nuclear fusion
IAEA

PAPER • OPEN ACCESS

The IFMIF-DONES control architecture: the state-of-the-art design of central and local control systems and communication networks

To cite this article: M. Cappelli *et al* 2025 *Nucl. Fusion* **65** 122003

OPEN ACCESS
IOP Publishing | International Atomic Energy Agency
Nuclear Fusion
Nucl. Fusion **65** (2025) 122003 (35pp)
https://doi.org/10.1088/1741-4326/adc1dd

The IFMIF-DONES control architecture: the state-of-the-art design of central and local control systems and communication networks

M. Cappelli[1,*], F. Ambi[2], E. Botta[2], J. Cruz[3], J. Diaz[3], R. Lorenzo[4], Z. Chen[5], D. Dwojewski[6], M. Giacchini[7], V. Gutierrez[8], M. Montis[7] and J. Sousa[9]

[1] ENEA, Frascati Research Center, Rome 00044, Italy
[2] Ansaldo Nucleare, Genova, Italy
[3] University of Granada, Granada, Spain
[4] IFMIF-DONES España, Granada, Spain
[5] Aalborg University, Aalborg, Denmark
[6] S2Innovation, Krakow, Poland
[7] INFN, Legnaro, Italy
[8] CIEMAT, Madrid, Spain
[9] IPFN, IST, Lisbon, Portugal

E-mail: mauro.cappelli@enea.it

Received 5 November 2024, revised 22 January 2025
Accepted for publication 18 March 2025
Published 25 September 2025

Abstract

The International Fusion Materials Irradiation Facility-DEMO-Oriented Neutron Source (IFMIF-DONES) is an advanced neutron source driven by an accelerator, designed to generate high-energy neutrons for testing materials intended for DEMO, the upcoming fusion reactor. Due to the plant's complexity, a reliable central control system is essential to manage and supervise operations safely. This paper reviews recent progress in the design of the control systems for IFMIF-DONES, with a focus on the transition into the full definition design phase. The aim is to provide here a clear and comprehensive description of the current state of the art in control systems design, outlining the latest advancements and challenges. The IFMIF-DONES control systems is composed of two levels: the central instrumentation and control systems (CICSs) and the local instrumentation and control systems, connected together by a complex set of communication networks and buses. CICS consists of three core systems: control data access and communication (CODAC), machine protection system (MPS), and safety control system (SCS), each tasked with specific functions. CODAC handles overall coordination, orchestration, and data management; MPS is responsible for machine protection; SCS ensures safety for personnel and the environment. The CICS architecture follows a hierarchical structure that supports a modular and scalable design, integrating redundancy and fault tolerance. Utilizing a distributed approach, the architecture incorporates fast devices and specialized networks

* Author to whom any correspondence should be addressed.

for real-time communication between control units. This paper details the current design status of each CICS system and outlines both ongoing and future integration plans within a unified control structure. One key challenge in this integration is synchronizing data acquisition and managing interlocks. Artificial intelligence tools can significantly enhance CICS subsystems, enabling data-driven decision-making, predictive maintenance, adaptive control, and intelligent optimization.

Keywords: IFMIF-DONES, I&C, safety control, data acquisition, fusion energy, machine protection

(Some figures may appear in colour only in the online journal)

List of acronyms

Acronym	Definition
AC	Alternating current
AI	Artificial intelligence
API	Application program interface
ARM	Area radiological monitoring
AS	Accelerator systems
ASIC	Application specific integrated circuit
ASME	American Society of Mechanical Engineers
AWS	Alarms and warning subsystem
CDCS	Control and data communication subsystem
CIC	Central instrumentation cubicle
CICS	Central instrumentation and control systems
CIS	Central interlock subsystem
CMPS	Central machine protection system
CODAC	Control data access and communication
COM	Communication
COS	Common operational state
COTS	Commercial off the shelf
CPS	Coordinated programmable safety (function)
CRS	Central control room equipment and human–machine interface subsystem
CS	Conventional systems
DAC	Derived air concentration
DAU	Data acquisition unit
DBA	Design basis accident
DC	Direct current
DEMO	Demonstration power plant
DI	Digital input
DMS	Data management subsystem
DMZ	DeMilitarized Zone Network
DO	Digital output
DONES	Demo Oriented Neutron Energy Source
DTN	Data transfer network
E/E/PE	Electrical/Electronic/Programmable Electronic systems
EMC	Electromagnetic compatibility
EMI	Electromagnetic interference
EMP	Electromagnetic pulse
EMS	Environmental monitoring subsystem
ENS	Early neutron source
EPS	Electric power system
EQ	Equipment qualification
ERMS	Effluent releases monitoring subsystem
EUC	Equipment under control (IEC-61508)
FMEA	Failure mode and effect analysis
FO	Optical fiber
FPGA	Field-programmable gate array
GOS	Global operational state
GRMS	Gaseous release measurement subsystem
GUI	Graphical user interface
HEPA	High efficiency particulate air
HFE	Human factor engineering
HFTM	High flux test module
HMI	Human machine interface
HP	Health physics
HPL	Health Physics Laboratory
HRLs	Heat removal loops
HT	Tritium - hydrogen gas
HTO	Tritium - water vapor
HV	High voltage
HVAC	Heating, ventilation and air conditioning
HW	Hardware
I&C	Instrumentation and control
IAEA	International Atomic Energy Agency
IC	Ionization chamber
ICS	Impurity control system
IDCS	Interlock data communication subsystem
IEC	International Electro-Technical Commission
IEEE	Institute of Electrical and Electronic Engineers
IFMIF	International Fusion Materials Irradiation Facility
IMS	Interface management system
IN	Interlock network
IP	Internet protocol
IRMS	Individual radiation monitoring subsystem
ISO	International Organization for Standardization
LC	Local controller
LCCS	Local conventional control system
LHS	Local hardwired safety function
LICS	Local instrumentation and control systems
LMPS	Local level machine protection system
LPF	Local passive safety function
LR	Low range
LS	Lithium systems
LSC	Local safety controller
LV	Low voltage
MPS	Machine protection system
MV	Medium voltage
NTP	Network time protocol
OPC UA	Open platform communications unified architecture
OSS	Occupational safety subsystem
PASS	Personal access safety subsystem
PBS	Plant breakdown structure
PFH	Probability of failure per hour
PLC	Programmable logic controller

PMS	Process monitoring subsystem
PRA	Probabilistic risk analysis
PSS	Plant safety subsystem
PST	Process safety time
PTP	Precision time protocol
QA	Quality assurance
R&D	Research and development
RAMI	Reliability, availability, maintainability, and inspectability
RAMSES	Radiation monitoring system for the environment and safety
REF	Reference
RF	Radiofrequency
RH	Remote handling
RSU	Radiological synthesis unit
RT	Real-time
SAR	Safety analysis report
SAT	On-site acceptance test
SCADA	Supervisory control and data acquisition
SCC	Supervision and central control subsystem
SCS	Safety control system
SDCS	Safety data communication subsystem
SFF	Safe failure fraction
SIC	Safety important class component
SIL	Safety interlock level
SSC	System, structure, or component
SW	Software
TBC	To be confirmed
TBD	To be defined
TCP/IP	Transmission control protocol over internet protocol
TMS	Timing subsystem
TS	Test systems
UDP	User datagram protocol
UPS	Uninterruptible power supply
WR	White rabbit
WS	Workstation

1. Introduction

In future fusion power plants, the first wall region will be exposed to a harsh radiation environment characterized by high-energy neutrons [1]. For the DEMO reactor, materials within the vessel will face neutron fluxes up to 5×10^{18} neutrons per square meter per second at a peak energy of 14.1 MeV. This intense radiation could cause significant damage, with potential displacement damage exceeding 10 displacements per atom (dpa) per year and a helium production rate of 10^{-13} appm/dpa. To ensure a safe design, access to a fusion-relevant neutron source is a critical priority [2].

Existing neutron sources cannot replicate the harsh radiation environment found in future fusion power plants [3]. An accelerator-based neutron source utilizing D-Li stripping reactions is considered the best option for producing the necessary neutron flux and spectrum [4, 5]. The EU provided funding through the EUROfusion Work Package Early Neutron Source (WPENS) and Fusion for Energy (F4E) to develop such a source, known as IFMIF-DONES [6–9]. This facility is outlined in the EU Roadmap [10].

The IFMIF-DONES Plant design consists of five primary systems [11]: the accelerator systems (AS), the lithium systems (LS), the test systems (TS), the plant systems (PS), and the central instrumentation and control systems (CICS). The AS produce a 5 MW deuteron beam that impinges on a liquid lithium target. The LS control lithium flow, heat removal, and purification. The high flux test module (HFTM) is part of the TS and houses material samples for testing. The I&C System, which includes the CICS, regulates plant operations, supported by PS.

The characteristics of these systems are widely described in several papers (see for example [12–14]) and their state-of-the-art design is presented in other papers of this journal's Special Issue.

This work focuses on the I&C System, whose overall architecture has been introduced in its various stages of progress in [15–18].

Control systems in particle accelerators are vital for ensuring precise operation, synchronization, protection and safety [19]. These systems manage complex machinery, instrumentation, and experiments, enabling high-energy physics research and various industrial applications.

Each experimental facility employs its own control framework for various reasons: historical period of the project, previous skills of the designers involved, proximity to the industry, in-house code development ability, emergence of innovative technologies on the market, maintenance management, to name just a few. It is therefore very difficult, if not impossible, to identify the best HW and SW technology solely based on technical evaluations.

As a result, each control system in accelerator facilities has its strengths and weaknesses. For example, EPICS [20] and TANGO [21] are the most widely used for large-scale facilities due to their scalability, while industrial SCADA systems based on PLCs and commercial tools are more suited for low-level HW control and instrumentation. Ultimately, the choice depends on the specific needs of the accelerator, including complexity, budget, and the scale of the control tasks involved. Most modern particle accelerators combine multiple control frameworks to achieve the best balance of flexibility, real-time control, and ease of use. This is also the approach followed in the design of the IFMIF-DONES control system, which may be called a hybrid control system, as will become clear later in the paper.

Therefore, a comparison with other similar facilities and plants, i.e. particle accelerators or more generally large research facilities, is beyond the scope of this work, whose sole objective is the high-level presentation of the architecture and requirements of the control system design, albeit often with particular attention to the SW and HW technologies currently considered as candidates. It should also be remembered that the entire project is still underway (in the so-called 'project definition phase'), therefore all choices may be subject to

revision by virtue of the technical, scientific or management needs of the project, or more simply due to the emergence of new technologies in the market or in research.

In this work, the approach to the IFMIF-DONES control is presented from a centralized perspective: local control systems will be described in terms of their requirements only, while their physical implementations are not considered here (they are discussed elsewhere, as their specific design depends on the type of physical system they have to control, whose physics can vary significantly from case to case).

A centralized vision for the control system of a plant is crucial for ensuring seamless integration (i.e. avoiding the need for custom-made SW or complex adaptations), coordination, and management of complex operations. By unifying the monitoring and control functions under a single, cohesive framework, it enables real-time visibility of processes across different subsystems, enhancing operational efficiency, decision-making, and safety. A centralized control system reduces the risk of errors, allows for quicker responses to anomalies or failures, and simplifies maintenance through streamlined diagnostics and troubleshooting. Moreover, it provides a scalable foundation for future upgrades, ensuring the plant can adapt to evolving technologies and operational demands, while maintaining reliability and performance.

This paper provides an overview of the current state of the overall design for the CICS, with a focus on the key advances in the three main CICS Systems: control data access and communication (CODAC), machine protection System (MPS) and safety control system (SCS), and their intercommunication with the local systems.

Since this is the first complete presentation of the IFMIF-DONES plant control system, priority was given to the descriptive approach of the entire project rather than critically evaluating individual problems, to which specific work will be dedicated in the future.

In particular, in section 2, the IFMIF-DONES control systems architecture is presented from a centralized perspective. Section 3 presents the current state of CODAC, while section 4 and section 5 present advancements in the design of MPS and SCS, respectively. Local control is widely described in section 6, while the communication networks are extensively introduced in section 7. Section 8 addresses the problem of protection and safety from a more transversal point of view, including the problem of comparison with the safety standard to follow. Finally, section 9 draws some conclusive lines that give a glimpse of some of the possible future developments that may accompany the next few years and the future phases of the project.

