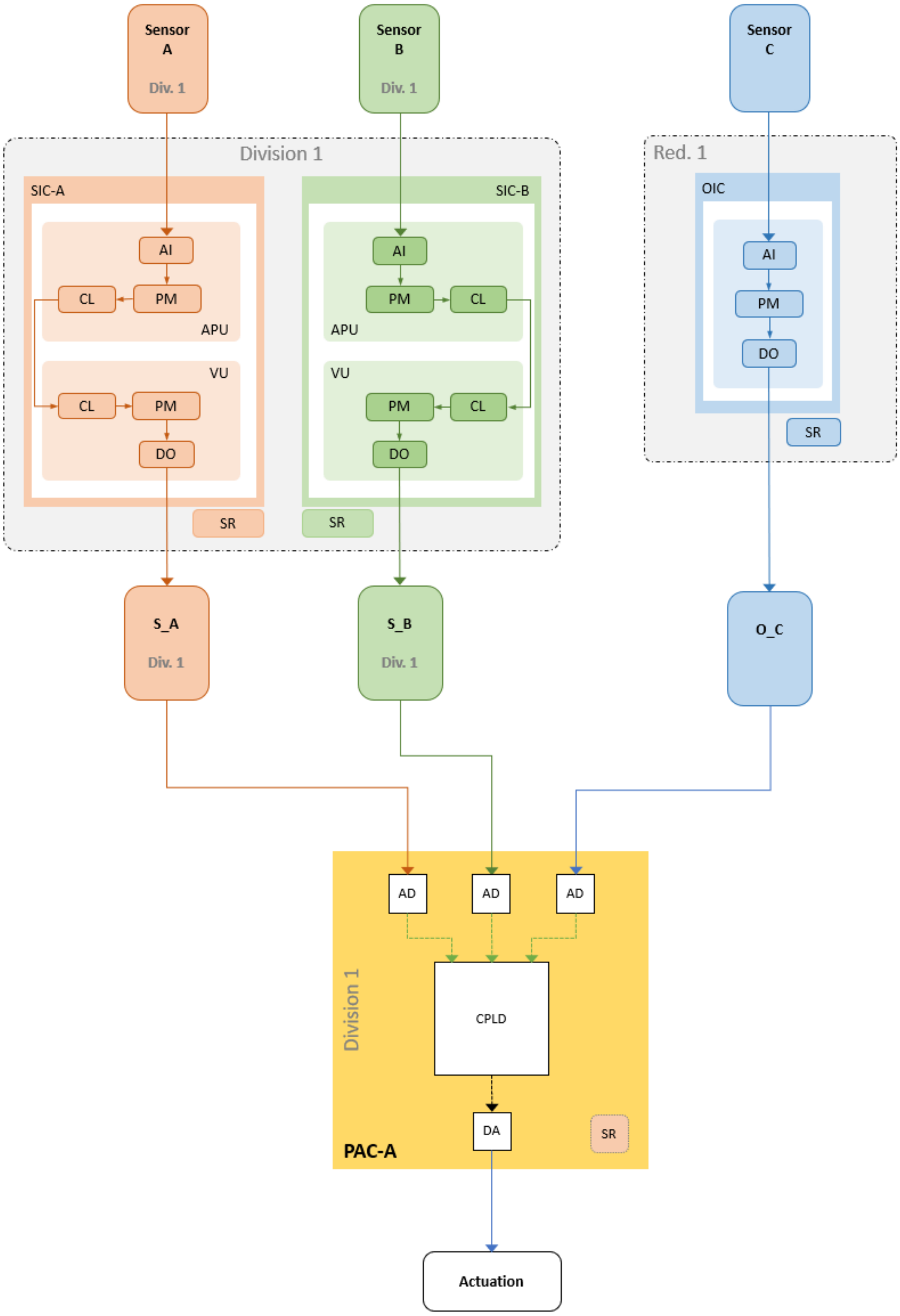


Figure 4.19 Base case (A1B1C1P1)

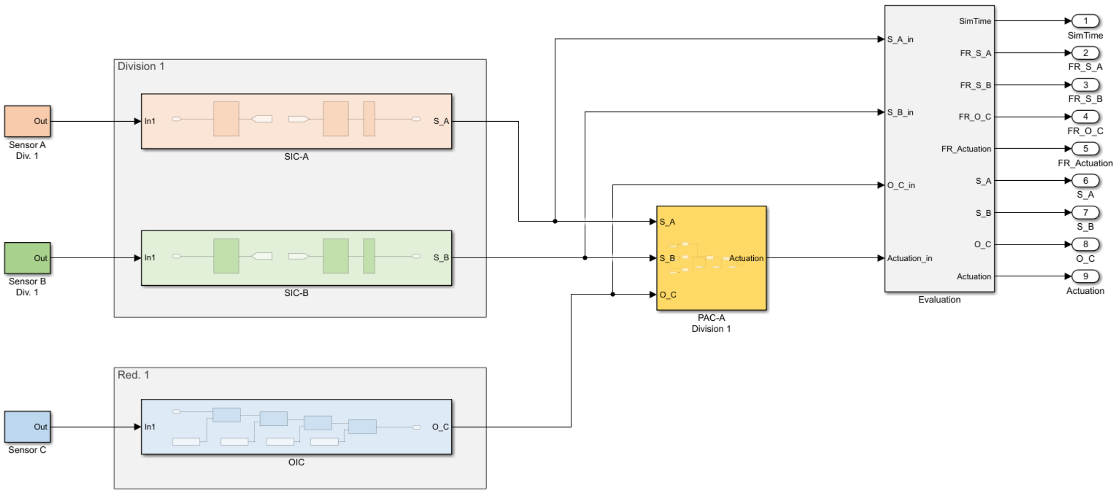


Figure 4.20 Simulation model of base case (A1B1C1P1) (Simulink)

This simulation model allows (among other things) the quantitative analysis of the individual actuation signals of the I&C systems (SIC-A, SIC-B, OIC) as well as the overall actuation by the PAC module (based on the actuation signals from the I&C systems). The analysis cases considered are therefore in detail:

- No S_A: The actuation signal S_A from SIC-A is not generated.
- No S_B: The actuation signal S_B from SIC-B is not generated.
- No O_C: The actuation signal O_C from OIC is not generated.
- No Actuation: The overall actuation signal is not generated. This can be a result of missing actuation signals from the I&C systems as well as failures within the PAC module.

To analyze these cases, a period of one million years was simulated (including statistical failures) using the simulation model in Figure 4.20 and evaluated during this simulation period[18] using the Simulink subsystem “Evaluation” (grey block on the far right of the image).

[18] It should be noted here that the individual repetitions (“simulation steps”) within Monte Carlo simulations of I&C systems are not completely independent of each other. Rather, in the GRS approach these also represent a chronological sequence, which means that recurring tests and repairs can also be considered in these simulations (see also /MUE 21/).

The estimated mean unavailabilities of the individual actuation signals calculated during a simulation run are shown as an example in Figure 4.21. After about one hundred thousand (1E+05) simulated years, the individual calculated values have already leveled off close to the final steady state results, so that no significantly different results can be expected for even longer simulation periods[19].

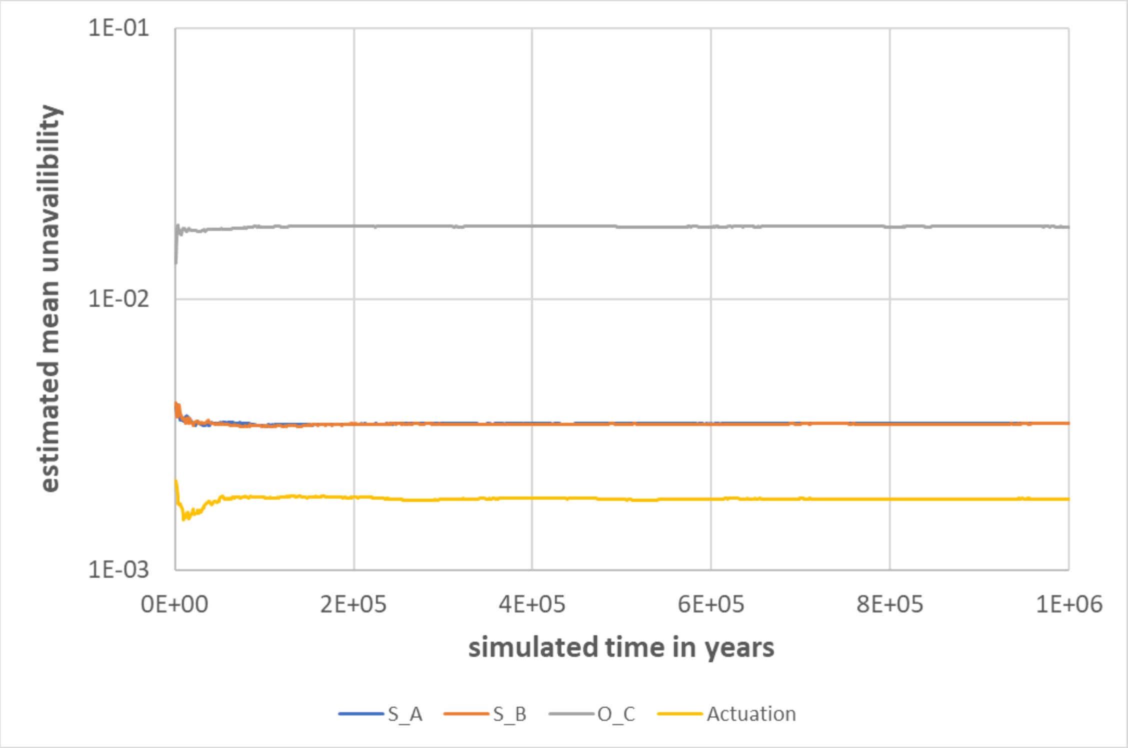


Figure 4.21 Estimated mean unavailabilities for base case during a simulation run

The same system was also analyzed with a fault tree analysis (FTA). The representative fault tree for the "no actuation" analysis case is shown in Figure 4.22. The triangles at the bottom of the fault tree refer to the fault trees attached there for the individual signals (S_A, S_B, O_C). In addition, the fault tree shown is itself part of the higher-level fault tree for "no success" (NO_SUCCESS[20]) (indicated by the triangle at the top of the fault tree).

[19] Longer simulation periods can nevertheless be relevant if minimal cut sets (MCS) are also considered (see further below in this section).

[20] In the "no success" fault trees for the model systems, only the success criterion is queried in each case, i.e., for the base case only whether the only actuation signal is present (in more complex models, for example, whether at least two actuation signals from different divisions are present).

The complete set of fault trees for the base case can be found in Appendix C.1 (including all basic events and results). Representative for the more complex model systems, the complete set of fault trees for model system A4B4C1P2-2 is also attached in Appendix C.2.

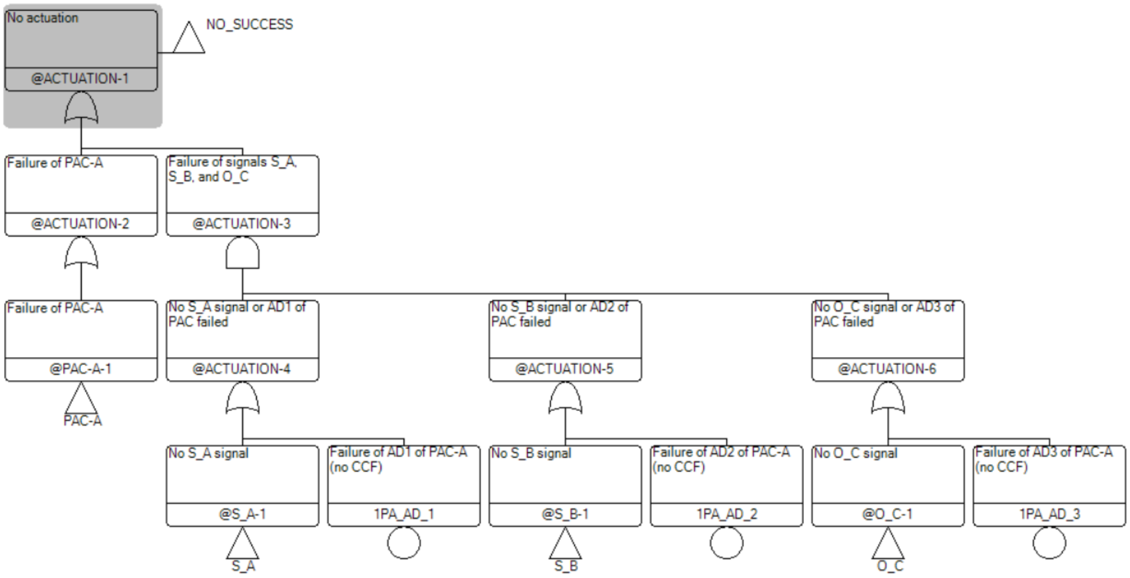
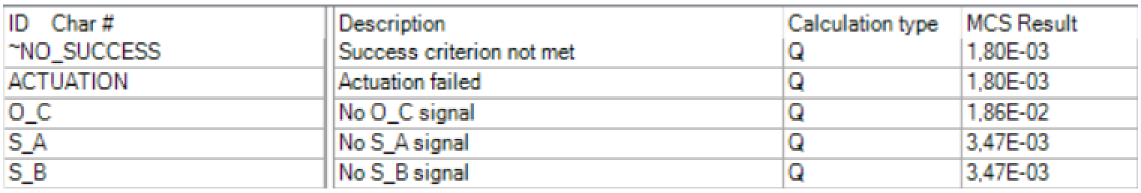

No actuation
@ACTUATION-1
NO_SUCCESS
Failure of PAC-A
@ACTUATION-2
Failure of signals S_A, S_B, and O_C
@ACTUATION-3
Failure of PAC-A
@PAC-A-1
PAC-A
No S_A signal or AD1 of PAC failed
@ACTUATION-4
No S_B signal or AD2 of PAC failed
@ACTUATION-5
No O_C signal or AD3 of PAC failed
@ACTUATION-6
No S_A signal
@S_A-1
S_A
Failure of AD1 of PAC-A (no CCF)
1PA_AD_1
No S_B signal
@S_B-1
S_B
Failure of AD2 of PAC-A (no CCF)
1PA_AD_2
No O_C signal
@O_C-1
O_C
Failure of AD3 of PAC-A (no CCF)
1PA_AD_3

Figure 4.22 Fault tree (”no actuation“) of base case

The RiskSpectrum software (version 1.4.0) was used to create the fault trees and subsequent analyses. The results for the mean unavailabilities obtained in this way for the analysis cases in the base case are shown as a screenshot in Figure 4.23. All basic events were of the type "tested" with a test interval of 0.5 years (4380 hours) and a fixed repair time of 8 hours.



ID Char #	Description	Calculation type	MCS Result
~NO_SUCCESS	Success criterion not met	Q	1,80E-03
ACTUATION	Actuation failed	Q	1,80E-03
O_C	No O_C signal	Q	1,86E-02
S_A	No S_A signal	Q	3,47E-03
S_B	No S_B signal	Q	3,47E-03

Figure 4.23 Results of analysis cases (RiskSpectrum – screenshot)

These results are compared in Table 4.4 with the corresponding results of the Monte Carlo simulations. Both methods provide very consistent results, differences only appear in the second decimal place and are to be expected due to the statistical behavior of Monte Carlo simulations.

Table 4.4 Mean unavailabilities for the base case in FTA and Monte Carlo simulation

Tool	No S_A	No S_B	No O_C	No Actuation
FTA	3.47E-03	3.47E-03	1.86E-02	1.80E-03
Monte Carlo	3.47E-03	3.46E-03	1.85E-02	1.82E-03

The FTA also provides the minimum cuts (MCS) for the analysis cases, which can be compared with the combinations contributing to the failures in the Monte Carlo simulations. Tables 4.5 to 4.8 therefore show the contributions of the MCS to the average unavailability (given as absolute values Q and as a percentage of the total unavailability) in FTA and MC simulation as well as the individual events that make up the MCS.

Table 4.5 Minimal cut sets (MCS) for the analysis case “No O_C”

#	Fault Tree Analysis (FTA)			Monte Carlo Simulation (MC)		
	Q	%	Event(s)	Q	%	Event(s)
1	7.86E-03	42.27	1_SENSOR_C_LOW	7.77E-03	42.05	1_SENSOR_C_LOW
2	5.25E-03	28.23	1O_AI	5.15E-03	27.90	1O_AI
3	3.94E-03	21.19	1O_PM	3.87E-03	20.94	1O_PM
4	8.77E-04	4.72	1O_DO	8.52E-04	4.61	1O_DO
5	7.89E-04	4.25	1O_SR	8.29E-04	4.49	1O_SR

Description of the event names in the order in which they are mentioned:
1_SENSOR_C_LOW – Sensor C of division 1 failed to low
1O_AI – Analog input module of division 1 of OIC failed
1O_PM – Processor module of division 1 of OIC failed
1O_DO – Digital out module of division 1 of OIC failed
1O_SR – Subrack of division 1 of OIC failed

Table 4.6 Minimal cut sets (MCS) for the analysis case “No S_A”

#	Fault Tree Analysis (FTA)			Monte Carlo Simulation (MC)		
	Q	**%**	**Event(s)**	**Q**	**%**	**Event(s)**
1	8.35E-04	24.08	1A_VU_DO	8.37E-04	24.09	1A_VU_DO
2	8.35E-04	24.08	1A_APU_AI	8.36E-04	24.07	1A_APU_AI
3	6.26E-04	18.06	1A_VU_PM	6.54E-04	18.83	1A_APU_PM
4	6.26E-04	18.06	1A_APU_PM	6.28E-04	18.07	1A_VU_PM
5	3.96E-04	11.41	1_SENSOR_A_LOW	3.78E-04	10.89	1_SENSOR_A_LOW
6	4.40E-05	1.27	1Y_APU_AI	4.46E-05	1.28	1Y_APU_AI
7	4.40E-05	1.27	1Y_VU_DO	4.10E-05	1.18	1Y_VU_DO
8	3.30E-05	0.95	1Y_VU_PM	2.84E-05	0.82	1Y_APU_PM
9	3.30E-05	0.95	1Y_APU_PM	2.65E-05	0.76	1Y_VU_PM

Description of the event names in the order in which they are mentioned:
1A_VU_DO – Digital out module of VU of division 1 of SIC-A failed
1A_APU_AI – Analog input module of APU of division 1 of SIC-A failed
1A_VU_PM – Processor module of VU of division 1 of SIC-A failed
1A_APU_PM – Processor module of APU of division 1 of SIC-A failed
1_SENSOR_A_LOW – Sensor A of division 1 failed to low
1Y_APU_AI – CCF of analog input modules of APU of SIC-A and SIC-B
1Y_VU_DO – CCF of digital out modules of VU of SIC-A
1Y_VU_PM – CCF of processor modules of VU of SIC-A
1Y_APU_PM – CCF of processor modules of APU of SIC-A

Table 4.7 Minimal cut sets (MCS) for the analysis case “No S_B”

#	Fault Tree Analysis (FTA)			Monte Carlo Simulation (MC)		
	Q	%	Event(s)	Q	%	Event(s)
1	8.35E-04	24.08	1B_VU_DO	8.39E-04	24.23	1B_APU_AI
2	8.35E-04	24.08	1B_APU_AI	8.34E-04	24.07	1B_VU_DO
3	6.26E-04	18.06	1B_VU_PM	6.32E-04	18.24	1B_APU_PM
4	6.26E-04	18.06	1B_APU_PM	6.21E-04	17.92	1B_VU_PM
5	3.96E-04	11.41	1_SENSOR_B_LOW	3.98E-04	11.48	1_SENSOR_B_LOW
6	4.40E-05	1.27	1Y_APU_AI	4.46E-05	1.29	1Y_APU_AI
7	4.40E-05	1.27	1Y_VU_DO	4.10E-05	1.18	1Y_VU_DO
8	3.30E-05	0.95	1Y_VU_PM	2.84E-05	0.82	1Y_APU_PM
9	3.30E-05	0.95	1Y_APU_PM	2.65E-05	0.77	1Y_VU_PM

Description of the event names in the order in which they are mentioned:
1B_VU_DO – Digital out module of VU of division 1 of SIC-B failed
1B_APU_AI – Analog input module of APU of division 1 of SIC-B failed
1B_VU_PM – Processor module of VU of division 1 of SIC-B failed
1B_APU_PM – Processor module of APU of division 1 of SIC-B failed
1_SENSOR_B_LOW – Sensor B of division 1 failed to low
1Y_APU_AI – CCF of analog input modules of APU of SIC-A and SIC-B
1Y_VU_DO – CCF of digital out modules of VU of SIC-A and SIC-B
1Y_VU_PM – CCF of processor modules of VU of SIC-A and SIC-B
1Y_APU_PM – CCF of processor modules of APU of SIC-A and SIC-B

Comparing the numerical values for the events in Table 4.6 (“No S_A”) with those in Table 4.7 (“No S_B”) provides an idea of the magnitude of the scatter of the results in the Monte Carlo simulations carried out for the base case. While the FTA provides identical results for SIC-A and SIC-B due to their identical structure, the Monte Carlo simulations differ by up to around 5 %. Overall, however, all results were in good agreement within the expected limits.

Table 4.8 Minimal cut sets (MCS) for the analysis case “No Actuation”, excerpt

#	Fault Tree Analysis (FTA)			Monte Carlo Simulation (MC)		
	Q	%	Event(s)	Q	%	Event(s)
1	8.79E-04	48.71	1PA_DA	8.75E-04	48.23	1PA_DA
2	4.40E-04	24.36	1PA_CPLD	4.48E-04	24.70	1PA_CPLD
3	4.40E-04	24.36	1PA_SR	4.46E-04	24.59	1PA_SR
4	4.40E-05	2.44	1PA_AD_Z	4.51E-05	2.48	1PA_AD_Z
5	3.45E-07	0.02	1Y_APU_AI; 1_SENSOR_C_LOW	NA[21]	0.00	1Y_APU_AI; 1_SENSOR_C_LOW
…	…	…	…	…	…	…

243	1.31E-10	0.00	1PA_AD_3;
			1_SENSOR_A_LOW;
			1_SENSOR_B_LOW
				NA	0.00	1PA_AD_3;
						1_SENSOR_A_LOW;
						1_SENSOR_B_LOW

244	1.24E-10	0.00	1O_SR;
			1_SENSOR_A_LOW;
			1_SENSOR_B_LOW
				NA	0.00	1O_SR;
						1_SENSOR_A_LOW;
						1_SENSOR_B_LOW

Description of the (visible) event names in the order in which they are mentioned:
1PA_DA – Digital-to-analog converter of PAC 1 failed
1PA_CPLD – Complex programmable logic device of PAC 1 failed
1PA_SR – Subrack of PAC 1 failed
1PA_AD_Z – CCF of all analog-to-digital converters of PAC 1
1Y_APU_AI – CCF of analog input modules of APUs of SIC-A and SIC-B
1_SENSOR_C_LOW – Sensor C of division 1 failed to low
1PA_AD_3 – Third analog-to-digital converter of PAC 1 failed
1_SENSOR_A_LOW – Sensor A of division 1 failed to low
1_SENSOR_B_LOW – Sensor B of division 1 failed to low
1O_SR – Subrack of division 1 of OIC failed

In this final validation step, the modeling with FTA and MC simulations delivered similar results overall, both quantitatively and qualitatively (within expected limits).

[21] NA - “Not Available”: as expectable, these failure combinations did not occur in the simulated time period of the Monte Carlo simulation due to their unlikely occurrence (see FTA results), so no numerical values can be calculated.

4.6 Conclusion

The validation of the methodological approach within this project followed a systematic and multi-stage process: The validation of the simulated SIC and OIC systems was conducted by comparing simulation results (AnTeS-SIC-sim and AnTeS-OIC-sim) with real systems (AnTeS-SIC-real and AnTeS-OIC-real). Fault combinations were systematically tested, the results of real and simulated systems were consistent. Further validation was performed through the comparison of PAC modules (AV42, generic PAC module, and simulated PAC module), whose response behavior to input conditions was found to be identical. To quantify probabilities for unfavorable system states, fault tree analyses (FTA) and Monte Carlo (MC) simulations of the base case were used. Both methods yielded highly consistent results, with minor variations within expected statistical limits. Minimal Cut Sets (MCS) were determined through both FTA and MC, providing additional model verification.

The validation of the methodological approach confirms a robust, transparent, and reliable system for analyzing I&C architectures. Particularly noteworthy is the systematic cross-validation through multiple independent methods, the strong agreement between real and simulated systems confirming the validity of the simulation models, the combination of qualitative and quantitative analyses allowing a comprehensive reliability assessment, and the high correlation between FTA and Monte Carlo results, validating the quantitative calculations.

Overall, the validation confirms that the applied methods and tools lead to reliable and consistent results, forming a solid foundation for further analyses conducted with all model systems described in the following chapter.

5 Analyses

5.1 Model Systems – Overview Individual Results

The model systems described in Chapter 3 were analyzed using the validated methodology from Chapter 0. The model systems described in Chapter 3 were analyzed using the validated methodology from Chapter 4. A complete and explicit validation was carried out for the base case (model system A1B1C1P1), whereas the analyses of the other model systems were conducted using fault tree analysis (FTA). However, the validated components and structures from the base case were reused in the other model systems, as all fundamental elements occur already in the base case configuration.

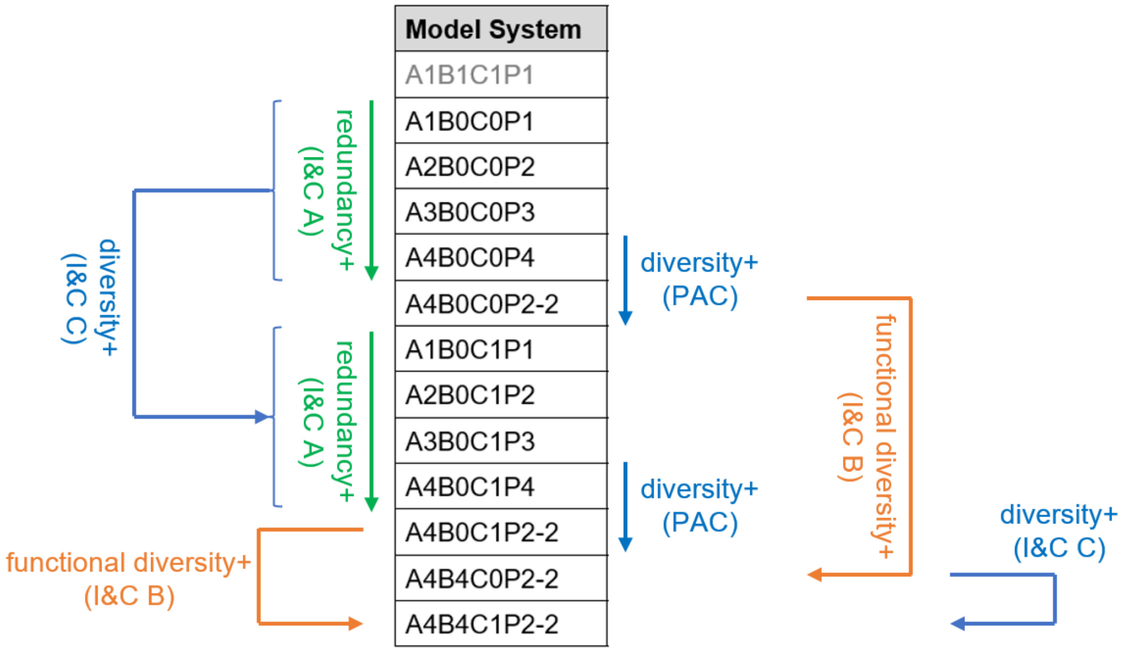
The results of the analyses, i.e., the calculated mean unavailabilities for each model system, are summarized in Table 5.1.

Table 5.1 Overview of results for all model systems

Model System	No Success	No S_A	No S_B	No O_C
A1B1C1P1	1.80E-03	3.47E-03	3.47E-03	1.86E-02
A1B0C0P1	1.39E-02	3.47E-03	-	-
A2B0C0P2	3.26E-04	1.79E-04	-	-
A3B0C0P3	3.06E-04	1.74E-04	-	-
A4B0C0P4	3.06E-04	1.74E-04	-	-
A4B0C0P2-2	1.74E-04	1.74E-04	-	-
A1B0C1P1	1.88E-03	3.47E-03	-	-
A2B0C1P2	1.38E-04	1.79E-04	-	1.86E-02
A3B0C1P3	1.35E-04	1.74E-04	-	1.86E-02
A4B0C1P4	1.35E-04	1.74E-04	-	1.86E-02
A4B0C1P2-2	4.18E-06	1.74E-04	-	1.86E-02
A4B4C0P2-2	1.55E-04	1.74E-04	1.74E-04	-
A4B4C1P2-2	3.78E-06	1.74E-04	1.74E-04	1.86E-02

These results are used in the following section 5.2 to provide a deeper insight into the effects of redundancy, functional diversity, and diversity on the reliability of I&C architectures.

5.2 Detailed Analyses



Model System
A1B1C1P1
A1B0C0P1
A2B0C0P2
A3B0C0P3
A4B0C0P4
A4B0C0P2-2
A1B0C1P1
A2B0C1P2
A3B0C1P3
A4B0C1P4
A4B0C1P2-2
A4B4C0P2-2
A4B4C1P2-2

Figure 5.1 Redundancy, diversity, and functional diversity within the model systems

Colored arrows, lines, and labels are used in Figure 5.1 to group the different model systems, which differ solely in their degree of redundancy (green), functional diversity (orange) or full diversity (blue). This results in the following specific groups:

- Redundancy+ (I&C A)
  - Within this group there are two quadruples of model systems which differ only in the number of subsystems of type SIC-A, including the PAC modules controlled by them.
  - The two quadruples are: A1B0C0P1 – A2B0C0P2 – A3B0C0P3 - A4B0C0P4, A1B0C1P1 – A2B0C1P2 – A3B0C1P3 – A4B0C1P4.
- Functional Diversity+ (I&C B)
  - Within this group are two pairs of model systems that differ only in whether or not additional SIC-B type subsystems are used as functional diversity.
  - The two pairs are: A4B0C0P2-2 – A4B4C0P2-2, A4B0C1P2-2 – A4B4C1P2-2.

- Diversity+ (I&C C)
  - Within this group there are five pairs of model systems, each of which differs only in the presence of the I&C system C.
  - The five pairs are: A1B0C0P1 – A1B0C1P1, A2B0C0P2 – A2B0C1P2, A3B0C0P3 – A3B0C1P3, A4B0C0P4 – A4B0C1P4, A4B4C0P2-2 – A4B4C1P2-2.

- Diversity+ (PAC)
  - This group comprises two pairs of model systems that differ only in terms of diversity in the PAC modules (4 x PAC-A ←→ 2 x PAC-A and 2 x PAC-B).
  - The two pairs are: A4B0C0P4 – A4B0C0P2-2, A4B0C1P4 – A4B0C1P2-2.

These groups are evaluated in the following three subsections.

5.2.1 Redundancy

Figure 5.2 illustrates effects of redundancy within the two quadruples of model systems of the group “Redundancy+ (I&C A)” (see above). The mean unavailabilities (as also given in Table 5.1) are shown under the individual names of the model systems. During the “transition” from one model to the next along an arrow, the mean unavailability changes according to the factor indicated above the arrow. Below each arrow is a numerical value that reflects the change in reliability[22].

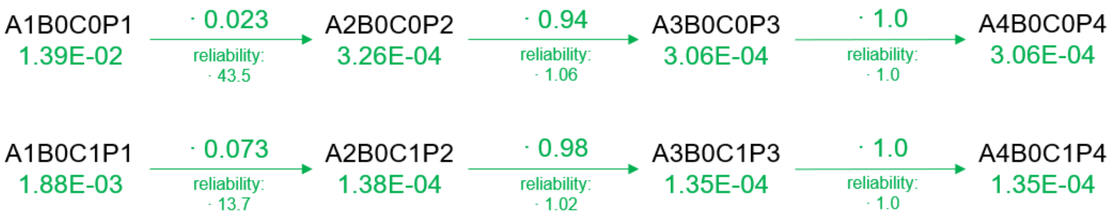


Figure 5.2 Effect of redundancy on the reliability for model systems

[22] Calculated here as reciprocal values of the factors for the mean unavailabilities.

The greatest probabilistic increase in reliability is achieved between no redundancy and one redundancy; a second additional redundancy only increases reliability comparatively little. If a third redundancy is added (i.e., using a total of four redundant subsystems), no further significant increase in reliability can be observed.

However, a fourth system can still be useful under certain circumstances, for example if one of the systems is unavailable during maintenance measures or due to individual failures. In this case, a comparatively high level of reliability can still be guaranteed during continued operation, so that a high degree of redundancy can increase availability, for example (if shutdowns are otherwise required in the event of unavailability, e.g., for regulatory reasons).

5.2.2 Functional Diversity

In purely probabilistic terms, functional diversity has only a comparable small influence on reliability, as can be seen in Figure 5.3 (for the two pairs of the group "Functional diversity (I&C B)"). In both cases considered there, the reliability increases only slightly, although the model systems on the right-hand side of the arrows each have four additional subsystems (SIC-B).

