LOGO CONFERENZA

Safety system final design for the ITER neutral beam injector test bed

A. Luchetta[*1,2], M. Battistella[1], S. Dal Bello[1], L. Grando[1,2], M. Moressa[1,2], C. Labate[3], F. Paolucci[3], and J. M. Arias[4]

[1] Consorzio RFX, Padova, Italy
[2] Institute for Plasma Science and Technology, National Council for Research, Padova, Italy
[3] Fusion for Energy, Barcelona, Spain
[4] ITER Organization, St. Paul-Lez-Durance, France

TUPDP041

*adriano.luchetta@igi.cnr.it

Abstract – ***MITICA is the test bed for the ITER heating neutral beam injector***. *We designed an extensive* ***computer-based safety system*** *(MS) to provide* ***occupational safety****, which 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. 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 poster 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 need to choose proven solutions, the system adopts industrial components* .

1. Introduction – MITICA

ITER requires powerful neutral beam injectors (HNB), for plasma additional heating and current drive [1]. HNBs with the ITER requirements in terms of **beam power (16.5 MW), ion energy (1 MeV), accelerated beam current (40A),** divergence (7mrad), 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 prototype, called MITICA, and testing it up to nominal performance.

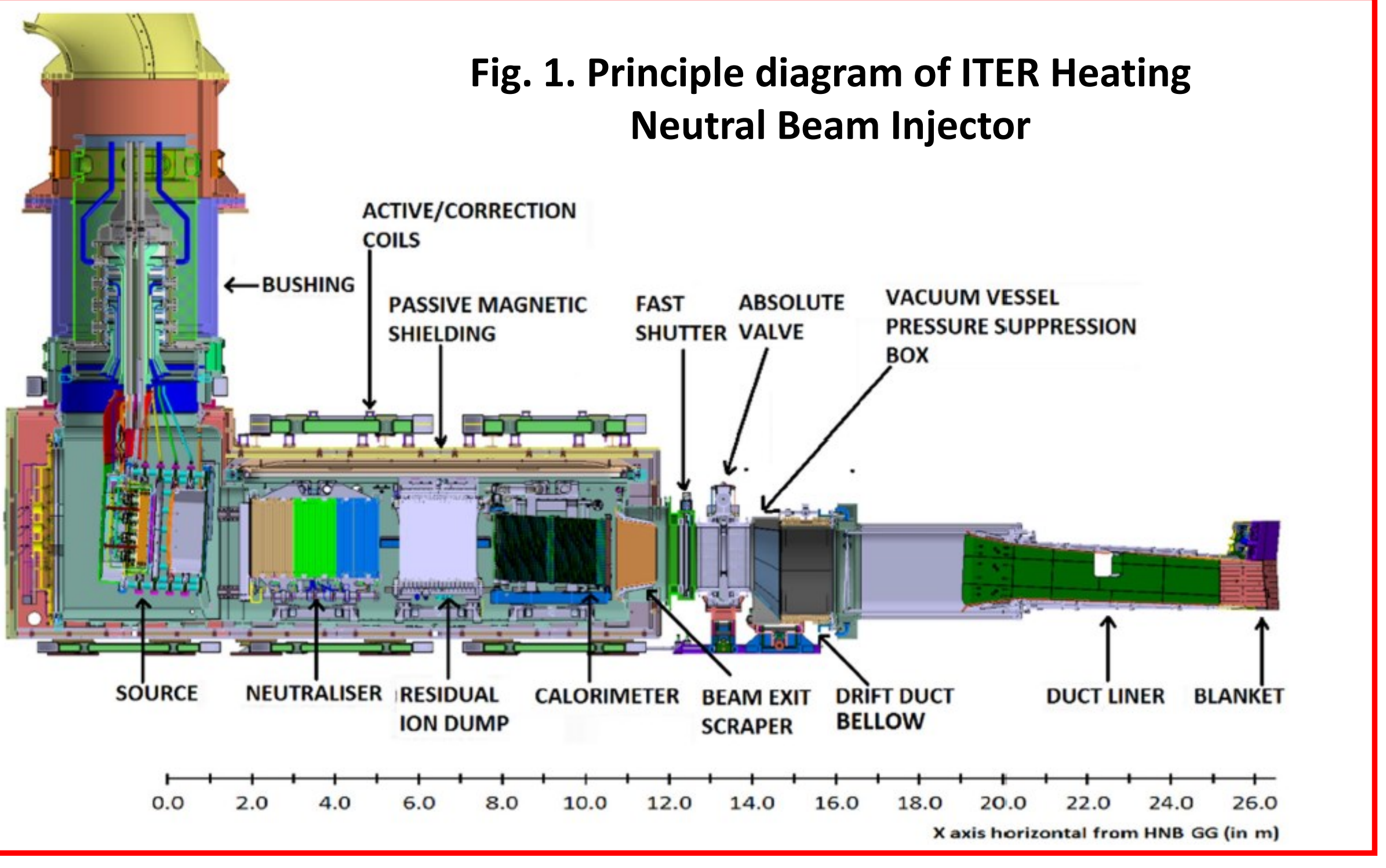


Fig. 1. Principle diagram of ITER Heating Neutral Beam Injector

2. MITICA safety – *to ensure people safety*

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 **MITICA safety system** (MS) 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.