2. DONES control systems architecture: a centralized perspective

The DONES I&C system features a hierarchical structure, similar to other experimental plants (see for example the ITER

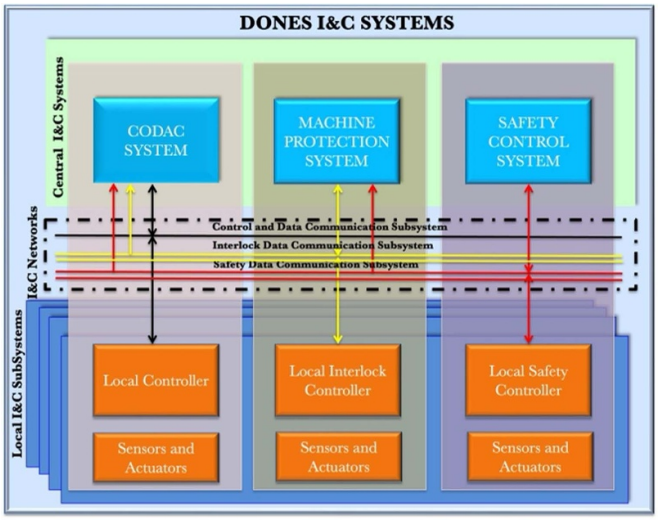

Figure 1. DONES I&C systems: general top-level architecture. Adapted from [15], Copyright (2019), with permission from Elsevier.

case [22–25], or other modern I&C systems for tokamaks [26]), with a top-level CICS overseeing local instrumentation and control systems (LICS).

The centralized control system relies on seamless data acquisition, processing, and command transmission to ensure smooth and safe operations. Data acquisition from various sources, such as sensors, equipment, and monitoring systems, allows the control system to gather real-time information about the plant processes. Data are then processed and analyzed to detect anomalies, optimize performance, and ensure compliance with operational parameters. Based on this analysis, the control system generates commands that are transmitted to local control systems, enabling precise adjustments and corrective actions. The user interface plays a critical role in system monitoring and control by providing operators with real-time insights into the plant performance, ensuring informed decision-making. Additionally, safety interlock functionalities are integrated into the system to automatically halt operations in hazardous situations, ensuring personnel and equipment are protected. This holistic approach to data management, analysis, and control ensures plant efficiency and safety.

The overall system employs a distributed control approach, granting local subsystems independence while maintaining central oversight. The CICS manages, monitors, and regulates plant parameters, stores data, and provides a system-wide view. It relies on supervisory tools to maintain constant communication with LICS and interact with other subsystems in RT. In figure 1 the general top-level architecture is shown (as an evolution of the preliminary design in [15]).

Sensors and actuators are here used as general terms, with specific implementations varying based on the system. They range from simple devices like thermocouples and flow meters to more complex diagnostic instruments. Actuators often include electromagnetic pumps, valves, or motors. While

detailed descriptions of these instruments are beyond the scope of this paper, they are discussed in specific papers on diagnostics [27] or elsewhere in this journal's issue. In principle, raw signal data is processed and converted into process variables (PVs), accessible throughout the plant. LICS are responsible for controlling subsystems and components to maintain PVs within specified ranges at a local level. I&C Systems typically include a HMI and operational monitoring capabilities at each hierarchical level.

The control architecture relies on a real-time distributed control system built using also open-source SW. Robust control HW, such as FPGAs and programmable automation controllers or PLCs, is employed. Communication networks, including Ethernet and 10 Gigabit Ethernet, facilitate the regulation and monitoring of the entire plant operation and status.

Figure 1 shows how the CICS is divided into three functional systems CODAC, MPS, and SCS. These systems maintain continuous, two-way communication with their counterparts at the local level using specific networks and buses. The basic architecture of CODAC, MPS, and SCS was introduced in [16–18].

Such a modular subdivision allows for a focused design approach while meeting the specific availability and security requirements of each system, which do not necessarily have to be the same. At the same time, this is an open-base architecture, enabling the adoption of either an industrial SCADA or open-source SW for implementation (while considering any future specific requirements that might affect the feasibility of one option over the other).

In figure 2 a decomposition of the CICS systems and subsystems is presented. The internal blocks of CODAC, MPS and SCS will be illustrated in sections 3–5.

In table 1 the main design specifications for the CICS architecture are reported.

In what follows an overview about the current design of the CODAC, MPS and SCS systems will be then provided, taking into account both ongoing and future integration plans within a unified control structure.

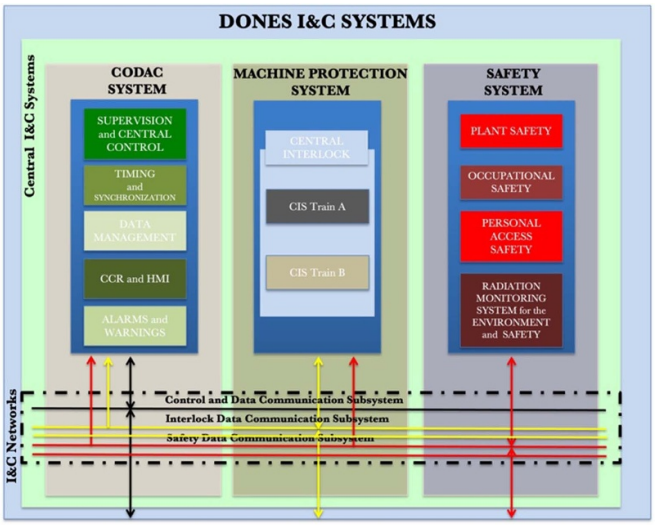

Figure 2. Decomposition of the DONES plant instrumentation and control subsystems. Adapted from [15], Copyright (2019), with permission from Elsevier.

Table 1. CICS general design specifications.

CICS system	Safety classified	Total number of signals/second (indicative numbers)	Quality class	Reference standards
CODAC	No	15 000 −25 000	QC-3/QC-4	Industrial
MPS	No	300–500	QC-3	IEC 61508, Safety integrity level
SCS	Yes	100 (SIC-1), 500 (SIC-2), 2000 (NSC))	QC-1/QC-2	IEC 61226, IEC 61513, IEC 61508

3. The CODAC system

A detailed description of the main components of the CODAC System, namely data management (DMS) subsystem, the HMI system, and the timing subsystem (TMS), has been preliminary given in [15, 16]. In what follows a summary and an updated insight will be provided.

3.1. CODAC functions

The control of the IFMIF-DONES plant relies on a network of complex systems managed by a central coordination and management system [15–18]. The CICS ensures comprehensive control over the entire IFMIF-DONES plant, handling the management, monitoring, and control of all plant parameters and variables, as well as data storage and visualization. It operates through a series of supervisory systems that maintain continuous, bidirectional communication with the LICS, which manage the local control of individual subsystems.

The CODAC System is the component of the CICS responsible for coordinating the local control systems of IFMIF-DONES, orchestrating their operations, and collecting and archiving all plant-generated data. Specifically, CODAC oversees the supervision and control of normal IFMIF-DONES system operations, ensuring that the MPS is not inadvertently triggered.

CODAC has been designed as a two-level architecture:

- Central CODAC system: This system coordinates control and monitoring across all PSs;
- Local conventional control system (LCCS): Integrated into each LICS, this system provides control functionality during normal operations.

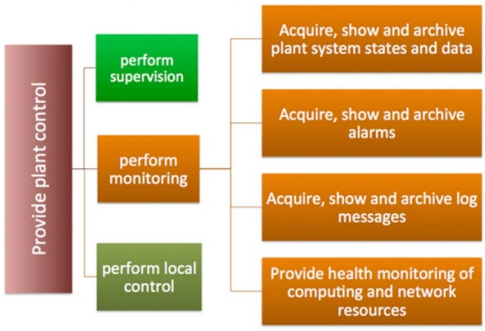

Figure 3. CODAC functional breakdown.

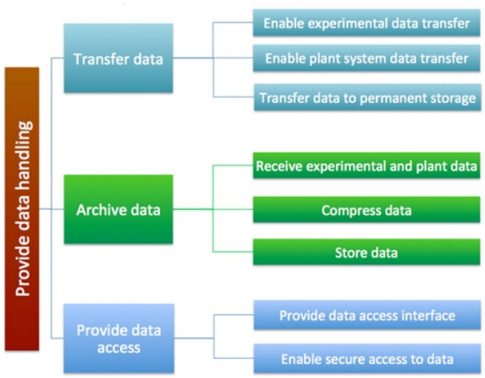

Figure 4. CODAC data handling functional breakdown.

The primary role of the CODAC system is to ensure the coordination of all technical systems within the plant—whether part of the AS, LS, TS, or PS—through configuration, synchronization, and data retrieval. Additional key functionalities of the central CODAC system include: monitoring all PSs; displaying system statuses for operators; automating scheduled operations; retrieving and storing data from all local systems; acquiring and archiving experimental data; managing alarms and warnings.

Moreover, CODAC monitors, archives, and displays the behavior of both the CMPS and the central SCS (CSCS). In response to actions initiated by CMPS or CSCS, CODAC can execute corrective or evasive measures to restore normal operation or safely shut down the plant.

Figure 3 shows the CODAC functional breakdown to provide plant control, while figure 4 presents a possible data handling functional breakdown.

3.2. CODAC subsystems

The central CODAC system is composed by six subsystems: SCC, TMS, DMS, CRS, AWS, and CDCS.

Each subsystem plays a vital role in ensuring that the CODAC system functions as the nerve center of the IFMIF-DONES plant, enabling coordinated control, monitoring, and data management across all operations. The main functions of each CODAC subsystems are described hereinafter.

3.2.1. The SCC subsystem. The SCC subsystem oversees the coordination and global management of plant operations. It ensures synchronization between local systems and the central control, orchestrating the smooth operation of all plant subsystems. It receives the information necessary for operation of the DONES plant from the local subsystems. The status of the plant operation will be displayed on the central control console of the SCC. Each LICS receives low-level commands as well as high-level commands from the CICS that result in multiple commands toward the process. The LICS is responsible for the interpretation of the high-level command and transform it into multiple unitary commands, controls their execution and sends back the execution status to the CICS. For state machines, the LICS shall send an execution status for each transition back to the CICS.

3.2.2. Timing subsystem (TMS). The overall time sequence of operation is centrally controlled by the timing signal imposed by the TMS. The TMS sends master clock signal to the TMS gateway of each system to synchronize all the clocks of the plant. The system provides accurate and synchronized timing across the entire plant, ensuring that all devices and systems operate in unison. This synchronization is vital for time-sensitive operations, data collection, and system coordination. A more detailed description of the operation of the TMS will be given in section 7 within the discussion on networking.

3.2.3. Data management subsystem (DMS). The DMS is responsible for archiving process information and system information. The DMS handles the acquisition, storage, and processing of both operational and experimental data generated by the plant. It ensures data integrity and availability for real-time analysis and post-operation reviews. Every LICS shall be able to send acquired or computed information to the CICS in raw data or engineering units. The DMS is also responsible for the integration of all data exchanged in the plant through the control framework.

3.2.4. Central control room equipment and HMI subsystem (CRS). The operator user interface in the central control room (CCR) provides the tools and interfaces that operators use to monitor, control, and manage the plant operations from the CCR. It ensures that plant personnel can interact with the system safely and efficiently by means of a HMI implemented in the operator console in order to permit the user to monitor, supervise and control all relevant processes. The aim of the operator user interface is to facilitate effective operation and control of the subsystems. The interface is graphic-based and animated with feedback information coming from the process, which helps the operator in making operational decisions.

3.2.5. Alarms and warnings subsystem (AWS). The AWS is responsible for detecting and managing alarms and warnings within the plant. It ensures timely notification of any abnormal

conditions or system failures, allowing operators to take corrective action promptly. The system delivers crucial information to operators via a CODAC system service designed for fault diagnosis and correction. The primary purpose of alarm annunciation is to alert operators to deviations from normal operating conditions. The ultimate goal is to prevent or minimize physical and economic losses by enabling operators to intervene in response to the conditions that triggered the alarm. Speed and precision in identifying alarms that require immediate attention are critical. A plant-wide alarm and warning management policy will be established to handle alarm situations and ensure corrective actions are taken to maintain continuous, safe, and normal operation.

3.2.6. Control and data communication subsystem (CDCS).

The CDCS ensures reliable communication across the plant technical systems. It facilitates the transmission of control commands, data collection, and system status updates between the central and local systems, ensuring the smooth operation of the entire facility.