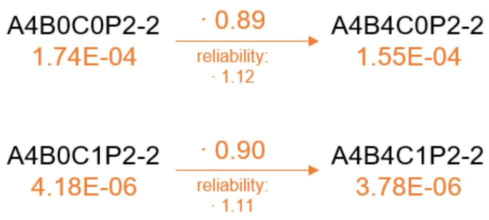


Figure 5.3 Effect of functional diversity on the reliability for model systems

From a deterministic point of view, functional diversity can nevertheless be of great benefit if, for example, systematic errors were made in the planning of the criteria for one of the subsystems. In such cases, the other, functionally diverse, subsystems (with other criteria) still provide reliability.

5.2.3 Diversity

(Complete or general) diversity consistently leads to a significant or even very large increase in reliability within the model system pairs in all (considered) cases of the "Diversity+ (PAC)" group in Figure 5.4.

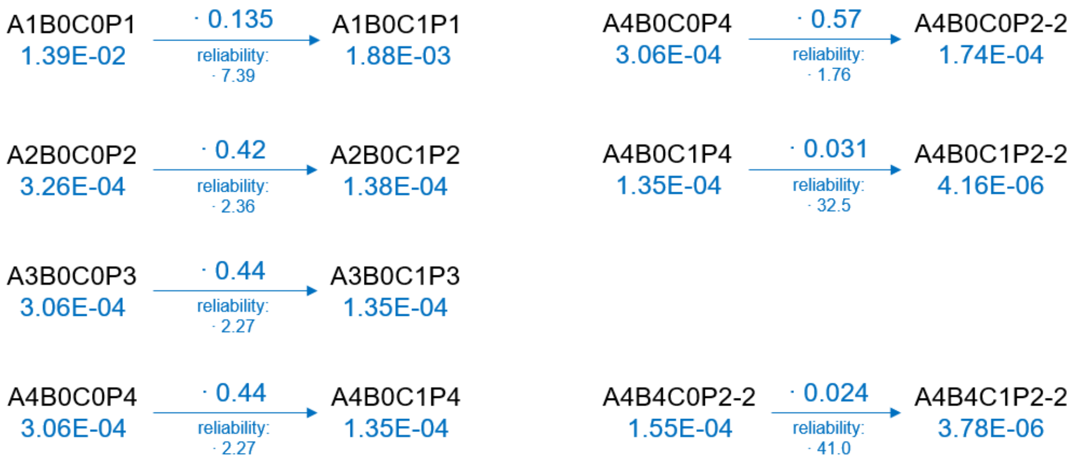


Figure 5.4 Effect of diversity on the reliability for model systems

Since diversity is an effective measure against CCFs in particular (and also offers a certain degree of protection against individual failures, as does pure redundancy), these results were to be expected. However, the qualitatively logical assumption that CCFs are of particular importance can also be underpinned (to a certain extent) by quantitative results here.

6 Summary and Conclusions

This report presents the systematic development, validation, and application of an advanced methodology for analyzing complete I&C architectures in nuclear power plants (NPPs), with a particular focus on the prioritization between safety I&C (SIC) and operational I&C (OIC). The study was conducted using the Analysis and Test System (AnTeS) developed by GRS, which integrates both real and simulated I&C components to enable comprehensive safety and reliability assessments.

6.1 Key Findings and Contributions

A structured approach was applied to investigate various model systems representing different configurations of SIC, OIC, and prioritization and actuation control (PAC) modules. These model systems were analyzed using fault tree analysis (FTA), a well-established probabilistic safety assessment method, to quantify failure probabilities and identify critical failure pathways.

A crucial aspect of this project was the development and testing **AnTeS-OIC-real**, **AnTeS-OIC-sim**, **AnTeS-PAC-real**, and **AnTeS-PAC-sim**. AnTeS-OIC-real is a newly developed real-hardware platform for analyzing operational I&C (OIC) systems within the AnTeS framework. It allows for direct testing of real OIC components, enabling fault injection and validation of system responses under defined failure conditions. This ensures that the behavior of real OIC modules can be assessed accurately and directly compared to simulated models. AnTeS-OIC-sim is a simulation-based counterpart to AnTeS-OIC-real, designed to model and analyze operational I&C (OIC) behavior using Matlab/Simulink. It enables detailed failure mode analysis and Monte Carlo simulations without requiring physical hardware. By comparing AnTeS-OIC-sim results with real-system data, the accuracy of the simulation models was thoroughly validated. AnTeS-PAC-real was developed to analyze the prioritization and actuation control (PAC) modules using real hardware, including commercial PAC units and a generic PAC module designed by GRS. This system enables fault injection and response testing under realistic conditions, allowing for a direct evaluation of PAC reliability and prioritization logic in nuclear safety applications. AnTeS-PAC-sim provides a fully simulated environment for PAC module analysis, implemented in Matlab/Simulink. It enables Monte Carlo simulations to assess PAC behavior under various failure scenarios. The results from AnTeS-PAC-sim were systematically cross-checked with

AnTeS-PAC-real, ensuring the reliability of both real and simulated PAC evaluations. These new components of the AnTeS platform significantly enhance its analytical capabilities by enabling in-depth evaluations of operational I&C and PAC systems alongside safety I&C. Their successful integration allowed for a more comprehensive validation process, improving the accuracy of reliability assessments and failure mode analyses.

The explicit validation of the methodology was conducted for the base case model (A1B1C1P1). This validation involved comparing real and simulated systems, ensuring that the computational models accurately reflected the behavior of actual digital I&C components. Additionally, Monte Carlo (MC) simulations were conducted to verify the FTA results, providing an independent cross-check of the calculated failure probabilities and system unavailability figures. The high level of consistency observed between these different methods confirms the robustness of the developed approach.

The results of the analyses demonstrate how different system architectures influence the overall reliability. The study provided detailed insights into the effects of redundancy, functional diversity, and general diversity on system availability and safety. Key findings include:

- **Redundancy**: Model systems with higher levels of redundancy exhibited significantly lower failure probabilities, underscoring the importance of multiple, independent SIC subsystems in enhancing reliability.
- **Functional Diversity**: The presence of functionally diverse actuation signals, derived from different sensor types or evaluation criteria, contributes to improved fault tolerance mainly from a deterministic point of view.
- **General Diversity**: Introducing different hardware platforms and/or software implementations for SIC and OIC systems was shown to mitigate common-cause failures (CCF), which are a critical concern in digital I&C architectures.
- **Prioritization Reliability**: The study confirmed that PAC modules play a decisive role in ensuring correct prioritization between SIC and OIC signals. Systems with diverse PAC implementations exhibited superior reliability compared to those relying on a single type of PAC module.

6.2 Regulatory and Safety Implications

From a regulatory perspective, the findings of this study are highly relevant for technical support organizations (TSOs) such as GRS and other national or international regulatory bodies overseeing nuclear safety. Digital I&C systems have become an integral part of modern NPPs, and their increasing complexity requires advanced analysis techniques to ensure compliance with stringent safety requirements.

This research directly supports the goals of deterministic and probabilistic safety assessments (DSA/PSA) as required by international safety standards, such as those set by the International Atomic Energy Agency (IAEA) and national regulatory authorities. The ability to accurately model, validate, and analyze I&C architectures is essential for:

1. **Licensing and Qualification**: The methodology developed in this project provides a robust framework for assessing digital I&C designs as part of the licensing process for new reactors or modernized I&C systems in existing plants.
2. **Common-Cause Failure (CCF) Mitigation**: The insights gained into redundancy and diversity can inform regulatory guidelines on minimizing the risk of simultaneous failures due to shared vulnerabilities.
3. **Risk-Informed Decision-Making**: By quantifying (generic) failure probabilities and identifying dominant failure modes, this study enables risk-informed regulatory decision-making, balancing deterministic safety principles with probabilistic risk assessments.
4. **Verification of Safety Claims**: Vendors and operators proposing digital I&C solutions can use the validated analysis framework to substantiate safety claims and demonstrate compliance with nuclear safety requirements.

6.3 Benefits for GRS

For GRS and other TSOs, this research represents a significant advancement in the capability to evaluate digital I&C architectures in a structured and scientifically sound manner. The complete development and successful testing of **AnTeS-OIC-real**, **AnTeS-OIC-sim**, **AnTeS-PAC-real**, and **AnTeS-PAC-sim** mark a major enhancement to the AnTeS platform, enabling the comprehensive assessment of safety and operational I&C interactions. This improved analytical capability is crucial for evaluating modern I&C

systems, where the interplay between SIC and OIC must be carefully assessed to ensure robust prioritization and actuation mechanisms.

Key benefits include:

- **Enhanced Analytical Capabilities**: GRS now has a validated toolset that integrates real and simulated I&C components, allowing them to conduct detailed failure mode analyses and reliability assessments more effectively.
- **Support for Regulatory Decision-Making**: The findings provide empirical data that can support regulatory reviews, ensuring that safety-critical I&C systems meet the required reliability thresholds.
- **Improved Industry Guidance**: The study contributes to the development of best practices for designing and evaluating digital I&C architectures, also helping operators and vendors implement safer and more resilient systems.
- **Knowledge Transfer and Training**: The insights gained from this research can be incorporated into training programs for regulators, engineers, and operators, strengthening the overall expertise within the nuclear safety community.

6.4 Conclusion and Outlook

Overall, this study demonstrates that the developed and applied methodology provides a reliable, systematic, and transparent approach for evaluating digital I&C architectures, particularly in the context of SIC-OIC prioritization. The robustness of the methodology was confirmed through multiple independent validation steps, including cross-verification with real systems and Monte Carlo simulations.

The successful development and integration of **AnTeS-OIC-real**, **AnTeS-OIC-sim**, **AnTeS-PAC-real**, and **AnTeS-PAC-sim** significantly enhance the ability of GRS to analyze complex I&C architectures with a level of detail and accuracy that was previously unattainable. These new tools will allow for more precise assessments of modern digital control systems, improving both safety evaluations and regulatory oversight.

The results provide a sound basis for future research and regulatory developments in the field of digital I&C safety. As digital technologies continue to evolve, further refinement of the methodology – including the incorporation of advanced AI-driven failure prediction models and extended common-cause failure analyses – could further enhance the ability of GRS to assess and improve nuclear safety.

Although digital I&C systems are becoming increasingly prevalent, analog I&C systems continue to play a crucial role in many nuclear power plants, particularly in legacy systems and hybrid architectures (with hard-wired/analog backup systems). Their proven reliability and resistance to certain types of cyber threats make them an essential component of nuclear safety, too. To further enhance the capabilities of AnTeS, it would be valuable to integrate additional modules specifically designed for the analysis of analog I&C systems. This would enable a more comprehensive assessment of mixed digital-analog architectures and support the evaluation of potential modernization strategies while ensuring continued regulatory compliance.

In conclusion, this work strengthens the analytical foundation for regulatory oversight and technical evaluations of digital I&C systems, ensuring that modern nuclear power plants maintain the highest levels of safety and reliability in their instrumentation and control architectures.

References

/ARE 07/ AREVA NP GmbH: *TELEPERM XS: AV42 priority module, installation and accessories*, TXS-2794-76-V1.0, 2007

/ARE 11/ AREVA NP GmbH: *TELEPERM XS (user manual): SPLM1-PC11 priority control*, TXS-2809-76-V1.0, 2011

/ARE 17/ AREVA NP GmbH: *TELEPERM XS (user manual): AV42 priority module, control types 1 to 3*, TXS-2823-76-V1.2, 2017

/ARI 15/ R. Arians, S. Arnold, S. Blum, M. Buchholz, A. Lochthofen, C. Quester, D. Sommer : *Entwicklung und Einsatz von Analysemethoden zur Beurteilung software-basierter leittechnischer Einrichtungen in deutschen Kernkraftwerken*, GRS-355, March 2015

/DIG 25/ OECD/NEA/WGRISK: *DIGMORE – A Realistic Comparative Application of DI&C Modelling Approaches for PSA*, project running until June 2026 under the leadership of GRS, 2025

/GRA 06/ Dr. Arnold Graf, Jörg Pflugbeil: *EPR Design, Instrumentation and Control*, presentation slides, Bonn/BMU, 02.11.2006

/GRS 25/ Ongoing GRS project*: Forschungsarbeiten zu Kran- und Hebezeugsteuerungen in kerntechnischen Anlagen mit Hilfe eines Testsystems*, funded by Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection of Germany, funding code: 4722R01210, 2025

/IEC 03/ IEC61158: *Working with PROFIBUS-DP, Device Description Data Files GSD*, Version: 2.2, April 2003

/MAT 25/ https://de.mathworks.com/products/simulink.html, website last accessed on January 7, 2025

/MUE 18/ C. Müller, J. Peschke, E. Piljugin: *Entwicklung und Erprobung eines Werkzeugs zur Sensitivitätsanalyse der Fehlerauswirkungen in der sicherheitsrelevanten digitalen Leittechnik*, GRS-494, March 2018

/MUE 21/ C. Müller, E. Piljugin, P. Gebhardt, J. Shvab: *AnTeS – Entwicklung und Anwendung des Analyse- und Testsystem der GRS*, GRS-648, March 2021

/MUE 21a/ C. Müller, E. Piljugin: *Forschungsarbeiten zur Entwicklung einer Bewertungsgrundlage für rechnerbasierte und programmierbare Leittechniksysteme in kerntechnischen Anlagen und Erforschung des Weiterentwicklungsbedarfs der dazugehörigen Anforderungen in der Leittechnik*, GRS-649, September 2021

/MUE 23/ C. Müller, J. Herb, P. Gebhardt J. Shvab: *AnTeS-NeCom – Analyse der Fehlerausbreitung in der Netzwerkkommunikation digitaler Leittechniksysteme mit Hilfe eines Testsystems*, GRS-689, September 2023

/MUE 24/ C. Müller, J. Herb, P. Gebhardt J. Shvab: *AnTeS-NeCom – Analysis of the Failure Propagation in the Network Communication of Digital I&C Systems with a Test System*, GRS-764, April 2024

/NAT 15/ D. Natarajan: *Reliable Design of Electronic Equipment* - Chapter: *Failure Mode and Effects Analysis*, ISBN 978-3-319-09110-5, Springer, London, 2015

/RUB 16/ R.Y. Rubinstein, D.P. Kroese: *Simulation and the Monte Carlo Method*, ISBN 978-1-118-63216-1, John Wiley & Sons, 2016

/SIE 02/ Siemens AG: *TELEPERM XP: The Process Control System for Economical Power Plant Control, System Overview*, 2002

/SIE 02a/ Siemens AG: *SIMATIC, Automatisierungssysteme S7-400, M7-400 aufbauen, Installationshandbuch*, Dokumentation 6ES7498-8AA03-8AA0, A5E00069480, April 2002

/SIE 06/ Siemens AG: *SIMATIC, Kommunikation mit Simatic, Systemhandbuch*, September 2006

/SIE 07/ Siemens AG: *SPPA T2000 (TXP) I&C, Refreshing Course*, 2007

/SIE 11/ Siemens AG: *Simatic S7-400, Automatisierungssystem S7-400, Baugruppendaten*, August 2011

/SIE 15/ Siemens AG: *PC-Stationen in Betrieb nehmen - Anleitung und Schnelleinstieg*, Projektierungshandbuch C79000-G8900-C156-17, January 2015

/XIN 08/ L. Xing, S.V. Amari: *Fault Tree Analysis* in K.B. Misra (Editor): *Handbook of Performability Engineering*, ISBN 978-1-84800-130-5, Springer, London, 2008

List of figures

List of tables

Abbreviations

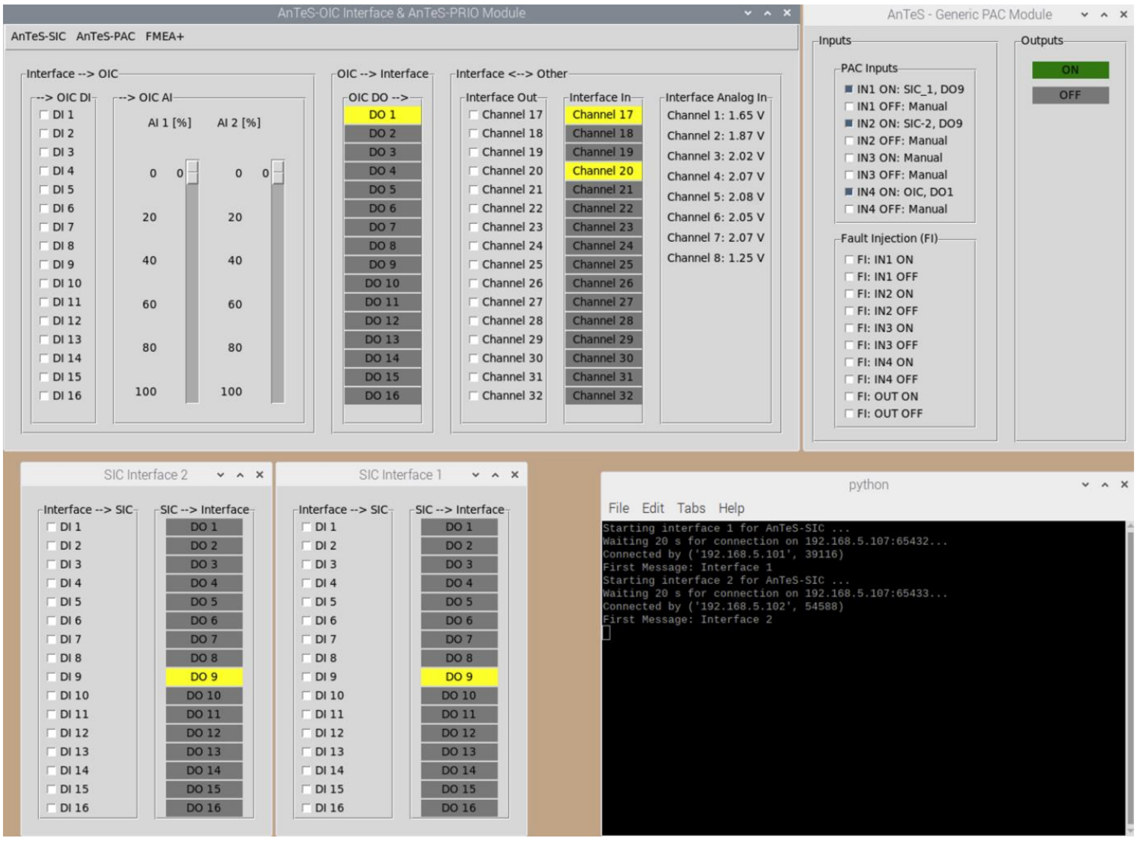
AI	Analog Input (Module)
AD	Analog-to-Digital Converter
AnTeS	Analysis and Test System
APU	Acquisition and Processing Unit
CCF	Common-Cause Failure
CL	Communication Link (Module)
CPLD	Complex Programmable Logic Device
DA	Digital-to-Analog Converter
DI	Digital Input (Module)
DO	Digital Output (Module)
DRPS	Diverse Reactor Protection System
ESFAS	Engineered Safety Features Actuation System
FI	Fault Injection
FMEA	Failure Mode and Effects Analysis
FMEA+	Extended Failure Mode and Effects Analysis
FR	Failure Rate
FTA	Fault Tree Analysis
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit
HMI	Human-Machine Interface
HWBS	Hard-wired Backup System
I&C	Instrumentation and Control (System)
MC	Monte Carlo (Simulation)
MCS	Minimal Cut Sets
NPP	Nuclear Power Plant
OIC	Operational Instrumentation and Control (System)
PAC	Prioritization and Actuation Control (Module)
PLC	Programmable Logic Controller
PM	Processor Module

PRPS	Primary Reactor Protection System
SIC	Safety Instrumentation and Control (System)
SR	Subrack
TXS	Teleperm XS
VU	Voting Unit

A Details on the Extension of AnTeS

A.1 AnTeS Interfaces

As part of the development and commissioning of the AnTeS-OIC-real and AnTeS-PAC-real submodules, GRS created the new interface (subrack) shown in Figure 2.13 and developed software for it. An example view of this software is shown in Figure A 1. Here, binary and analog signals can be exchanged with AnTeS-OIC-real (Siemens Simatic S7), but also signals with other components (e.g., the AV42 of AnTeS-PAC-real). In addition, freely configurable, generic PAC modules (including fault injection) can also be emulated using the software developed for this device (see upper right window in Figure A 1).



Channel 1: 1.65 V
Channel 2: 1.87 V
Channel 3: 2.02 V
Channel 4: 2.07 V
Channel 5: 2.08 V
Channel 6: 2.05 V
Channel 7: 2.07 V
Channel 8: 1.25 V

■ IN1 ON: SIC_1, DO9
□ IN1 OFF: Manual
■ IN2 ON: SIC-2, DO9
□ IN2 OFF: Manual
□ IN3 ON: Manual
□ IN3 OFF: Manual
■ IN4 ON: OIC, DO1
□ IN4 OFF: Manual

```
Starting interface 1 for AnTeS-SIC ...
Waiting 20 s for connection on 192.168.5.107:65432...
Connected by ('192.168.5.101', 39116)
First Message: Interface 1
Starting interface 2 for AnTeS-SIC ...
Waiting 20 s for connection on 192.168.5.107:65433...
Connected by ('192.168.5.102', 54588)
First Message: Interface 2
```

Figure A 1 Software for AnTeS-OIC-real Interface and generic PAC module (screenshot)

For more convenient handling of the other interfaces (to AnTeS-SIC-real, i.e., TXS), it is also possible to connect to and control them directly from the new software (see the two windows in the bottom left-hand area of Figure A 1). In addition, automated FMEA+

analyses can be carried out both with the controlled systems and with the internal generic PAC module (for FMEA+ see Section 4.1). Additional information is output via a console (window at the bottom right of the picture).

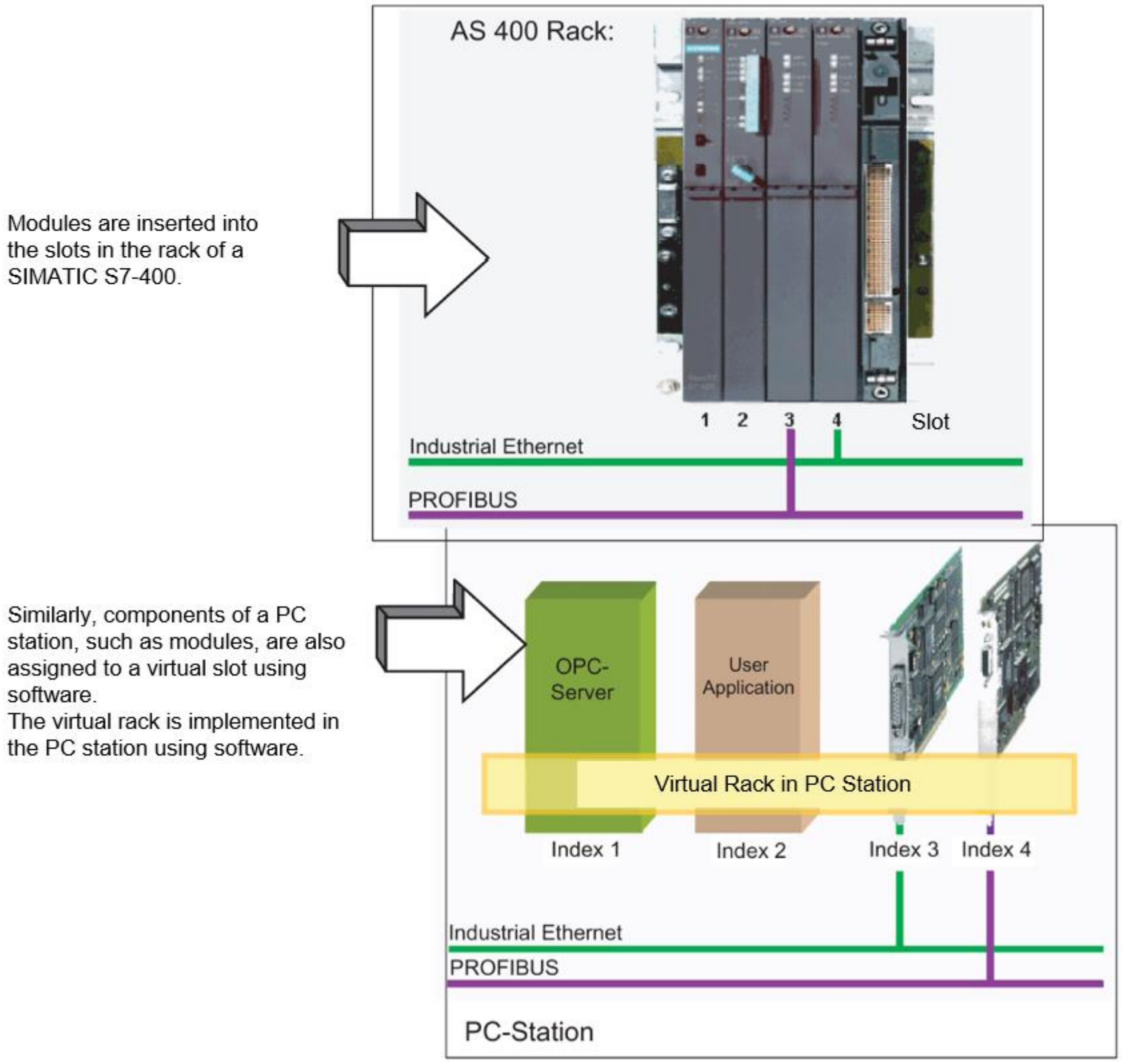
A.2 AnTeS-OIC-real: Installation and Commissioning

The development and commissioning of the AnTeS-OIC-real submodule was a process in which a wide variety of procedures and approaches were tried out. This section describes some of the insights gained but does not claim to be a complete description. In particular, it is not intended to be a substitute for learning courses or manuals. Rather, this section is intended to give an impression of the process and at the same time document important information for internal GRS use on a permanent basis.

The first step of the installation and commissioning was formally the installation of the real OIC (based on components of the Siemens Simatic S7 platform) in a cabinet and the establishment of the power supply[23] (via a 24 V power supply unit in the cabinet). Further installation and commissioning was then carried out largely on the basis of descriptions provided by Siemens /SIE 15/. The engineering (programming) of the system can be carried out from a central engineering station (a standard PC system at GRS), which has been connected to the OIC system via an Ethernet connection.

Two different licensed software suites are available as the engineering environment at GRS: Totally Integrated Automation (TIA Portal) V13 and V16. The versions differ mainly in their range of functions and support for older devices. TIA Portal enables complete access to the entire digitized automation system, from digital planning and integrated engineering to transparent operation.

[23] In fact, tests were carried out in advance in a separate subrack, and the system was repositioned within the cabinet even after the initial installation. At this and subsequent points in this section, no further reference is made to possible intermediate steps and tests.

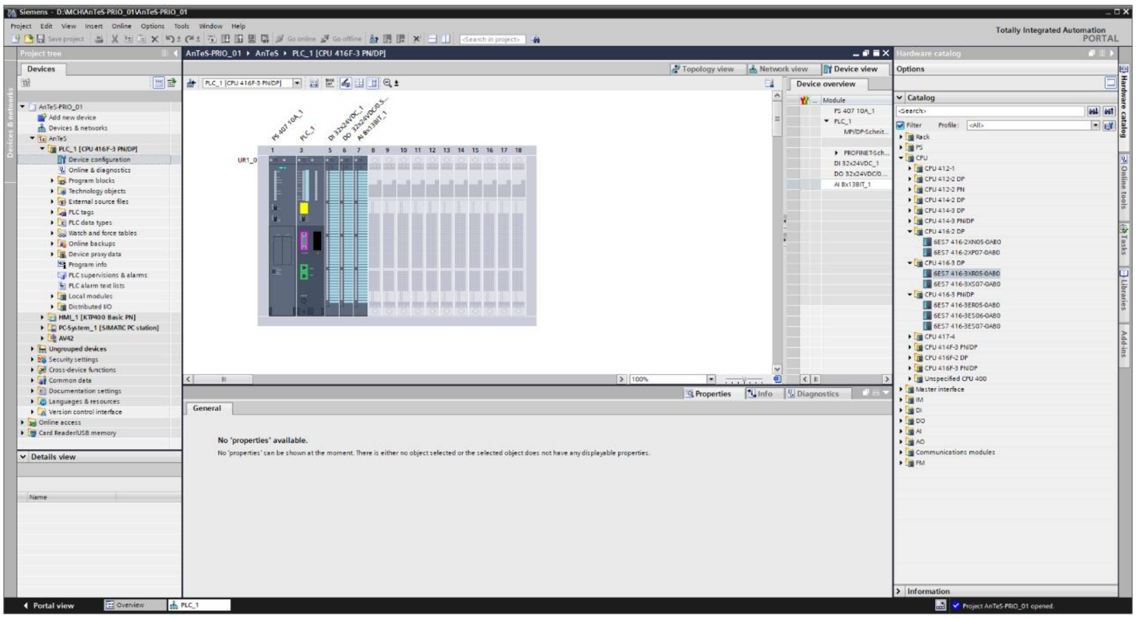


AS 400 Rack:
Modules are inserted into the slots in the rack of a SIMATIC S7-400.
1
2
3
4
Slot
Industrial Ethernet
PROFIBUS
Similarly, components of a PC station, such as modules, are also assigned to a virtual slot using software.
The virtual rack is implemented in the PC station using software.
OPC-Server
User Application
Virtual Rack in PC Station
Index 1
Index 2
Index 3
Index 4
Industrial Ethernet
PROFIBUS
PC-Station

Figure A 2 Structure and engineering within the Siemens Simatic S7 platform (schematic, simplified).

The original image is from /SIE 15/ but has been captioned in English for this report.

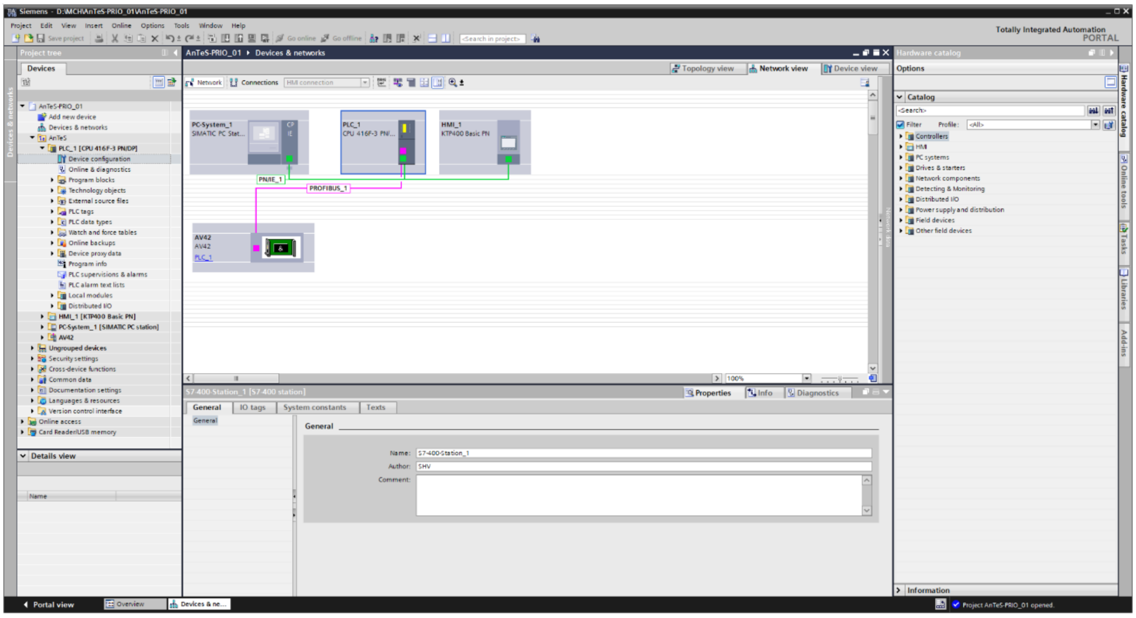
The two illustrations below give an impression of the TIA Portal engineering environment. The so-called device view can be seen centrally in Figure A 3 and the network view in Figure A 4.



No 'properties' available.

No 'properties' can be shown at the moment. There is either no object selected or the selected object does not have any displayable properties.

Figure A 3 Device view in TIA Portal



S7-400-Station_1 [S7-400 station]

General

Name: S7-400-Station_1
Author: SHV
Comment:

Figure A 4 Network view in TIA Portal

For documentation purposes, all Simatic S7 components used for AnTeS-OIC-real are listed below[24], as they can also be found in the TIA Portal hardware catalog, for example:

[24] A second subrack with slightly different components is available at GRS, but the ones listed here correspond to the standard configuration of AnTeS-OIC-real.