3. Safety analysis – *to identify risks and risk mitigation*

Safety analysis must be carried out with the support of safety experts as it 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, and **to qualify the required reliability of SIFs**. Ref. [3] 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 (see Fig. 2). The SIF reliability is qualified by means of four Safety Integrity Levels (from 1 to 4, see Table 1) 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.

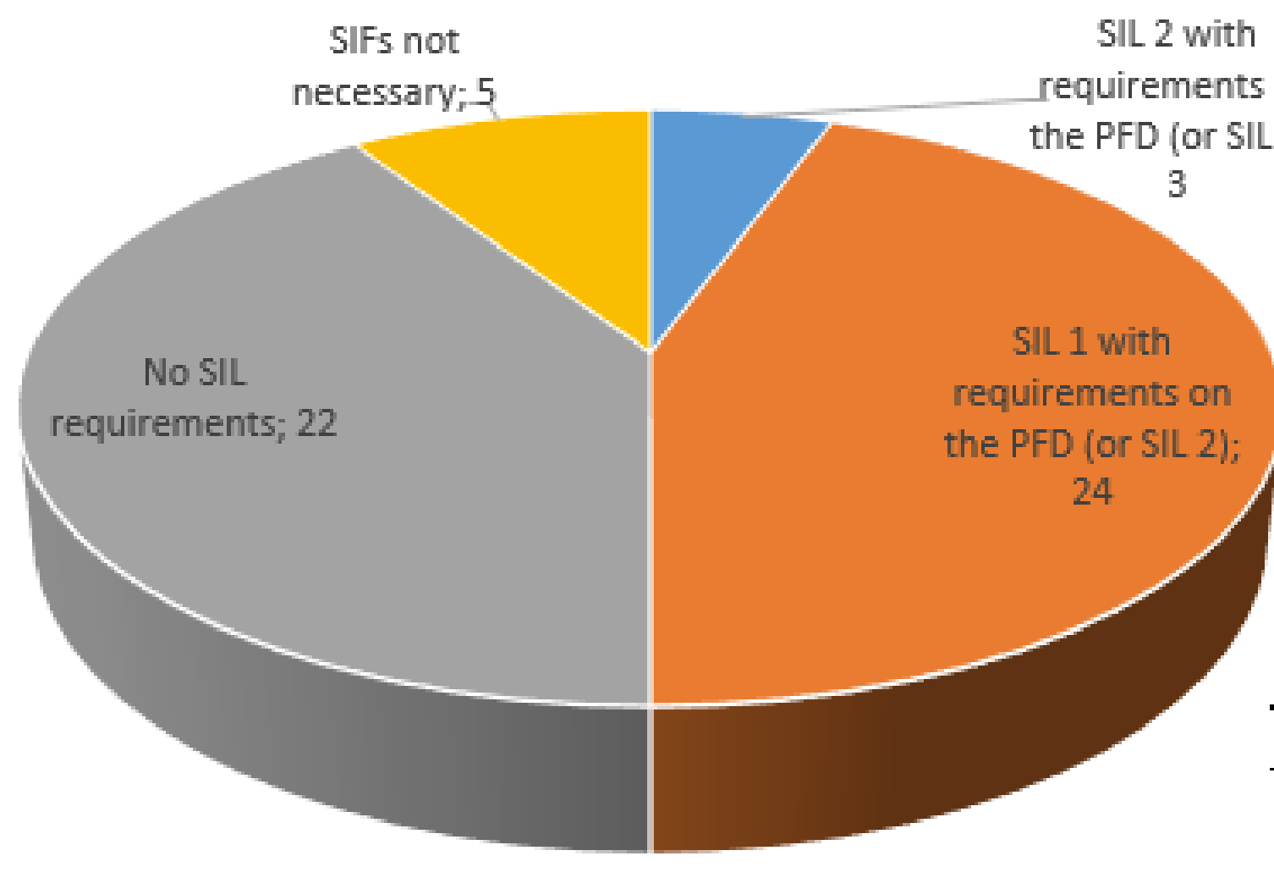


Fig. 2. Classification of SIFs by SIL

Table 1. SIL definition vs probability of failure on demand (PFD)

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

4. Conservative vs innovative approach – reliability first

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 conservative. Sensors, actuators, hardware, and software platforms must be safety-tested and qualified. Innovation may result in unacceptable figures in terms of risk mitigation. The realization of a **central safety system, which manages (nearly) all safety aspects** in an experimental research device, in **not trivial**. 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**. MS centrally coordinates all safety issues to ensure **coordinated interventions** and provide structured information to safety managers, who must make safety decisions.

