ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP041

SAFETY SYSTEM FINAL DESIGN FOR THE ITER HEATING NEUTRAL BEAM INJECTOR TEST BED

A. Luchetta†[1], M. Battistella, S. Dal Bello, L. Grando[1], M. Moressa[1], Consorzio RFX, Padova, Italy
C. Labate, F. Paolucci, Fusion for Energy, Barcelona, Spain
J. M. Arias, ITER Organization, St. Paul-Lez-Durance, France
[1]also at CNR – Institute for Plasma Science and Technology, Padova, Italy

Abstract

MITICA, the test bed for the ITER heating neutral beam injector, will use an extensive computer-based safety system (MS) to provide occupational safety. The MS will integrate all personnel safety aspects. After a detailed risk analysis to identify the possible hazards and associated risks, we determined the safety instrumented functions (SIFs), needed to mitigate safety risks, and the associated Safety Integrity Levels (SIL), as prescribed in the IEC 61508 technical standard on functional safety of electrical/electronic/programmable electronic safety-related systems. Finally, we verified the SIFs versus the required SIL. We identified about 50, allocated to SIL2 and SIL1.

Based on the system analysis, we defined the MS architecture, also considering the following design criteria: Using IEC 61508 and IEC 61511 (Safety instrumented systems for the process industry) as guidelines; Using system hardware to allow up to SIL3 SIFs; Using certified software tools to allow programming up to SIL3 SIFs. The SIL3 requirement for hardware/software derives from the need to minimize the share of the failure probability, thus allowing maximum share to sensors and actuators.

The paper presents the requirements for the MITICA safety systems and the system design to meet them. Due to the required system reliability and availability, the hardware architecture is fully redundant for all components involved in safety functions. Given the requirement to choose proven solutions, the system implementation adopts industrial components.

INTRODUCTION

ITER requires powerful neutral beam injectors (HNB), for plasma additional heating and current drive [1]. The heating beams are produced through electrostatic acceleration of H^- or D- (Deuterium) ions, up to 1 MeV, followed by ion neutralization. Atoms need to be neutral to penetrate the high magnetic field surrounding the plasma. Negative ions are used since their neutralization efficiency at ion energy exceeding 100 keV is much greater than that of positive ions.

HNBs with the ITER requirements in terms of beam power (16.5 MW), ion energy (1 MeV), accelerated beam current (40 A), divergence (7 mrad), and pulse length (3600 s) do not exist and, therefore, the HNB development is carried out through a dedicated facility, called the Neutral Beam Test Facility (NBTF) [2], aimed at developing the ITER full-size HNB test bed [3], called MITICA, and testing it up to nominal performance.

This paper reports the design of the MITICA safety system. After a brief discussion on safety in MITICA, we summarize in the paper the system analysis executed and briefly discuss the apparent antinomy of using proven and also innovative solutions. We then present the system requirements, the applied design concepts, the proposed hardware architecture, and the approach followed for software development. Finally, we discuss the planned system commissioning.

OVERVIEW OF MITICA SAFETY

While ITER HNBs require nuclear and occupational safety, MITICA is only required to ensure personnel safety, as the nuclear risk does not demand for a specific nuclear-class safety system. The hazards in MITICA are mainly related to high voltage, explosive and asphyxiating gasses, radiation, fire, and high pressure coolants.

We decided to develop a dedicated system, called MITICA safety system (MS) and based on programmable electronics, to manage and coordinate all safety issues at MITICA experiment level. This choice was also pushed by the Regulatory Authority, which requires a centralized safety system to issue the license to operate the plant.

Functional Safety

The purpose of MS is to reduce the risk of serious injury to personnel to an acceptable level. Functional safety of programmable electronics is the subject of the technical standard IEC 61508, which is a general standard accompanied with specific standards dedicated to specific applications, such as oil, automotive and process industry (IEC 61511). As we can figure out MITICA as a process, we decided to base the MS development on the technical standards IEC 61508 and IEC 61511. Adhering to these standards during the whole life-cycle of the safety systems provides a methodology for the risk analysis and mitigation and for system design, verification, implementation, testing, and maintenance. It also supports the developers in defining the correct level of risk mitigation and improves the quality of the final product.