- PS 407 10A
  - Power supply module
  - Article number: 6ES7 407-0KA02-0AA0
  - Slot: 1&2
- CPU 416F-3 PN/DP
  - Processor (CPU) module
  - Article number: 6ES7 416-3FR05-0AB0
  - Firmware: V5.3
  - Slot: 3&4
- DI 32x24VDC
  - Digital (“binary”) input module, 32 channels
  - Article number: 6ES7 421-1BL01-0AA0
  - Slot: 5
- DO 32x24VDC/0.5A
  - Digital (“binary”) output module, 32 channels
  - Article number: 6ES7 422-1BL00-0AA0
  - Slot: 6
- AI 8x13BIT
  - Analog input module, 8 channels, 13-bit resolution for reading and digitizing
  - Article number:6ES7 431-1KF00-0AB0
  - Slot: 7

In principle, engineering can be carried out for the OIC with TIA Portal in the same way as with SPACE for SIC. However, as a more modern system, TIA Portal has many additional options that are best learned by attending special courses from Siemens. At this point, it is only explicitly pointed out that it is essential to familiarize oneself with the principle of “process images” within SIMATIC-S7 in order to learn.

A.3 AnTeS-PAC-real: Installation and Commissioning

A.3.1 AV42 PAC Module

While the commissioning of AnTeS-OIC-real was comparatively unproblematic and could therefore be outlined briefly in the previous section, the commissioning of AV42 (a PAC module of AnTeS-PAC-real) was much more challenging. This section also serves as documentation within GRS.

The AV42 module (manufacturer Framatome, formerly Areva) is intended for controlling and monitoring safety-relevant actuators that respond to commands from both SIC and OIC systems. The AV42 has the task of prioritizing the commands from the SIC over the commands from the OIC system /ARE 17/. It can control and monitor drives in a nuclear power plant either alone or in combination with other PAC modules (e.g., SPLM1-PC11), whereby one AV42 module is assigned to one drive.

The control and monitoring of drives by AV42 includes the following tasks:

- Control of a drive from several operating stations (e.g., control room, front panel of the AV42)
- Generation of a higher priority for commands from SIC systems than commands from OIC systems
- Generation of actuation commands (output signals)
- Generation of feedback signals to the I&C (e.g., SIC, OIC, control room)
- Command abort on request (e.g., torque protection for drives, end position feedback)

The AV42 module can be used for the following actuators:

- Solenoid valves
- Continuous drives (e.g., pump motor)
- Actuators (e.g., isolation valves, butterfly valves)
- Servo drives (e.g., control valves)

The operating mode can be set via firmware parameters for this purpose. The electrical connections of the AV42 are usually implemented in the corresponding subrack as basic wiring (wire-wrap connections). The wiring also takes into account the position of the

AV42 modules in the module rack, the bus address for Profibus DP, the operating mode, and other settings (parameterization via wiring) /ARE 07/.

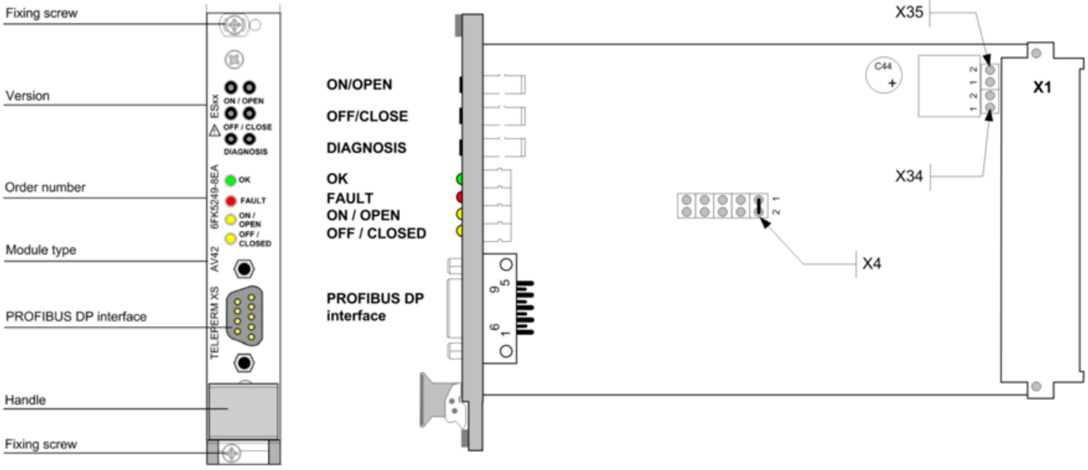


Figure A 5 Operating elements, interface, and jumpers of the AV42 /ARE 17/

Figure A 5 shows the front and side view of an AV42. All I/O signals and the module's power supply are routed out of the module rack via the rear X1 connector, with Profibus network communication taking place via the interface on the front panel.

The module contains the following internal jumpers:

- Jumper X4: This jumper must be plugged in (factory setting of jumper X4: 1-2).
- Jumper X34: To prevent open-circuit monitoring from responding, a jumper plug must be inserted in position 1-2 of jumper socket X34 at the unused command output CMDOFF (pin Z20).
- Jumper X35: To prevent the open-circuit monitoring from responding, a jumper plug must be inserted in position 1-2 of the jumper socket X35 at the unused command output CMDON (pin Z20).

Simulation commands (ON/OFF/Diagnosis) can be activated via a coding plug on the front panel. The AV42 module can and should be connected to a Profibus DP network via the Profibus interface on the front panel. This interface is also used for further parameterization (configuration) of the module. In addition, a functioning Profibus connection is also required for basic, error-free operation.

The connection of the AV42 to AnTeS-OIC-real (Simatic S7) is therefore described in more detail below.

The manufacturer of the AV42 module (Framatome, formerly AREVA) has provided the following files required for the integration of the module into the Simatic S7 platform:

- siem80bd.gsd
    - GSD file of the AV42
    - GSD ("General Station Description") files are ASCII files with a series of standardized keywords that uniquely describe certain attributes of a DP[25] slave devices /IEC 03/
- AV42test.pbp
    - The PBP ("Profibus Periphery") data files are related to Siemens Profibus. The PBP file is a Profibus ASCII Exported Data and allowing the user to configure masters and slaves).

After installation of the GSD file, the AV42 module is available in the TIA Portal hardware catalog and can be inserted into projects by drag and drop. As long as the service unit is not reinstalled, AV42 modules are already permanently available within the TIA Portal hardware catalog.

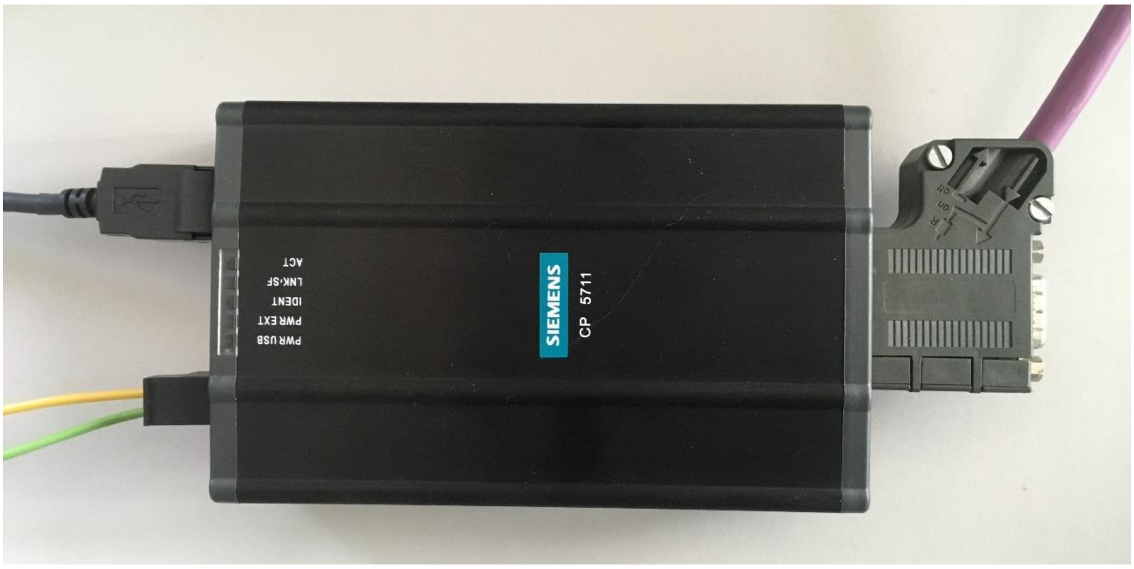
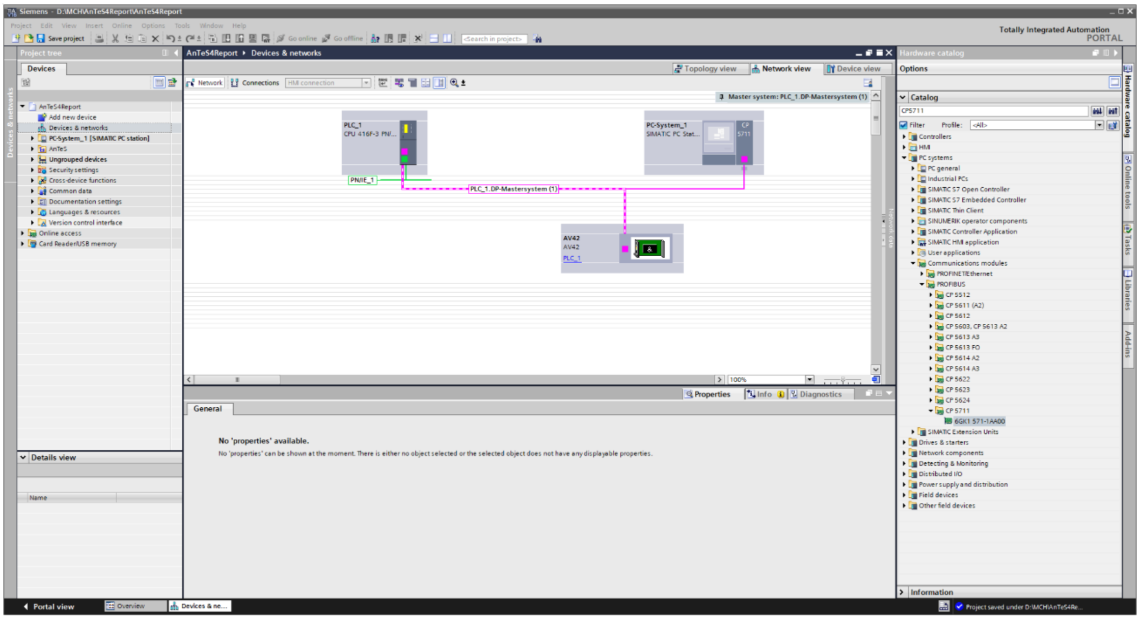


Figure A 6 CP 5711 module for Profibus communication

For communication between the programming device (service unit including TIA Portal) and the AV42 module, a CP 5711 module (Profibus communication processor, Figure A 6) from the hardware catalog must be added to the project within TIA Portal (as this

[25] "Distributed Periphery" (Profibus)

module is available for AnTeS-OIC-real at GRS). By adding the CP 5711 module, a PC system is automatically integrated into the project (within TIA Portal). It must be ensured that “DP master class 2” is set as the operating mode for the CP 5711 module (in TIA Portal). Once an AV42 module to be controlled has also been added to the project in TIA Portal, the Profibus connections can be specified in the network view of TIA Portal (Figure A 7).



Siemens - D:\MCH\AnTeS4Report\AnTeS4Report

No 'properties' available.

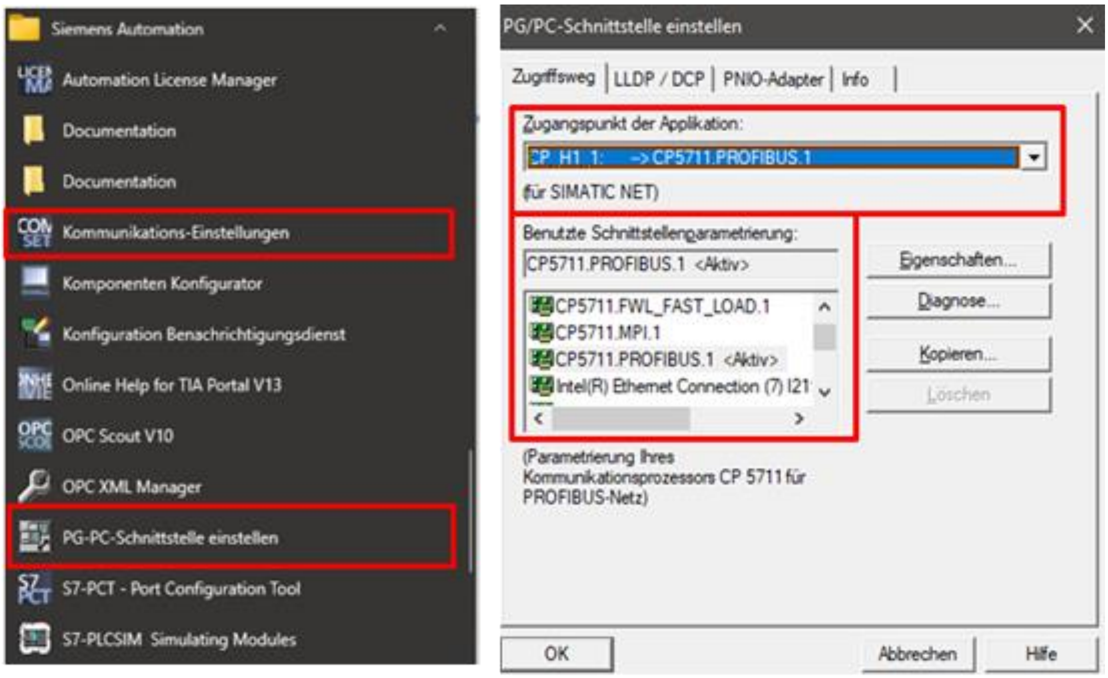
No 'properties' can be shown at the moment. There is either no object selected or the selected object does not have any displayable properties.

Project saved under D:\MCH\AnTeS4Re...

Figure A 7 Network view of TIA Portal with PLC (OIC), service unit (PC system), and AV42 module connected via Profibus

To carry the configuration of the AV42 module (e.g., operating mode) using the AV42 Configuration Tool (Software from AREVA, Figure A 9), the settings shown in Figure A 8 are necessary[26] (hint: alternatively also possible via communication settings in TIA Portal)

[26] This was only necessary once and only needs to be carried out again when the service unit is re-installed.


Siemens Automation
Automation License Manager
Documentation
Documentation
Kommunikations-Einstellungen
Komponenten Konfigurator
Konfiguration Benachrichtigungsdienst
Online Help for TIA Portal V13
OPC Scout V10
OPC XML Manager
PG-PC-Schnittstelle einstellen
S7-PCT - Port Configuration Tool
S7-PLCSIM Simulating Modules
PG/PC-Schnittstelle einstellen
Zugriffsweg
LLDP / DCP
PNIO-Adapter
Info
Eigenschaften...
Diagnose...
Kopieren...
Löschen
OK
Abbrechen
Hilfe

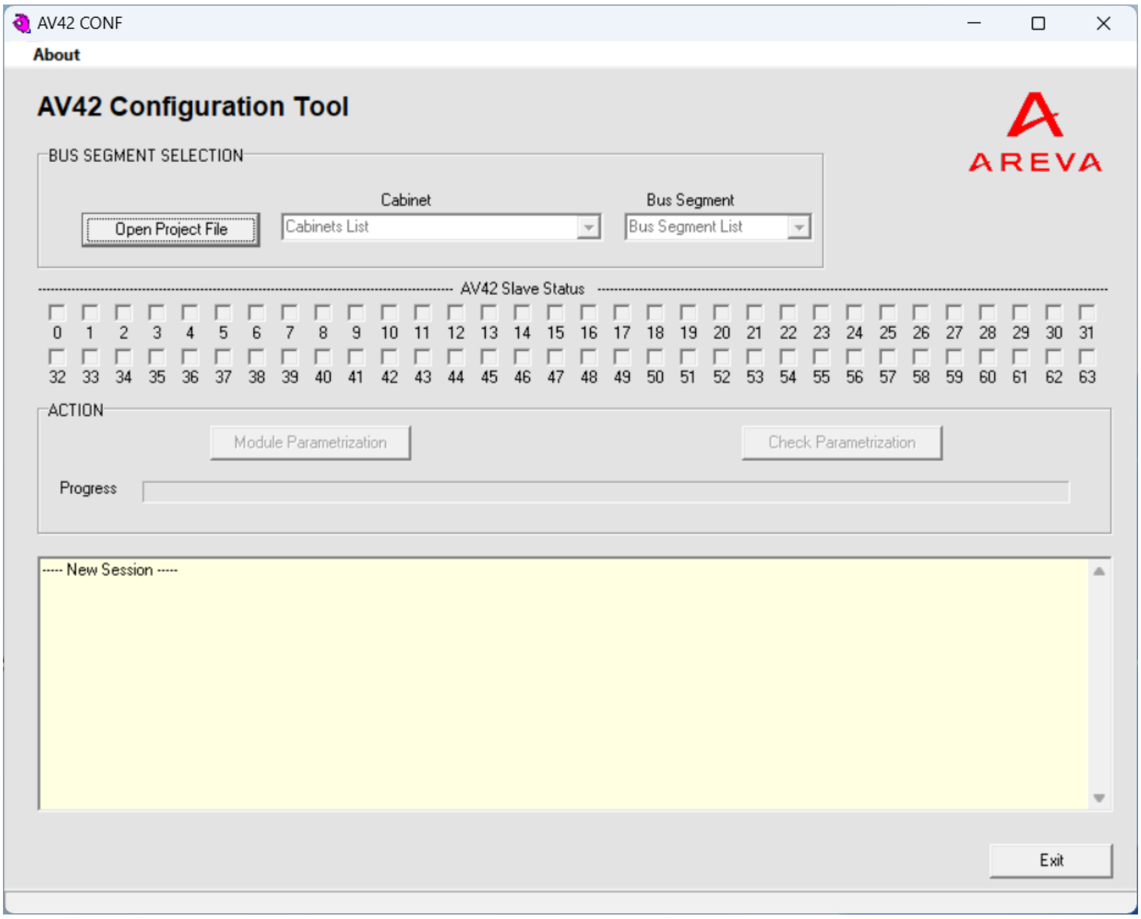
Zugangspunkt der Applikation:
CP_H1_1: --> CP5711.PROFIBUS.1
(für SIMATIC NET)

Benutzte Schnittstellenparametrierung:
CP5711.PROFIBUS.1 <Aktiv>

CP5711.FWL_FAST_LOAD.1
CP5711.MPI.1
CP5711.PROFIBUS.1 <Aktiv>
Intel(R) Ethernet Connection (7) I21

(Parametrierung Ihres Kommunikationsprozessors CP 5711 für PROFIBUS-Netz)

Figure A 8 PG/PC interface settings and how to access them in the Windows Start menu (left-hand side)



---- New Session ----

Figure A 9 AREVA AV42 Configuration Tool

One possible way to configure an AV42 module is listed here:

- Press “Check Parametrization” button, the parameters of the connected AV42 are then compared with the parameters of the corresponding configuration file (PBP file, see above).
- Parameters for which a discrepancy between the connected AV42 and the PBP file is detected are displayed in the text field (of the AV42 Configuration Tool).
- When the “Module Parameterization” button is pressed, the parameters of the AV42 are overwritten with those from the PBP file (confirmed in the text field)
- When the “Check Parametrization” button is pressed again, no more errors should be displayed, as the parameters of the parameterized AV42 and the PBP file match

In July 2023, GRS received a test subrack for AV42 modules (see Figure 2.12) as a permanent loan from the manufacturer (Framatome). After checking the functionality of the test subrack using the documentation supplied by Framatome (/ARE 07/, /ARE 17/), it was decided to use this subrack for the expansion of AnTeS.

A.3.2 SPLM1-PC11 PAC Module

As only AV42 PAC modules (or generic PAC modules based on them) were used in this project (within AnTeS-PAC-real), the SPLM1-PC11 modules also available at GRS are only presented here in very brief form. SPLM1-PC11 modules serve as an option for the diverse prioritization and actuation of safety-relevant drives. For this, they typically cooperate with an AV42 modules (Figure A 10) /ARE 11/.

An SPLM1-PC11 module detects and processes signals from the safety I&C system, feedback signals from the controlled device (actuator), and ON/OPEN or OFF/CLOSE commands from the connected AV42 module. Alternatively, the SPLM1-PC11 can also process signals directly from control panels (after an explicit switchover).

As a result of the processing, the SPLM1-PC11 issues commands to the controlled device, feedback signals to the safety I&C system, and feedback signals to control panels.

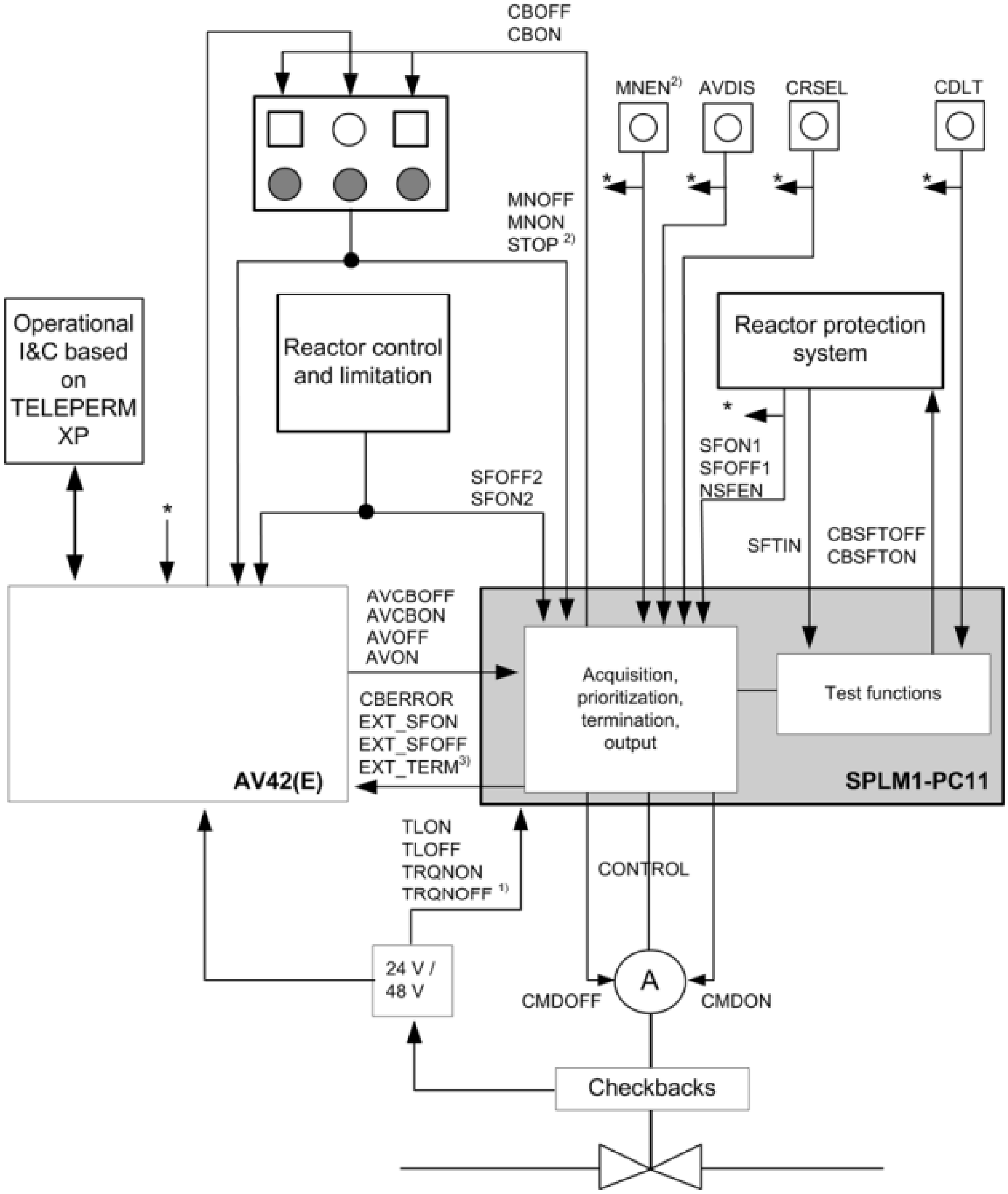
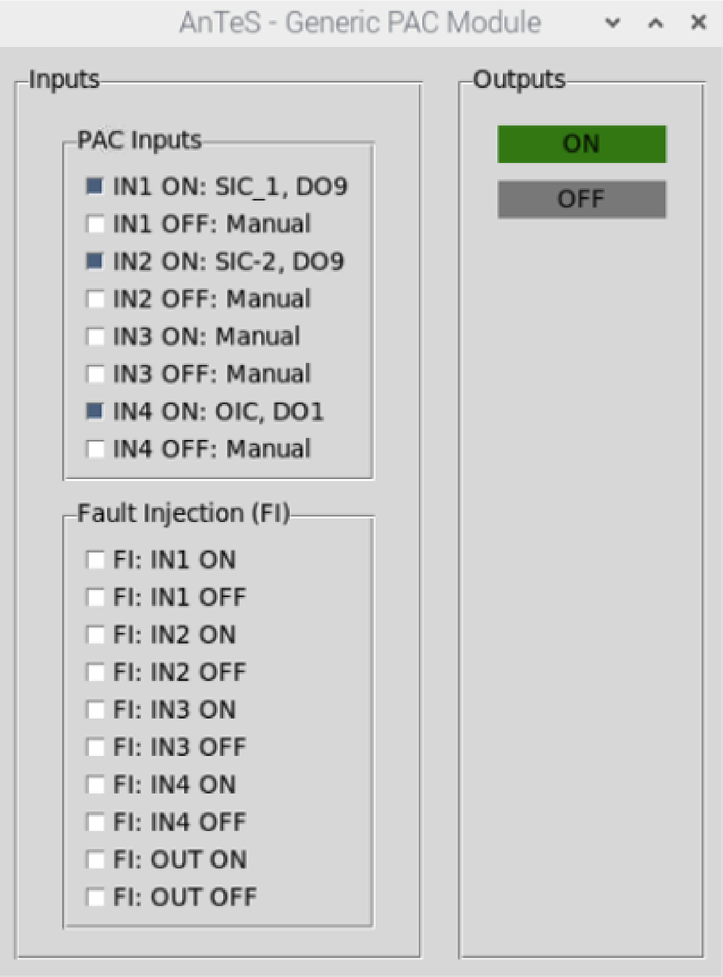


Figure A 10 SPLM1-PC11 module cooperating with an AV42 module

This image was taken from /ARE 11/.

A.3.3 Generic PAC Module

The generic PAC module of GRS as part of AnTeS-PAC-real was developed on the basis of the behavior of AV42 modules and implemented on specially designed hardware (compare also Section 4.4). At this point, this (freely configurable) module, including the possibility of fault injection, is only shown as a screenshot in Figure A 11.



AnTeS - Generic PAC Module

Inputs

PAC Inputs

- ■ IN1 ON: SIC_1, DO9
- □ IN1 OFF: Manual
- ■ IN2 ON: SIC-2, DO9
- □ IN2 OFF: Manual
- □ IN3 ON: Manual
- □ IN3 OFF: Manual
- ■ IN4 ON: OIC, DO1
- □ IN4 OFF: Manual

Fault Injection (FI)

- □ FI: IN1 ON
- □ FI: IN1 OFF
- □ FI: IN2 ON
- □ FI: IN2 OFF
- □ FI: IN3 ON
- □ FI: IN3 OFF
- □ FI: IN4 ON
- □ FI: IN4 OFF
- □ FI: OUT ON
- □ FI: OUT OFF

Outputs

Figure A 11 AnTeS-PAC-real: generic PAC module

B All Model Systems

B.1 Model System A1B1C1P1 (Base Case)