5. System requirements – design input

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

The SIF identification also defines the set of input out-put signals required. In MS we decided to only **manage digital signals**. 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 demanding** as safety actions are performed via mechanical components, which have operating times of the order of 500 ms.

6. Hardware architecture – full redundancy

Industrial supplier provide safety systems that can be certified up to specific SIL levels. 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. Components: **Siemens SIMATIC S7-410-5H, ET 200SP HA – WinCC OA**

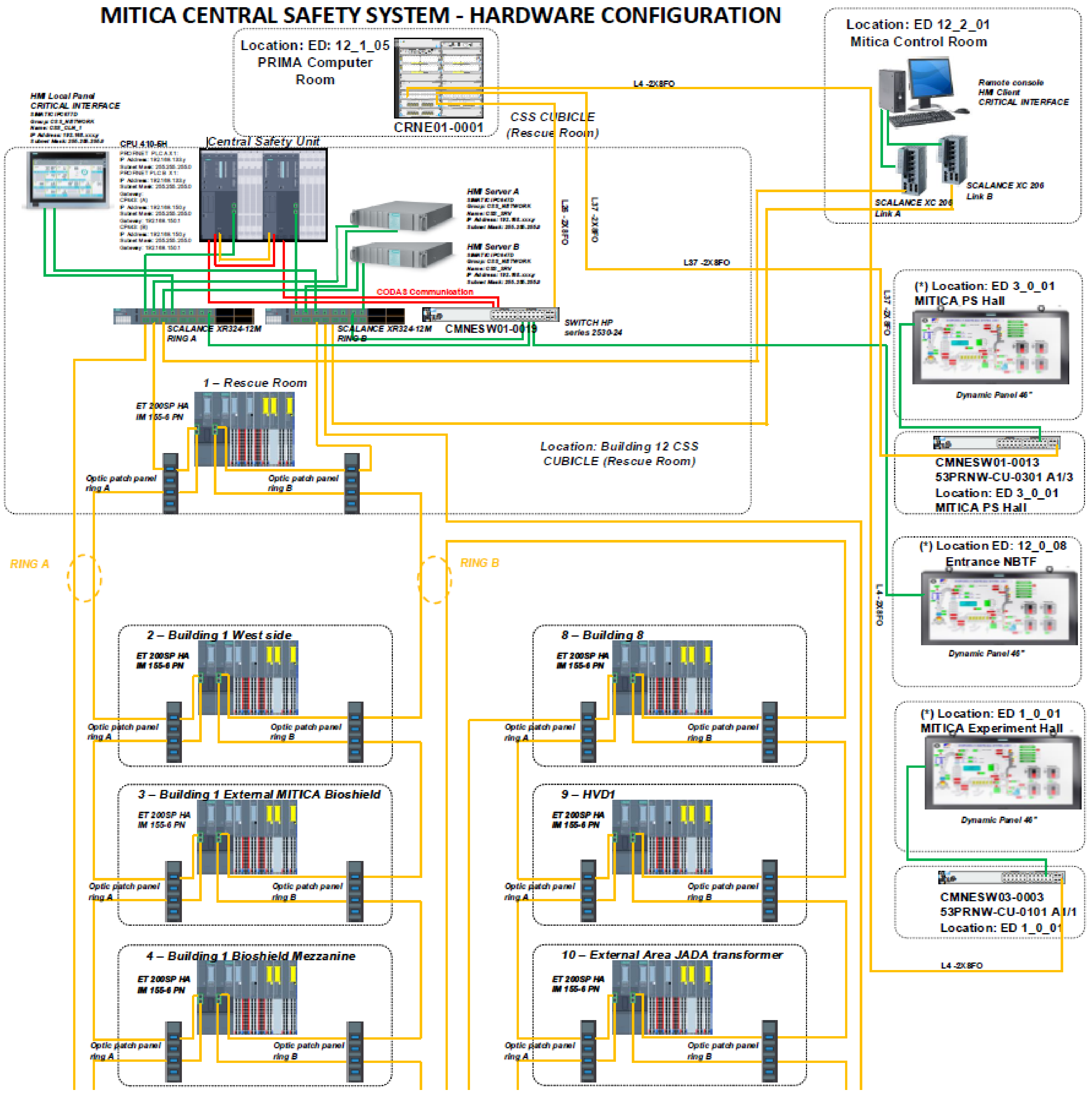
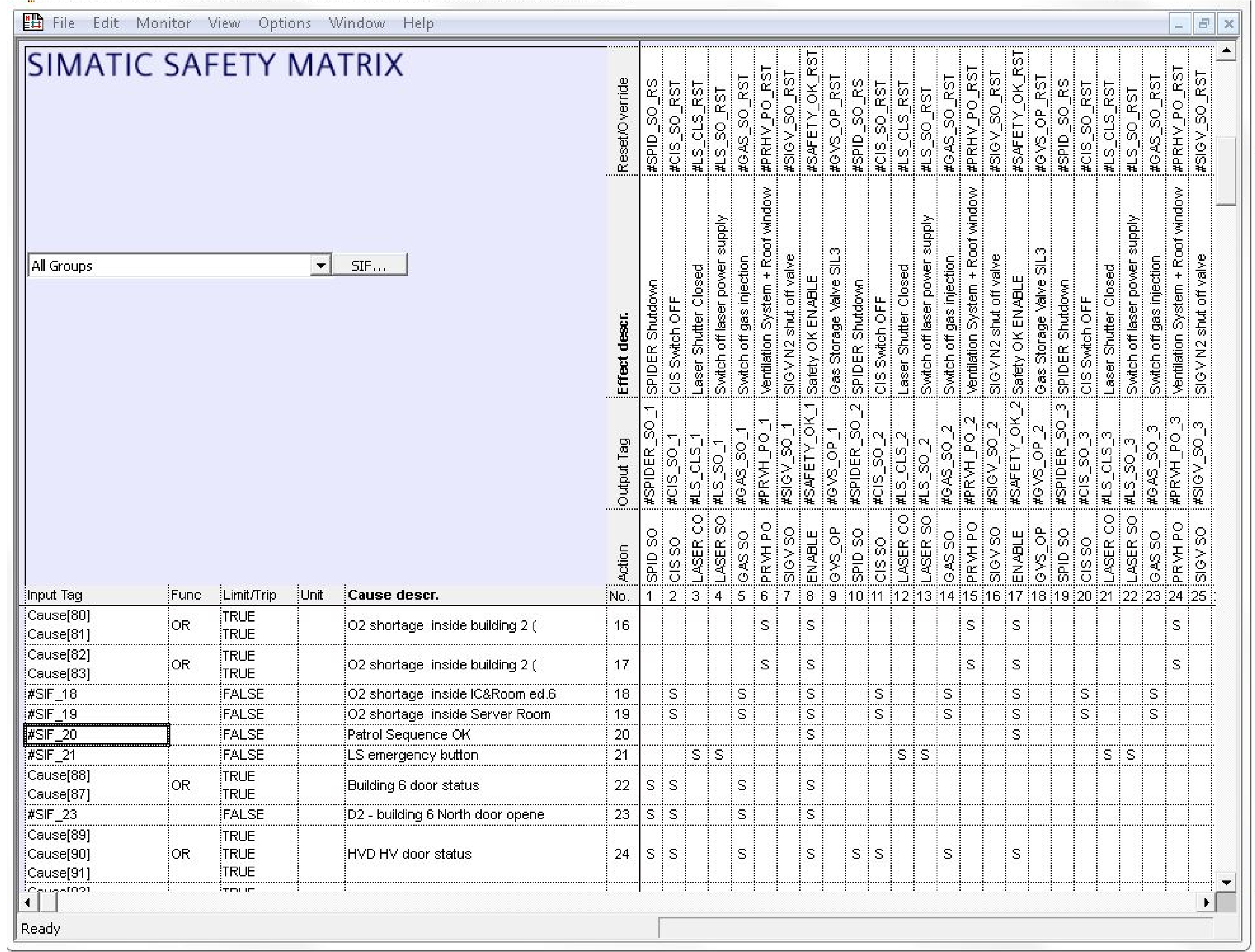


Fig. 3. Fully redundant hardware architecture – up to SIL3 reliability

7. Software development – data driven approach

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. 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.