SAFETY ANALYSIS

Safety analysis must be carried out with the support of safety experts as this is a very sensitive activity. The purpose of the analysis is to identify all possible hazards, to quantify the risks, to define the required safety instrumented functions (SIF) to mitigate the unacceptable risks,

* Work supported by Fusion for Energy, ITER Organization, and EUROfusion
† adriano.luchetta@igi.cnr.it

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP041

and to qualify the required reliability of SIFs. Ref. [4] reports the safety analysis process executed on MITICA along with the analysis results. The safety analysis identified about 50 SIFs to be executed on call and for which the low-demand mode of IEC 61508 applies. The SIF reliability is qualified by means of four Safety Integrity Levels (from 1 to 4) which represent intervals of SIF probability of failure on demand (PFD) in low-demand mode and probability of failure per hour (PFH) in continuous mode. Table 1 shows the SIL definition in low-demand mode in terms of PFD as per IEC 61508. Figure 1 shows the classification of the defined SIFs obtained by applying a Layer Of Protection Analysis (LOPA) according to IEC 61511.

Table 1: Safety Integrity Levels

SIL	PFD
1	$10^{-1} – 10^{-2}$
2	$10^{-2} – 10^{-3}$
3	$10^{-3} – 10^{-4}$
4	$10^{-4} – 10^{-5}$

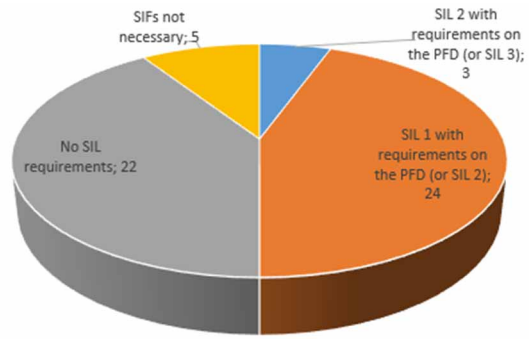

Figure 1: MITICA SIF reliability classification.

CONSERVATION VS INNOVATION

The SIL requirements for the MITICA SIFs ask for a high-reliability I&C system to reach the desired SIL.

The implementation of high-reliability safety systems must be very conservative. Technical standards require that the used components, such as sensors, actuators, hardware, and software platforms, be safety-tested and qualified for specific safety reliability levels. Therefore, the use of innovative elements in the process may be imprudent, strongly discouraged, and very often may result in unacceptable figures in terms of risk mitigation.

Despite the above conservative approach, the realization of a central safety system, which manages (nearly) all safety aspects in an experimental research device, in not trivial. The realization of a central safety system is also the choice of ITER and a practice followed in other fusion experiments [5]. The innovative element of our application is the global approach that brings many different aspects of safety together and manages them in a unified way. In conventional installations, many partial safety systems usually handle specific risks and operate in isolation. MS centrally coordinates all safety issues to ensure coordinated interventions and provide structured information to safety managers who need to make safety decisions. Specific aspects worth mentioning are the centralized management of the temporary sensor by-pass in case of faulty sensors and the exclusion of individual safety functions due to faulty sensors or actuators. Furthermore, MS operates in high-level logics, using a state approach that defines global operating states associated with permitted/prohibited actions in the plant, making safety controlled at the supervisory level.

SYSTEM REQUIREMENTS

The safety analysis provides the requirements in terms of SIFs and associated SIL allocation.

The SIF identification also defines the set of input output signals required. In MS we decided to only manage digital signals. When a given SIF relies on some analogue measurements, then local electronics is provided to implement the required signal processing and generate fault/alarm digital signals. Input signals are generated by a wide set of sensors that in some cases are installed exclusively for safety reasons, in some other cases industrial plant systems provide them for both operation and safety, as in the case of the grounding switches of the power supply systems.

Output signals usually feed industrial components provided in industrial plant systems, such as medium voltage circuit breakers and gas feeding line valves.

The size of the MS in terms of digital input/output (I/O) signals is 400 input signals and 150 output signals, organized into 12 remote I/O nodes located in different NBTF buildings and outdoor areas with maximum distances of approximately 200 m.