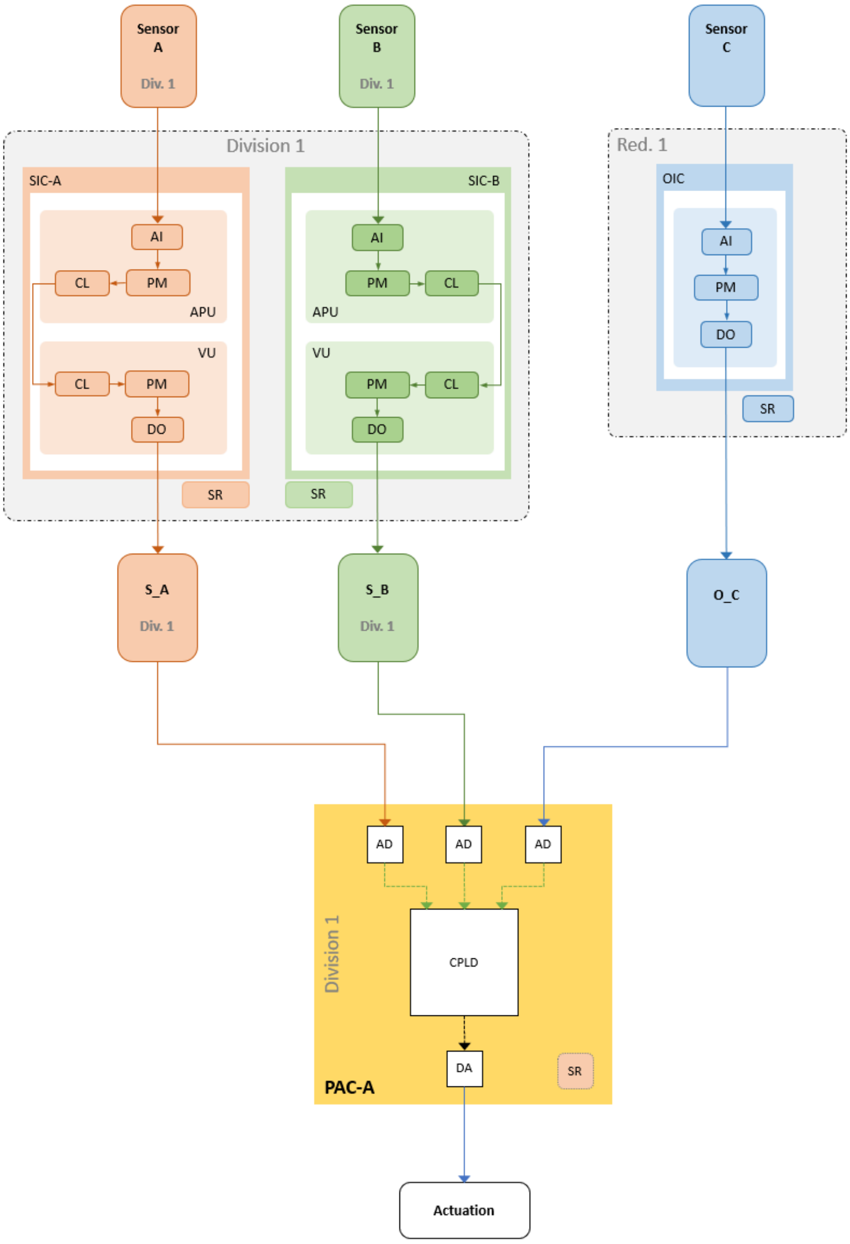


Figure B 1 Model system A1B1C1P1

B.2 Model System A1B0C0P1

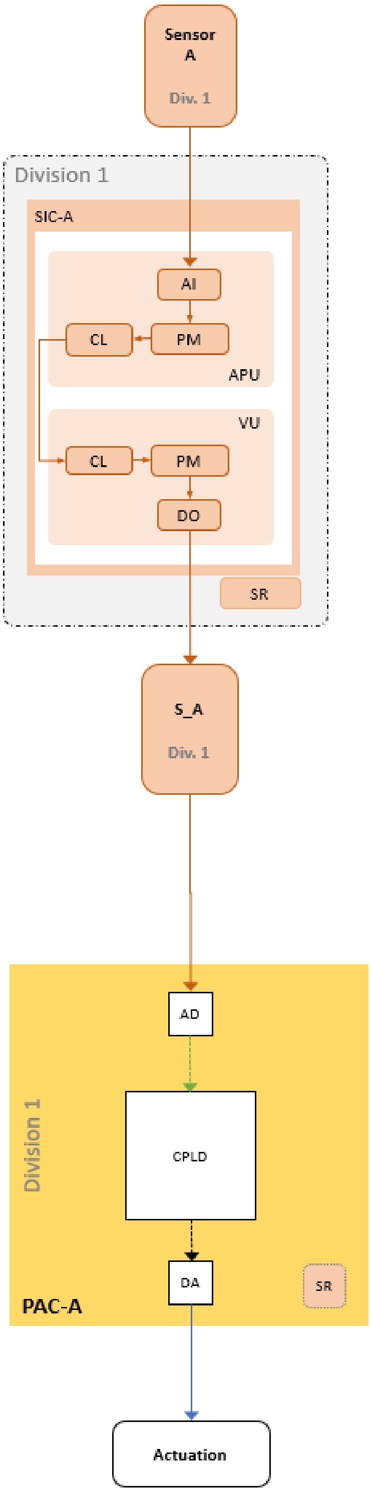


Figure B 2 Model system A1B0C0P1

B.3 Model System A2B0C0P2

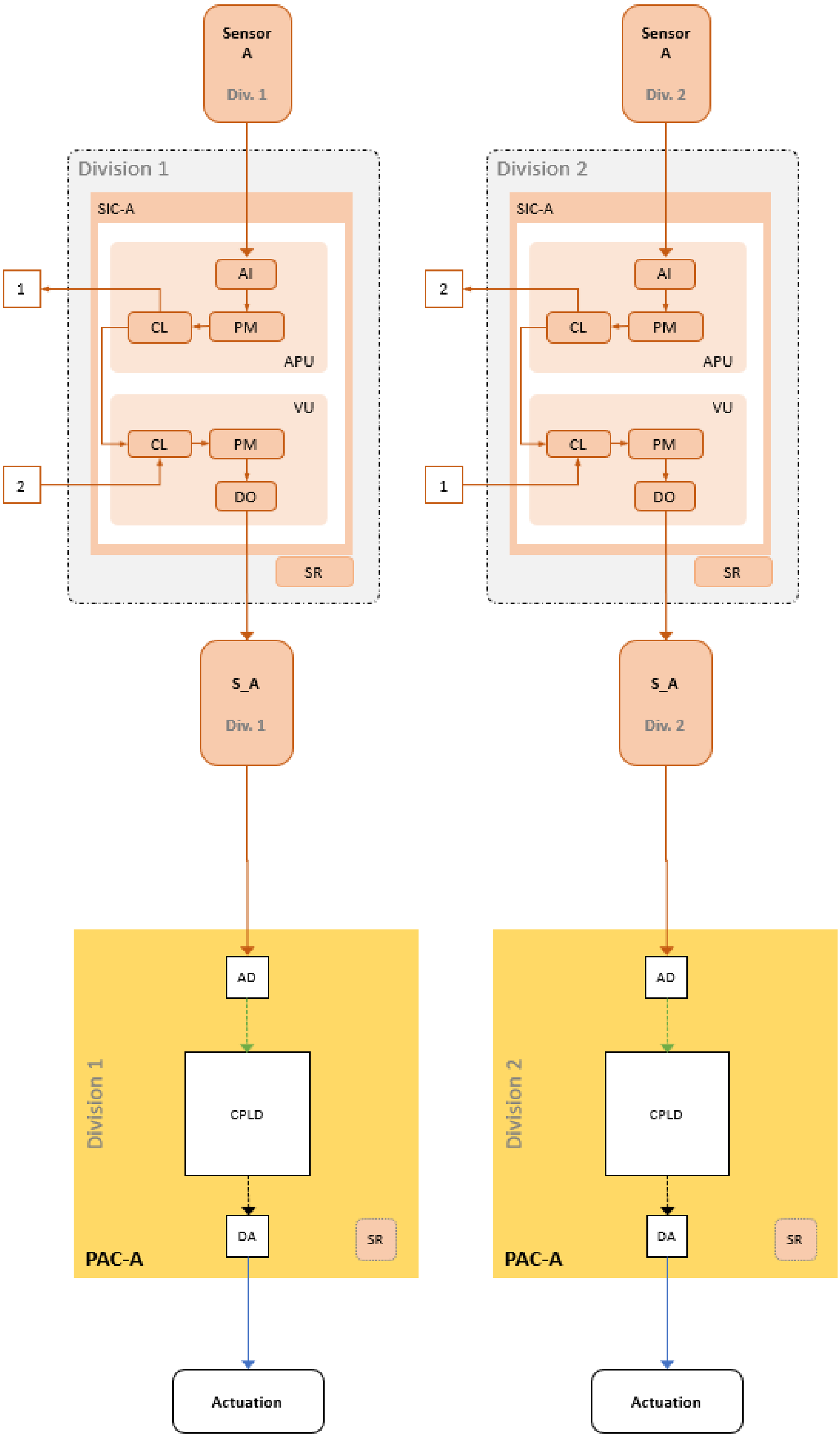


Figure B 3 Model system A2B0C0P2

B.4 Model System A3B0C0P3

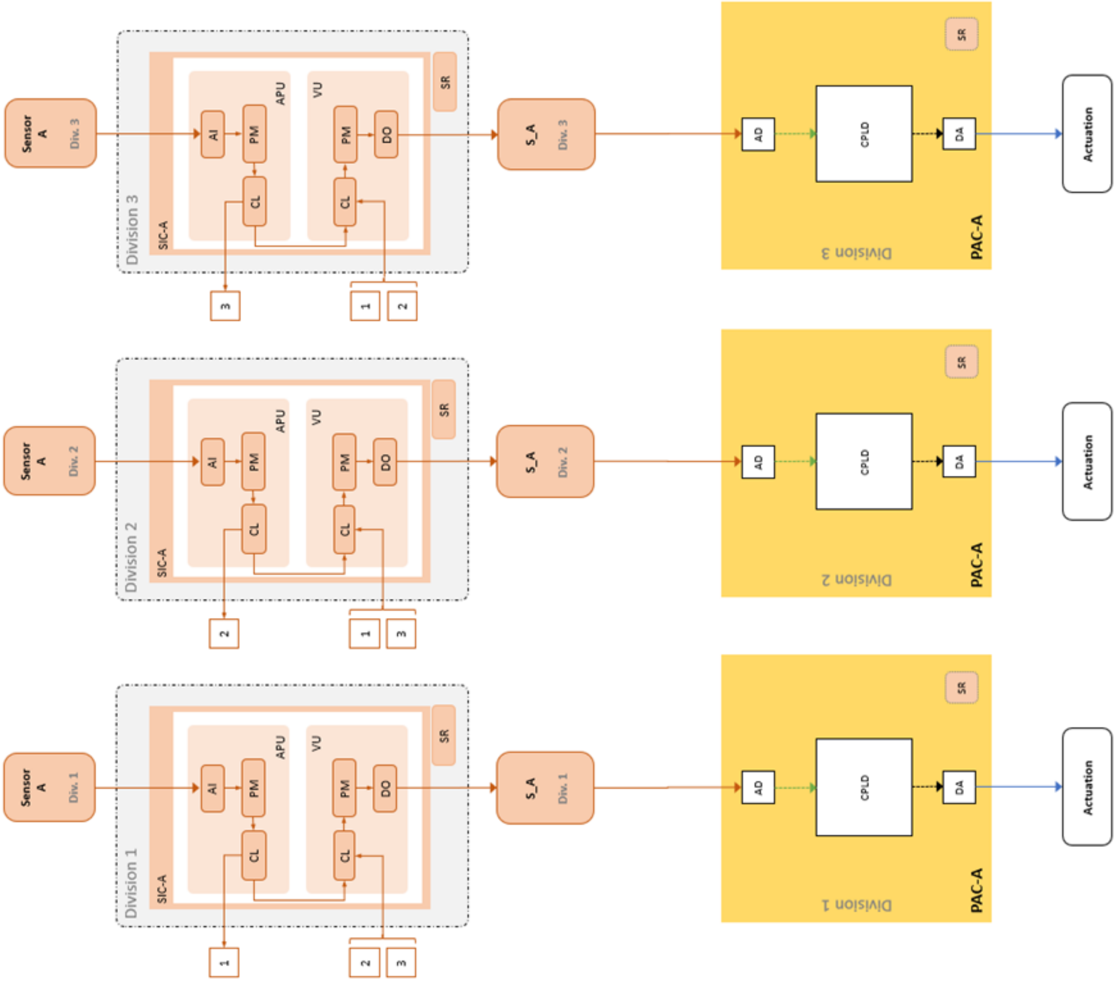


Figure B 4 Model system A3B0C0P3

B.5 Model System A4B0C0P4

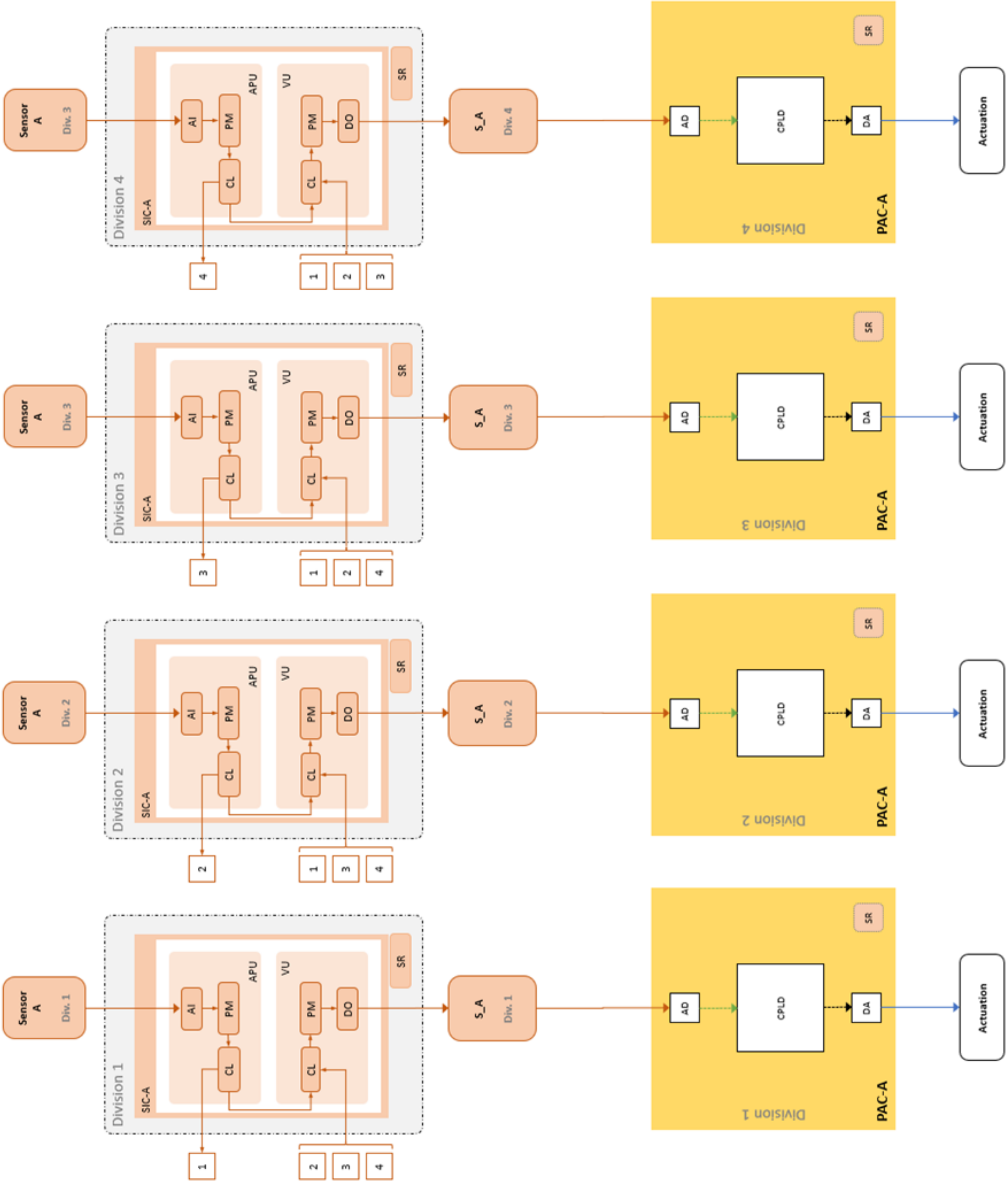


Figure B 5 Model system A4B0C0P4

B.6 Model System A4B0C0P2-2

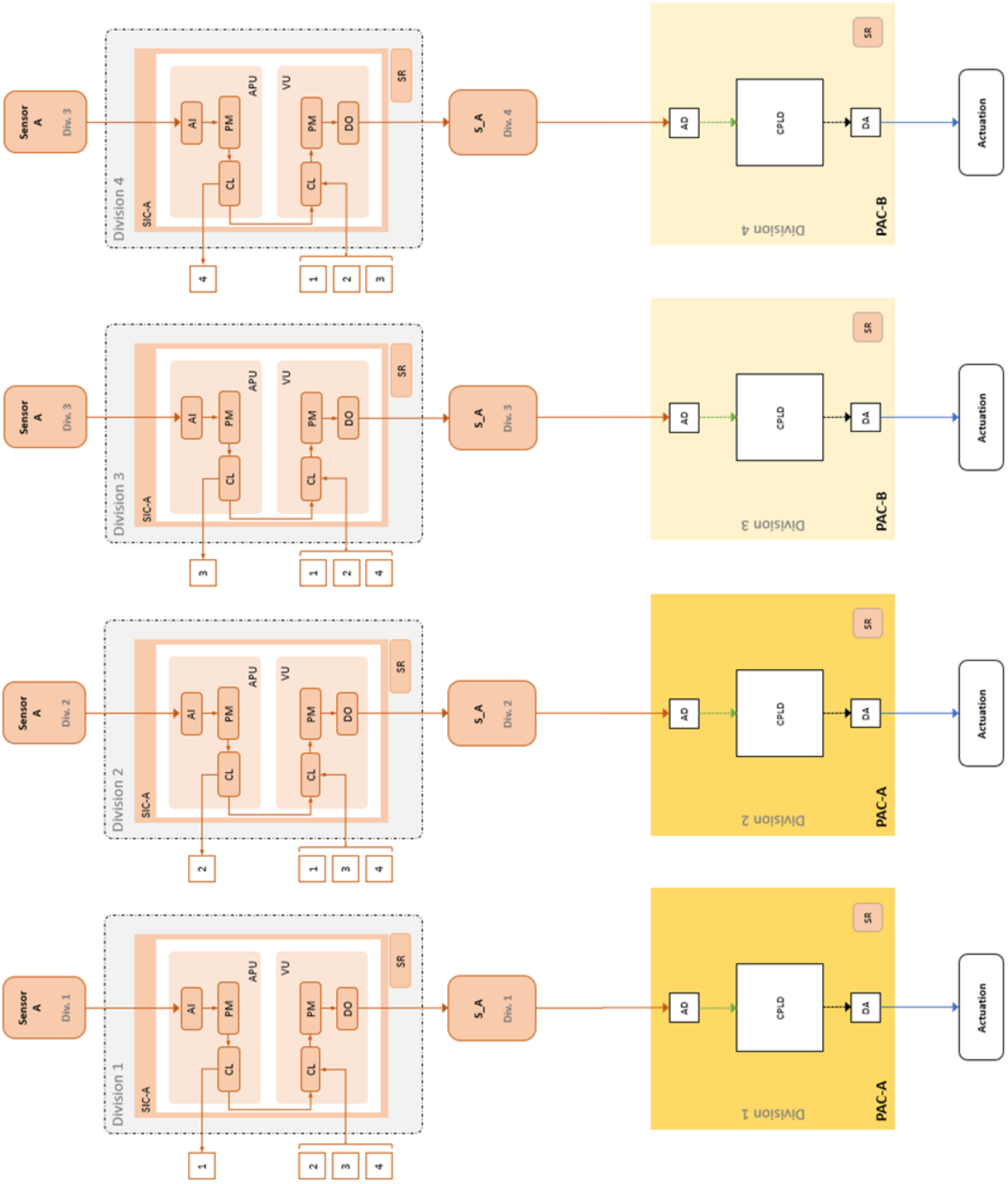


Figure B 6 Model system A4B0C0P2-2

B.7 Model System A1B0C1P1

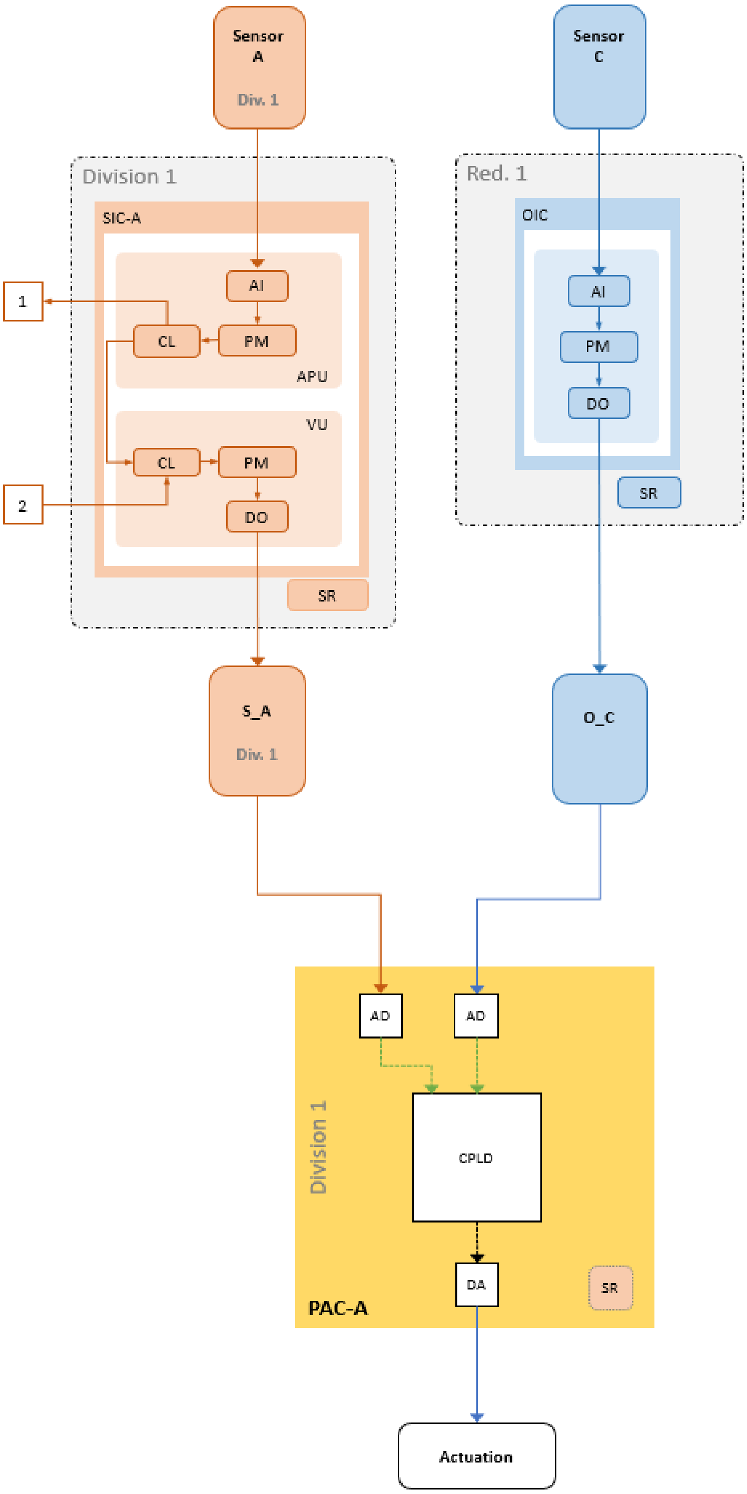


Figure B 7 Model system A1B0C1P1

B.8 Model System A2B0C1P2

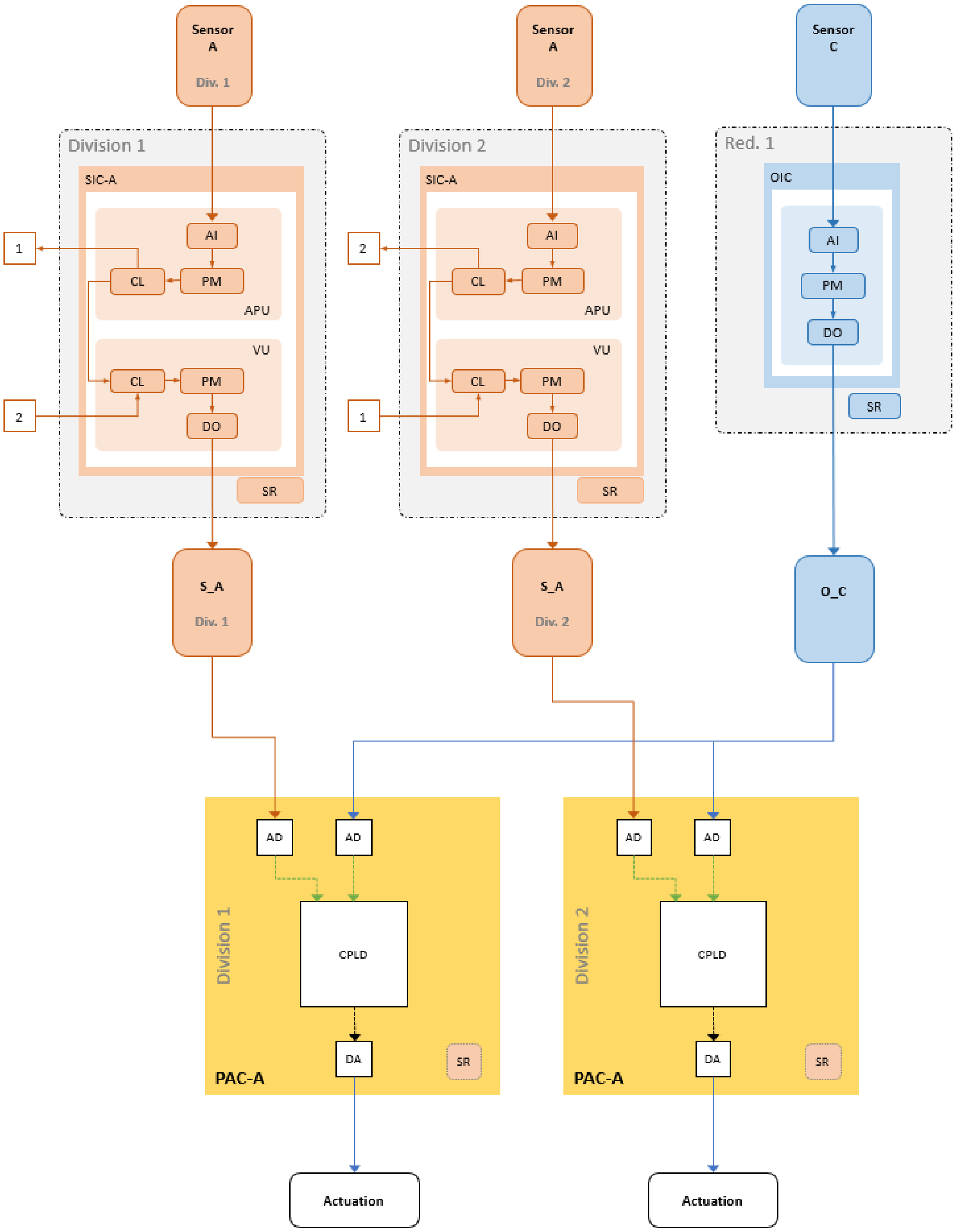


Figure B 8 Model system A2B0C1P2

B.9 Model System A3B0C1P3

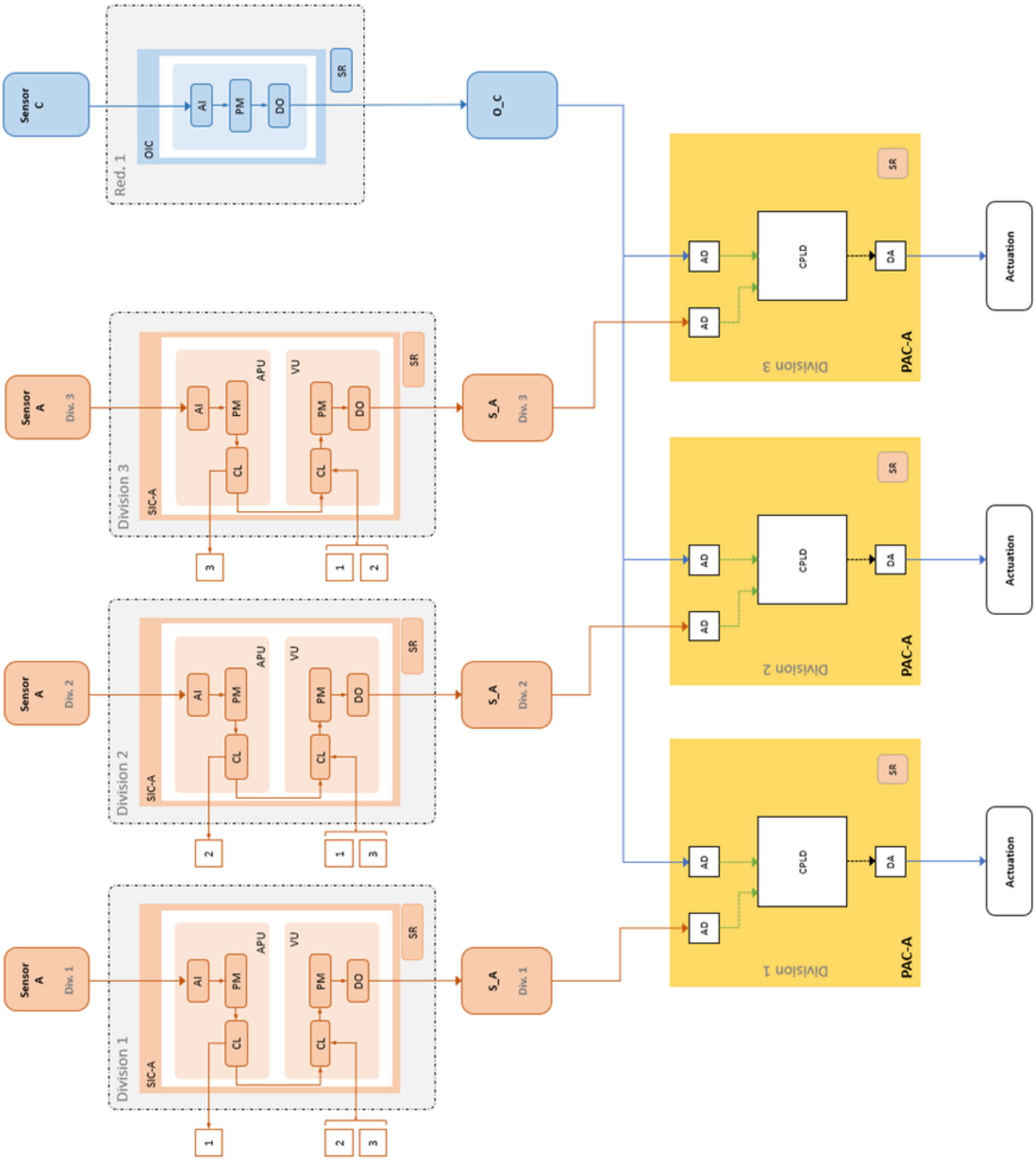


Figure B 9 Model system A3B0C1P3

B.10 Model System A4B0C1P4

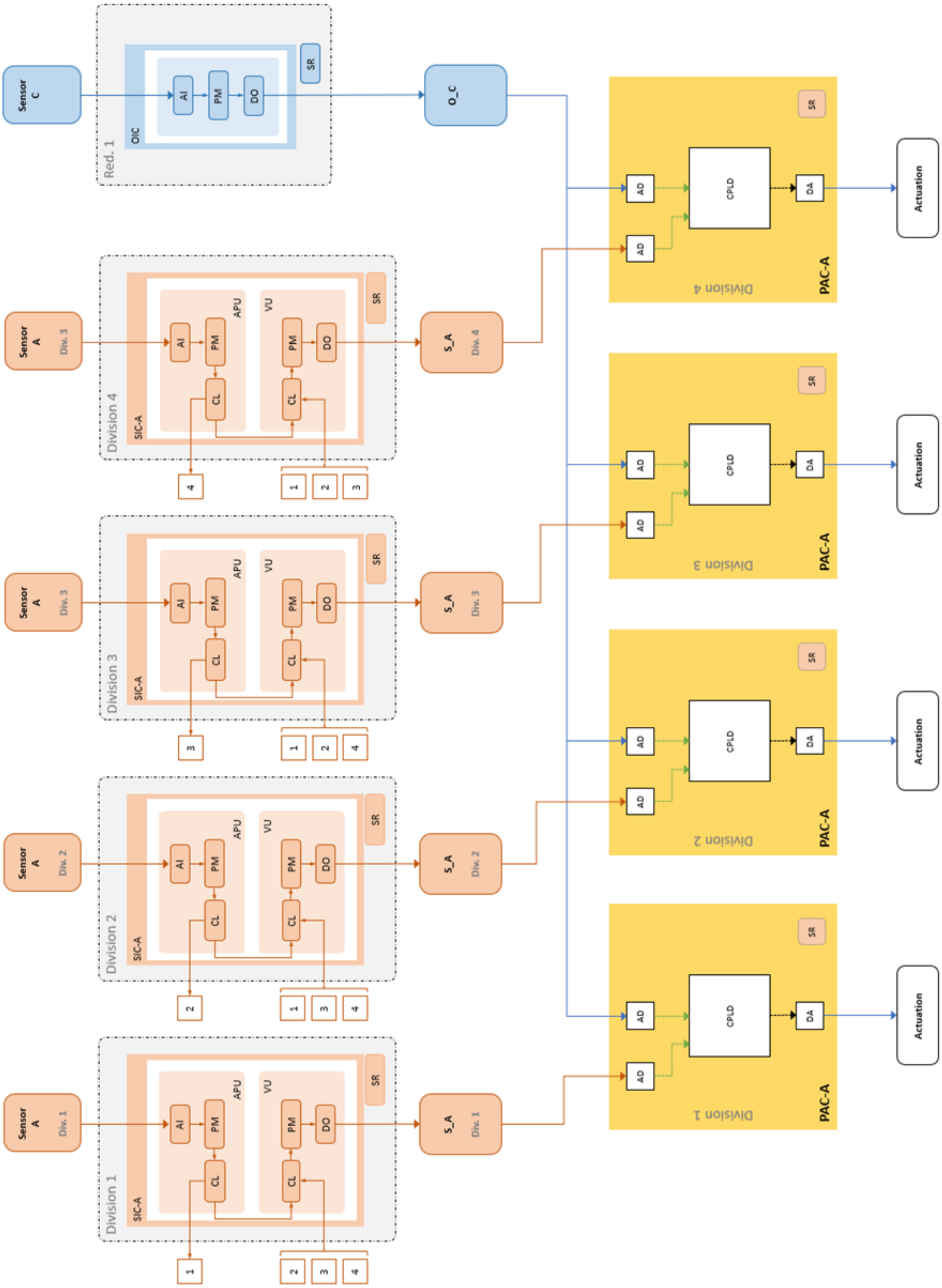


Figure B 10 Model system A4B0C1P4

B.11 Model System A4B0C1P2-2

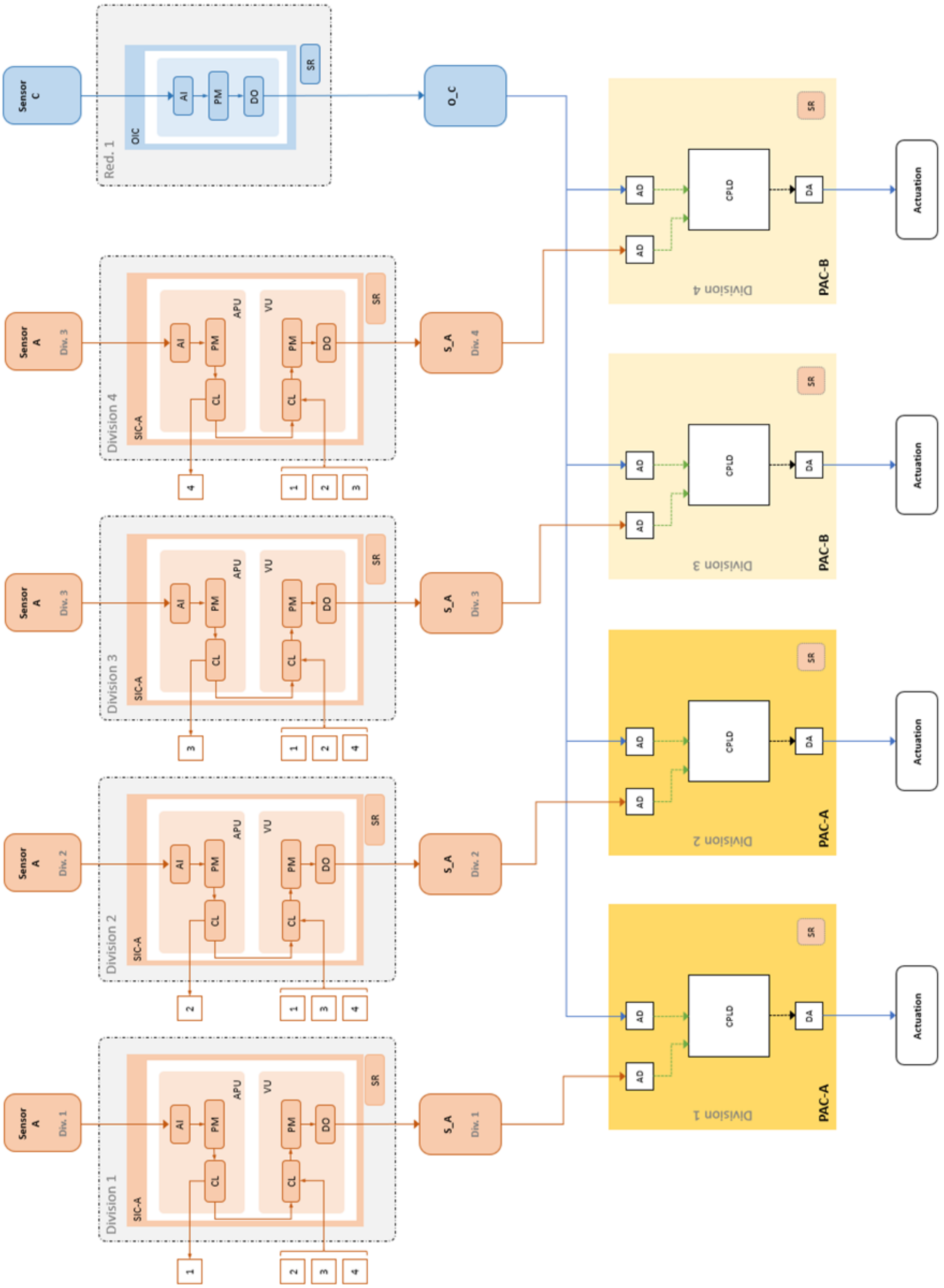


Figure B 11 Model system A4B0C1P2-2

B.12 Model System A4B4C0P2-2

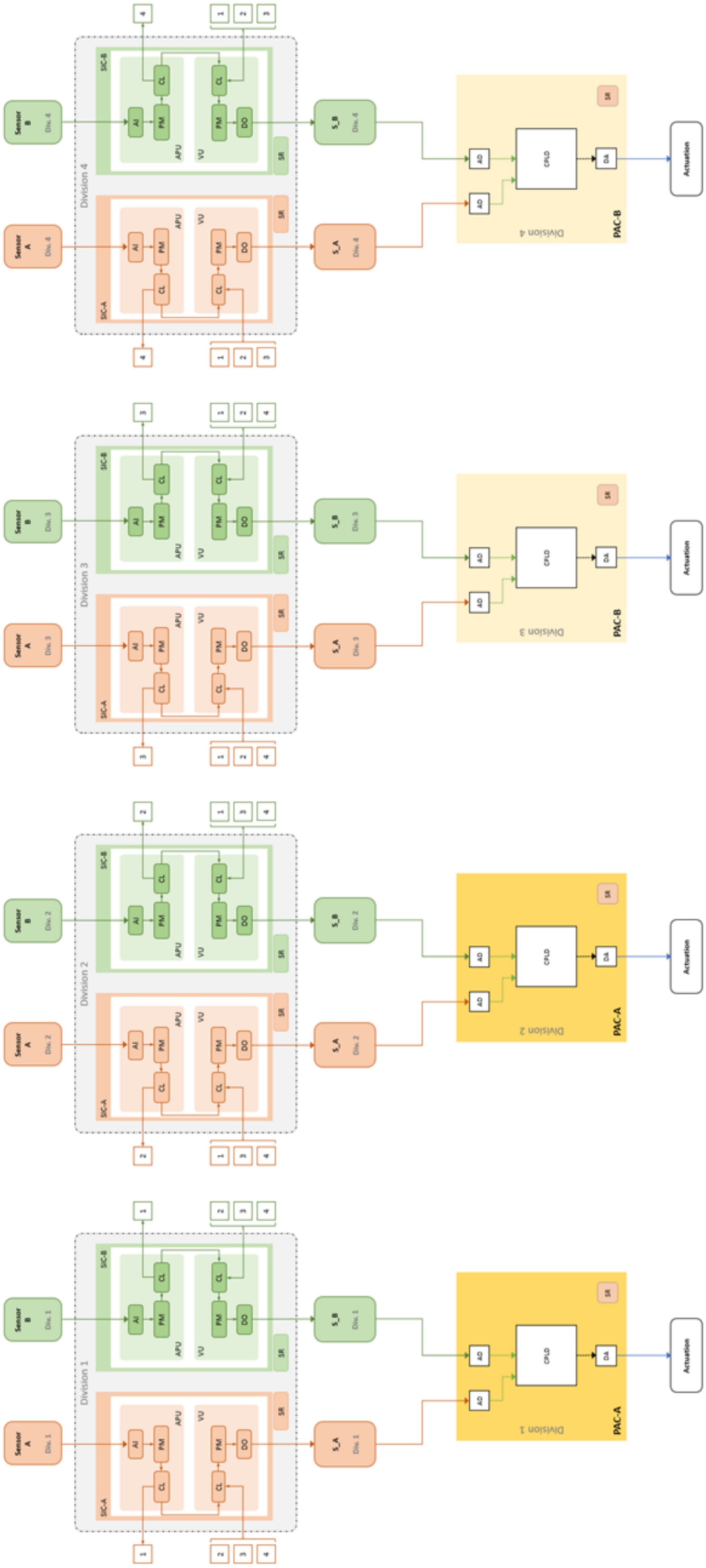


Figure B 12 Model system A4B4C0P2-2

B.13 Model System A4B4C1P2-2

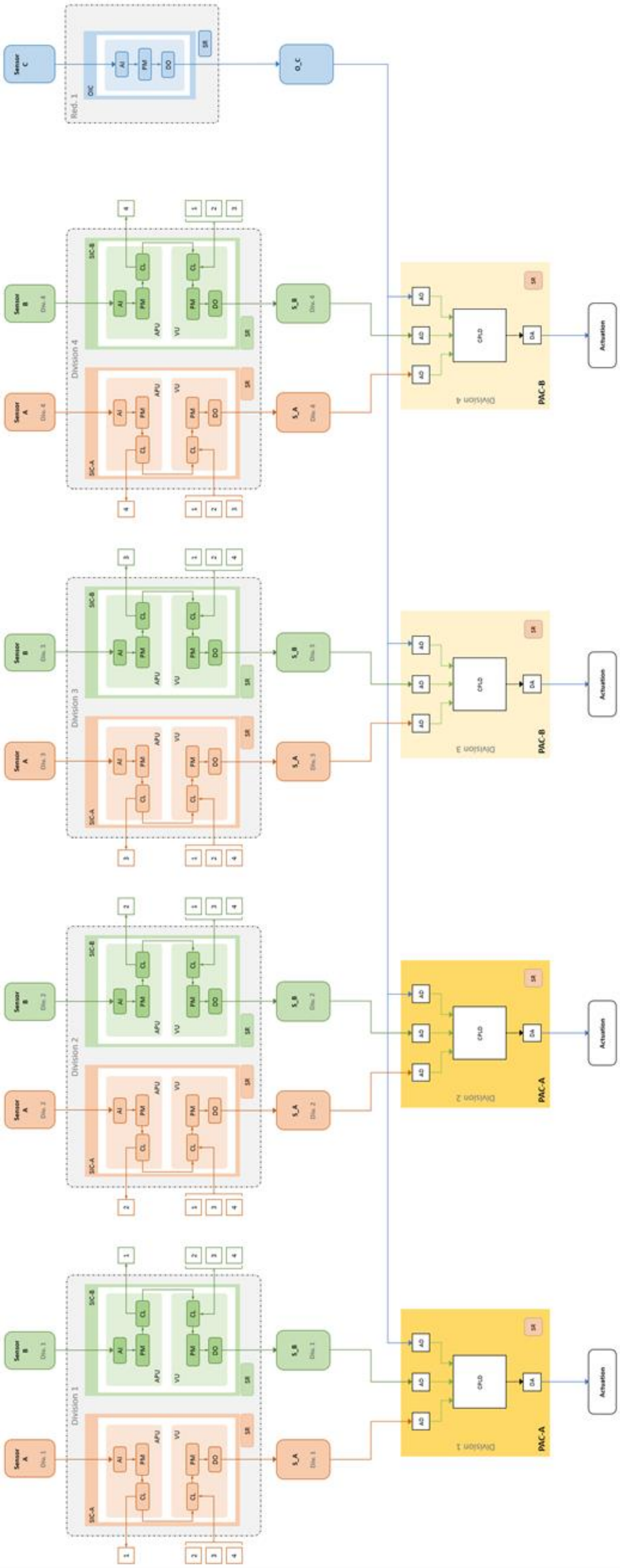
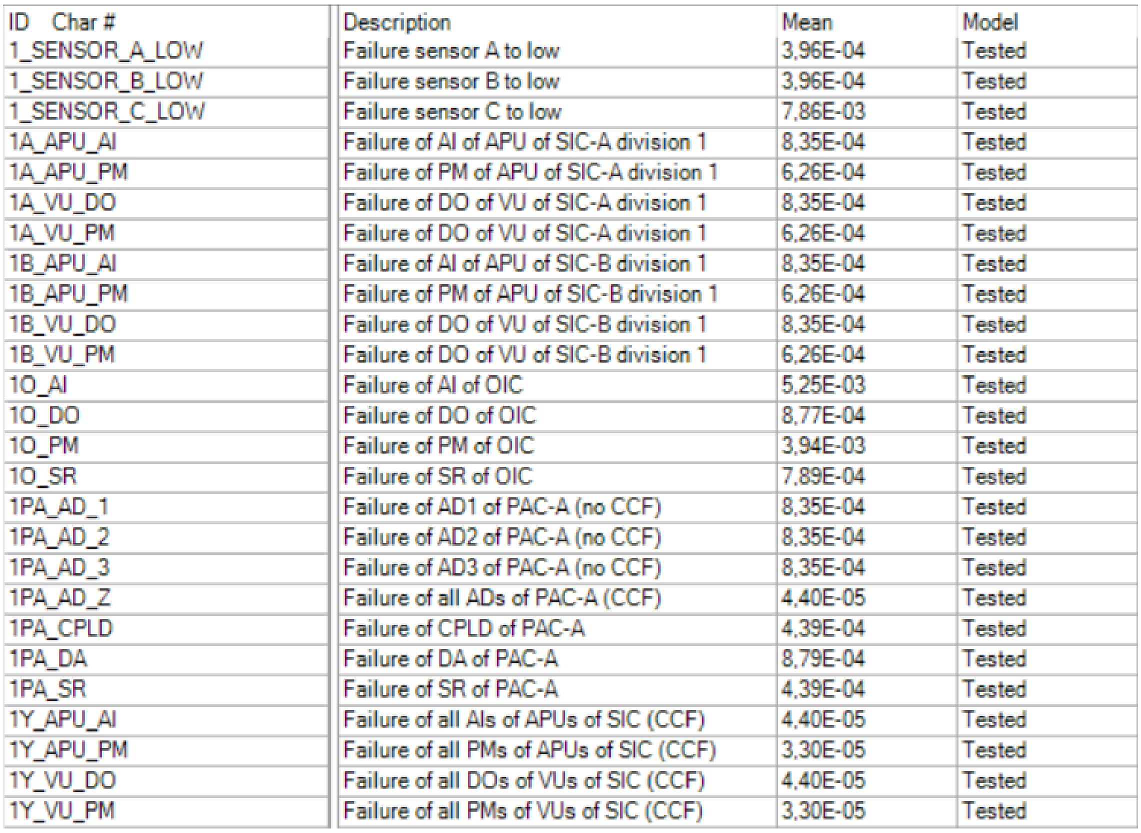


Figure B 13 Model system A4B4C1P2-2

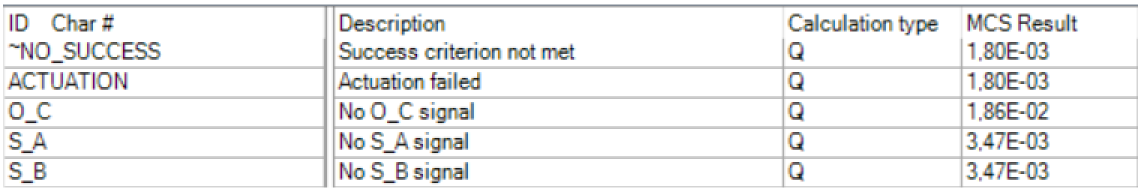
C Selected Complete Fault Trees

C.1 Model System A1B1C1P1 (Base Case)



ID	Char #	Description	Mean	Model
1_SENSOR_A_LOW		Failure sensor A to low	3,96E-04	Tested
1_SENSOR_B_LOW		Failure sensor B to low	3,96E-04	Tested
1_SENSOR_C_LOW		Failure sensor C to low	7,86E-03	Tested
1A_APU_AI		Failure of AI of APU of SIC-A division 1	8,35E-04	Tested
1A_APU_PM		Failure of PM of APU of SIC-A division 1	6,26E-04	Tested
1A_VU_DO		Failure of DO of VU of SIC-A division 1	8,35E-04	Tested
1A_VU_PM		Failure of DO of VU of SIC-A division 1	6,26E-04	Tested
1B_APU_AI		Failure of AI of APU of SIC-B division 1	8,35E-04	Tested
1B_APU_PM		Failure of PM of APU of SIC-B division 1	6,26E-04	Tested
1B_VU_DO		Failure of DO of VU of SIC-B division 1	8,35E-04	Tested
1B_VU_PM		Failure of DO of VU of SIC-B division 1	6,26E-04	Tested
1O_AI		Failure of AI of OIC	5,25E-03	Tested
1O_DO		Failure of DO of OIC	8,77E-04	Tested
1O_PM		Failure of PM of OIC	3,94E-03	Tested
1O_SR		Failure of SR of OIC	7,89E-04	Tested
1PA_AD_1		Failure of AD1 of PAC-A (no CCF)	8,35E-04	Tested
1PA_AD_2		Failure of AD2 of PAC-A (no CCF)	8,35E-04	Tested
1PA_AD_3		Failure of AD3 of PAC-A (no CCF)	8,35E-04	Tested
1PA_AD_Z		Failure of all ADs of PAC-A (CCF)	4,40E-05	Tested
1PA_CPLD		Failure of CPLD of PAC-A	4,39E-04	Tested
1PA_DA		Failure of DA of PAC-A	8,79E-04	Tested
1PA_SR		Failure of SR of PAC-A	4,39E-04	Tested
1Y_APU_AI		Failure of all AIs of APUs of SIC (CCF)	4,40E-05	Tested