3.3. Local CODAC controllers

The local CODAC controllers are responsible for detecting and monitoring selected variables within the system. These controllers maintain direct interfaces with the central CODAC for notifications and the exchange of information related to the plant normal control. Local CODAC controllers act as field controllers, responding to signals—either from sensors or from central CODAC—with appropriate control actions. Conceptually, the local CODAC controllers are distinct from local interlock controllers (LICs) and local safety controllers (LSCs), which are dedicated to exchanging data with the CMPS and the SCS, respectively.

The local CODAC controller modules can have associated control functions and/or monitoring and communication functions, with associated high-level functions:

- Control function module: local events detection, execution of local actions, acknowledgement of central CODAC commands, execution of central CODAC commands, transmission of measured data to the central CODAC.
- Monitoring and communication module: time synchronization, system health monitoring, export diagnostic data to the central CODAC, export archive data to the central CODAC.

3.4. CODAC services

From a SW perspective, the CODAC System consists of a group of servers running a set of SW services collectively known as ‘CODAC Services’. These services handle all the tasks required by the CODAC system, with some services (such as HMI, alarm and warning, or storage services) potentially utilizing the same framework, while others (like the timing system) may be implemented separately. The CODAC services are accessible by various CODAC clients, each running task-specific applications that can connect to and utilize the available services (as illustrated in figure 5).

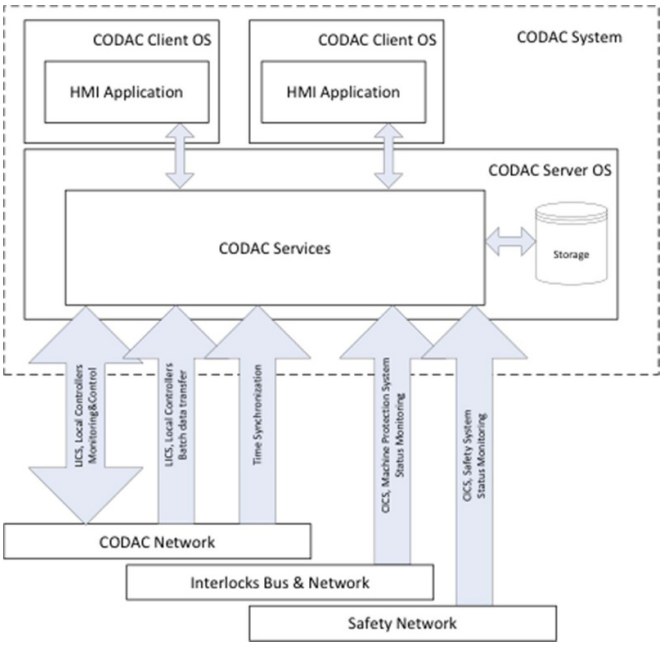

Figure 5. CODAC main components identification: software architecture.

The CODAC services provide supervisory and control (SCADA) functions across the entire plant. Each service is designed to perform a specific task transparently, offering a clear and well-defined interface. This interface acts as a boundary between CODAC, local I&C systems, computational functions, and data storage. Task-specific HMI applications, referred to as ‘CODAC clients’, can leverage these services for different purposes, such as operator control, diagnostics, or power management.

The CODAC services include:

- Alarm system—This service is responsible for monitoring, recording, and handling abnormal situations reported by the plant I&C system and other systems required for operation. It supports both automatic actions and operator interventions. The system continuously tracks alarm triggers within the control system and assists the operator by promptly alerting them to conditions requiring attention. It provides guidance, enables access to dedicated displays, executes commands, and allows for the acknowledgment of alarms. Additionally, the service ensures that alarms are communicated to relevant stakeholders, such as through a GUI, logging into the central database, and providing tools for generating reports and analyzing alarm patterns, including their frequency and occurrence.
- Electronic logbooks—The goal of this service is recording the execution of procedures and activities during operation and tests.

- Workflow scheduler—This application offers the support for the execution of the sequence of commands involving a given set of LCC.
- Health monitoring—This service enables the continuous monitoring and diagnostic assessment of both the SW and HW infrastructure. It ensures that all components of the system are functioning optimally, identifying potential issues before they escalate into significant problems. By tracking the health of the infrastructure, this service helps maintain system reliability and performance, allowing for timely interventions and maintenance when necessary.
- Database management—This service is responsible for overseeing the storage and retrieval of data within the system. It ensures that all relevant information is organized, secure, and easily accessible for both operational needs and analysis. By maintaining a structured database, this service facilitates efficient data management, allowing for quick access to historical data, reports, and real-time information, which is essential for informed decision-making and system performance.

The CODAC services exchange data with the LCCS by means of the CODAC Network, and with the MPS and SCS systems at CICS level.

The exchanged data encompasses the following categories:

- LICS LC monitoring and control: This data set reflects the current status of the controlled LICS and is refreshed with each control cycle. It features a bidirectional data flow that includes both control and monitoring information. The CODAC network facilitates the transfer of such data, with each system required to report its status to the CICS by providing the current local state known as the common operational state (COS).
- LICS LC batch data transfer: This type of data is collected by the LC at high speed and may require local processing. Consequently, the transfer can be delayed and batched for efficiency. Similar to the monitoring and control data, this information is also transferred via the CODAC network or CDCS.
- CICS MPS status monitoring: This data flow captures the current status of the MPS, including the interlock statuses obtained from all local protection systems. This data is transmitted through the interlock bus and network or IDCS.
- CICS safety system status monitoring: This flow of data reflects the current status of the safety systems and includes interlock statuses acquired from all safety elements. This information is transferred via the safety control network or SDCS.

3.5. Control framework technology for CODAC

The primary control framework currently employed for the IFMIF-DONES control systems is the EPICS control infrastructure. EPICS is an open-source SW platform (first released in 1994 but become open source and freely distributable in 2004), which is continuously maintained by a community of researchers across different scientific facilities. It benefits from numerous contributions and custom developments tailored for specific solutions, devices, and platforms.

This choice is driven by various constraints and considerations. First, EPICS is widely adopted in control systems for particle accelerator facilities and has already been implemented in LIPAc, a prototype of the IFMIF-DONES constructed in Rokkasho, Japan.

Second, the integration of some LICS using EPICS alongside others utilizing industrial solutions that communicate via standard protocols is a strong requirement.

On the other hand, for the MPS and SCS, an industrial SCADA solution has been proposed to ensure compliance with reliability standards (see sections 4 and 5).

This coexistence of two distinct control system technologies results in a hybrid control framework, necessitating a gateway for intercommunication between EPICS and the industrial SCADA. The dual SCADA systems introduce challenges related to protocol compatibility and potential delays or bottlenecks. Consequently, ongoing optimizations aim to mitigate these issues, such as developing simulators to assess delays arising from protocol exchanges and striving to achieve greater system homogeneity. The relative significance of the two systems (EPICS and industrial SCADA) will ultimately depend on the volume of signals exchanged, particularly the number of EPICS input/output controllers (IOCs) integrated into the system. This topic remains under discussion and will be explored further in dedicated works, as it extends beyond the current scope.

3.6. CODAC intercommunication

Three distinct network interfaces facilitate communication between CICS and LICS:

- Control network: This shared interface manages all aspects related to the SCC, AWS, CRS, and common information stored by the DMS.
- Timing network: Dedicated to the TMS, this interface ensures precise synchronization across the control systems.
- Massive data network: Designed for handling large volumes of data, this network transmits raw data from fast controllers, internal sensor variables, and other information that may not be managed at the CICS level but is essential for optimization and predictive maintenance. This data also feeds into the DMS.

Regarding the last network, it is important to consider that the plant will, in many cases, manage extremely high data rates (i.e. greater than 10 kHz) for fast data logging and for expected artificial intelligence (AI) technologies processing such data in RT. For instance, as an illustrative example, if some signals generate approximately 3 GB of data per second, with 5000 signals of this type, more than 250 TB of data could be generated daily. This has significant implications for network traffic and storage management.

Figure 6 illustrates the arrangement of the CODAC components and their associated network interfaces. Further

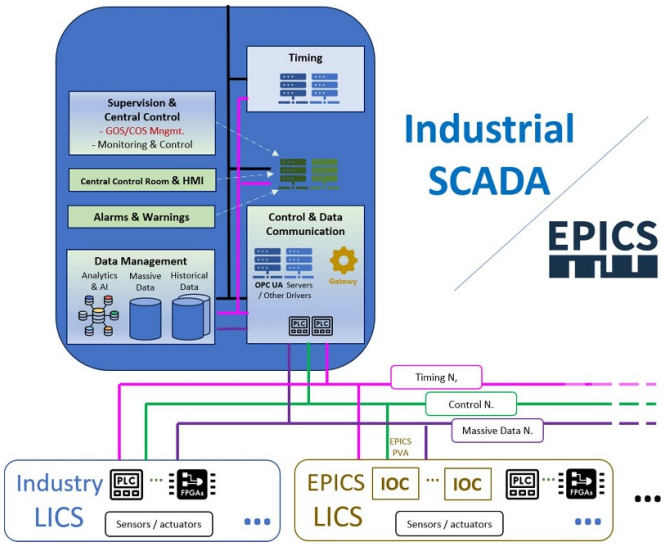

Figure 6. CODAC components and network interfaces.

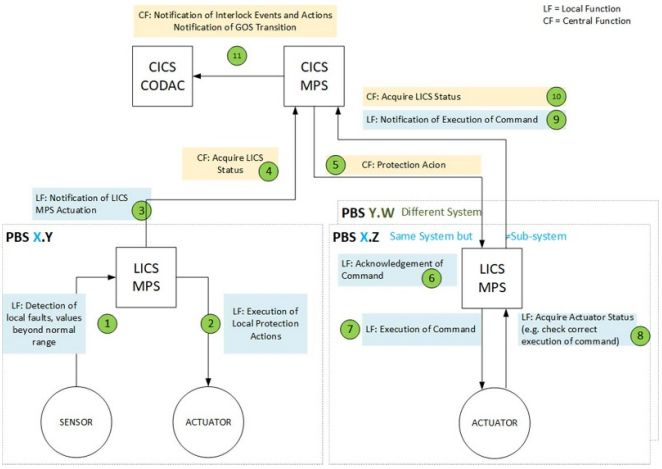

Figure 7. Local and central MPS functions. Reproduced from [18]. CC BY 4.0.

details on IFMIF-DONES networking will be given in section 7.

As a primary requirement, the CODAC networks must support both ProfiNet and EtherCAT protocols. Additionally, the integration of the OPC UA protocol is essential for facilitating communication between controllers and service applications. For interactions between CODAC services and operator WSs, the use of web protocols such as HTML5, HTTPS, and FTP is foreseen. Furthermore, implementing a redundant infrastructure is also a critical requirement to ensure system reliability and availability.

3.7. CODAC RAMI

The CODAC system is required to maintain an inherent availability of no less than 98% during scheduled operation times, which is essential for achieving the overall target of 70% plant operation availability over the calendar year, along with a maximum inherent availability requirement of 75% during scheduled operation (see [11] for the project input requirements). A dedicated RAMI analysis will validate these objectives for the CODAC design. Design decisions, such as a redundant architecture, enhance the confidence that these targets can be achieved. As a supervisory system, CODAC must remain operational throughout various maintenance phases of the plant. Switching off the CODAC is only anticipated in the event of a complete plant shutdown. To further maximize availability and facilitate maintenance activities without necessitating a full shutdown, critical components (such as servers, UPS units, and disks) will be duplicated and mounted on skids for easy replacement. These requirements highlight the need for high availability within the CODAC control framework.

4. The MPS system

The MPS is designed to safeguard the investment in the IFMIF-DONES plant, ensuring that no significant loss of investment or operational time occurs due to faults in the SSCs.

The MPS implements protection strategies across various levels of the plant, both local and central, to optimize machine protection and prevent:

- Failures of systems or equipment components
- Failures in the central or local control systems
- Incorrect operations

This is achieved using dedicated sensors, actuators, and high-integrity logic solvers. It is important to note that all safety-related aspects, including environmental, occupational, and radiological safety, are handled by the SCS.