The timing requirements of the SIF are not very demanding as safety actions are performed via mechanical components, which have operating times of the order of 500 ms.

DESIGN CRITERIA

We designed MS following the guidelines of the functional safety technical standards and the ITER guidelines for the implementation of ITER occupational safety systems [6].

Due to the SIL requirements for SIFs, for MS hardware and software, we decided to use industrial system components that allow for the implementation of SIF up to SIL 3, such as SIL3 certified logic solvers, fieldbuses, remote input/output stations, and software development tools.

Fortunately, the timing constraints of MS SIFs are not demanding. This greatly simplifies the implementation of the system since it can be achieved by using programmable controllers as logic solvers, for which there is solid experience in safety applications and for which reliability figures are available and well-known.

Since the MS sensors and actuators reside in several different locations within the NBTF, we mandatorily adopted a distributed input/output system.

We also decided to equip the logic solver with a powerful graphical user interface. This point is qualifying as i) a rich operator interface helps safety managers to manage critical situations when they have to make quick safety decisions,

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP041

(ii) an advanced SCADA-based interface can implement crucial safety functions (and associated data transmission to the logic solver), such as temporary bypassing of sensors and overriding of safety functions. We decided to implement a fully-redundant safety system, with the exception of sensors and actuators, as many of them are complex devices that do not provide redundant signals. The design effort in these cases was to use diversification in fault detection and effect generation.

HARDWARE ARCHITECTURE

Some industrial constructors provide safety systems that can be certified up to specific SIL level. The solution chosen for MS consists of a fully redundant, distributed architecture based on a programmable controller with Profinet fieldbus on Ethernet, fail-safe remote input/output, and SCADA based operator interface [7-10].

Figure 2 shows an excerpt of the MS hardware architecture (in total, the number of remote input/output nodes is 12).

All Profinet links are implemented using optical fibers, except those inside the central cubicle that use copper. Dynamic panels are not redundant, as they just display information without any safety requirements.

Since the NBTF environment is a source of electromagnetic interference (EMI), we must use electromagnetic compatibility (EMC) best practices to minimize possible unwanted effects on electronics due to EMI.