1Y_APU_PM		Failure of all PMs of APUs of SIC (CCF)	3,30E-05	Tested
1Y_VU_DO		Failure of all DOs of VUs of SIC (CCF)	4,40E-05	Tested
1Y_VU_PM		Failure of all PMs of VUs of SIC (CCF)	3,30E-05	Tested

Figure C 1 Basic events (screenshot from RiskSpectrum)



ID	Char #	Description	Calculation type	MCS Result
~NO_SUCCESS		Success criterion not met	Q	1,80E-03
ACTUATION		Actuation failed	Q	1,80E-03
O_C		No O_C signal	Q	1,86E-02
S_A		No S_A signal	Q	3,47E-03
S_B		No S_B signal	Q	3,47E-03

Figure C 2 Analysis cases results (screenshot from RiskSpectrum)

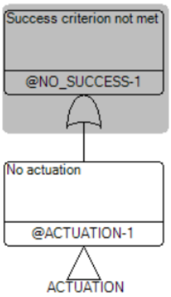


Figure C 3 Top event fault tree ("success criterion not met")

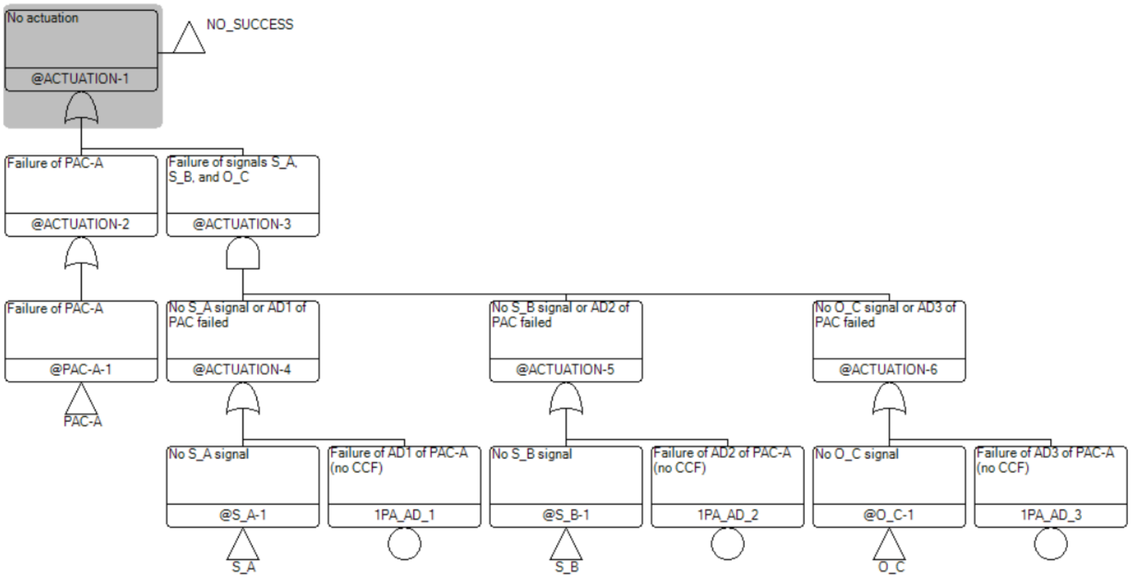

No actuation
@ACTUATION-1
NO_SUCCESS
Failure of PAC-A
@ACTUATION-2
Failure of signals S_A, S_B, and O_C
@ACTUATION-3
Failure of PAC-A
@PAC-A-1
PAC-A
No S_A signal or AD1 of PAC failed
@ACTUATION-4
No S_B signal or AD2 of PAC failed
@ACTUATION-5
No O_C signal or AD3 of PAC failed
@ACTUATION-6
No S_A signal
@S_A-1
S_A
Failure of AD1 of PAC-A (no CCF)
1PA_AD_1
No S_B signal
@S_B-1
S_B
Failure of AD2 of PAC-A (no CCF)
1PA_AD_2
No O_C signal
@O_C-1
O_C
Failure of AD3 of PAC-A (no CCF)
1PA_AD_3

Figure C 4 Fault tree for missing actuation signal ("no actuation")

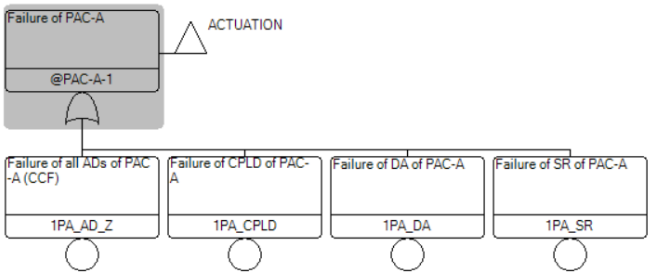


Figure C 5 Fault tree for failure of PAC

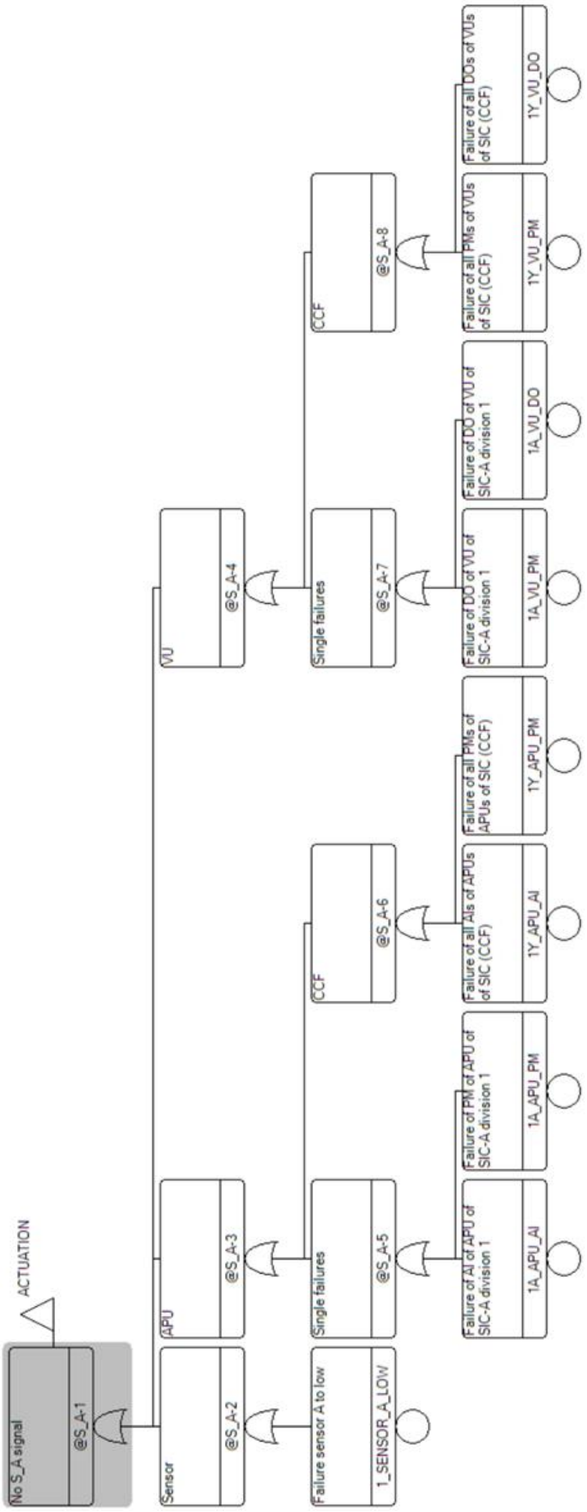

ACTUATION
No S_A signal
@S_A-1
Sensor
@S_A-2
Failure sensor A to low
1_SENSOR_A_LOW
APU
@S_A-3
Single failures
@S_A-5
Failure of AI of APU of SIC-A division 1
1A_APU_AI
Failure of PM of APU of SIC-A division 1
1A_APU_PM
CCF
@S_A-6
Failure of all AIs of APUs of SIC (CCF)
1Y_APU_AI
Failure of all PMs of APUs of SIC (CCF)
1Y_APU_PM
VU
@S_A-4
Single failures
@S_A-7
Failure of DO of VU of SIC-A division 1
1A_VU_PM
Failure of DO of VU of SIC-A division 1
1A_VU_DO
CCF
@S_A-8
Failure of all PMs of VUs of SIC (CCF)
1Y_VU_PM
Failure of all DOs of VUs of SIC (CCF)
1Y_VU_DO

Figure C 6 Fault tree “no S_A signal”

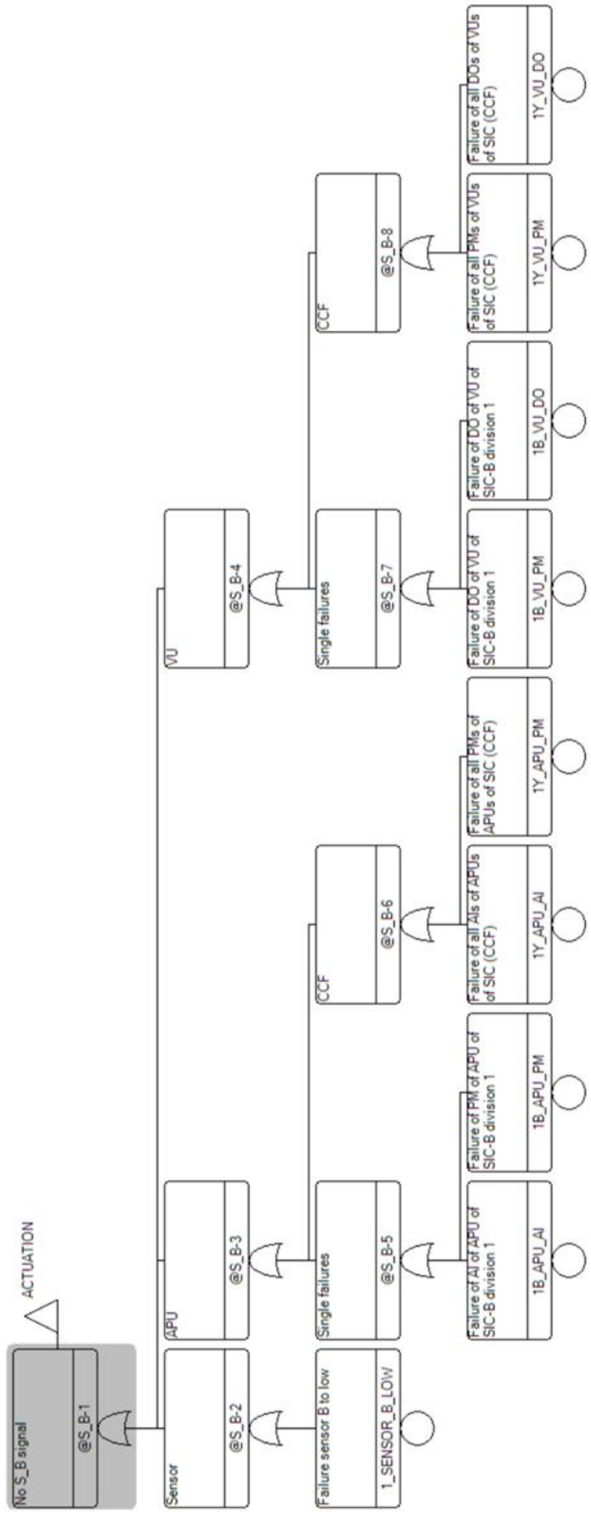

ACTUATION
No S_B signal
@S_B-1
Sensor
@S_B-2
Failure sensor B to low
1_SENSOR_B_LOW
APU
@S_B-3
Single failures
@S_B-5
Failure of AI of APU of SIC-B division 1
1B_APU_AI
Failure of PM of APU of SIC-B division 1
1B_APU_PM
CCF
@S_B-6
Failure of all AIs of APUs of SIC (CCF)
1Y_APU_AI
Failure of all PMs of APUs of SIC (CCF)
1Y_APU_PM
VU
@S_B-4
Single failures
@S_B-7
Failure of DO of VU of SIC-B division 1
1B_VU_PM
Failure of DO of VU of SIC-B division 1
1B_VU_DO
CCF
@S_B-8
Failure of all PMs of VUs of SIC (CCF)
1Y_VU_PM
Failure of all DOs of VUs of SIC (CCF)
1Y_VU_DO

Figure C 7 Fault tree “no S_B signal”

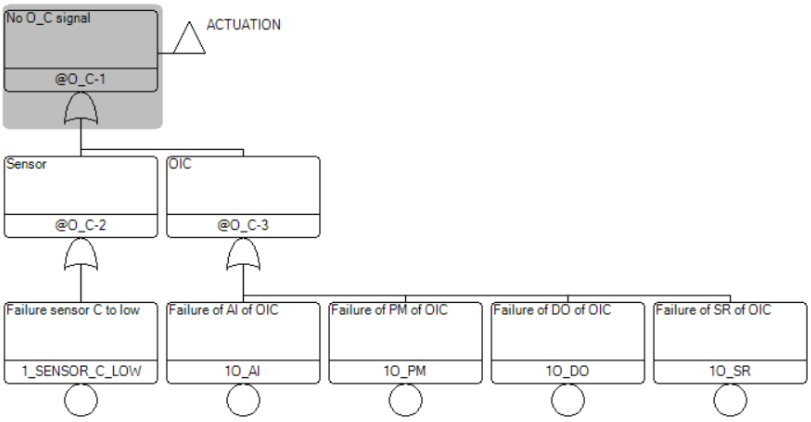
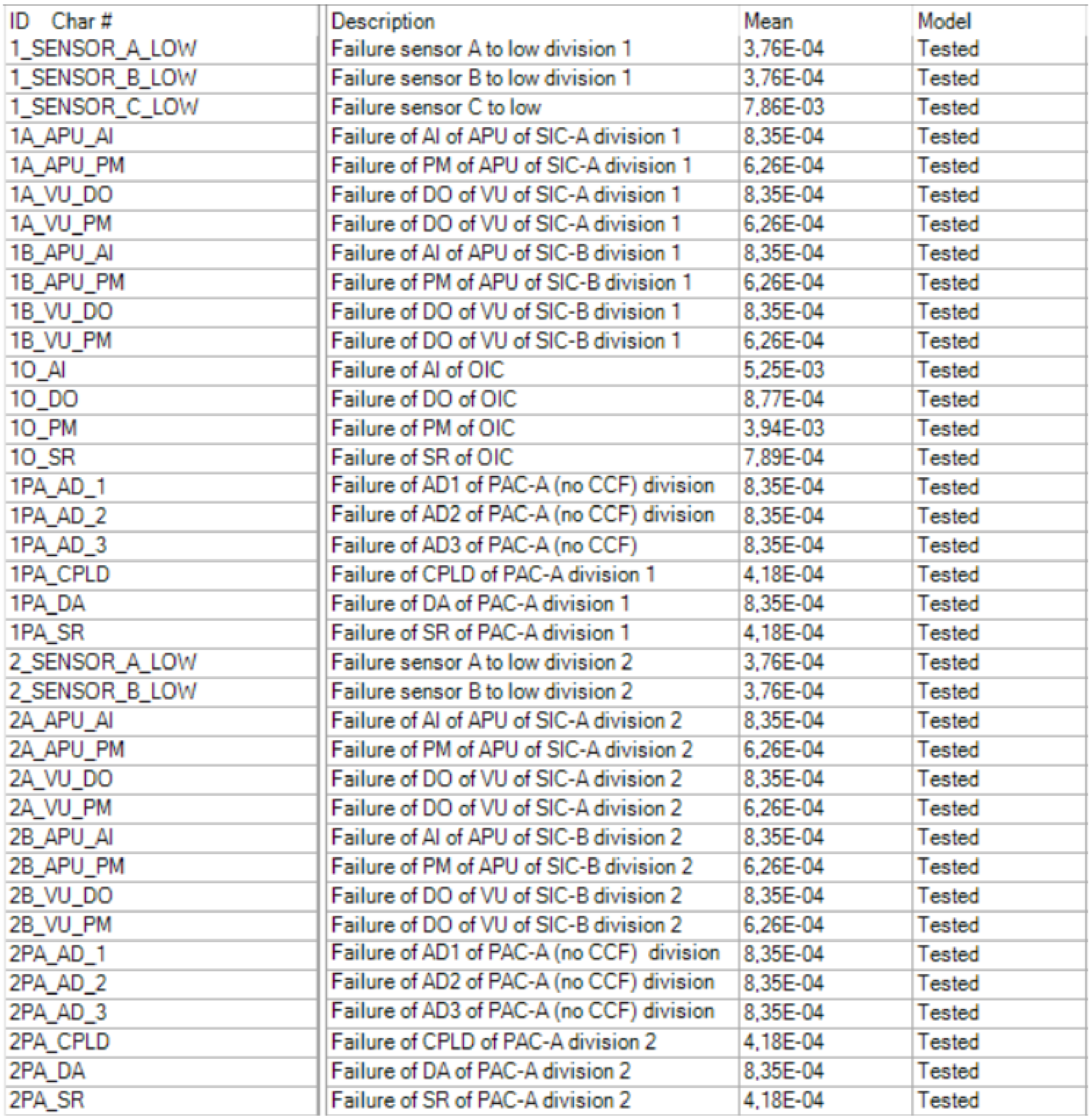


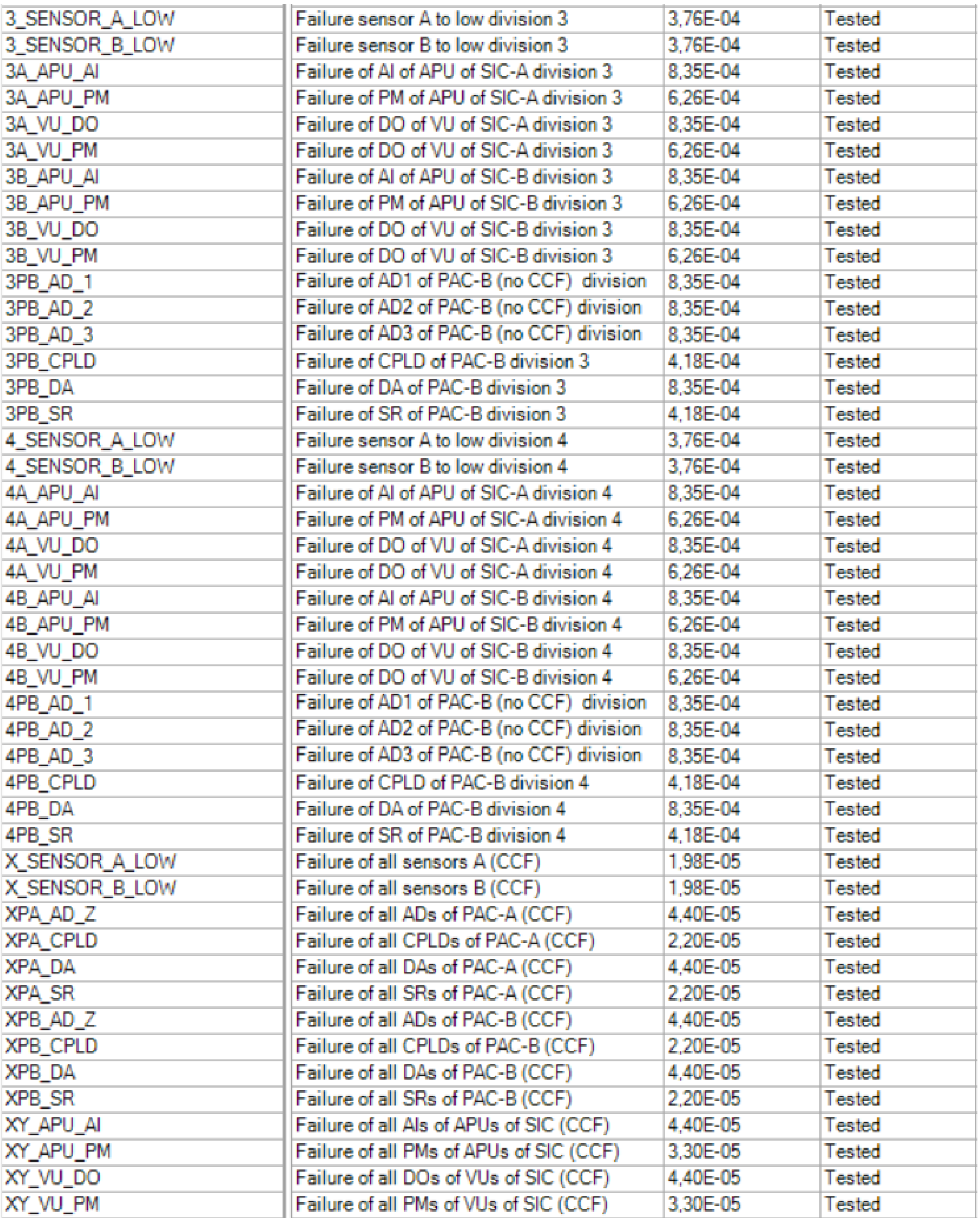
Figure C 8 Fault tree “no O_C signal”