The MPS is structured in a two-tier architecture (figure 7):

1. Central MPS (CMPS): responsible for plant-wide protection actions, which is divided into:
   a. The central interlock subsystem (CIS), further split into CIS Train A and CIS Train B;
   b. The IDCS.
2. Local MPS (LMPS): implemented within each LICS to manage protection events locally, confined to its respective subsystem.

The communication between CIS and MPS within the LICS is managed through the IDCS (described in section 7).

In the current design of IFMIF-DONES, the MPS functions are categorized into two primary levels:

1. Primary machine protection functions:
   a. Executing the central MPS functions.
   b. Supervising the local MPS functions.
   c. Managing the overall MPS system globally.

Table 2. MPS list of functions.

MPS functions	Beam reset to zero
	Fast beam stop
	Slow beam stop
	Gate valve open inhibit
	Beam condition (e.g., low/high duty cycle)
	Emergency backplate cooling
	Lithium loop shutdown
	Electromagnetic pump stop (lithium systems)
	Beam duct isolation (via gate valve closure)
	Isolation of secondary loop (at the heat exchanger inlets and outlets)
	HVAC isolation
	Activation of redundant pump (lithium systems)
	Switch flow to redundant filter (lithium systems)

2. Service functions:
   a. Providing supporting functions that ensure effective machine protection.

The CIS coordinates these interlock functions via the IDCS and collaborates with the local interlock systems in the corresponding LICS. The CIS supervises local interlock implementations and activates additional protections as necessary to mitigate or eliminate detected hazardous conditions.

The preliminary list of MPS functions is reported in table 2.

These functions are critical for ensuring the safety and protection of the IFMIF-DONES plant in case of various faults or hazardous conditions.

The main assumptions for the current MPS design are:

1. EPICS is the reference SCADA for CODAC (yet not the only one);
2. WinCC OA is the reference SCADA for MPS;
3. The central interlock protection functions implemented by the CIS shall be conform to safety integrity level 3 (SIL 3), where SIL is defined according to IEC 61508 [28].

Assumption #3 is currently under investigation as it imposes significant constraints on the MPS without being based on a formal risk assessment. One of the key parameters driving the MPS architecture selection is the time requirement, defined as half of the process safety time (PST). PST represents the time interval between a fault that could potentially lead to a hazardous situation and the actual occurrence of the hazard, if the protection mechanism does not act.

The main interlock event for the MPS is the Beam Shutdown. A group of beam shutdown events are associated with the MPS, for which the required processing time for the central MPS controller ranges from 30 μs to 1 ms, with most events demanding a response within 100 μs.

Considering that some sensors, such as thermocouples, have response times that extend into seconds, it is expected that some interlock chains will allow for a more tolerant MPS processing time, potentially up to several hundred milliseconds.

The design requirements for the IFMIF-DONES MPS can be compared with those of the LIPAc MPS. Some design choices have been established '*a priori*,' also based on the available literature from similar facilities, with the aim of improving the overall reliability by design. Notable design decisions include:

- Redundant CIS: the system incorporates full redundancy, with two independent trains (Train A and Train B) and key components duplicated for added reliability.
- Physical separation of components: the components of the two trains are installed in separate cubicles. Currently, it is assumed that these cubicles will be located in the same room.
- Minimized use of I/O modules: the MPS architecture reduces the use of I/O modules, opting instead for communication of interlock events and actions via the IDCS. I/O modules are anticipated to be used only for interfacing with the Safe PLC of the plant safety system (PSS) and for manual hardwired override functions.

Other aspects, such as the implementation of redundancy and the specific list of components, are contingent on the choice of technology, which may be subject to change in the future.

The reference architecture for the MPS groups interlocks into three main categories:

1. Slow interlocks: These are managed by a 'slow architecture' using PLC controllers, where a central MPS processing time of a few hundred milliseconds (around 300 ms) is acceptable. This requirement was defined in the preliminary design and carried through to the detailed design phase.
2. Fast interlocks: Managed by a 'fast architecture' based on fast controllers, this category requires central MPS processing times in the millisecond range. The fast controller is typically connected to FPGA and/or logic solvers for data acquisition.
3. Super-fast interlocks: For time-critical functions with response times as short as 30 μs, direct connections are used. These bypass the Ethernet network, linking the central MPS directly to the field.

The CIS is subdivided into four functional and HW modules to allow for operational flexibility, easier maintenance, and progressive integration/commissioning (figure 8):

1. Supervisor module
2. System protection modules (SPMs)
3. CODAC interface module
4. SCS interface module

This modular design provides a structured and scalable approach to system protection, meeting the diverse time and functional requirements of the different interlock categories.

The primary goal of modularity in the CIS design is to enable:

- Seamless integration: New local implementations of the MPS within LICS can be integrated into an already existing

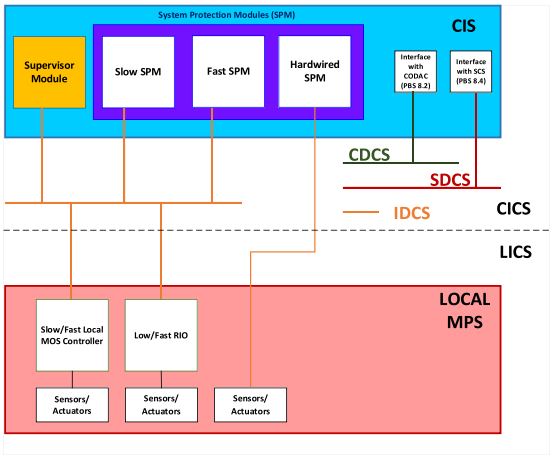

Figure 8. MPS central interlock subsystem (CIS) and its interfaces.

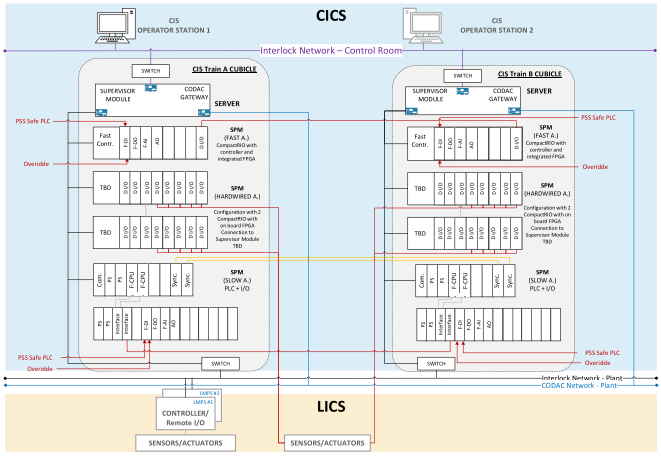

Figure 9. MPS CIS Train A and Train B cubicles.

and operational version of the CIS with minimal changes to the currently running components from the previous version.

- Flexible modifications: The modular structure allows for the modification, or even disconnection, of one module while ensuring that other CIS functions continue to operate without interruption.
- Performance-based separation: Interlock functions requiring different response times can be distributed across distinct protection modules, ensuring that the system can handle varying levels of performance requirements efficiently.

This modular approach enhances flexibility, scalability, and maintenance efficiency, supporting both the expansion and maintenance of the MPS without compromising overall system integrity.

The CIS modules are designed to handle different aspects of system management and protection with specific high-level functions, outlined as follows (see figure 9):

1. Supervisor module:
   a. Interface with MPS HMI: Ensures communication with the MPS HMI in the control room.

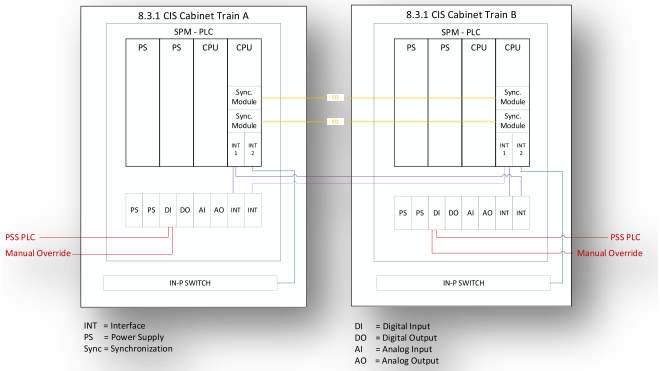

Figure 10. MPS CIS Train A and Train B interlock logics (SPM-PLC).

   b. Non-critical data exchange: Interfaces with LICS to exchange non-critical data, such as health monitors and diagnostics.
   c. Interlock events logging: Manages the logging of interlock events for future review and diagnostics.
   d. Time synchronization: Distributed via the IN to all CIS components (supervisor module, SPMs, WSs).
   e. Centralized alarm and data management: Handled by CODAC systems, with subsystems such as the DMS and the AWS.
2. SPMs (see figure 10):
   a. Receive interlock signals: Collect interlock signals from LICS.
   b. Send interlock commands: Issue interlock commands back to LICS.
   c. Receive local notifications: Notify central systems of locally implemented interlock actions.
   d. Implement interlock logic: Interlock logic is implemented within PLCs or FPGAs.
3. CODAC interface module:
   a. Data exchange with SCC: Manages necessary data exchange for plant operation.
   b. Data routing: Routes monitoring data to the central DMS and alarms to the central AWS.
   c. EPICS integration: Converts data to EPICS PVs if needed for system integration.
4. SCS interface module:
   a. Receive SCS information: Gathers status information from SCS servers and cubicles according to their categorization for monitoring and analysis.

It should be observed that the input/output (I/O) response times are dependent on the branch handling the interlock signal (slow, fast, or hardwired). This implies that if an input signal is classified as 'slow,' the output will also be slow.

Two proposed configurations for the hardwired system include:

- Option 1: CIS directly connected to LICS sensors/actuators.
- Option 2: CIS FPGA connected to LMPS FPGA.

These configurations need to be further assessed, particularly from the perspective of complexity, performance, reliability, availability, and probability of failure per hour (PFH). Option 1 is noted as unstable due to the potential for EMI and may lead to a safety risk, as there is no feedback regarding the status of the LICS or the plant.

The CIS slow architecture is designed for interlock functions with a processing time slower than 300 ms. It utilizes a Train A and Train B redundancy system to ensure reliability and availability.

The optical fiber (FO) synchronization link between the CPUs of Train A and Train B enables seamless role exchange in case the active CPU becomes unavailable. Each CPU operates as either the master or standby, depending on the initial configuration. From the system's operational perspective, this switchover is transparent, allowing the system to behave as though only one CPU is active. Both CPUs are connected to the same set of remote I/O through two separate branches, ensuring one branch serves as a backup for the other in case of failure.

The slow architecture of the system minimizes the use of I/O modules, as interlock signals are primarily exchanged through the IDCS network. During the preliminary design phase of the MPS, the SIEMENS S7-400-FH PLC was considered the optimal candidate technology, meeting SIL-3 according to IEC 61508 standards. However, newer available technologies should be explored in the future to address potential obsolescence.

Secure communication between the safety programs running on the fail-safe CPU (F-CPU) and the fail-safe inputs/outputs occurs through standard PROFIBUS DP or PROFINET IO networks, which use the higher-level safety protocol PROFIsafe. The ET 200M distributed I/O modules were selected as compatible with the S7-400F/FH Systems. This choice should be reviewed in the future, taking into account the product lifecycle and the availability of modern alternatives.

The fast architecture is designed to handle interlock functions with more demanding timing requirements, ranging from a few milliseconds up to 300 ms. In scenarios requiring rapid beam shutdown, the processing time required by the CIS is approximately 100 μs. Therefore, the fast architecture must be capable of meeting this stringent requirement.

During the preliminary design phase of the MPS, the FPGA technology was considered the best candidate to meet the time constraints while allowing for flexible reconfiguration of MPS logic. The NI CompactRIO platform was chosen due to its proven performance and extensive testing within the ITER CIS framework, which shares many technical commonalities with the IFMIF-DONES system, including PFH and timing requirements.