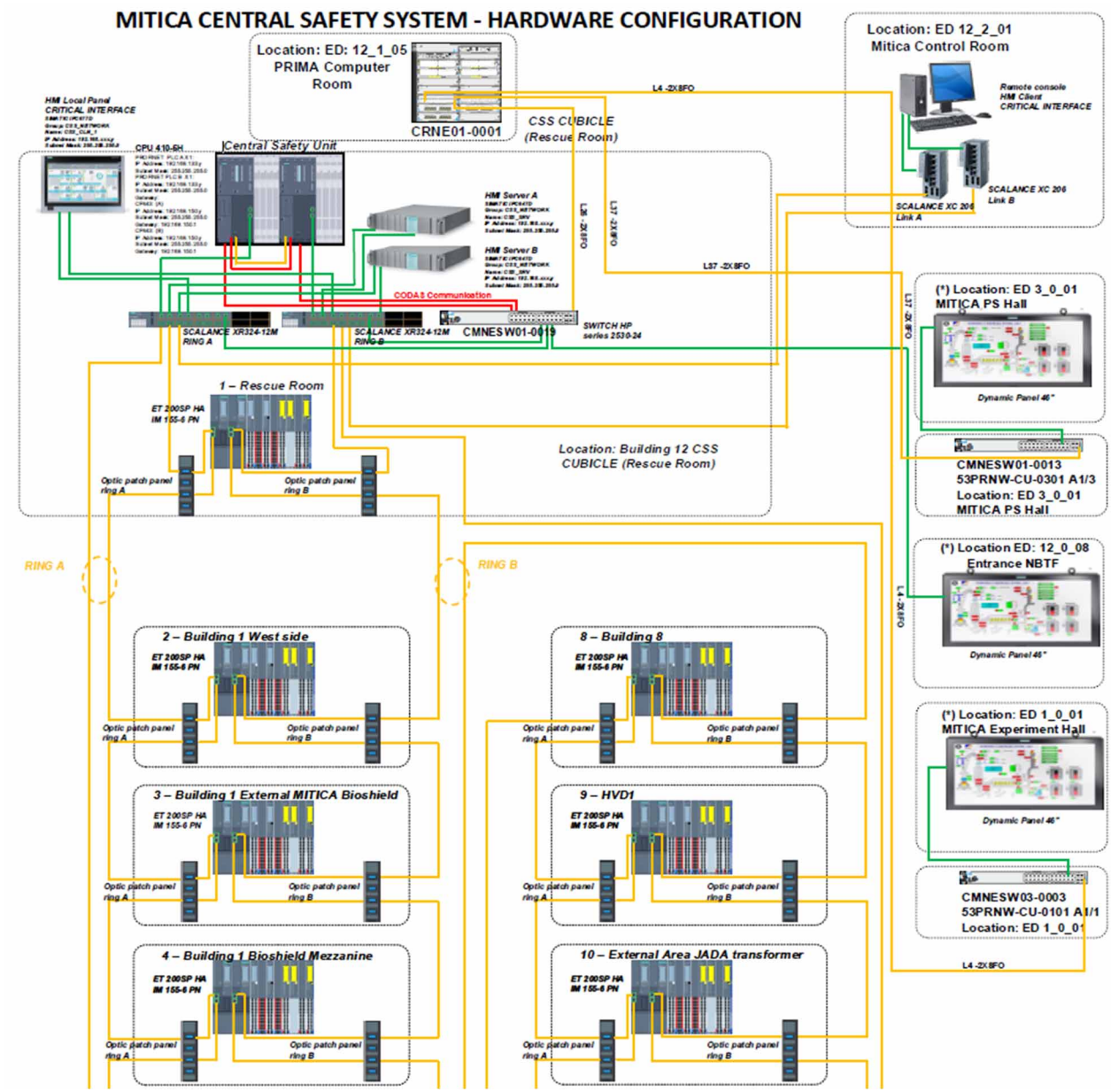

Figure 2: MS fully-redundant hardware architecture (excerpt).

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP041

The MS central cubicle and remote I/O cabinets will be qualified for EMC (sheet thicknesses and conductive sheaths) and will use three-stage EMI filters on the feeding power supply.

All cable feedthroughs will use EMC cable glands. Signal cables will be shielded and shields will be earthed at the entrance of any cabinet/cabinet. All cubicles/cabinets will be grounded locally, as close as possible.

SOFTWARE DEVELOPMENT

The certification of software is in general a critical activity. Siemens provides a set of software development tools that help producing programs that can be certified.

MS uses two of them, the SIMATIC F-Systems and Matrix Tool [11, 12].

The former is a library of certified blocks. If the programmer writes a new block by only using F-blocks inside, the new block is automatically certified.

The latter is a graphical tool organized as an incident matrix. The programmer can program a SIF by configuring SIF causes (events that require the SIF execution) on a row and SIF effects (actions to execute the SIF) on a column and checking the row-column intersection. The Matrix Tool is also invaluable during system commissioning as it can produce detailed automatic reports when testing individual SIFs. Figure 3 shows how to configure a SIF using Matrix Tool.

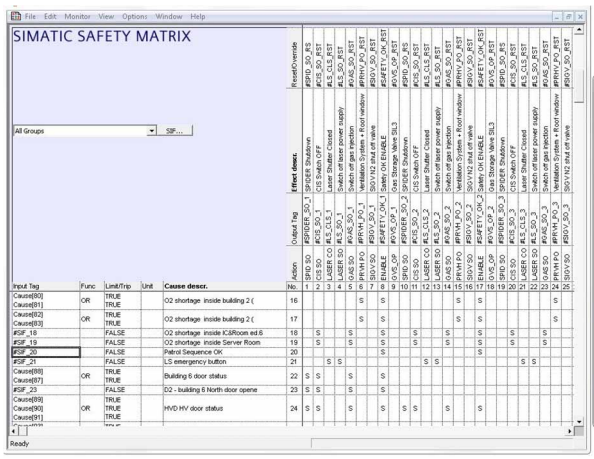

Figure 3: Example of SIF configuration via matrix tool.