C.2 Model System A4B4C1P2-2



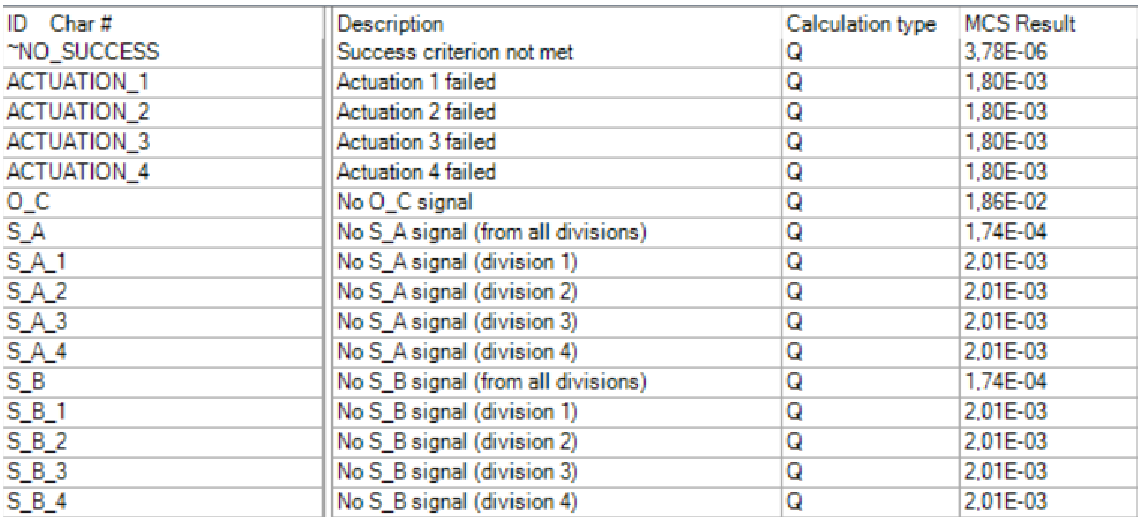
ID Char #	Description	Mean	Model
1_SENSOR_A_LOW	Failure sensor A to low division 1	3,76E-04	Tested
1_SENSOR_B_LOW	Failure sensor B to low division 1	3,76E-04	Tested
1_SENSOR_C_LOW	Failure sensor C to low	7,86E-03	Tested
1A_APU_AI	Failure of AI of APU of SIC-A division 1	8,35E-04	Tested
1A_APU_PM	Failure of PM of APU of SIC-A division 1	6,26E-04	Tested
1A_VU_DO	Failure of DO of VU of SIC-A division 1	8,35E-04	Tested
1A_VU_PM	Failure of DO of VU of SIC-A division 1	6,26E-04	Tested
1B_APU_AI	Failure of AI of APU of SIC-B division 1	8,35E-04	Tested
1B_APU_PM	Failure of PM of APU of SIC-B division 1	6,26E-04	Tested
1B_VU_DO	Failure of DO of VU of SIC-B division 1	8,35E-04	Tested
1B_VU_PM	Failure of DO of VU of SIC-B division 1	6,26E-04	Tested
1O_AI	Failure of AI of OIC	5,25E-03	Tested
1O_DO	Failure of DO of OIC	8,77E-04	Tested
1O_PM	Failure of PM of OIC	3,94E-03	Tested
1O_SR	Failure of SR of OIC	7,89E-04	Tested
1PA_AD_1	Failure of AD1 of PAC-A (no CCF) division	8,35E-04	Tested
1PA_AD_2	Failure of AD2 of PAC-A (no CCF) division	8,35E-04	Tested
1PA_AD_3	Failure of AD3 of PAC-A (no CCF)	8,35E-04	Tested
1PA_CPLD	Failure of CPLD of PAC-A division 1	4,18E-04	Tested
1PA_DA	Failure of DA of PAC-A division 1	8,35E-04	Tested
1PA_SR	Failure of SR of PAC-A division 1	4,18E-04	Tested
2_SENSOR_A_LOW	Failure sensor A to low division 2	3,76E-04	Tested
2_SENSOR_B_LOW	Failure sensor B to low division 2	3,76E-04	Tested
2A_APU_AI	Failure of AI of APU of SIC-A division 2	8,35E-04	Tested
2A_APU_PM	Failure of PM of APU of SIC-A division 2	6,26E-04	Tested
2A_VU_DO	Failure of DO of VU of SIC-A division 2	8,35E-04	Tested
2A_VU_PM	Failure of DO of VU of SIC-A division 2	6,26E-04	Tested
2B_APU_AI	Failure of AI of APU of SIC-B division 2	8,35E-04	Tested
2B_APU_PM	Failure of PM of APU of SIC-B division 2	6,26E-04	Tested
2B_VU_DO	Failure of DO of VU of SIC-B division 2	8,35E-04	Tested
2B_VU_PM	Failure of DO of VU of SIC-B division 2	6,26E-04	Tested
2PA_AD_1	Failure of AD1 of PAC-A (no CCF) division	8,35E-04	Tested
2PA_AD_2	Failure of AD2 of PAC-A (no CCF) division	8,35E-04	Tested
2PA_AD_3	Failure of AD3 of PAC-A (no CCF) division	8,35E-04	Tested
2PA_CPLD	Failure of CPLD of PAC-A division 2	4,18E-04	Tested
2PA_DA	Failure of DA of PAC-A division 2	8,35E-04	Tested
2PA_SR	Failure of SR of PAC-A division 2	4,18E-04	Tested

Figure C 9 Basic events 1/3 (screenshot from RiskSpectrum)



3_SENSOR_A_LOW	Failure sensor A to low division 3	3,76E-04	Tested
3_SENSOR_B_LOW	Failure sensor B to low division 3	3,76E-04	Tested
3A_APU_AI	Failure of AI of APU of SIC-A division 3	8,35E-04	Tested
3A_APU_PM	Failure of PM of APU of SIC-A division 3	6,26E-04	Tested
3A_VU_DO	Failure of DO of VU of SIC-A division 3	8,35E-04	Tested
3A_VU_PM	Failure of DO of VU of SIC-A division 3	6,26E-04	Tested
3B_APU_AI	Failure of AI of APU of SIC-B division 3	8,35E-04	Tested
3B_APU_PM	Failure of PM of APU of SIC-B division 3	6,26E-04	Tested
3B_VU_DO	Failure of DO of VU of SIC-B division 3	8,35E-04	Tested
3B_VU_PM	Failure of DO of VU of SIC-B division 3	6,26E-04	Tested
3PB_AD_1	Failure of AD1 of PAC-B (no CCF) division	8,35E-04	Tested
3PB_AD_2	Failure of AD2 of PAC-B (no CCF) division	8,35E-04	Tested
3PB_AD_3	Failure of AD3 of PAC-B (no CCF) division	8,35E-04	Tested
3PB_CPLD	Failure of CPLD of PAC-B division 3	4,18E-04	Tested
3PB_DA	Failure of DA of PAC-B division 3	8,35E-04	Tested
3PB_SR	Failure of SR of PAC-B division 3	4,18E-04	Tested
4_SENSOR_A_LOW	Failure sensor A to low division 4	3,76E-04	Tested
4_SENSOR_B_LOW	Failure sensor B to low division 4	3,76E-04	Tested
4A_APU_AI	Failure of AI of APU of SIC-A division 4	8,35E-04	Tested
4A_APU_PM	Failure of PM of APU of SIC-A division 4	6,26E-04	Tested
4A_VU_DO	Failure of DO of VU of SIC-A division 4	8,35E-04	Tested
4A_VU_PM	Failure of DO of VU of SIC-A division 4	6,26E-04	Tested
4B_APU_AI	Failure of AI of APU of SIC-B division 4	8,35E-04	Tested
4B_APU_PM	Failure of PM of APU of SIC-B division 4	6,26E-04	Tested
4B_VU_DO	Failure of DO of VU of SIC-B division 4	8,35E-04	Tested
4B_VU_PM	Failure of DO of VU of SIC-B division 4	6,26E-04	Tested
4PB_AD_1	Failure of AD1 of PAC-B (no CCF) division	8,35E-04	Tested
4PB_AD_2	Failure of AD2 of PAC-B (no CCF) division	8,35E-04	Tested
4PB_AD_3	Failure of AD3 of PAC-B (no CCF) division	8,35E-04	Tested
4PB_CPLD	Failure of CPLD of PAC-B division 4	4,18E-04	Tested
4PB_DA	Failure of DA of PAC-B division 4	8,35E-04	Tested
4PB_SR	Failure of SR of PAC-B division 4	4,18E-04	Tested
X_SENSOR_A_LOW	Failure of all sensors A (CCF)	1,98E-05	Tested
X_SENSOR_B_LOW	Failure of all sensors B (CCF)	1,98E-05	Tested
XPA_AD_Z	Failure of all ADs of PAC-A (CCF)	4,40E-05	Tested
XPA_CPLD	Failure of all CPLDs of PAC-A (CCF)	2,20E-05	Tested
XPA_DA	Failure of all DAs of PAC-A (CCF)	4,40E-05	Tested
XPA_SR	Failure of all SRs of PAC-A (CCF)	2,20E-05	Tested
XPB_AD_Z	Failure of all ADs of PAC-B (CCF)	4,40E-05	Tested
XPB_CPLD	Failure of all CPLDs of PAC-B (CCF)	2,20E-05	Tested
XPB_DA	Failure of all DAs of PAC-B (CCF)	4,40E-05	Tested
XPB_SR	Failure of all SRs of PAC-B (CCF)	2,20E-05	Tested
XY_APU_AI	Failure of all AIs of APUs of SIC (CCF)	4,40E-05	Tested
XY_APU_PM	Failure of all PMs of APUs of SIC (CCF)	3,30E-05	Tested
XY_VU_DO	Failure of all DOs of VUs of SIC (CCF)	4,40E-05	Tested
XY_VU_PM	Failure of all PMs of VUs of SIC (CCF)	3,30E-05	Tested

Figure C 10 Basic events 2/3 (screenshot from RiskSpectrum)



ID Char #	Description	Calculation type	MCS Result
~NO_SUCCESS	Success criterion not met	Q	3,78E-06
ACTUATION_1	Actuation 1 failed	Q	1,80E-03
ACTUATION_2	Actuation 2 failed	Q	1,80E-03
ACTUATION_3	Actuation 3 failed	Q	1,80E-03
ACTUATION_4	Actuation 4 failed	Q	1,80E-03
O_C	No O_C signal	Q	1,86E-02
S_A	No S_A signal (from all divisions)	Q	1,74E-04
S_A_1	No S_A signal (division 1)	Q	2,01E-03
S_A_2	No S_A signal (division 2)	Q	2,01E-03
S_A_3	No S_A signal (division 3)	Q	2,01E-03
S_A_4	No S_A signal (division 4)	Q	2,01E-03
S_B	No S_B signal (from all divisions)	Q	1,74E-04
S_B_1	No S_B signal (division 1)	Q	2,01E-03
S_B_2	No S_B signal (division 2)	Q	2,01E-03
S_B_3	No S_B signal (division 3)	Q	2,01E-03
S_B_4	No S_B signal (division 4)	Q	2,01E-03

Figure C 11 Basic events 3/3 (screenshot from RiskSpectrum)

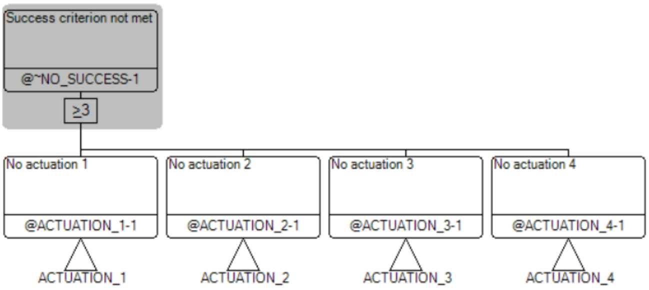


Figure C 12 Top event fault tree (“success criterion not met”)

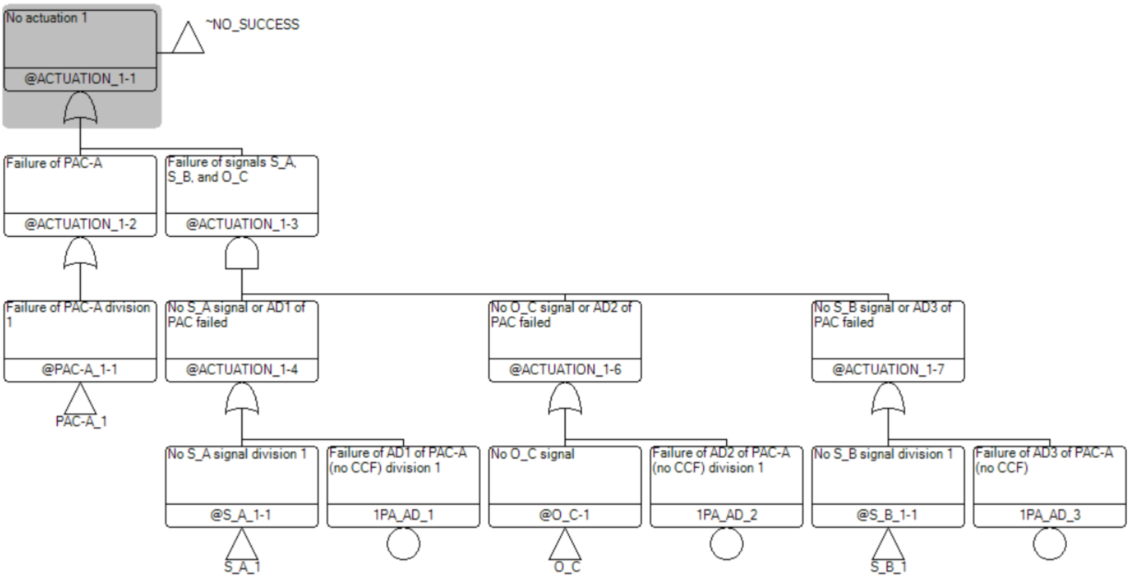

No actuation 1
@ACTUATION_1-1
~NO_SUCCESS
Failure of PAC-A
@ACTUATION_1-2
Failure of signals S_A, S_B, and O_C
@ACTUATION_1-3
Failure of PAC-A division 1
@PAC-A_1-1
PAC-A_1
No S_A signal or AD1 of PAC failed
@ACTUATION_1-4
No O_C signal or AD2 of PAC failed
@ACTUATION_1-6
No S_B signal or AD3 of PAC failed
@ACTUATION_1-7
No S_A signal division 1
@S_A_1-1
S_A_1
Failure of AD1 of PAC-A (no CCF) division 1
1PA_AD_1
No O_C signal
@O_C-1
O_C
Failure of AD2 of PAC-A (no CCF) division 1
1PA_AD_2
No S_B signal division 1
@S_B_1-1
S_B_1
Failure of AD3 of PAC-A (no CCF)
1PA_AD_3

Figure C 13 Fault tree for missing actuation signal (“no actuation”) from division 1

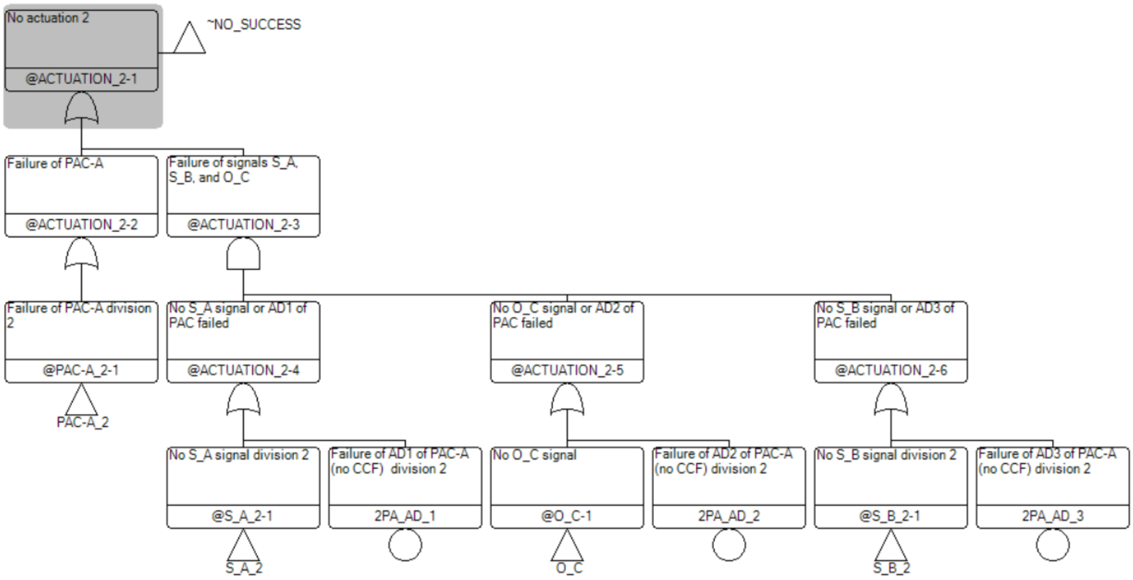

No actuation 2
@ACTUATION_2-1
~NO_SUCCESS
Failure of PAC-A
@ACTUATION_2-2
Failure of signals S_A, S_B, and O_C
@ACTUATION_2-3
Failure of PAC-A division 2
@PAC-A_2-1
PAC-A_2
No S_A signal or AD1 of PAC failed
@ACTUATION_2-4
No O_C signal or AD2 of PAC failed
@ACTUATION_2-5
No S_B signal or AD3 of PAC failed
@ACTUATION_2-6
No S_A signal division 2
@S_A_2-1
S_A_2
Failure of AD1 of PAC-A (no CCF) division 2
2PA_AD_1
No O_C signal
@O_C-1
O_C
Failure of AD2 of PAC-A (no CCF) division 2
2PA_AD_2
No S_B signal division 2
@S_B_2-1
S_B_2
Failure of AD3 of PAC-A (no CCF) division 2
2PA_AD_3

Figure C 14 Fault tree for missing actuation signal (“no actuation”) from division 2

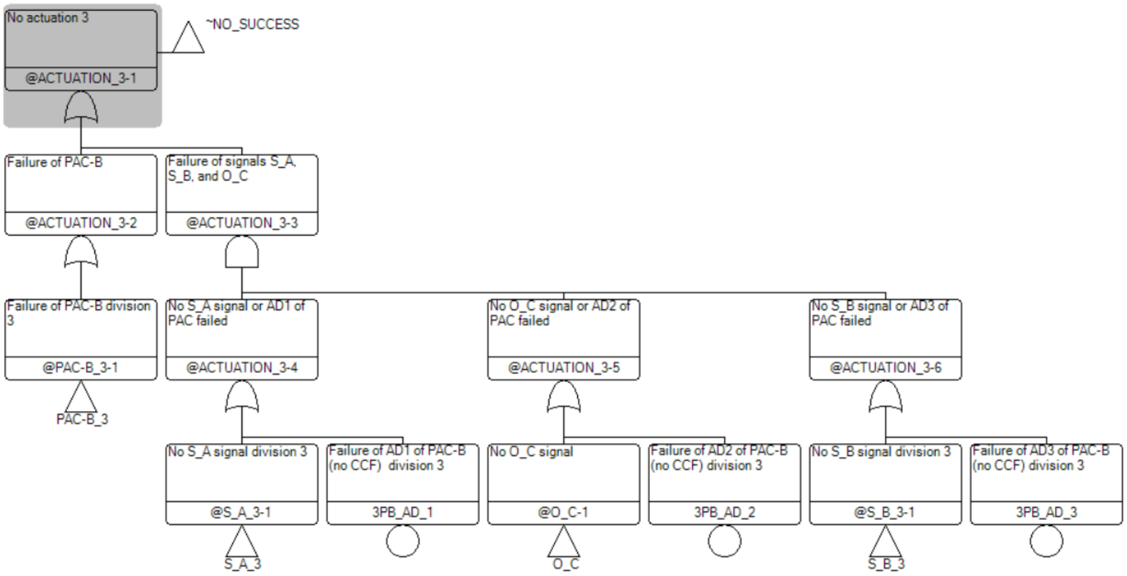

No actuation 3
@ACTUATION_3-1
~NO_SUCCESS
Failure of PAC-B
@ACTUATION_3-2
Failure of signals S_A, S_B, and O_C
@ACTUATION_3-3
Failure of PAC-B division 3
@PAC-B_3-1
PAC-B_3
No S_A signal or AD1 of PAC failed
@ACTUATION_3-4
No O_C signal or AD2 of PAC failed
@ACTUATION_3-5
No S_B signal or AD3 of PAC failed
@ACTUATION_3-6
No S_A signal division 3
@S_A_3-1
S_A_3
Failure of AD1 of PAC-B (no CCF) division 3
3PB_AD_1
No O_C signal
@O_C-1
O_C
Failure of AD2 of PAC-B (no CCF) division 3
3PB_AD_2
No S_B signal division 3
@S_B_3-1
S_B_3
Failure of AD3 of PAC-B (no CCF) division 3
3PB_AD_3

Figure C 15 Fault tree for missing actuation signal (“no actuation”) from division 3

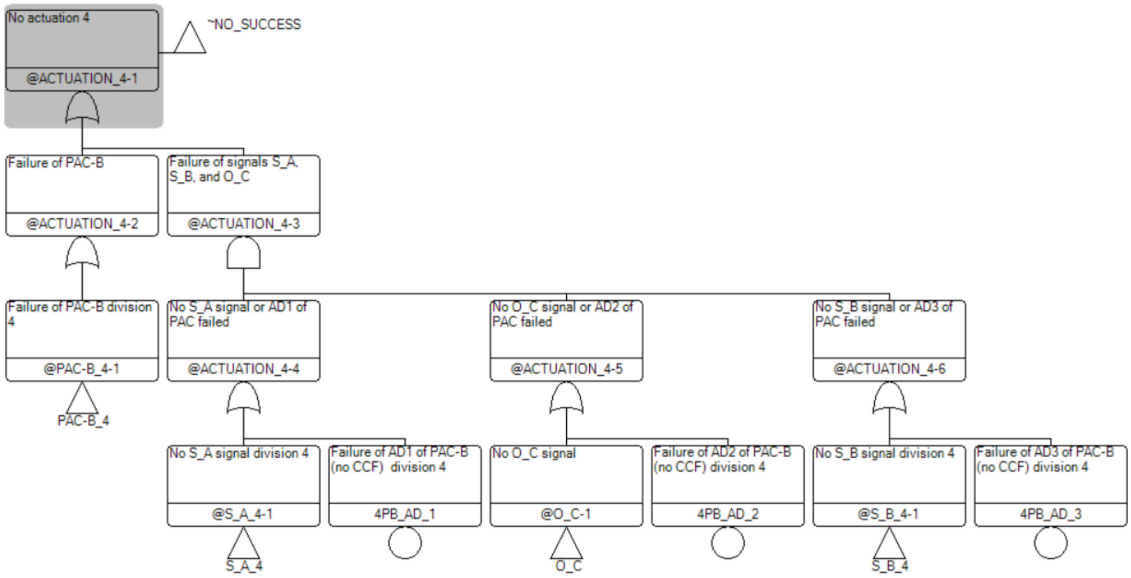

No actuation 4
@ACTUATION_4-1
~NO_SUCCESS
Failure of PAC-B
@ACTUATION_4-2
Failure of signals S_A, S_B, and O_C
@ACTUATION_4-3
Failure of PAC-B division 4
@PAC-B_4-1
PAC-B_4
No S_A signal or AD1 of PAC failed
@ACTUATION_4-4
No O_C signal or AD2 of PAC failed
@ACTUATION_4-5
No S_B signal or AD3 of PAC failed
@ACTUATION_4-6
No S_A signal division 4
@S_A_4-1
S_A_4
Failure of AD1 of PAC-B (no CCF) division 4
4PB_AD_1
No O_C signal
@O_C-1
O_C
Failure of AD2 of PAC-B (no CCF) division 4
4PB_AD_2
No S_B signal division 4
@S_B_4-1
S_B_4
Failure of AD3 of PAC-B (no CCF) division 4
4PB_AD_3

Figure C 16 Fault tree for missing actuation signal (“no actuation”) from division 4

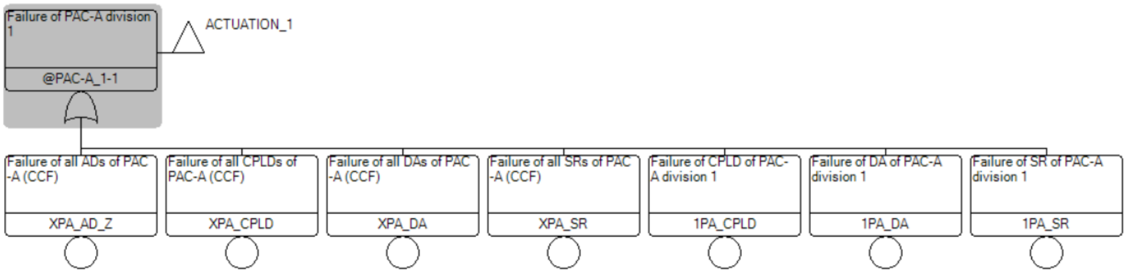

Failure of PAC-A division 1
@PAC-A_1-1
ACTUATION_1
Failure of all ADs of PAC-A (CCF)
XPA_AD_Z
Failure of all CPLDs of PAC-A (CCF)
XPA_CPLD
Failure of all DAs of PAC-A (CCF)
XPA_DA
Failure of all SRs of PAC-A (CCF)
XPA_SR
Failure of CPLD of PAC-A division 1
1PA_CPLD
Failure of DA of PAC-A division 1
1PA_DA
Failure of SR of PAC-A division 1
1PA_SR

Figure C 17 Fault tree for failure of PAC (division 1)

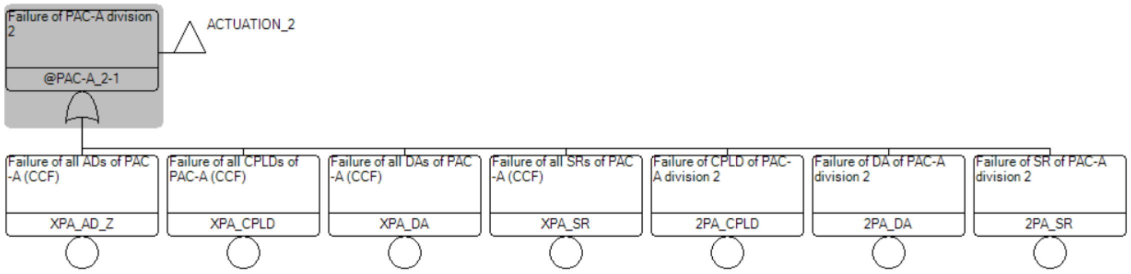

Failure of PAC-A division 2
@PAC-A_2-1
ACTUATION_2
Failure of all ADs of PAC-A (CCF)
XPA_AD_Z
Failure of all CPLDs of PAC-A (CCF)
XPA_CPLD
Failure of all DAs of PAC-A (CCF)
XPA_DA
Failure of all SRs of PAC-A (CCF)
XPA_SR
Failure of CPLD of PAC-A division 2
2PA_CPLD
Failure of DA of PAC-A division 2
2PA_DA
Failure of SR of PAC-A division 2
2PA_SR

Figure C 18 Fault tree for failure of PAC (division 2)

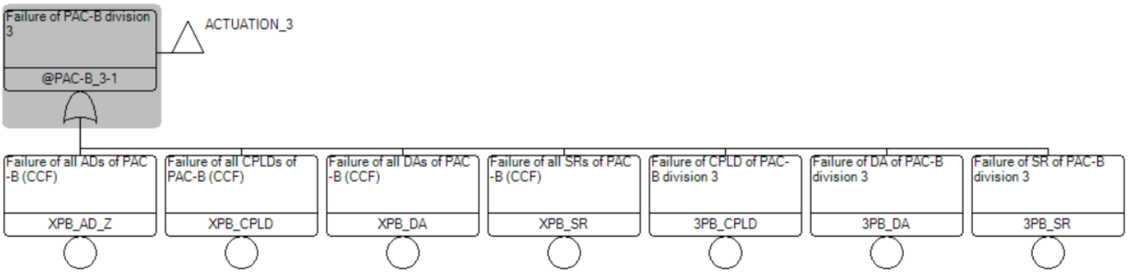

Failure of PAC-B division 3
@PAC-B_3-1
ACTUATION_3
Failure of all ADs of PAC -B (CCF)
XPB_AD_Z
Failure of all CPLDs of PAC-B (CCF)
XPB_CPLD
Failure of all DAs of PAC -B (CCF)
XPB_DA
Failure of all SRs of PAC -B (CCF)
XPB_SR
Failure of CPLD of PAC-B division 3
3PB_CPLD
Failure of DA of PAC-B division 3
3PB_DA
Failure of SR of PAC-B division 3
3PB_SR

Figure C 19 Fault tree for failure of PAC (division 3)

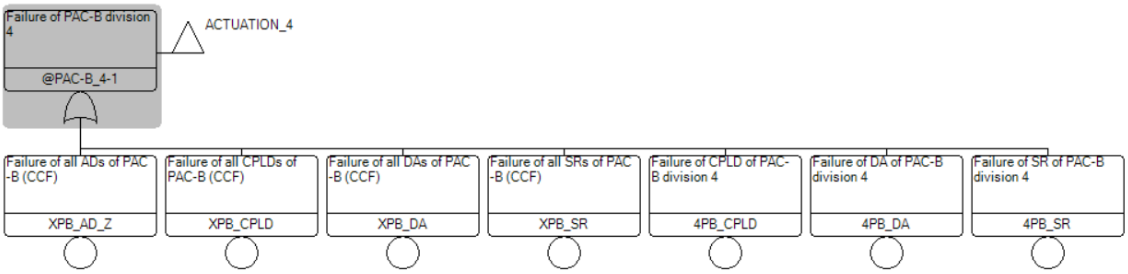

Failure of PAC-B division 4
@PAC-B_4-1
ACTUATION_4
Failure of all ADs of PAC -B (CCF)
XPB_AD_Z
Failure of all CPLDs of PAC-B (CCF)
XPB_CPLD
Failure of all DAs of PAC -B (CCF)
XPB_DA
Failure of all SRs of PAC -B (CCF)
XPB_SR
Failure of CPLD of PAC-B division 4
4PB_CPLD
Failure of DA of PAC-B division 4
4PB_DA
Failure of SR of PAC-B division 4
4PB_SR

Figure C 20 Fault tree for failure of PAC (division 4)

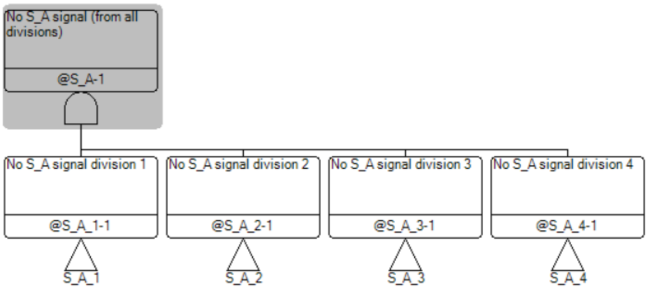


Figure C 21 Fault tree “no S_A signal (from all divisions)”