The proposed fast controller architecture for the ITER CIS [22, 23], known as the 'double decker,' aims to achieve a PFH of less than 10^{-7}, which is the same target set for the IFMIF-DONES CIS. This architecture features two CompactRIO chassis linked via FO connections for synchronization and coordination. Each chassis operates in parallel and includes inter-chassis diagnostics. The current IFMIF-DONES CIS design is therefore based as much as possible on the modules already tested for the similar ITER CIS. However, there are notable differences between the fast interlock system design for DONES and that of ITER (figure 11):

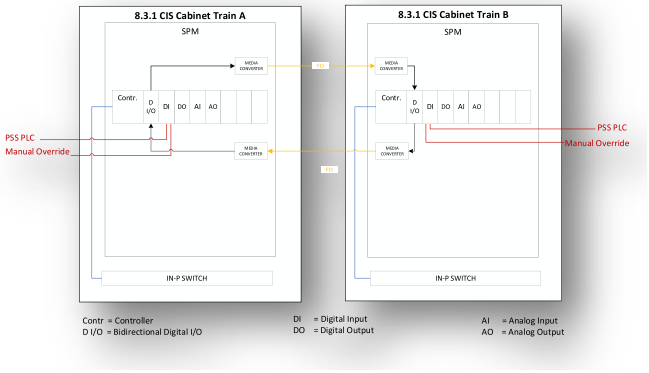

Figure 11. MPS CIS Train A and Train B input and output signals (SPM).

- Integrated controller: The DONES system does not utilize an external PC host to supervise diagnostics for the fast controller (including I/O modules and FPGA) or to connect to the supervisor module through the IN. Instead, a CompactRIO chassis with an integrated controller has been selected. This choice will need to be evaluated concerning its impact on PFH.
- COTS I/O modules: The design incorporates COTS I/O modules that are SIL-3 certified, which have only recently become available.
- Data transmission method: Unlike previous designs, the transmission of critical data, interlock events, and actions does not rely on hardwired connections between the I/O modules of the LICS-MPS fast controllers and the I/O modules of the CIS fast controller. Instead, critical data are exchanged over the IN.
- Analog inputs/outputs: The design still includes analog input and analog output signals, even though vendors suggest using only digital inputs and digital outputs for future projects.

The 'Hardwired Architecture' (figure 12) for the MPS CIS is designed to manage interlocks with stringent timing requirements, specifically needing a processing time of less than 30 microseconds for the CIS. The only identified event necessitating such a rapid processing time is the beam shutdown.

To achieve such speed, not only must the CIS process information quickly, but the entire chain—from event detection to beam shutdown—must also operate at high speed. Therefore, an architecture utilizing direct connections (i.e., without network interferences) was introduced to connect the CIS directly to the field, despite vendor recommendations against this approach for various reasons.

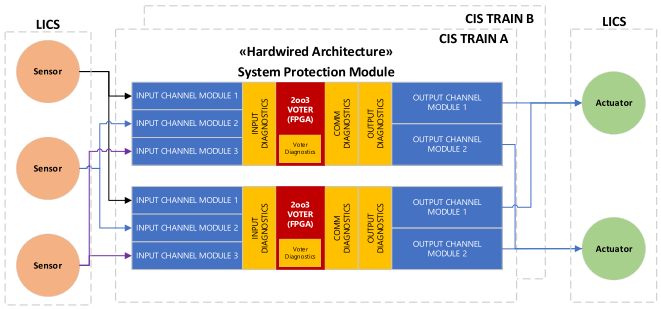

Figure 12. MPS hardwired architecture.

The only viable option available, given the time constraints and the requirement for SIL-3 functions, was the ITER 'double decker' architecture based on NI CompactRIO, which claims a PFH of less than 10^{-7} (SIL-3) [22, 23]. It is essential to calculate the PFH for the two different options being considered.

Two options for direct connection to the LICS were explored:

1. CIS direct connection to LICS sensors/actuators (Option 1): This configuration is estimated to provide response times ranging from 5 μs to 20 μs using TTL inputs and outputs.
2. CIS FPGA connected to LICS MPS FPGA (Option 2): This option is expected to have a minimum response time of 100 μs.

Several studies have been conducted, and a review of the system based on current technologies is underway. It is important to note that during the detailed design phase of the MPS, priority was given to meeting the SIL-3 requirement. Currently, however, this requirement might be considered as unnecessary with the real processing time for the CIS. Therefore some changes to the MPS design will be possible in the near future based on a reconsideration of the SIL requirements.

5. The SCS system

The IFMIF-DONES SCS is a dedicated safety-grade protection system designed to implement all identified protection functions for the safety of personnel and the environment.

The SCS encompasses two primary types of safety I&C functions:

1. *Radiological* safety functions: These include measures for radiological safety, crisis management, and environmental protection.
2. *Occupational* safety functions: These functions control, operate, and monitor specific parts of the process to protect individuals and the environment from non-radiological hazards.

The SCS carries out the following key functions:

(a) Coordinates individual automatic protections as defined in the safety procedures;
(b) Enables manual control by operators for safety functions where operators are authorized;
(c) Displays essential data for operator supervision and control concerning safety.

The SCS is structured in an independent and dedicated architecture to minimize interactions with CSs. It comprises three main components:

1. Central safety I&C
2. Local safety I&C
3. Dedicated networks: SDCS

The SCS is primarily made up of the following four subsystems:

1. Plant safety subsystem (PSS)
2. Occupational safety subsystem (OSS)
3. Personal access safety subsystem (PASS)
4. Radiation monitoring subsystem for the environment and safety (RAMSES)

Each of the four subsystems within the SCS has distinct and complementary functions. The SDCS serves as a service subsystem, facilitating the proper flow of data between these subsystems (PSS, OSS, PASS, RAMSES) and other subsystems.

5.1. Plant safety subsystem (PSS)

The SCS.PSS (SCS-plant safety subsystem) ensures the application of the principle of defense in depth by implementing technological safeguards designed to prevent or mitigate the consequences of 'postulated' accidents affecting workers, the public, and the environment. It consists of two main components: local level and central level.

A safety function is deemed 'central' (figure 13) when the cause (sensor) and effect (actuator) are situated in different subsystems. In this case, the signal indicating that a safety threshold has been reached, originating from the first LICS (LICS-1), is communicated to the second LICS (LICS-2) via the Central SCS.PSS. The monitoring data (e.g., safety threshold reached, safety function activation, actuator states) is presented to the control-room operator on the safety HMI and CODAC.

A safety function is considered 'local' (figure 14) when both the cause (sensor) and effect (actuator) are located within the same subsystem. In this scenario, the function operates locally and autonomously within the plant safety system. Monitoring data, such as safety threshold breaches, safety function activations, and actuator states, are transmitted to the central SCS.PSS for display on safety HMI and CODAC. If needed, a command from a control room operator is sent to the safety local instrumentation controller in the LICS. In cases where the involvement of the central SCS.PSS is particularly significant, a 'central function' model may be more appropriate.

The remaining three subsystems of the SCS are specifically designed to provide direct protection to personnel and their living environment. These subsystems are critical for ensuring

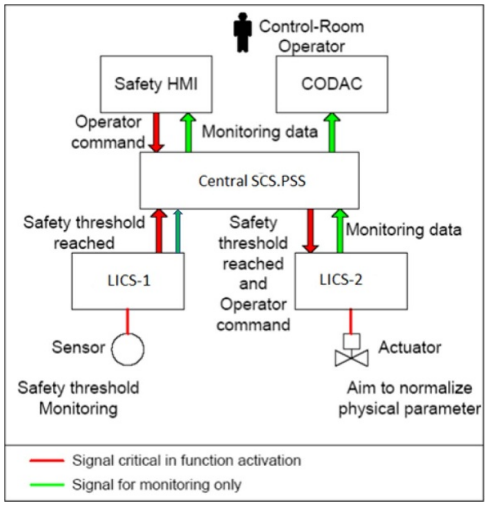

Figure 13. SCS central function.

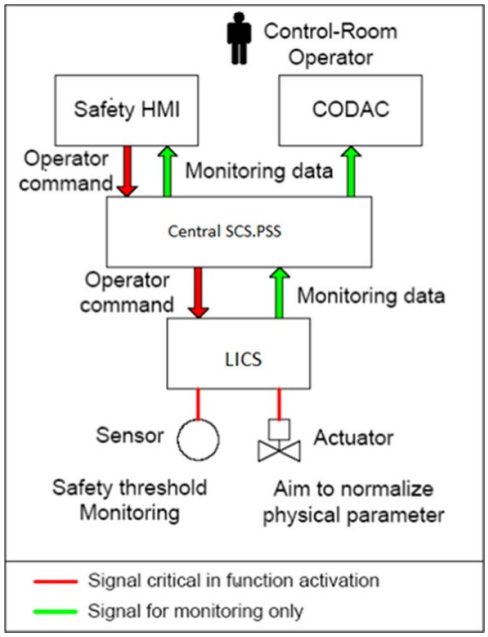

Figure 14. SCS local function.

occupational safety and environmental protection. Together, these subsystems create a robust framework for ensuring that all personnel are protected from various hazards while maintaining a safe operational environment within the plant.

5.2. Occupational safety subsystem (OSS)

The SCS.OSS is dedicated to protecting individuals (workers and the public) from various non-radiological hazards, including toxicological, physical, electrical, cryogenic, and other risks that may arise within the plant under both normal and abnormal conditions. Key functions and features of the OSS include:

- Monitoring exposure risks: OSS continuously monitors the overall exposure risk and health status of each worker by utilizing specialized SW packages designed for this purpose.
- Data inputs: The system receives input data from other LICS and associated systems. Examples include room CO_2 concentration data and fire extinguisher status from the fire protection system. Future expansions may include data from systems such as a static magnetic field monitoring system.
- No active actuations: As most commercially available instruments are classified for non-safety-relevant applications, the OSS does not directly actuate safety measures. Instead, monitoring data is interpreted by trained operators, who are responsible for manually initiating protective actions according to established plant procedures.
- Coordination with other SCS subsystems: If a process is involved, operators may communicate with the SCS.PSS for protective actions. If access to a hazardous area needs to be restricted or the area evacuated, operators will coordinate with the PASS.
- Sizing and record keeping: OSS will be designed based on personnel numbers and zone classifications relative to the risk levels of non-radiological hazards. It will maintain detailed records for each worker's total exposure to risks, incorporating data from various subsystems and periodic monitoring (e.g., thermoluminescent dosimeters, TLDs). Such data include:

    a. Radiation exposure (including contamination) from radioactive materials.
    b. Chemical exposure from radioactive materials.
    c. Chemical exposure from non-radioactive materials.
    d. Electromagnetic exposure from induced static magnetic fields.

- Shift communication: At the beginning of each work shift, the OSS will communicate each worker's status to the PASS to grant access permissions. This process involves authorizing the operator's badge for opening doors or turnstiles through badge readers for specific areas or activities.

5.3. Personal access safety subsystem (PASS)

The SCS.PASS is designed to manage and control access to specific areas within the plant where there are significant risks, including both radiological and non-radiological hazards. Its key functions and characteristics include:

1. Stopping hazardous equipment: PASS can stop equipment or devices if an unauthorized intrusion is detected.
2. Banning access: It has the authority to prohibit access to areas if a risk is identified.
3. Controlling access to safety airlocks: PASS oversees personnel access to safety airlocks, ensuring only authorized individuals can enter.
4. Interlocking with other safety subsystems: PASS can interlock with other safety subsystems to enhance overall safety protocols.

A fundamental capability of PASS is the remote control of door openings and the ability to bypass interlock bars, contingent on the plant status and the assessed hazard level (both radiological and conventional).

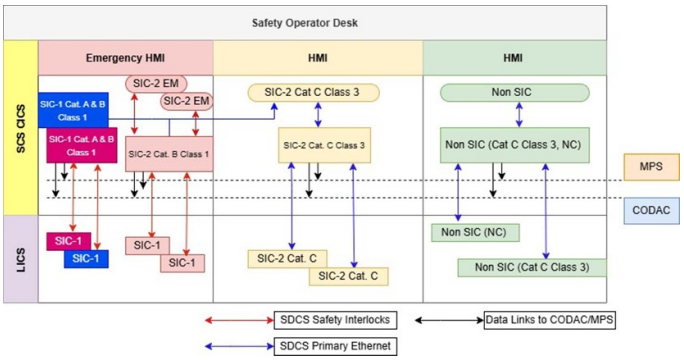

Figure 15. SCS: central versus local architecture.

PASS categorizes its functions into two safety levels:

- SIC-1: This level encompasses critical interlock functions designed to ensure:
  - Access mode: No beam or hazards in the designated area.
  - Beam mode: No personnel present in the restricted zone and immediate beam shutdown upon detection of an intrusion.
- SIC-2 (or NonSIC): This level focuses on managing personnel access to areas with identified risks.