The PLC control program is organized into two independent sections called Safety and Standard. The safety section handles all safety-relevant functions, while the standard section takes care of organization and communication tasks that do not affect safety. The PLC-SCADA data transfer is also divided into two data sets. Data for pure visualization uses Profinet, where safety-sensitive data, such as sensor bypass, SIF override and state transition commands, is handled using ProfiSafe, the SIL 3 certified Profinet profile.

Operating States

The operation of MITICA is modelled through operating states that define permitted and prohibited activities. The top-level operating states are Long-Term Maintenance, Short-Term Maintenance, Test and Conditioning, and Beam Operation. A given SIF may be active in one or more operational states and inactive in others. Since operating states are safety-relevant, we must manage state transitions within the safety system. In fact, it is the responsibility of the safety manager to command the transition from the current state to another permitted state. The safety manager selects a new state on the SCADA system, which forwards the chosen state transition command to the PLC. The state transition procedure is an example of a safety function performed at the SCADA level. Other examples are sensor bypass and SIF override.

Self-Diagnosis

A qualifying characteristic for the system reliability, availability, and operation is its capability of timely detecting hardware faults through self-diagnosis.

Each hardware component (input/output fail-safe modules. Profinet interfaces, network switches, CPUs) has advanced self-diagnosis features, and therefore, we can continuously monitor the system integrity.

SYSTEM COMMISSIONING

It is important to define in advance the procedure to test a safety system. It is also important to document the tests executed to the maximum extent. We plan to execute during the system implementation three different test sessions, referred to as factory acceptance tests (FAT), site acceptance tests (SAT) and safety specific tests.

Factory Acceptance Tests

In the first stage of the system implementation, we require to build a prototype consisting of the PLC, two remote I/O nodes, interconnecting fieldbus, and SCADA. The prototype must demonstrate the feasibility of the system functions before the complete construction and installation phases. In the FAT, we will check the data transmission between remote I/O and PLC and between PLC and SCADA. We will also verify the software structure and the segregation between the safety-related and standard programs.

Site Acceptance Tests

After FAT, the system is constructed and installed at the final site. The SAT purpose is to check the correct installation of the system components with particular care of cabling, cable installation, and compliance with the EMC requirements. The SAT will include full testing of:

- Faults/alarms from sensors to remote I/O and PLC;
- Commands from PLC to remote I/O to actuators;
- State machine operation;
- Variable transmission from/to PLC and SCADA;
- SCADA graphical interface.

Safety-Specific Tests

In this phase, we will test each single SIF. The SIF test will include:

- Test of each single SIF cause: a single cause (fault/alarm) at a time is generated at the sensor level

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP041

and the correct SIF execution is checked. The timing of the SIF execution is recorded. The correct visualization on the SCADA graphical panel is verified and the reporting in the SCADA alarm system is checked.
- SIF Test of each operating state where it is active;
- Test report for each SIF on all single trials executed.

The execution of the safety-specific tests is very demanding in terms of time and personnel involved; in time because the single test trials to execute are many for each SIF; in personnel because most of the plant unit experts must be involved to check their sensors and actuators.

There is another reason, based on previous experience on safety systems [13], why we expect a long duration of the safety-specific tests. In fact, the execution of these tests requires that no other parallel activities are performed on MITICA: just think of the effect of an untimely aperture of a controlled door during the tests by personnel who go and come for other installation or maintenance activities. We cannot have the whole MITICA plant available for months during the safety tests, so we have to agree with the NBTF site management to execute the tests in time windows, interleaved with other site activities. This is the source of unavoidable delays since restarting an interrupted test session requires to resume the MS and plant conditions as before the interruption. The delay due to concurrent activities during the safety system commissioning is a general problem during the construction of experimental research devices.

VERIFICATION OF SAFETY INSTRUMENTED FUNCTIONS

The SIL of the implemented SIFs must be verified taking into account the PFD of all components in the SIF chain including sensors, cabling, input modules, data transmission system, PLC, output modules, and actuators. The purpose of this verification is to make sure that the actual implementation meets the SIL requirements.