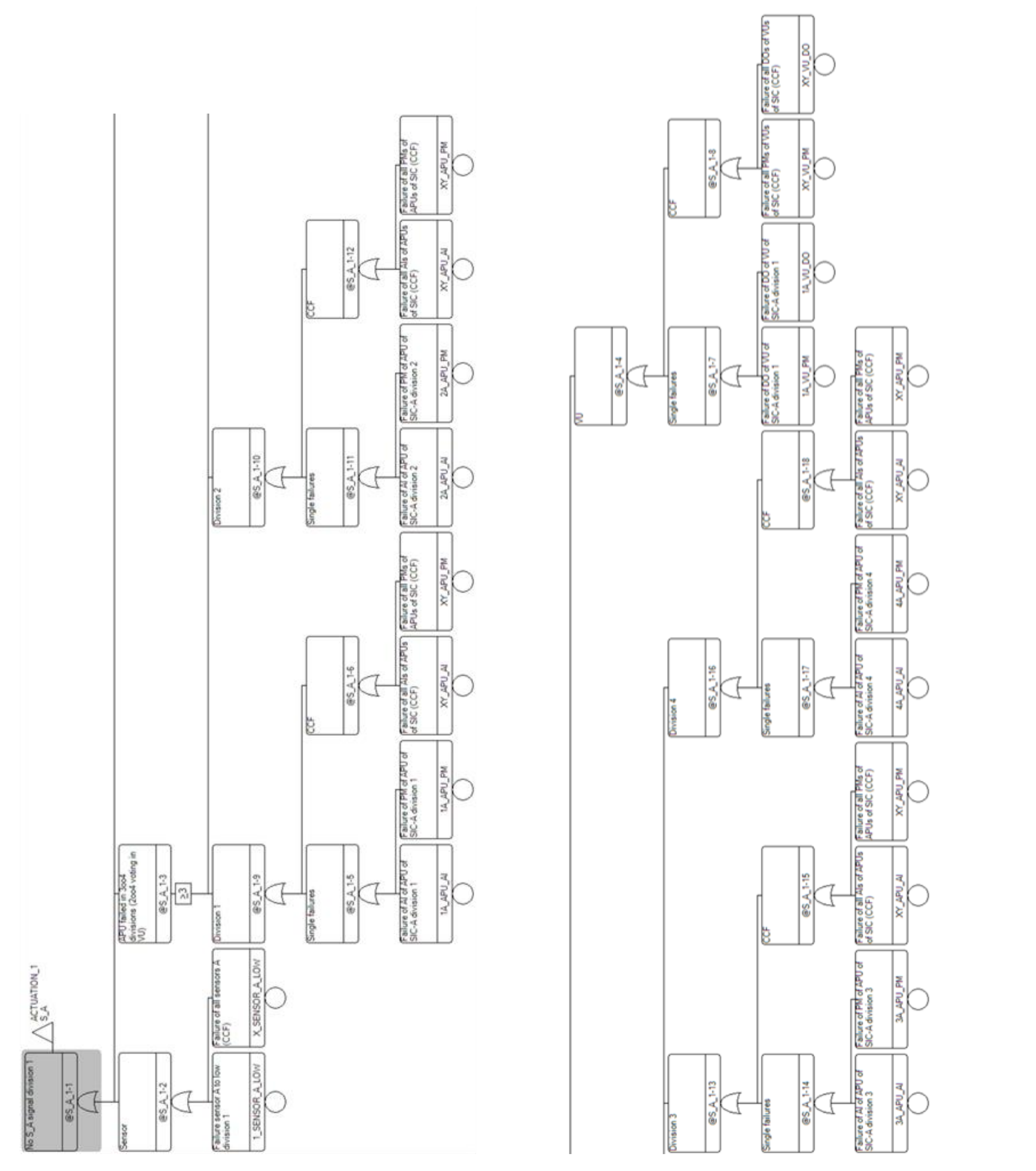

No S_A signal division 1
@S_A_1-1
ACTUATION_1
S_A
Sensor
@S_A_1-2
Failure sensor A to low division 1
1_SENSOR_A_LOW
Failure of all sensors A (CCF)
X_SENSOR_A_LOW
APU failed in 3oo4 divisions (2oo4 voting in VU)
@S_A_1-3
≥3
Division 1
@S_A_1-9
Single failures
@S_A_1-5
Failure of AI of APU of SIC-A division 1
1A_APU_AI
Failure of PM of APU of SIC-A division 1
1A_APU_PM
CCF
@S_A_1-6
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 2
@S_A_1-10
Single failures
@S_A_1-11
Failure of AI of APU of SIC-A division 2
2A_APU_AI
Failure of PM of APU of SIC-A division 2
2A_APU_PM
CCF
@S_A_1-12
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 3
@S_A_1-13
Single failures
@S_A_1-14
Failure of AI of APU of SIC-A division 3
3A_APU_AI
Failure of PM of APU of SIC-A division 3
3A_APU_PM
CCF
@S_A_1-15
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 4
@S_A_1-16
Single failures
@S_A_1-17
Failure of AI of APU of SIC-A division 4
4A_APU_AI
Failure of PM of APU of SIC-A division 4
4A_APU_PM
CCF
@S_A_1-18
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
VU
@S_A_1-4
Single failures
@S_A_1-7
Failure of DO of VU of SIC-A division 1
1A_VU_PM
Failure of DO of VU of SIC-A division 1
1A_VU_DO
CCF
@S_A_1-8
Failure of all PMs of VUs of SIC (CCF)
XY_VU_PM
Failure of all DOs of VUs of SIC (CCF)
XY_VU_DO

Figure C 22 Fault tree “no S_A signal division 1”

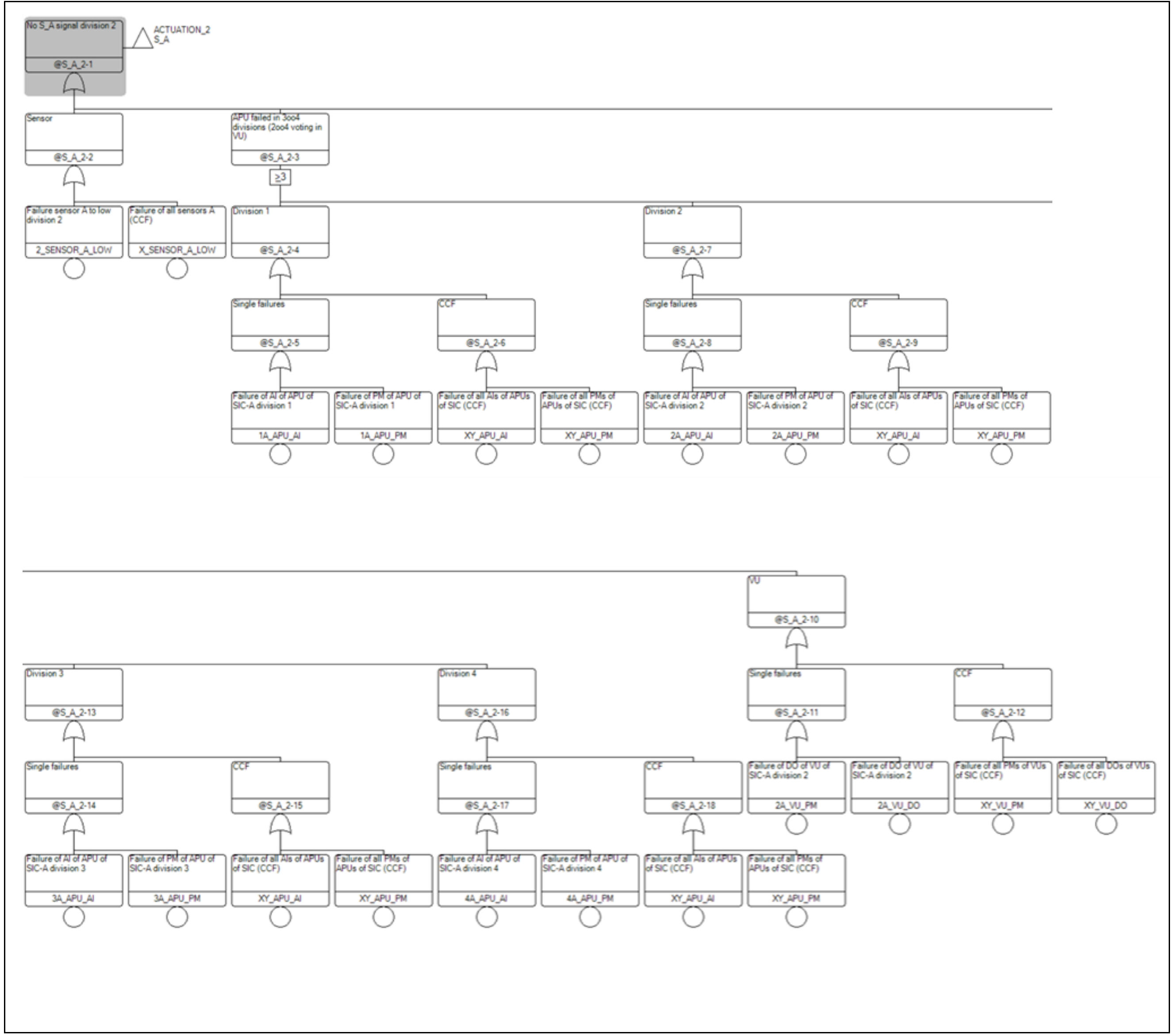

No S_A signal division 2
@S_A_2-1
ACTUATION_2
S_A
Sensor
@S_A_2-2
APU failed in 3oo4 divisions (2oo4 voting in VU)
@S_A_2-3
≥3
Failure sensor A to low division 2
2_SENSOR_A_LOW
Failure of all sensors A (CCF)
X_SENSOR_A_LOW
Division 1
@S_A_2-4
Division 2
@S_A_2-7
Single failures
@S_A_2-5
CCF
@S_A_2-6
Single failures
@S_A_2-8
CCF
@S_A_2-9
Failure of AI of APU of SIC-A division 1
1A_APU_AI
Failure of PM of APU of SIC-A division 1
1A_APU_PM
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Failure of AI of APU of SIC-A division 2
2A_APU_AI
Failure of PM of APU of SIC-A division 2
2A_APU_PM
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
VU
@S_A_2-10
Division 3
@S_A_2-13
Division 4
@S_A_2-16
Single failures
@S_A_2-11
CCF
@S_A_2-12
Single failures
@S_A_2-14
CCF
@S_A_2-15
Single failures
@S_A_2-17
CCF
@S_A_2-18
Failure of DO of VU of SIC-A division 2
2A_VU_PM
Failure of DO of VU of SIC-A division 2
2A_VU_DO
Failure of all PMs of VUs of SIC (CCF)
XY_VU_PM
Failure of all DOs of VUs of SIC (CCF)
XY_VU_DO
Failure of AI of APU of SIC-A division 3
3A_APU_AI
Failure of PM of APU of SIC-A division 3
3A_APU_PM
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Failure of AI of APU of SIC-A division 4
4A_APU_AI
Failure of PM of APU of SIC-A division 4
4A_APU_PM
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM

Figure C 23 Fault tree “no S_A signal division 2”

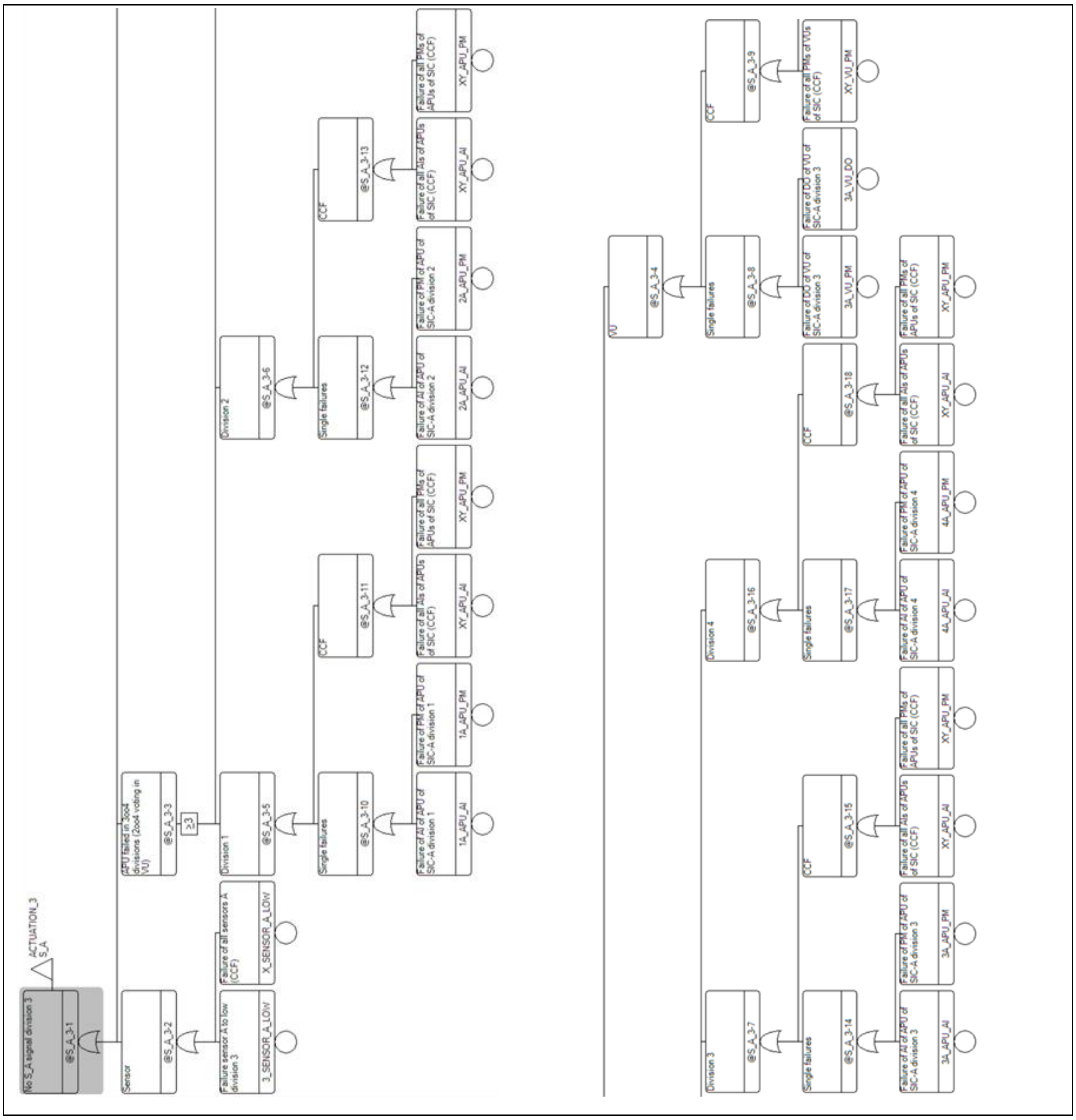

No S_A signal division 3
@S_A_3-1
ACTUATION_3
S_A
Sensor
@S_A_3-2
Failure sensor A to low division 3
3_SENSOR_A_LOW
Failure of all sensors A (CCF)
X_SENSOR_A_LOW
APU failed in 3oo4 divisions (2oo4 voting in VU)
@S_A_3-3
≥3
Division 1
@S_A_3-5
Single failures
@S_A_3-10
Failure of AI of APU of SIC-A division 1
1A_APU_AI
Failure of PM of APU of SIC-A division 1
1A_APU_PM
CCF
@S_A_3-11
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 2
@S_A_3-6
Single failures
@S_A_3-12
Failure of AI of APU of SIC-A division 2
2A_APU_AI
Failure of PM of APU of SIC-A division 2
2A_APU_PM
CCF
@S_A_3-13
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 3
@S_A_3-7
Single failures
@S_A_3-14
Failure of AI of APU of SIC-A division 3
3A_APU_AI
Failure of PM of APU of SIC-A division 3
3A_APU_PM
CCF
@S_A_3-15
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 4
@S_A_3-16
Single failures
@S_A_3-17
Failure of AI of APU of SIC-A division 4
4A_APU_AI
Failure of PM of APU of SIC-A division 4
4A_APU_PM
CCF
@S_A_3-18
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
VU
@S_A_3-4
Single failures
@S_A_3-8
Failure of DO of VU of SIC-A division 3
3A_VU_PM
Failure of DO of VU of SIC-A division 3
3A_VU_DO
CCF
@S_A_3-9
Failure of all PMs of VUs of SIC (CCF)
XY_VU_PM

Figure C 24 Fault tree “no S_A signal division 3”

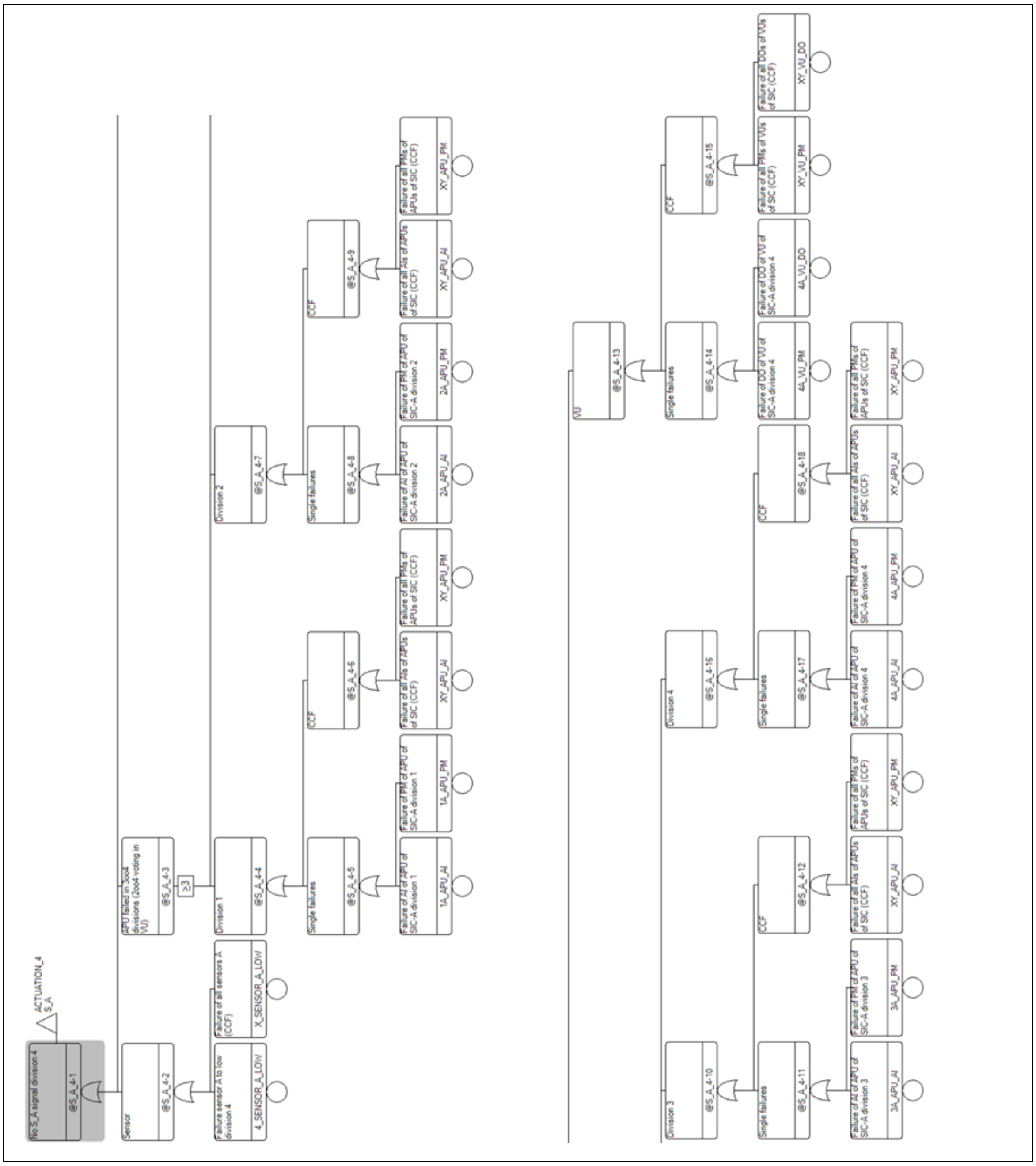

ACTUATION_4
S_A
No S_A signal division 4
@S_A_4-1
Sensor
@S_A_4-2
Failure sensor A to low division 4
4_SENSOR_A_LOW
Failure of all sensors A (CCF)
X_SENSOR_A_LOW
APU failed in 3oo4 divisions (2oo4 voting in VU)
@S_A_4-3
≥3
Division 1
@S_A_4-4
Single failures
@S_A_4-5
Failure of AI of APU of SIC-A division 1
1A_APU_AI
Failure of PM of APU of SIC-A division 1
1A_APU_PM
CCF
@S_A_4-6
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 2
@S_A_4-7
Single failures
@S_A_4-8
Failure of AI of APU of SIC-A division 2
2A_APU_AI
Failure of PM of APU of SIC-A division 2
2A_APU_PM
CCF
@S_A_4-9
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 3
@S_A_4-10
Single failures
@S_A_4-11
Failure of AI of APU of SIC-A division 3
3A_APU_AI
Failure of PM of APU of SIC-A division 3
3A_APU_PM
CCF
@S_A_4-12
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 4
@S_A_4-16
Single failures
@S_A_4-17
Failure of AI of APU of SIC-A division 4
4A_APU_AI
Failure of PM of APU of SIC-A division 4
4A_APU_PM
CCF
@S_A_4-18
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
VU
@S_A_4-13
Single failures
@S_A_4-14
Failure of DO of VU of SIC-A division 4
4A_VU_PM
Failure of DO of VU of SIC-A division 4
4A_VU_DO
CCF
@S_A_4-15
Failure of all PMs of VUs of SIC (CCF)
XY_VU_PM
Failure of all DOs of VUs of SIC (CCF)
XY_VU_DO

Figure C 25 Fault tree "no S_A signal division 4"

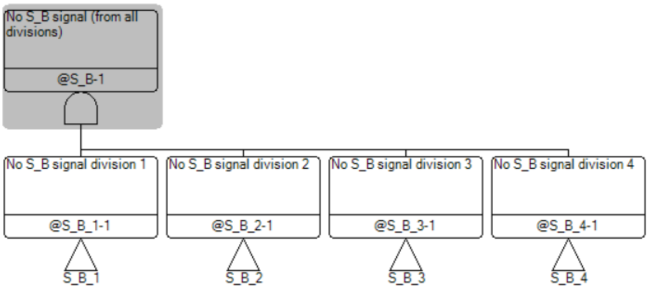


Figure C 26 Fault tree "no S_B signal (from all divisions)"

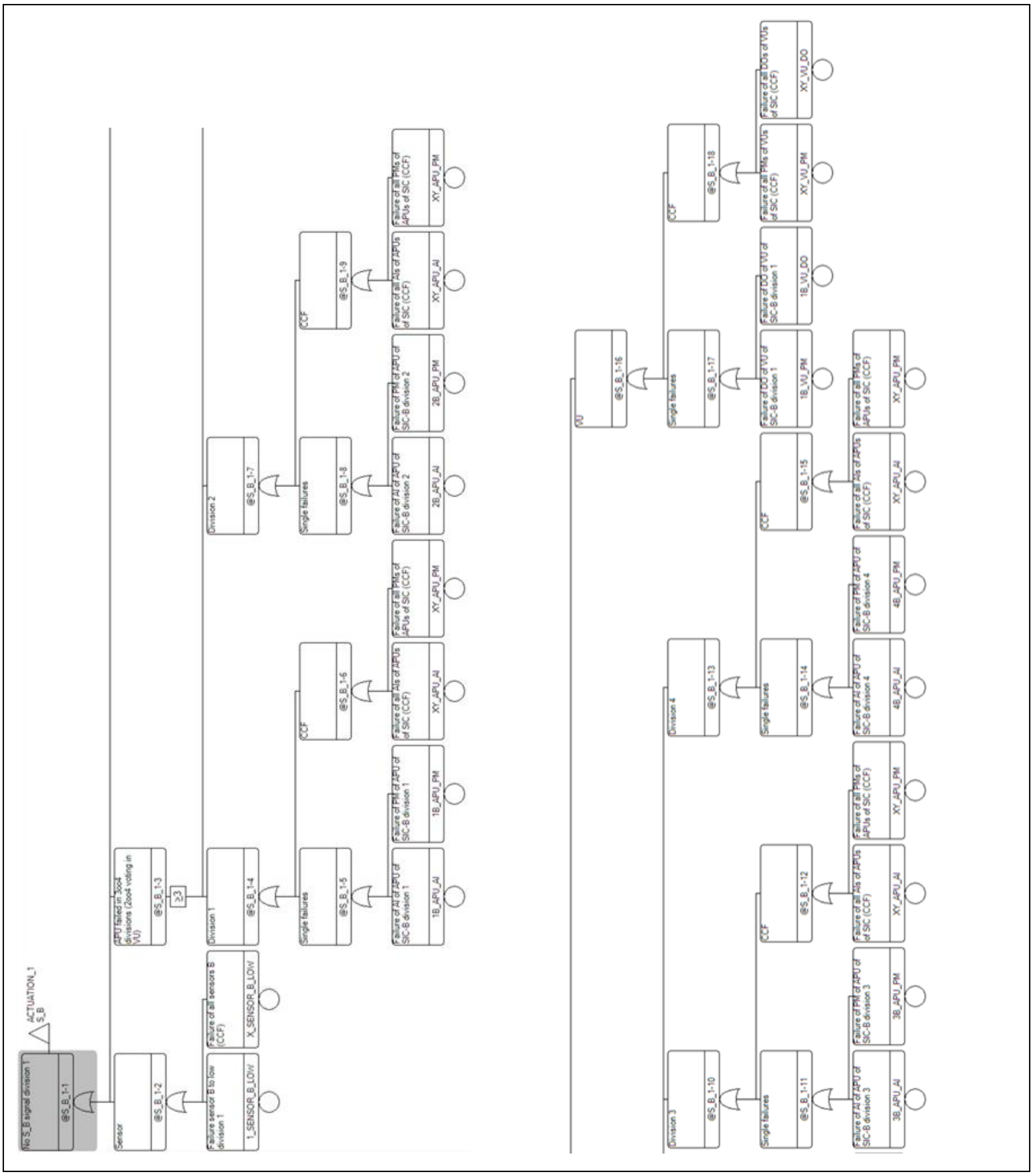

No S_B signal division 1
@S_B_1-1
ACTUATION_1
S_B
Sensor
@S_B_1-2
Failure sensor B to low division 1
1_SENSOR_B_LOW
Failure of all sensors B (CCF)
X_SENSOR_B_LOW
APU failed in 3oo4 divisions (2oo4 voting in VU)
@S_B_1-3
≥3
Division 1
@S_B_1-4
Single failures
@S_B_1-5
Failure of AI of APU of SIC-B division 1
1B_APU_AI
Failure of PM of APU of SIC-B division 1
1B_APU_PM
CCF
@S_B_1-6
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 2
@S_B_1-7
Single failures
@S_B_1-8
Failure of AI of APU of SIC-B division 2
2B_APU_AI
Failure of PM of APU of SIC-B division 2
2B_APU_PM
CCF
@S_B_1-9
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 3
@S_B_1-10
Single failures
@S_B_1-11
Failure of AI of APU of SIC-B division 3
3B_APU_AI
Failure of PM of APU of SIC-B division 3
3B_APU_PM
CCF
@S_B_1-12
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 4
@S_B_1-13
Single failures
@S_B_1-14
Failure of AI of APU of SIC-B division 4
4B_APU_AI
Failure of PM of APU of SIC-B division 4
4B_APU_PM
CCF
@S_B_1-15
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
VU
@S_B_1-16
Single failures
@S_B_1-17
Failure of DO of VU of SIC-B division 1
1B_VU_PM
Failure of DO of VU of SIC-B division 1
1B_VU_DO
CCF
@S_B_1-18
Failure of all PMs of VUs of SIC (CCF)
XY_VU_PM
Failure of all DOs of VUs of SIC (CCF)
XY_VU_DO

Figure C 27 Fault tree “no S_B signal division 1”

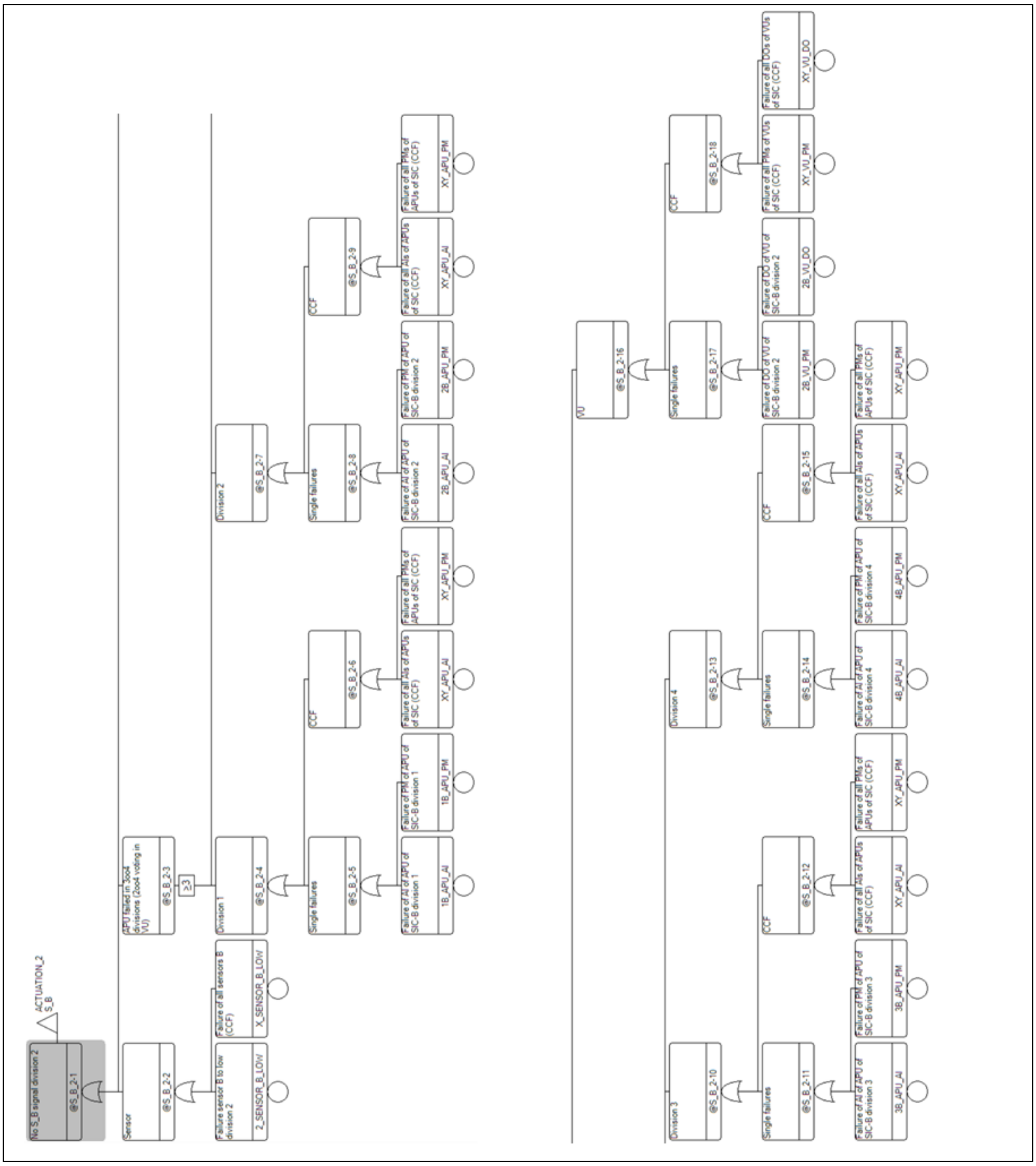

ACTUATION_2 S_B
No S_B signal division 2
@S_B_2-1
Sensor
@S_B_2-2
Failure sensor B to low division 2
2_SENSOR_B_LOW
Failure of all sensors B (CCF)
X_SENSOR_B_LOW
APU failed in 3oo4 divisions (2oo4 voting in VU)
@S_B_2-3
≥3
Division 1
@S_B_2-4
Single failures
@S_B_2-5
Failure of AI of APU of SIC-B division 1
1B_APU_AI
Failure of PM of APU of SIC-B division 1
1B_APU_PM
CCF
@S_B_2-6
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 2
@S_B_2-7
Single failures
@S_B_2-8
Failure of AI of APU of SIC-B division 2
2B_APU_AI
Failure of PM of APU of SIC-B division 2
2B_APU_PM
CCF
@S_B_2-9
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 3
@S_B_2-10
Single failures
@S_B_2-11
Failure of AI of APU of SIC-B division 3
3B_APU_AI
Failure of PM of APU of SIC-B division 3
3B_APU_PM
CCF
@S_B_2-12
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 4
@S_B_2-13
Single failures
@S_B_2-14
Failure of AI of APU of SIC-B division 4
4B_APU_AI
Failure of PM of APU of SIC-B division 4
4B_APU_PM
CCF
@S_B_2-15
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
VU
@S_B_2-16
Single failures
@S_B_2-17
Failure of DO of VU of SIC-B division 2
2B_VU_PM
Failure of DO of VU of SIC-B division 2
2B_VU_DO
CCF
@S_B_2-18
Failure of all PMs of VUs of SIC (CCF)
XY_VU_PM
Failure of all DOs of VUs of SIC (CCF)
XY_VU_DO