The PASS interacts closely with the OSS to ensure that worker statuses and permissions are up to date and that access is granted or denied based on real-time safety assessments.

5.4. Radiation monitoring subsystem for the environment and safety (RAMSES)

The SCS.RAMSES plays a vital role in safeguarding personnel by continuously monitoring dose rates in areas at risk of ionizing radiation exposure. Its primary functions include:

1. Continuous monitoring: RAMSES ensures permanent surveillance of radiation levels in potentially hazardous areas and specific activities where contamination risks exist.
2. Alarm activation: It compares measured dose levels against predetermined alarm thresholds. If dose levels exceed acceptable limits, it triggers alarms and interlocks to prevent further exposure.

The integration of RAMSES with PASS is essential for maintaining access control based on radiation levels. This collaboration prevents personnel from entering areas where radiation exposure exceeds acceptable limits.

RAMSES consists of homogeneous subsystems classified according to safety and seismic standards, with distributed equipment connected to a safety network at two levels:

1. Remote management via Ethernet: Enables data acquisition and remote management of the system.
2. Dedicated connections for state change communication: Communicates state changes (logic 0–1) that initiate actions from PSS, PASS, or activate area alarms.

Given that IFMIF-DONES is classified as a radiological facility from a licensing perspective, the SCS reference design adheres to rigorous standards. Safety functions are classified according to IEC 61226 into categories A, B, C, or unclassified. These classifications align with IEC 61513, denoting various safety function requirements (safety interlock, safety actuation, data acknowledgment).

According to current licensing practices, only the firmware segment responsible for logic state changes (0–1) needs to undergo qualification via validation and verification (V&V) SW procedures.

5.5. General requirements for the SCS architecture

The reference architecture for the SCS is designed (see figure 15) with a comprehensive set of requirements applicable to all four subsystems (PSS, OSS, PASS, and RAMSES).

These requirements ensure that the system maintains a high level of safety and reliability. Here's a detailed breakdown of the established requirements:

1. Boolean connections
   Connections between SIC-1 components (Category A, Class 1) shall be exclusively Boolean. This ensures that the safety-critical elements communicate using binary logic, providing a clear and unambiguous method for signaling safety status. Similarly, connections between SIC-2 components (Category B, Class 1) must also be exclusively Boolean. This requirement maintains consistency in communication for safety functions.
2. Safety logics
   Safety logics within both SIC-1 and SIC-2 classified components shall be Boolean. This ensures that all safety-related decisions and processing within these components follow the same logical structure, enhancing reliability.
3. Dedicated hardwired consoles for SIC-1
   Hardwired consoles classified as SIC-1 shall be dedicated solely to emergency functions (e.g., push buttons for immediate action). These consoles are designed for critical emergency response, although they may not be credited from a safety point of view.
4. Dedicated hardwired consoles for SIC-2
   Hardwired consoles classified as SIC-2 shall serve dual functions: emergency (e.g., push buttons) and monitoring

(e.g., lights and horns). These consoles can be credited for operator action from a safety perspective, providing additional functionality beyond emergency response.

5. Computerized HMIs for SIC-2
   Computerized HMIs classified as SIC-2 (Category C, Class 3) shall connect via Ethernet networks to SIC-1 and SIC-2 CICS for monitoring functions. These connections will not permit remote actions, ensuring that critical safety functions are not compromised through external control. Additionally, SIC-2 components shall connect exclusively through Ethernet networks for all functions, including safety and administrative purposes.
6. Connections for Non-SIC components
   Computerized HMIs classified as Non-SIC shall also connect via Ethernet networks to Non-SIC systems/components for all functions (safety and administrative) while adhering to the assigned IEC 61513 classification.
7. Data packet status reporting
   Any SCS subsystem shall send a data packet describing its status to all other SCS subsystem with a lower classification. This ensures that all subsystems maintain awareness of each other's operational status, facilitating coordinated responses to any safety concerns.
8. SCS HMI
   The safety systems can be operated through HMIs located in the central control room and any service control room (housed in different buildings) on the basis of the environmental and redundancy requirements to be satisfied. Each operator of the emergency HMI (in both control rooms) is allowed to display information and to send commands related to both Train A and Train B.

5.6. SCS design considerations

To meet the stringent safety requirements for SIC-1 and SIC-2 Cat B functions, the system architecture must include redundancy, separation, and fail-safe design principles, ensuring reliability and minimizing risks in both normal and abnormal operations. The key requirements are outlined as follows.

I. Redundancy and separation
The control system should be structured into two fully independent I&C trains to ensure both safety and reliability. These two trains operate separately and are powered independently to maintain operational continuity even in the event of failure:

- Train A: Powered by SIC Train A external power supply.
- Train B: Powered by SIC Train B external power supply.

This ensures that any fault in one train will not affect the operation of the other, increasing both system availability and safety.

II. Emergency manual override
Emergency manual override procedures for SIC-1 and SIC-2 Cat B manual commands should be clearly defined, and these procedures must be limited to essential functions by design to prevent unintended use. These override procedures must be submitted to and accepted by the Regulatory Body to ensure compliance with safety standards.

III. Marshalling cubicles and location
SIC-1 marshalling cubicles (if required, for example, cubicles placed between field components and the CICS) must be located in dedicated rooms. These cubicles cannot be installed in CODAC hutches due to safety segregation rules. This physical separation helps ensure the integrity of the system in the event of an emergency or fault.

IV. Preferred architecture for high safety and availability
For SCS systems/components classified as Class 1 and Class 2 according to IEC 61513, where both high safety and availability are critical, the following architecture principles should be applied:

- 2oo3 (2-out-of-3) logic treatment for sensors is the preferred approach when both high safety and redundancy are needed. In this configuration, two out of three sensors must agree to trigger an action, providing fault tolerance while minimizing the risk of false positives.
- Redundant safety actuators should be used to maintain system integrity. This redundancy ensures that failure of a single actuator does not compromise the overall function of the system.

V. Sensor redundancy architecture
The level of redundancy required for sensors depends on the nature of the sensor itself:

- 1oo2 (1-out-of-2) architecture can be used for sensors that cannot activate spuriously. This allows one sensor out of two to trigger the system, ensuring safety without sacrificing availability.
- 2oo3 architecture is preferred for sensors that can activate spuriously, as it offers the best balance between safety and availability by requiring two out of three sensors to confirm a trigger, thus reducing the chances of false alarms.

VI. Failsafe design principles
Whenever possible, safety functions should be designed to be failsafe, adhering to the following principles:

1. The safe state must be clearly identified.
2. In the event of a power loss, the system should drive actuators to a safe position.
3. Actuator commands should be designed to de-energize to trip, ensuring that the system defaults to a safe state in case of failure.

4. The control logic should be designed to be intrinsically failsafe, meaning that any failure will automatically result in a transition to a safe condition.
5. In the case of communication loss between systems exchanging critical data, the receiving system must automatically enter a safe state.

This design philosophy ensures that the system is robust, with appropriate redundancy, separation, and safety mechanisms built in. These features, combined with clear emergency manual override procedures and a failsafe design approach, will help maintain safety and availability in the plant, protecting both personnel and the environment in all operational conditions. To ensure optimal safety and reliability in the control of actuators and overall system functionality, several key principles and technologies should be implemented in SIC-1 and SIC-2 Cat B I&C systems, specifically regarding actuator logic, safety functions, and network usage.

VII. Actuators control logic

Actuators should operate using positive logic wherever possible. In this configuration:

- A signal set to 1 corresponds to normal behavior.
- When a safety function is triggered or in the event of a defect or power loss, the signal changes to 0, which then triggers the safety function.

This approach helps to ensure that any failure leads to the activation of the safety response, a fundamental principle of failsafe design. Actuators that require additional power to remain in or move to a safe position (i.e., shunt release actuators) should be avoided as far as possible. This reduces the risk of failure due to loss of power or other faults, as the system should default to a safe state without relying on additional energy.

VIII. Boolean logic for safety interlocks

Safety interlock signals for SIC-1 I&C subsystems or components and SIC-2 I&C subsystems or components implementing Cat B functions should be limited to Boolean logic. Acquisition, combination, comparison, and transmission of these interlock signals must always involve Boolean (on/off) types of inputs and outputs, simplifying the safety logic and enhancing reliability.

IX. Accepted technologies for safety functions

Based on the experience from similar plants (e.g., ITER, ESS, PSI, SNS, CERN), safety functions should be implemented using one of the following three high-reliability technologies:

1. Hard-wired logic systems: These use relays controlled by PLCs, with twisted pair wiring to provide robust, low-complexity interconnections.
2. Dedicated electronic logic cards: For example, the HIMA Planar4 series, which implements logic gates in standard, modular sub-rack-mounted cards. The interconnections between these gates are achieved by wiring the card inputs and outputs on the sub-rack backplane (soldering or wrapping).
3. FPGA technology: Only if the FPGA modules have been certified for safety-related applications, and they should be limited to SIC-2 systems/components. FPGA-based systems allow flexibility but must meet stringent safety qualifications.

A combination of the above technologies is allowed to achieve the required system availability and safety standards.

X. Restrictions on network use for safety functions

When sized according to IEC 61 226, these systems should not use Ethernet networks for exchanging critical information related to safety function execution between components. This ensures the integrity and security of the safety-critical communications. Connection to a protected Ethernet network is allowed but should be limited to monitoring and diagnostic purposes at a high level (not for safety-critical actions).

XI. Health monitoring and diagnostic

The SIC-1 system should use solid-state technology for health monitoring and diagnostics. This technology should be capable of reporting detailed module states via serial links or networks. The monitoring and safety functions must remain independent by design. This independence ensures that failures in the monitoring system do not affect the safety-critical aspects of the system. The monitoring subsystems should be classified as SIC-2 Category C Class 3, participating in the overall process monitoring.

XII. Interfaces between SIC-1, SIC-2, CODAC, and CIS

One method to interface SIC-1 and SIC-2 Cat B with CODAC and CIS is by using hardwired links. This provides a highly reliable, direct connection for critical information. Another method is using serial links or networks, particularly for the flow of health monitoring data. However, critical safety information should not rely on these communication methods to ensure redundancy and reliability. To ensure the Category C classified systems meet safety and reliability standards, especially for SIC-2 I&C systems and Non-SIC I&C systems implementing Category C functions, specific architectural, HW, and SW requirements must be followed.

Here is an overview of the key points related to the implementation of these systems and overall system safety:

A. Category C classified systems implementation

1. Class 3 Compliance (IEC 61513)
   All Category C classified systems (SIC-2 I&C systems and Non-SIC I&C systems) must be implemented according to Class 3 as specified by IEC 61513. This includes using industrial PLCs and/or industrial FPGA technologies, which have proven reliability in industrial environments.
2. Networking and SCADA architecture
   The architecture of Category C systems should be network-based and utilize a computerized SCADA system for control and monitoring. HW for these systems must be industrial with a significant track record of performance in similar environments.

Application-oriented SW can be used, including black-box solutions with embedded SW, as long as they meet relevant safety standards.

3. SW compliance (IEC 62138)
   SW development for Category C classified systems must be compliant with IEC 62138 to meet Cat C safety requirements. This standard ensures that the SW design and testing processes are adequate for the level of risk associated with these systems.

B. Non-classified safety functions

Parts of the SCS performing non-classified safety functions do not require compliance with IEC 61513. Instead, they should comply with IEC 61508 to ensure adequate system reliability. These non-classified subsystems should also rely on networking-based architectures and a computerized SCADA, with industrial-grade HW to ensure reliability.

XIII. Integration of SCS subsystems

As the SCS comprises four main subsystems (SCS.PSS, SCS.OSS, SCS.PASS, SCS.RAMSES), each is potentially classified differently in terms of SIC requirements. Despite different SIC classifications for components, all four subsystems should be visible and accessible from the central control room as a single system. Operators should be able to access any subsystem server by entering the corresponding IP address on the safety network Ethernet rings, part of the SDCS.

XIV. Architecture layer connections

The lower part of the architecture consists of four separate legs, connecting the SCS cubicles to the LICS. Each leg will have distinct configurations based on performance and physical requirements.

The upper part of the architecture ensures seamless integration of safety data, allowing operator access and connection to the CODAC gateway. This is achieved by connecting CICS cubicles to the operator WSs via at least two independent Ethernet rings.

There must be a clear separation between the two network levels:

- From operator workstations (WSs) to servers.
- From servers/PLCs/gateways to LICS.