CONCLUSION

We have defined the guidelines to develop the MITICA safety system according to technical standards IEC 61508 and IEC 61511. We have set the requirements of the MITICA safety system with regard to safety instrumented functions, interface signals with sensors and actuators, space and time constraints. We have established the system architecture based on the ITER prescriptions for safety systems and the defined requirements. The system is based on proven industrial components and uses certified software tools to develop safety-relevant software. We have defined in advance the test procedure to allocate the correct time slots to execute the system commissioning. The system design successfully passed the final design review, and therefore, the system is ready to build.

ACKNOWLEDGEMENTS

This work has been carried out within the framework of the ITER-RFX Neutral Beam Test Facility (NBTF) Agreement and F4E-OFC-280 contract.

It has received funding from the ITER Organization and Fusion for Energy. The views and opinions expressed herein do not necessarily reflect those of the ITER Organization.

REFERENCES

[1] R. S. Hemsworth *et al.,"* Overview of the design of the ITER heating neutral beam injectors*", New J. Phys.*, vol. 19, p. 025005, Feb. 2017. doi:10.1088/1367-2630/19/2/025005

[2] V. Toigo *et al*., "Progress in the ITER neutral beam test facility", *Nucl. Fusion,* vol. 59, no. 8, p. 086058, Sep. 2019. doi:10.1088/1741-4326/ab2271

[3] V. Toigo *et al*., "The PRIMA Test Facility: SPIDER and MITICA test-beds for ITER neutral beam injectors", *New J. Phys.*, vol. 19, p. 085004, Aug. 2017. doi:10.1088/1367-2630/aa78e8

[4] L. Grando *et al*., "Functional safety assessment process for MITICA safety system in the ITER neutral beam test facility", *Fusion Eng. Des.*, vol. 193, p. 113678, Aug. 2023. doi:10.1016/j.fusengdes.2023.113678

[5] J. Schacht *et al*., "Realization of the requirements for a safe operation of Wendelstein 7-X", *Fusion Eng. Des.*, vol. 152, p. 111468, Mar. 2020. doi:10.1016/j.fusengdes.2020.111468

[6] A. Wallander, "Plant Control Design Handbook", ITER, Saint-Paul-Lez-Durance, France, UID 27LH2V, June 2023.

[7] SIMATIC PCS 7 process control system CPU 410-5H Process Automation System Manual, Siemens, 09/2014, A5E31622160-AB, https://cache.industry.siemens.com/dl/files/822/74736822/att_82021/v1/CPU_410_5H_en_en-US.pdf

[8] SIMATIC NET Industrial Ethernet switches SCALANCE XR-300M Compact Operating Instructions, Siemens, 05/2023, A5E02661171-17, https://cache.industry.siemens.com/dl/files/138/41299138/att_1142467/v1/BAK_SCALANCE-XR-300M_76.pdf

[9] SIMATIC ET 200SP HA Distributed I/O system - System Manual, Siemens, 03/2022, A5E39261167-AJ, https://cache.industry.siemens.com/dl/files/088/109813088/att_1113623/v1/et200sp_ha_system_en-US_en-US.pdf

[10] SIMATIC WinCC Open Architecture Version 3.18 Documentation, Siemens, https://www.winccoa.com/documentation/WinCCOA/3.18/en_US/index.htm

[11] SIMATIC Industrial Software SIMATIC S7 F Systems Engineering V6.4 Upd1 Readme, Siemens, 05/2023, A5E52460964-AB, https://cache.industry.siemens.com/dl/files/121/109817121/att_1129292/v2/Readme_en-US.pdf

[12] SIMATIC Industrial Software Safety Matrix Engineering Tool V6.3 Upd2 Readme, 07/2020, A5E44178868-AC, https://cache.industry.siemens.com/dl/files/093/109781093/att_1103902/v1/Readme.pdf

[13] A. Luchetta *et al*., "As built design, commissioning and integration of the SPIDER and NBTF central safety systems", *Fusion Eng. Des.*, 190, May 2023, 113536. doi:10.1016/j.fusengdes.2023.113536