Figure C 28 Fault tree “no S_B signal division 2”

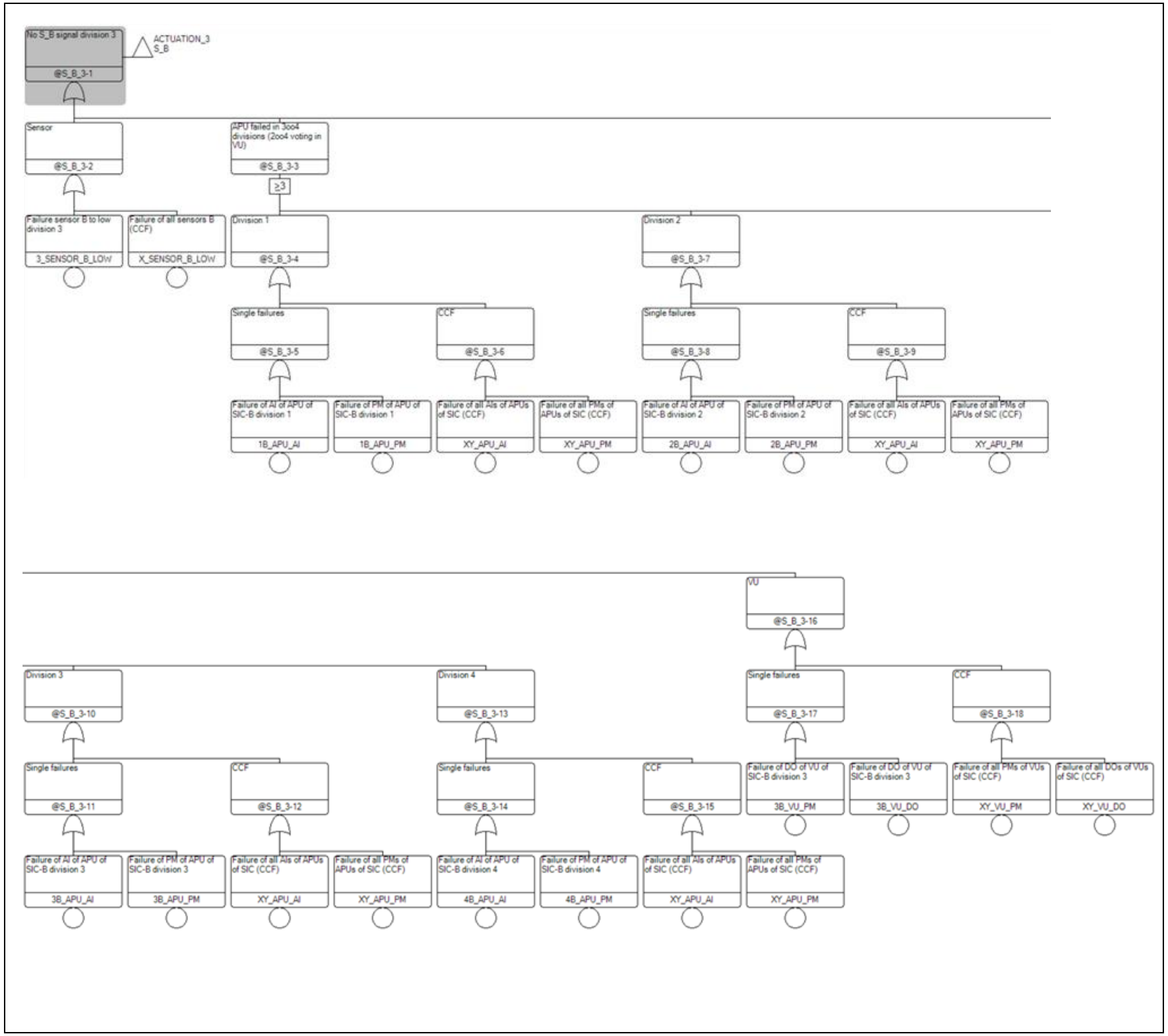

No S_B signal division 3
@S_B_3-1
ACTUATION_3
S_B
Sensor
@S_B_3-2
APU failed in 3oo4 divisions (2oo4 voting in VU)
@S_B_3-3
≥3
Failure sensor B to low division 3
3_SENSOR_B_LOW
Failure of all sensors B (CCF)
X_SENSOR_B_LOW
Division 1
@S_B_3-4
Division 2
@S_B_3-7
Single failures
@S_B_3-5
CCF
@S_B_3-6
Single failures
@S_B_3-8
CCF
@S_B_3-9
Failure of AI of APU of SIC-B division 1
1B_APU_AI
Failure of PM of APU of SIC-B division 1
1B_APU_PM
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Failure of AI of APU of SIC-B division 2
2B_APU_AI
Failure of PM of APU of SIC-B division 2
2B_APU_PM
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
VU
@S_B_3-16
Division 3
@S_B_3-10
Division 4
@S_B_3-13
Single failures
@S_B_3-17
CCF
@S_B_3-18
Single failures
@S_B_3-11
CCF
@S_B_3-12
Single failures
@S_B_3-14
CCF
@S_B_3-15
Failure of DO of VU of SIC-B division 3
3B_VU_PM
Failure of DO of VU of SIC-B division 3
3B_VU_DO
Failure of all PMs of VUs of SIC (CCF)
XY_VU_PM
Failure of all DOs of VUs of SIC (CCF)
XY_VU_DO
Failure of AI of APU of SIC-B division 3
3B_APU_AI
Failure of PM of APU of SIC-B division 3
3B_APU_PM
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Failure of AI of APU of SIC-B division 4
4B_APU_AI
Failure of PM of APU of SIC-B division 4
4B_APU_PM
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM

Figure C 29 Fault tree “no S_B signal division 3”

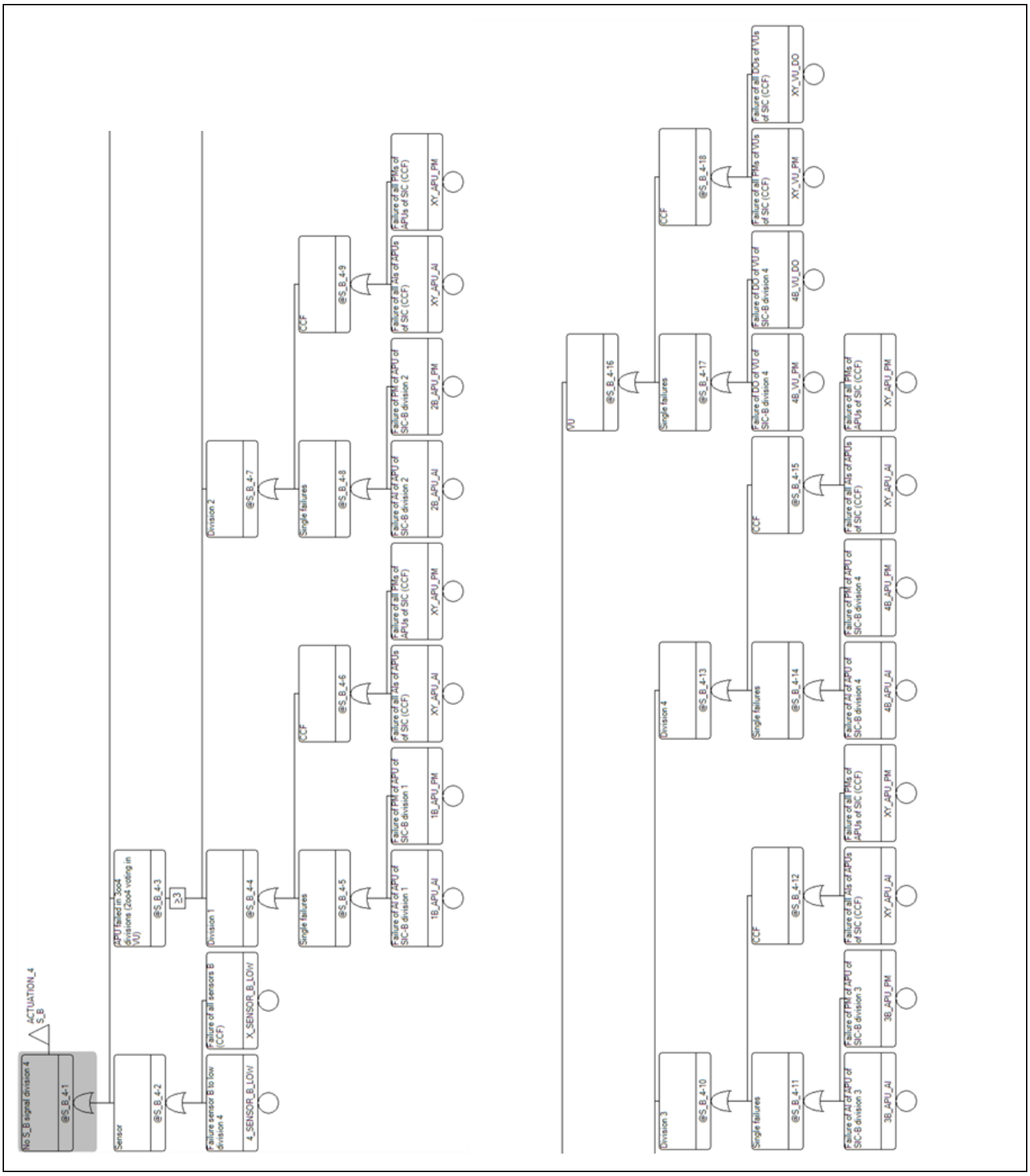

No S_B signal division 4
@S_B_4-1
ACTUATION_4
S_B
Sensor
@S_B_4-2
Failure sensor B to low division 4
4_SENSOR_B_LOW
Failure of all sensors B (CCF)
X_SENSOR_B_LOW
APU failed in 3oo4 divisions (2oo4 voting in VU)
@S_B_4-3
≥3
Division 1
@S_B_4-4
Single failures
@S_B_4-5
Failure of AI of APU of SIC-B division 1
1B_APU_AI
Failure of PM of APU of SIC-B division 1
1B_APU_PM
CCF
@S_B_4-6
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 2
@S_B_4-7
Single failures
@S_B_4-8
Failure of AI of APU of SIC-B division 2
2B_APU_AI
Failure of PM of APU of SIC-B division 2
2B_APU_PM
CCF
@S_B_4-9
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 3
@S_B_4-10
Single failures
@S_B_4-11
Failure of AI of APU of SIC-B division 3
3B_APU_AI
Failure of PM of APU of SIC-B division 3
3B_APU_PM
CCF
@S_B_4-12
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
Division 4
@S_B_4-13
Single failures
@S_B_4-14
Failure of AI of APU of SIC-B division 4
4B_APU_AI
Failure of PM of APU of SIC-B division 4
4B_APU_PM
CCF
@S_B_4-15
Failure of all AIs of APUs of SIC (CCF)
XY_APU_AI
Failure of all PMs of APUs of SIC (CCF)
XY_APU_PM
VU
@S_B_4-16
Single failures
@S_B_4-17
Failure of DO of VU of SIC-B division 4
4B_VU_PM
Failure of DO of VU of SIC-B division 4
4B_VU_DO
CCF
@S_B_4-18
Failure of all PMs of VUs of SIC (CCF)
XY_VU_PM
Failure of all DOs of VUs of SIC (CCF)
XY_VU_DO

Figure C 30 Fault tree “no S_B signal division 4”

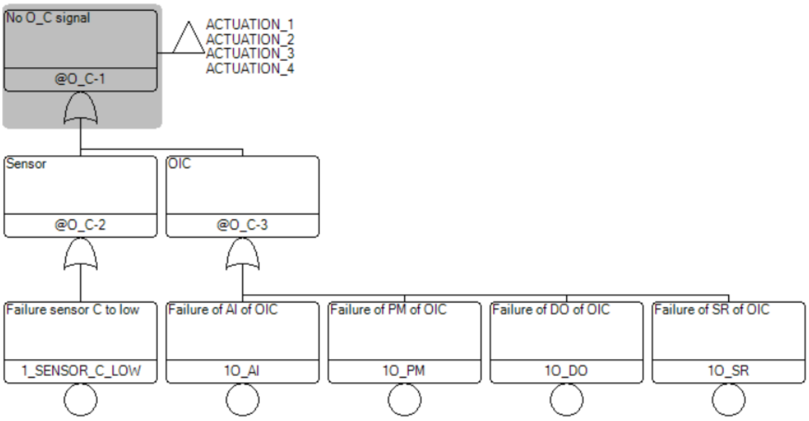


Figure C 31 Fault tree “no O_C signal”

D German Summary

D.1 Einführung

Die fortschreitende Digitalisierung der Leittechnik (I&C) von Kernkraftwerken führt zu immer komplexeren Systemarchitekturen. Dabei spielen sowohl Sicherheits-I&C-Systeme (SIC) als auch Betriebs-I&C-Systeme (OIC) eine zentrale Rolle. Während SIC für sicherheitskritische Funktionen wie Reaktorschutz, Notabschaltung und die Aktivierung sicherheitstechnischer Systeme verantwortlich ist, dient OIC der Steuerung und Regelung von Prozessen im Normalbetrieb.

In vielen modernen Kernkraftwerken erfolgt die Steuerung sicherheitsrelevanter Komponenten sowohl durch SIC als auch durch OIC. Damit wird sichergestellt, dass die betreffenden Systeme unter normalen Betriebsbedingungen effizient arbeiten, gleichzeitig aber im Notfall durch SIC angesteuert werden können. Eine zuverlässige Priorisierung ist zwischen OIC- und SIC-Signalen ist daher notwendig, um sicherzustellen, dass sicherheitskritische Befehle jederzeit Vorrang vor betrieblichen Steuerungssignalen haben.

Das übergeordnete Ziel des Projekts bestand in der Entwicklung einer systematischen Methodik zur Bewertung digitaler I&C-Architekturen in Kernkraftwerken, insbesondere im Hinblick auf die Priorisierung zwischen SIC und OIC. Dies umfasste:

- Die Entwicklung und Validierung eines analytischen Rahmens, mit dem I&C-Architekturen hinsichtlich ihrer Zuverlässigkeit und Sicherheit bewertet werden können.

- Die Erweiterung und Nutzung des Analysis and Test System (AnTeS), das sowohl reale als auch simulierte I&C-Komponenten integriert.

- Die Analyse unterschiedlicher I&C-Architekturen unter Berücksichtigung von Redundanz, funktionaler Diversität und allgemeiner Diversität.

- Die Durchführung umfassender Fehlermodellierungen und Sicherheitsanalysen, um die Auswirkungen verschiedener Designentscheidungen auf die Systemzuverlässigkeit zu untersuchen.

Durch diese Arbeiten wurde eine fundierte Grundlage für die Beurteilung digitaler I&C-Systeme in bestehenden und zukünftigen Kernkraftwerken geschaffen.

D.2 Das Analyse- und Testsystem (AnTeS) der GRS

Das von der GRS entwickelte Analyse- und Testsystem (AnTeS) stellt eine flexible Plattform zur Untersuchung digitaler I&C-Systeme dar. Es kombiniert reale Hardwarekomponenten mit Simulationen, um realistische Betriebs- und Fehlerbedingungen nachzustellen.

Die Struktur von AnTeS basiert auf vier zentralen Modulen:

1. **AnTeS-SIC**: Modellierung und Test von Sicherheits-I&C-Systemen.

   - **AnTeS-SIC-real**: Physische Implementierung eines SIC-Systems basierend auf Teleperm XS von Framatome.

   - **AnTeS-SIC-sim**: Simulation eines SIC-Systems zur Durchführung analytischer Bewertungen.

2. **AnTeS-OIC**: Modellierung und Test von Betriebs-I&C-Systemen.

   - **AnTeS-OIC-real**: Physische Implementierung eines OIC-Systems basierend auf Siemens Simatic S7.

   - **AnTeS-OIC-sim**: Simulation eines OIC-Systems für Sicherheitsanalysen.

3. **AnTeS-PAC**: Untersuchung von Priorisierungs- und Ansteuerungskontrollmodulen.

   - **AnTeS-PAC-real**: Reale PAC-Module, darunter AV42 von Framatome.

   - **AnTeS-PAC-sim**: Simulierte PAC-Modelle zur Untersuchung von Entscheidungsprozessen in I&C-Architekturen.

4. **AnTeS-FIELD**: Integration realer und simulierter Feldsysteme zur Untersuchung der Interaktion zwischen I&C-Systemen und technischen Komponenten.

   - **AnTeS-FIELD-real**: Reale Aktuatoren, Ventile und Sensoren zur Nachbildung realer Bedingungen.

   - **AnTeS-FIELD-sim**: Simulation von Feldsystemen zur Untersuchung komplexer Szenarien.

Durch diese modulare Struktur kann AnTeS verschiedene I&C-Architekturen flexibel modellieren und analysieren.

D.3 Modellsysteme

Zur systematischen Untersuchung wurden verschiedene Modellsysteme/-architekturen definiert, die unterschiedliche Grade an Redundanz und Diversität aufweisen. Das Basisfallmodell (**A1B1C1P1**) umfasst beispielsweise:

- **A1**: Ein Teilsystem SIC-A (ohne Redundanz).
- **B1**: Ein zu SIC-A funktional diversitäres Teilsystem SIC-B (ohne Redundanz innerhalb dieses Teilsystems).
- **C1:** Ein einzelnes OIC-System zur betrieblichen Steuerung.
- **P1:** Ein PAC-Modul zur Priorisierung zwischen SIC- und OIC-Signalen.

Um die Auswirkungen von Redundanz und Diversität zu bewerten, wurden inklusive Basisfall insgesamt 13 Modellsysteme betrachtet, beispielsweise:

- **A4B4C1P2-2:**
    - Vier redundante SIC-A- und SIC-B-Subsysteme.
    - Ein OIC-System.
    - Vier diversifizierte PAC-Module (2 x PAC-A und 2 x PAC-B) zur robusteren Priorisierung

Durch die gewählten Modellvarianten konnten verschiedene Sicherheitsaspekte in unterschiedlichen Systemkonfigurationen untersucht werden.

D.4 Validierung

Der Ansatz der GRS zur Analyse von I&C-Architekturen und -Systemen, der im Rahmen dieses Projekts erweitert und auf Modellsysteme angewendet wurde, sieht vor, dass sowohl qualitative als auch quantitative Ergebnisse möglichst mit mindestens zwei verschiedenen Methoden und Werkzeugen gewonnen werden. Dies dient dazu, die

Ergebnisse der Analysen abzusichern, insbesondere gegen unbeabsichtigte Fehler (innerhalb der Analysen selbst).

AnTeS-SIC-real und AnTeS-OIC-real haben zudem die Aufgabe sicherzustellen, dass die Beobachtungen in den Analysen nicht nur frei von versehentlichen Fehlern sind, sondern dass die Modellierung (z. B. der simulierten Modellsysteme innerhalb von AnTeS oder der modellierten Fehlerbäume) das reale Verhalten echter Komponenten korrekt widerspiegelt.

Hierzu wird ein durch Texte und Bilder beschriebenes System funktional sowohl mit realen als auch mit simulierten Komponenten. In beiden Implementierungen können definierte Fehlerszenarien aktiviert oder deaktiviert werden (Fault Injection). Durch die automatische Konfiguration aller denkbaren Fehlerkombinationen (via Fault Injection) und die systematische Erfassung des jeweiligen Gesamtzustands wird eine tabellarische Auflistung aller möglichen Systemzustände erstellt. Dabei erfolgt eine Bewertung, ob der jeweilige Zustand als vollständiger Systemausfall zu betrachten ist oder nicht („FMEA+“).

Dasselbe Ergebnis kann auch manuell erzielt werden, indem ein Experte die Tabelle (FMEA+) auf Basis der Systembeschreibung händisch erstellt und ausfüllt. Alle drei Ansätze – mit Hilfe realer, simulierter AnTeS-Module oder die manuelle Erstellung – dienen der gegenseitigen Verifikation, da alle drei Methoden (bei fehlerfreier Durchführung) zur selben Ergebnistabelle führen.

Die bislang beschriebenen Analyseschritte liefern jedoch nur qualitative Ergebnisse und geben beispielsweise keine Auskunft darüber, wie wahrscheinlich ein ungünstiger Zustand ist. Um quantitative Ergebnisse zu erhalten, stehen zwei verschiedene Methoden zur Verfügung, die sich ebenfalls gegenseitig überprüfen: Fehlerbaumanalysen (FTA) und Monte-Carlo-Simulationen (MC) unter Verwendung simulierter I&C-Systeme.

Neben quantitativen Ergebnissen liefern diese beiden Methoden auch qualitative Aussagen (beispielsweise sogenannte Minimalschnitte – MCS), die ebenfalls miteinander verglichen werden können. Dies ermöglicht eine zusätzliche Verifikation sowohl der Ergebnisse als auch der Modellierungen (in FTA oder MC).

Insgesamt liefert die GRS-Methodik sowohl qualitative als auch quantitative Ergebnisse, die jeweils aus drei bzw. zwei unterschiedlichen Methoden gewonnen werden. Diese methodische Redundanz macht Implementierungsfehler sehr unwahrscheinlich (wenngleich Fehler in der Systembeschreibung oder deren Interpretation nicht vollständig ausgeschlossen werden können).

D.5 Analysen

Die im Abschnitt 3.2 beschriebenen Modellsysteme wurden wie im Abschnitt 4.1 beschrieben analysiert. Während für den Basisfall (Modellsystem A1B1C1P1) eine vollständige Validierung durchgeführt wurde, erfolgten die Analysen der anderen Modellsysteme hauptsächlich mittels Fehlerbaumanalysen (FTA).

Die Ergebnisse der Analysen, d. h. die berechneten mittleren Nichtverfügbarkeiten für jedes Modellsystem, sind in Tabelle D 1 zusammengefasst

Tabelle D 1 Übersicht Ergebnisse für alle Modellsysteme

Modellsystem	Keine Auslösung (insgesamt)	Kein Signal von SIC-A	Kein Signal von SIC-B	Kein Signal von OIC
A1B1C1P1	1,80E-03	3,47E-03	3,47E-03	1,86E-02
A1B0C0P1	1,39E-02	3,47E-03	-	-
A2B0C0P2	3,26E-04	1,79E-04	-	-
A3B0C0P3	3,06E-04	1,74E-04	-	-
A4B0C0P4	3,06E-04	1,74E-04	-	-
A4B0C0P2-2	1,74E-04	1,74E-04	-	-
A1B0C1P1	1,88E-03	3,47E-03	-	-
A2B0C1P2	1,38E-04	1,79E-04	-	1,86E-02
A3B0C1P3	1,35E-04	1,74E-04	-	1,86E-02
A4B0C1P4	1,35E-04	1,74E-04	-	1,86E-02
A4B0C1P2-2	4,18E-06	1,74E-04	-	1,86E-02
A4B4C0P2-2	1,55E-04	1,74E-04	1,74E-04	-
A4B4C1P2-2	3,78E-06	1,74E-04	1,74E-04	1,86E-02

Durch den Vergleich der Ergebnisse ausgewählter Untergruppen aller Modellsysteme konnten Erkenntnisse zur Wirksamkeit von Redundanzen, funktionalen Diversitäten und allgemeiner Diversitäten gewonnen werden.

D.5.1 Redundanz

Der größte Wirkungszuwachs wird zwischen einem System ohne Redundanz und einem mit einer zusätzlichen Redundanz beobachtet.

Eine zweite zusätzliche Redundanz verbessert die Zuverlässigkeit nur noch gering.

Eine dritte zusätzliche Redundanz (d. h. z. B. insgesamt vier redundante Teilsysteme SIC-A) bringt keine signifikante weitere Erhöhung der Systemzuverlässigkeit.

Trotzdem kann eine vierfache Redundanz in bestimmten Fällen nützlich sein, beispielsweise wenn während Wartungsmaßnahmen oder durch Einzelausfälle eines der Systeme nicht verfügbar ist. In solchen Situationen kann eine hohe Redundanz das Gesamtsystem betriebsbereit halten und so die Verfügbarkeit erhöhen.

D.5.2 Funktionale Diversität

In den betrachteten Fällen steigt die Zuverlässigkeit nur geringfügig durch funktionale Diversität, obwohl beispielsweise erheblich viele zusätzliche Teilsysteme (z. B. vier SIC-B-Teilsysteme) verfügbar sind.

Aus deterministischer Sicht kann funktionale Diversität jedoch sehr nützlich sein. Falls beispielsweise ein systematischer Fehler in der Planung der Sicherheitskriterien für eines der Teilsysteme auftritt, sorgt die funktionale Diversität dafür, dass die anderen Teilsysteme mit alternativen Kriterien weiterhin zuverlässig funktionieren

D.5.3 Allgemeine Diversität

Diversität ist eine effektive Maßnahme gegen GVA (Common Cause Failures, CCF) und bietet auch Schutz gegen individuelle Ausfälle, ähnlich wie Redundanz. Die Ergebnisse bestätigen die Annahme, dass CCFs einen bedeutenden Einfluss haben können und dass Diversitätsstrategien eine wirksame Gegenmaßnahme darstellen.

D.6 Zusammenfassung und Fazit

Dieser Bericht beschreibt die systematische Entwicklung, Validierung und Anwendung einer fortschrittlichen Methodik zur Analyse kompletter I&C-Architekturen in Kernkraftwerken, mit besonderem Fokus auf die Priorisierung zwischen Sicherheits-I&C (SIC) und Betriebs-I&C (OIC). Die Untersuchung wurde unter Verwendung des von der GRS entwickelten Analyse- und Testsystems (AnTeS) durchgeführt, das sowohl reale als auch simulierte I&C-Komponenten integriert, um eine umfassende Bewertung der Sicherheit und Zuverlässigkeit zu ermöglichen.

D.6.1 Wichtige Erkenntnisse und Beiträge

Ein strukturierter Ansatz wurde verwendet, um verschiedene Modellsysteme zu untersuchen, die unterschiedliche Konfigurationen von SIC, OIC und Priorisierungsmodulen (PAC) repräsentieren. Diese Modellsysteme wurden mittels Fehlerbaumanalysen untersucht, um Fehlerwahrscheinlichkeiten zu quantifizieren und kritische Fehlerpfade zu identifizieren.

Ein zentraler Aspekt des Projekts war die vollständige Entwicklung und Erprobung von:

- **AnTeS-OIC-real** und **AnTeS-OIC-sim**,
- **AnTeS-PAC-real** und **AnTeS-PAC-sim**.

AnTeS-OIC-real stellt ein neu entwickeltes AnTeS-Modul für die Analyse von Betriebs-I&C-Systemen dar. Sie ermöglicht:

- Direkte Tests mit realen OIC-Komponenten,
- Fehlereinspeisung und Validierung von Systemreaktionen unter definierten Fehlerbedingungen,
- Vergleich realer OIC-Module mit simulierten Modellen** zur Überprüfung der Modellierungsgenauigkeit.

AnTeS-OIC-sim ist das simulationsbasierte Gegenstück zu AnTeS-OIC-real. Es wurde in Matlab/Simulink implementiert und ermöglicht:

- Detaillierte Analysen von Fehlerverhalten und Ausfallmodi,

- Monte-Carlo-Simulationen, ohne dass physische Hardware erforderlich ist.
- Vergleich mit realen Systemdaten zur Validierung der Simulationen.

AnTeS-PAC-real wurde entwickelt, um die Priorisierungs- und Antriebssteuerung (PAC) mit realer Hardware zu analysieren. Es umfasst:

- Kommerzielle PAC-Module sowie ein generisches PAC-Modul, das von der GRS entwickelt wurde.
- Tests unter realistischen Bedingungen, um die Zuverlässigkeit der PAC-Module und ihre Priorisierungslogik zu bewerten.

AnTeS-PAC-sim bietet eine vollständig simulierte Umgebung für die Analyse von PAC-Modulen und wurde ebenfalls in Matlab/Simulink implementiert. Es ermöglicht:

- Monte-Carlo-Simulationen, um das Verhalten von PAC-Modulen unter verschiedenen Fehlerbedingungen zu bewerten.
- Systematische Kreuzvalidierung der Ergebnisse mit AnTeS-PAC-real, um die Verlässlichkeit sowohl realer als auch simulierter PAC-Analysen sicherzustellen.

Durch die Integration dieser neuen Komponenten in AnTeS konnten die Analysefähigkeiten erheblich verbessert werden. Die erfolgreiche Validierung dieser Module führte zu präziseren Zuverlässigkeitsbewertungen und detaillierteren Fehleranalysen.

Die Methodik wurde explizit für das Basisfallmodell (A1B1C1P1) validiert, indem:

- Vergleiche zwischen realen und simulierten Systemen durchgeführt wurden,
- Monte-Carlo-Simulationen zur Überprüfung der FTA-Ergebnisse eingesetzt wurden,
- Eine hohe Übereinstimmung zwischen den verschiedenen Methoden nachgewiesen wurde, was die Robustheit des entwickelten Ansatzes bestätigt.

Die Analyseergebnisse zeigen, wie unterschiedliche Systemarchitekturen die Gesamtzuverlässigkeit beeinflussen. Wichtige Erkenntnisse umfassen:

- Redundanz: Modellsysteme mit höherer Redundanz wiesen signifikant niedrigere Ausfallwahrscheinlichkeiten auf.
- Funktionale Diversität: Die Verwendung funktional unterschiedlicher Auslösesignale (z. B. durch Verwendung diversitärer Sensortypen und Bewertungskriterien) trägt insbesondere aus deterministischer Sicht zur Fehlertoleranz bei.
- Allgemeine Diversität: Der Einsatz unterschiedlicher Hardware- und Software-Plattformen für SIC- und OIC-Systeme reduzierte das Risiko von GVA (Common-Cause Failures, CCF) erheblich.
- Zuverlässigkeit der Priorisierung: PAC-Module spielen eine zentrale Rolle bei der korrekten Priorisierung von SIC- und OIC-Signalen. Modellsysteme mit diversifizierten PAC-Implementierungen zeigten eine höhere Zuverlässigkeit.

D.6.2 Regulatorische und sicherheitstechnische Implikationen

Die Ergebnisse dieser Studie sind besonders relevant für Organisationen, die sich mit der technischen Bewertung und Regulierung der nuklearen Sicherheit befassen. Digitale I&C-Systeme sind inzwischen integrale Bestandteile moderner Kernkraftwerke, und ihre zunehmende Komplexität erfordert fortschrittliche Analysetechniken, um sicherzustellen, dass sie den strengen Sicherheitsanforderungen entsprechen.

Diese Forschung unterstützt deterministische und probabilistische Sicherheitsbewertungen (DSA/PSA), die durch internationale Sicherheitsstandards – etwa der IAEA – vorgegeben sind.

D.6.3 Fazit und Ausblick

Diese Studie zeigt, dass die entwickelte Methodik eine zuverlässige, systematische und transparente Herangehensweise zur Bewertung digitaler I&C-Architekturen bietet, insbesondere im Hinblick auf die SIC-OIC-Priorisierung.

Die Methodik wurde durch mehrere unabhängige Validierungsschritte bestätigt, darunter:

- Vergleich mit realen Systemen,
- Monte-Carlo-Simulationen zur Überprüfung probabilistischer Ergebnisse,
- Systematische Kreuzvalidierung zwischen verschiedenen Methoden.

Die erfolgreiche Entwicklung und Integration von AnTeS-OIC-real, AnTeS-OIC-sim, AnTeS-PAC-real und AnTeS-PAC-sim ermöglicht nun eine detaillierte Analyse komplexer I&C-Architekturen mit einer deutlich verbesserten Genauigkeit gegenüber bisherigen Ansätzen.

Die Ergebnisse bieten eine belastbare Grundlage für zukünftige Forschungsarbeiten und regulatorische Entwicklungen im Bereich der digitalen I&C-Sicherheit. Zukünftige Erweiterungen könnten umfassen:

- Einbindung von KI-gestützten Modellen zur Fehlerprognose,
- Detailliertere Analysen von GVA (CCFs),
- Integration weiterer Analysemodule für analoge I&C-Systeme, da diese in bestehenden Anlagen weiterhin eine wesentliche Rolle spielen.

Obwohl digitale I&C-Systeme zunehmend dominieren, bleiben analoge I&C-Systeme ein essenzieller Bestandteil vieler Kernkraftwerke, insbesondere in älteren Anlagen und hybriden Architekturen. Ihre bewährte Zuverlässigkeit und Widerstandsfähigkeit gegenüber bestimmten Cyber-Bedrohungen unterstreichen ihre sicherheitstechnische Bedeutung.

Durch diese Arbeit wird eine wissenschaftlich fundierte Basis für regulatorische Bewertungen und sicherheitstechnische Analysen geschaffen, um sicherzustellen, dass moderne Kernkraftwerke auch in Zukunft höchste Sicherheits- und Zuverlässigkeitsstandards erfüllen.

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Boltzmannstraße 14
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

Kurfürstendamm 200
10719 Berlin
Telefon +49 30 88589-0
Telefax +49 30 88589-111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon +49 531 8012-0
Telefax +49 531 8012-200

www.grs.de

ISBN 978-3-911727-14-3