Servers in each cubicle provide a separation layer between the operators and the safety controllers, ensuring controlled access to critical safety functions.

Category A subsystems may optionally include hard-wired emergency control desks, while they are mandatory for Category B subsystems. These desks should be connected directly to the safe PLCs for emergency/recovery operations, offering an additional layer of safety control.

An additional degree of separation between the SCS and the non-safety-classified CODAC system is achieved through the CODAC gateway. The CODAC gateway design and responsibility fall to CODAC system designers, ensuring it is adequately separated from safety-critical functions.

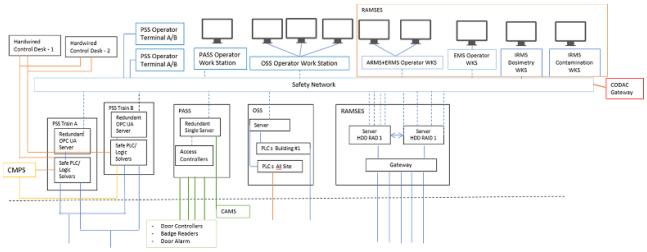

Figure 16. SCS architecture: preliminary overall design. Reproduced from [18]. CC BY 4.0.

The connection to the Central MPS is currently monodirectional, allowing SCS.PSS to send its working status to the MPS.

XV. Reliability and availability requirements

According to the IFMIF-DONES SAR (see the paper on Safety in this journal issue for more details), the overall system failure probability must be lower than $10-^{6}$ yr^{-1} for each postulated initiating event. The contribution of each safety control chain (such as the SCS.PSS) to personnel protection must ensure a failure probability of less than 10^{-3}/event.

The SCS must maintain inherent availability over its scheduled operation time at more than 98% to contribute to the global target of 70% plant operation availability.

On the basis of all the key requirements described above (I–XV) a preliminary overall design architecture is reported in figure 16.

5.7. Preliminary SCS.PSS architecture

The SCS.PSS architecture design outlines critical requirements and considerations to ensure compliance with SIC-1 and SIL-3 or SIL-4 safety standards. The architecture prioritizes redundancy, fault tolerance, and fast response times for safety-critical functions. Here is a summary of the main key points:

I. SCS.PSS safety requirements

1. SIC and SIL compliance: All SCS.PSS safety functions must comply with SIC-1 standards and at least SIL-3 HW/SW requirements. For SIL-4 compliance, specific components such as HIMA Planar-4 may be used.
2. Double redundant trains: Two independent trains (Train A and Train B) are required for signal acquisition, processing, and safety signal generation. Each train must be physically separated (cubicles located in different rooms) to ensure redundancy and avoid common-mode failures.
3. Redundant communication channels: Every I/O physical signal must have double redundant communication channels, ensuring signal integrity and availability in case of failures.
4. Safety interlock signals: Safety interlock signals are generated by sensors, DAUs, and local interlock systems with at least 1oo2 voting logic. For higher safety and reliability, 2oo3 voting logic is recommended where feasible. Output

signals sent to LICS must also use 1oo2 voting logic as a minimum standard for safety-critical functions.
5. SIL-3 (or SIL-4) connections: All connections between Central SCS.PSS and PS LICS must comply with SIL-3 (or higher) to ensure signal integrity and meet safety-critical performance standards.
6. Safety logic actuation equipment: Equipment responsible for safety logic actuation (such as FPGA, PLC, or hard-wired systems) should not be integrated into servers, ensuring separation and independence from non-safety functions.

II. Monitoring and management via OPC UA

1. Redundant OPC UA servers: A redundant OPC UA server (e.g., a WINCC OA© server) is required for each train, ensuring remote monitoring and management of the system. The server must have redundant critical components such as dual power supplies, RAID HDDs, and network interfaces. The OPC UA server will handle communication with FPGA/Slow PLC/Logic solver units and should be common to all cubicles within the same train.
2. Remote management: All CICS devices should be manageable from remote systems using OPC UA over Ethernet. This may include:
   - Siemens© devices using WINCC OA©.
   - HIMA Planar-4 devices using the HIMA OPC-Server toolkit.
   - NI CompactRIO© using the LabVIEW© OPC UA Toolkit, which is compatible with both Windows© and NI© Linux Real-Time OS. However, it cannot run on controllers using Phar Lap ETS or targets running VxWorks.

III. Fast actuation requirement

The maximum actuation time of 1 ms, measured from the safety alarm trigger on the LICS safety board to the actuation on the LICS, is a defined constraint. This timing can be achieved using specific HW configurations:

1. NI© Compact RIO (SIL-3).
2. A special combination of HIMA Planar-4 (SIL-4) components.

IV. HW and cubicle configuration

Currently, two 42 U cubicles are planned: one for Train A and one for Train B. Each cubicle is designed to handle around 200 safety signals (100 effective signals due to redundancy).

5.8. Preliminary SCS.OSS architecture

The SCS.OSS is focused on managing safety related to non-radiological risks and ensuring the safety of workers by monitoring their exposure to various hazards, including radiological ones through its integration with other subsystems. Here is a breakdown of the main functions and architectural requirements.

I. Key safety functions of SCS.OSS

A. Monitor non-radiological risks: SCS.OSS is tasked with tracking and managing non-radiological hazards within the facility, providing essential input into the overall safety framework.
B. Track total worker exposure: The system consolidates data on worker exposure to both radiological and non-radiological risks through a dedicated SW package that handles job hazard risk evaluations in compliance with occupational safety standards (see [29]).
C. Data exchange with SCS.RAMSES: SCS.OSS integrates with SCS.RAMSES to gather data on each worker's accumulated dose rate (radiological exposure), which contributes to the overall exposure tracking.
D. Data exchange with SCS.PASS: SCS.OSS communicates with SCS.PASS to share information on the residual exposure allowance for each worker and help manage their shift schedules to stay within safe limits.

II. Architectural features of SCS.OSS

A. Non-SIC classification: Since SCS.OSS is not handling radiological risks directly, it is classified as Non-SIC, meaning that its design does not need to adhere to the strict standards required for radiological safety systems.
B. Main cubicle design: The SCS.OSS CICS design includes a single 42 U cubicle with a separation of safety functions via dedicated safe controllers (i.e. PLCs) for different facility areas:
   - One PLC bar, with hot stand-by backup, is dedicated to the main building.
   - Another PLC bar, also with hot stand-by backup, is dedicated to all other facility areas.
   - The PLC bars handle the monitoring and processing of non-radiological risks in these respective zones.
C. Double redundant communication channels: The system will employ double redundant communication channels within the safety network, ensuring reliable data transmission between components.
D. Single alarm input signals: The system accepts alarm signals from a single sensor/DAU, with single actuation logics applied for any incoming alarms, which simplifies the architecture for non-radiological risk monitoring.
E. Field connections: The connections between the SCS.OSS cubicle and field components (sensors, DAUs, etc) may be bus-based or through digital input, depending on the sensor and interface requirements.
F. Real-time communication: The SCS.OSS will have real-time communication capabilities with both SCS.PSS and SCS.PASS. These subsystems handle emergency safety logic actuation, allowing SCS.OSS to exchange critical safety data in real-time.

G. Single server configuration: A single server (non-redundant) is acceptable for managing and monitoring SCS.OSS operations, provided that it meets the necessary performance and safety requirements.

It should be observed that each PLC responsible for monitoring non-radiological risks in the main building must be distinct from the PLC responsible for monitoring the same risks in other buildings. This separation ensures that failure in one area does not impact safety monitoring in another.

5.9. Preliminary SCS.PASS architecture

The SCS.PASS is classified as SIC-1 in the SAR rev. 2(see [30]) as its primary role is to prevent unauthorized or unsafe access to areas with potential risks (both radiological and non-radiological). Here is a breakdown of the main functions and architecture.

I. Key functions of SCS.PASS

A. Access control and interlock signals:

- SIC-1: Responsible for preventing access to high-risk areas (such as those with high radiological or non-radiological risks).
- SIC-2 or Non-SIC: Focuses on preventing access to or maintaining presence in areas with moderate or incoming risks. This segmentation is in line with typical practices in accelerator-driven facilities.

B. Inter-system communication:

- Building System Doors: SCS.PASS communicates with doors/gates provided by the building system.
- SCS.RAMSES: Receives data on radiological risks and exposures.
- SCS.OSS: Monitors non-radiological risks and tracks workers' total exposure.
- SCS.PSS: Acquires alarm data from neutron monitors and real-time tritium detectors.

C. On-field components: The system includes control panels, operator WSs, badge readers, door controllers, visual alarms, horns, cameras, and interphone systems, all of which are connected to SCS.PASS and monitored.

II. Key design considerations

SCS.PASS will rely on COTS components that have proven operational histories in both industrial and radiological-risk environments. The use of COTS components is intended to balance cost efficiency with the system's safety requirements. Critical doors or gates must be equipped with independent sensors (e.g., mechanical position switches), which SCS.PASS will directly acquire to ensure safe operation and maintain the necessary SIC level in the safety chain. These sensors are hard-wired into the system for reliability and direct control.

III. Architectural components of SCS.PASS

SCS.PASS cubicles and WSs in the central control room are based on the following assumptions:

A. Redundant single server: The server has redundant components, including two power supplies, two hard disk drives (HDDs) in RAID 1, and two Ethernet cards, all connected via a dedicated TCP/IP Ethernet network to the on-field components. This server manages access controllers and acquires data from badge readers, controls door lock/unlock operations, and activates local alarms and warnings.

B. Access controllers: Access controllers are managed by the server and are responsible for:
   a. Acquiring data from badge readers to track personnel transit.
   b. Commanding doors for locking/unlocking.
   c. Activating local alarms/warnings.

C. On-field components: These are divided into four categories:
   a. COTS sensors on doors (160 units).
   b. COTS alarms and warnings (80 units).
   c. COTS interphones (74 units).
   d. COTS cameras (92 units).

These components will interface with SCS.PASS for access control, monitoring, and safety management.

IV. Redundancy and reliability

Due to its SIC-1 classification, SCS.PASS may need to be implemented with double independent trains housed in two separate rooms. This would ensure that, in case of an external threat (e.g., fire or inability to access the control room), the system remains operational from a separate location. The architecture must ensure that the system's mean time between failures exceeds 10 000 h, translating to a 99.99% reliability target based on component failure rates.

V. Integration with other SCS systems

SCS.RAMSES, SCS.OSS, and SCS.PSS all communicate with SCS.PASS via the Safety Network to share alarm and status data necessary for safe operation and logical access decisions. The communication infrastructure for independent sensors is directly hardwired into SCS.PASS to avoid compromising the SIC-1 safety level. The network for SCS.PASS is shared with the SCS.RAMSES LICS cubicles, given their similar SIC-1 requirements. Routers and switches can be co-located to optimize space, while maintaining reliable network segmentation and redundancy.

5.10. Preliminary SCS.RAMSES architecture

The SCS.RAMSES is designed to monitor radiological risks in the plant, with extensive on-field components and complex communication networks with other subsystems (SCS.PSS, SCS.PASS, etc). It is based on COTS platforms with a proven history in similar industrial and radiological environments.

Here's an overview of the system's architecture and components:

A. Central RAMSES (RAMSES CICS): They are composed by:

- Redundant servers: Two independent servers are housed in the same cubicle to provide functional redundancy, ensuring system reliability.
- Redundant Ethernet network: The CICS connects to all on-field components and subsystems via a redundant Ethernet network, providing robust communication pathways.
- Terminal server (Gateway/Switch): Used to collect signals from the radiological synthesis unit-type 2 (RSU2) and/or directly from the RAMSES subsystems according to predefined communication protocols.
- Operator WSs: Located in the CR with multiple monitors and graphical interfaces for system control and monitoring.

B. Local RAMSES (RAMSES LICS): They are classified as:

• Radiological synthesis unit-type 1 (RSU1):

o Collects prompt digital outputs (logic state 0–1) from on-field monitors, indicating local malfunctions, prealarms, or alarms.
o Used to generate area alarms and transmit cumulative alarm outputs to the SCS.PSS or SCS.PASS for activating safety actions.

o Radiological synthesis unit-type 2 (RSU2):

o Collects text data from sensors or DAUs and the alarm conditions from RSU1.
o Acts as a gateway, transmitting the collected data to the RAMSES servers using a unified protocol, standardizing communication across the system.