				Reset/Override		#SPID_SO_RS	#CIS_SO_RST	#LS_CLS_RST	#LS_SO_RST	#GAS_SO_RST	#PRHV_PO_RST	#SIGV_SO_RST	#SAFETY_OK_RST	#GVS_OP_RST	#SPID_SO_RS	#CIS_SO_RST	#LS_CLS_RST	#LS_SO_RST	#GAS_SO_RST	#PRHV_PO_RST	#SIGV_SO_RST	#SAFETY_OK_RST	#GVS_OP_RST	#SPID_SO_RS	#CIS_SO_RST	#LS_CLS_RST	#LS_SO_RST	#GAS_SO_RST	#PRHV_PO_RST	#SIGV_SO_RST
				Effect descr.		SPIDER Shutdown	CIS Switch OFF	Laser Shutter Closed	Switch off laser power supply	Switch off gas injection	Ventilation System + Roof window	SIGV N2 shut off valve	Safety OK ENABLE	Gas Storage Valve SIL3	SPIDER Shutdown	CIS Switch OFF	Laser Shutter Closed	Switch off laser power supply	Switch off gas injection	Ventilation System + Roof window	SIGV N2 shut off valve	Safety OK ENABLE	Gas Storage Valve SIL3	SPIDER Shutdown	CIS Switch OFF	Laser Shutter Closed	Switch off laser power supply	Switch off gas injection	Ventilation System + Roof window	SIGV N2 shut off valve
				Output Tag		#SPIDER_SO_1	#CIS_SO_1	#LS_CLS_1	#LS_SO_1	#GAS_SO_1	#PRVH_PO_1	#SIGV_SO_1	#SAFETY_OK_1	#GVS_OP_1	#SPIDER_SO_2	#CIS_SO_2	#LS_CLS_2	#LS_SO_2	#GAS_SO_2	#PRVH_PO_2	#SIGV_SO_2	#SAFETY_OK_2	#GVS_OP_2	#SPIDER_SO_3	#CIS_SO_3	#LS_CLS_3	#LS_SO_3	#GAS_SO_3	#PRVH_PO_3	#SIGV_SO_3
				Action		SPID SO	CIS SO	LASER CO	LASER SO	GAS SO	PRVH PO	SIGV SO	ENABLE	GVS_OP	SPID SO	CIS SO	LASER CO	LASER SO	GAS SO	PRVH PO	SIGV SO	ENABLE	GVS_OP	SPID SO	CIS SO	LASER CO	LASER SO	GAS SO	PRVH PO	SIGV SO
Input Tag	Func	Limit/Trip	Unit	Cause descr.	No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Cause[80] Cause[81]	OR	TRUE TRUE		O2 shortage inside building 2 (	16						S		S							S		S							S	
Cause[82] Cause[83]	OR	TRUE TRUE		O2 shortage inside building 2 (	17						S		S							S		S							S	
#SIF_18		FALSE		O2 shortage inside IC&Room ed.6	18		S			S			S			S			S			S			S			S		
#SIF_19		FALSE		O2 shortage inside Server Room	19		S			S			S			S			S			S			S			S		
#SIF_20		FALSE		Patrol Sequence OK	20								S									S								
#SIF_21		FALSE		LS emergency button	21			S	S								S	S								S	S			
Cause[88] Cause[87]	OR	TRUE TRUE		Building 6 door status	22	S	S			S			S																	
#SIF_23		FALSE		D2 - building 6 North door opene	23	S	S			S			S																	
Cause[89] Cause[90] Cause[91]	OR	TRUE TRUE TRUE		HVD HV door status	24	S	S			S			S		S	S			S			S								

Fig. 4. Configuration of SIFs by Matrix Tool – Data driven approach

8. Conclusion – ready to build

We have:

- Defined the guidelines to develop the MITICA safety system according to IEC 61508 and IEC 61511
- Set the requirements of the MITICA safety system with regard to safety instrumented functions
- Defined the interface signals with sensors and actuators
- Defined space and time constraints
- established the system architecture and software tools for programming

The system is based on **proven industrial components and uses certified software tools** to develop safety-relevant software.

The system design successfully passed the final design review and the system is ready for implementation.

References

[1] R.S. Hemsworth et al., New J. Phys, vol. 19 025005, Feb. 2017. doi 10.1088/1367-2630/19/2/025005
[2] V. Toigo et al., Nucl. Fusion. vol. 59, 086058, July 2019. doi 10.1088/1741-4326/ab2271
[3] L. Grando et al., Fusion Eng. Des., vol. 193, Aug. 2023. doi 10.1016/j.fusengdes.2023.113678

Acknowledgements - This work has been carried out within the framework of the ITER-Consorzio RFX Neutral Beam Test Facility Agreement and Fusion for Energy – RFX contract F4E-OFC-280. 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.