C. RAMSES on-field components: They are composed by monitors and sensors:

o Non-safety-related sensors: Single sensors connected to RAMSES for general monitoring tasks.
o Safety-related sensors: Redundant/duplicated sensors, such as neutron chipmunk detectors or tritium monitors, used for critical safety monitoring and directly connected to SCS.PSS.
o Sensors must have both Ethernet/RS-485 interfaces for remote management and hardwired digital outputs (logic state 0–1) for alarm and malfunction communication to RAMSES and other safety systems.
o Area alarm units: Local alarms activated when a critical threshold is reached, connected to RSU1 for initiating area-wide safety actions.

D. RAMSES networking: The networking architecture of RAMSES supports the interconnection of various on-field components, RSUs, and the central CICS. It is designed to ensure reliable, low-latency communication between safety-critical components. It is basically composed by:

a. RS-485 or Ethernet.
b. Sensors/DAUs are connected to RSU2 via RS-485 or Ethernet, depending on the specific device and location.
c. Future enhancements may include WiFi connections for sensors/DAUs.
d. Hardwired (Logic State 0–1).
e. Sensors/DAUs connected to RSU1 and SCS.PSS for direct control and alarm triggering are hardwired with a logic state 0–1 signal (0–24 V DC, with a possible increase to 30 V DC to mitigate voltage drops along longer lines).
f. Ethernet Media.
g. RSU1 connects to RSU2 via Ethernet for transmitting alarm conditions and real-time monitoring data.
h. RSU2 connects to RAMSES CICS via Ethernet for unified data collection and control.
i. Safety network: The operator workstations, central RAMSES, and other SCS subsystems are interconnected through the safety network via Ethernet cables, ensuring seamless data flow and control.

It should be observed that the V&V for the SIC-1 firmware of monitoring devices is primarily limited to the portion of the monitor generating the digital output (hardwired alarm/malfunction signal). This ensures that critical alarms are transmitted accurately and reliably.

In particular, sensors related to critical safety functions (SIC-1) such as neutron and tritium monitors must be hardwired to SCS.PSS and follow stringent V&V procedures for alarm accuracy and reliability.

Moreover, for safety purposes, area alarms must be triggered by RSU1 based on real-time input from sensors and DAUs. These alarms can prompt immediate safety actions or restrict access through interlocks managed by SCS.PASS.

6. DONES local control systems

The LICS for IFMIF-DONES is designed with a modular and scalable architecture, enabling seamless integration across multiple subsystems. This architecture is crucial for managing various components of the complex plant operations.

Local control systems serve as critical nodes in the plant control architecture, performing essential functions to ensure smooth operations within their assigned subsystems. Here's an overview of their key functionalities:

1. Receiving commands from the central control system: LICS units receive instructions from the CICS, which coordinates overall plant operations. These commands dictate the specific actions to be taken by the LICS, such as adjusting equipment parameters or triggering specific processes.

2. Interfacing with specific actuators and sensors: Each LICS interfaces directly with local actuators and sensors, allowing for precise control and monitoring within its designated area of responsibility. Actuators may control valves, motors, or other mechanical devices, while sensors provide real-time feedback on pressure, temperature, flow, and other critical parameters.
3. Real-time control of actuators based on received commands and sensor data: LICS units execute the commands they receive by controlling actuators in real-time. They continuously monitor sensor feedback to ensure the commands are correctly executed and adjust the actuators as necessary to maintain desired operational conditions.
4. Data preprocessing and transmission back to the central control system: In addition to controlling actuators, LICS units also perform data preprocessing, filtering raw sensor data to eliminate noise and package relevant information before sending it back to the CICS. This enables more efficient central data processing and faster decision-making.
5. Self-monitoring and fault detection capabilities: LICS units are equipped with self-monitoring and fault detection mechanisms, which help identify issues such as actuator malfunctions, sensor failures, or communication problems. These capabilities ensure that potential failures are detected early, preventing larger system breakdowns.
6. Interface with CICS: LICS maintains continuous communication with the CICS, sending back sensor data, system status, and alerts for anomalies. This interaction is vital for maintaining system-wide coordination and making real-time adjustments based on the overall plant performance.

The key distinctive feature of IFMIF-DONES lies in the vast number and wide variety of systems that require control. There are currently a total of 41 systems to be managed, divided into different physical and engineering groups (AS, TS, LS, PS), along with auxiliary systems that support them. For instance, AS require high control responsiveness, TS ensure the accurate reading of scientific data collected by sensors, whereas PS and LS are based on more industrial processes. Additionally, the RH system includes numerous telemanipulation devices that need to be controlled.

Therefore, the control system architecture designed for IFMIF-DONES needs to be as homogeneous as possible, incorporating principles of modularity, scalability, and flexibility to meet the diverse needs and requirements of IFMIF-DONES. The most recent facilities like ITER and ESS can be taken as reference plants, but the architecture presented here is inevitably based on the experience gained from LIPAc, a prototype for the IFMIF-DONES accelerator.

The LICS architecture for IFMIF-DONES (figure 17) has been designed on the base of the following features:

1. Comparison of voting arrangements.
2. Hardwired signal topology.
3. Fieldbus communication protocols.
4. Fast or slow controllers.

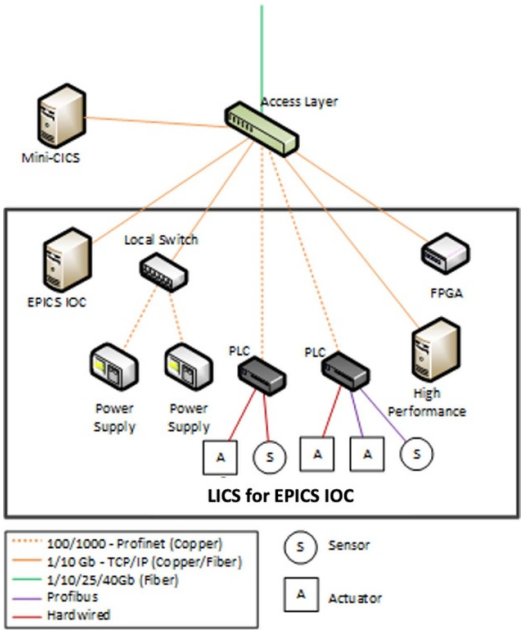

Figure 17. LICS architecture: preliminary overall design.

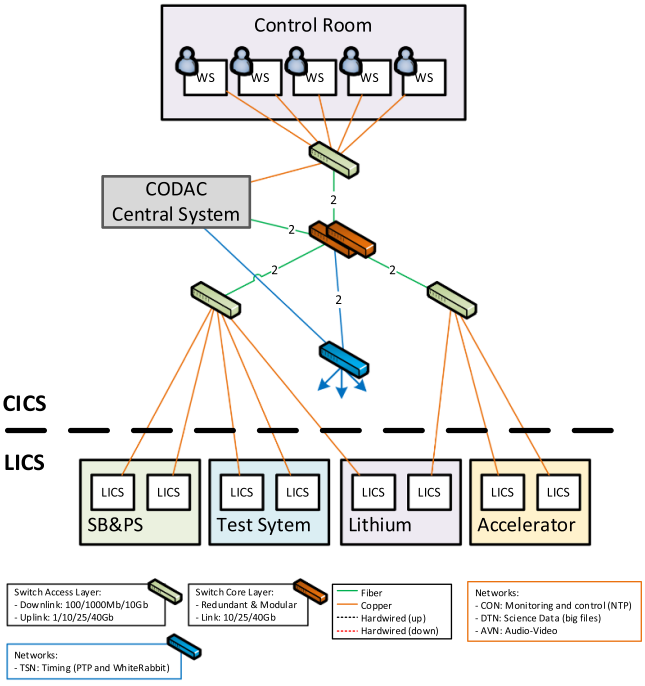

Figure 18. LICS architecture: preliminary CODAC design.

5. Data preprocessing and transmission.
6. Networks and interfaces with CICS.
7. Timing and timestamp.

6.1. CODAC LICS design

The primary functions and goals of the LICS for the CODAC system in DONES include monitoring all control parameters and their statuses, configuring the LICS, and transmitting scientific data. The key challenges in designing a LICS

architecture involve achieving a level of flexibility and scalability that is sufficiently homogeneous, especially considering the vast number and variety of LICS present in DONES (figure 18).

Due to the non-critical nature of the system, the I&C associated with the CODAC system is utilized solely for monitoring or controlling the system's devices. Consequently, the voting configuration for any sensor or actuator within the system should be set to 1oo1, or equal to a given value related to the PFH between two maintenance times (i.e. 'short' and 'long' maintenance). For accessibility purposes, the I&C can be duplicated; however, the configuration will still adhere to the 1oo1 arrangement, as the LICS under the CODAC system are designed primarily for monitoring and basic system control.

All hardwired signals must be standardized to guarantee compatibility, enhance reliability, minimize noise, and mitigate the risks of miscommunication and signal degradation. Consequently, standard voltage and current signals will be implemented for most sensors and actuators. Specifically, analogue signals will include voltage ranges of 0 V to +10 V, 0 V to +24 V, −5 V to +5 V, and −10 V to +10 V, along with current ranges of 4 mA to 20 mA. Digital signals will operate at 24 V DC, employing positive logic for process control and negative logic for fail-safe operations. When TTL signals are required, they can operate at 5 V DC.

For low-intensity signals, a tailored approach is necessary, which involves utilizing twisted pair cables, 360-degree shielded cables, and ensuring proper grounding. Signal return paths and differential signals should be employed whenever feasible, and suitable grounding topologies must be implemented to prevent floating configurations.

Given the wide variety of sensors at IFMIF-DONES, some sensors and actuators utilize communication protocols rather than hardwired connections, accommodating both low and high sampling frequencies. The main connection scheme is from the sensor to the DAU and from the DAU to the PLC in the LICS through field bus.

For low-speed communication, the RS-232 and RS-485 protocols over PROFIBUS are employed due to their reliability and speed (alternatively, Modbus and Modbus TCP/IP as well as PROFINET could be employed). It is essential that instruments from different systems within IFMIF-DONES or utilizing different protocols are not mixed on the same field bus.

For high-speed instrumentation, devices will be categorized by type, and specific communication protocols will be chosen based on the environmental conditions and requirements. These protocols may be proprietary to the I&C system or could include standard communication methods, such as Manchester Encoding, to ensure message delivery and integrity.

Additionally, certain instrumentation necessitates an adaptation stage, such as analogue-to-digital converters (ADCs), which will communicate with a controller via the respective device's communication protocol. These components are located in the control cubicle, where the analogue signal cable connects to the instrument and vice versa.

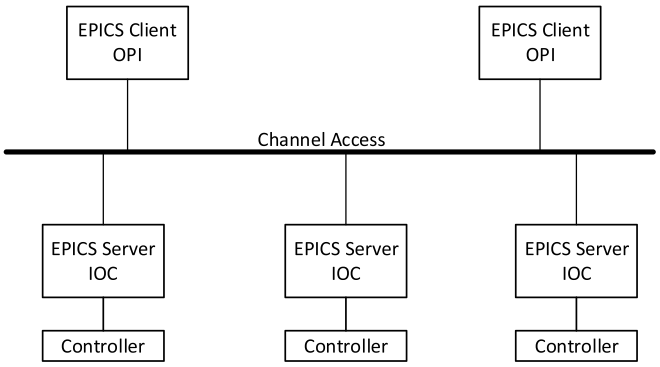

Figure 19. EPICS client–server communication in LICS.

To address the challenges posed by the controller diversity and the resulting maintenance complexities, a limited selection of controller types has been adopted. This approach reduces stock diversity, and the skill set required for maintenance personnel while enhancing the compatibility of the controllers.

Two categories of controllers have been established: slow controllers and fast controllers. As a general guideline, any process with a response time exceeding 100 ms typically employs Slow Controllers, while Fast Controllers are suited for applications with shorter response times. Furthermore, the use of COTS devices is encouraged due to their advantages, including reliability, cost-effectiveness, streamlined integration, and reduced development time.

The Siemens© S7-1200 and S7-1500 PLCs, or similar models, have been designated as Slow Controllers owing to their operational lifespan, advanced features, and optional OPC-UA communication protocol. For Fast Controllers, together with Siemens© S7-1500 CPU piloting a Siemens© TMFAST module (FPGA based on Intel© Quartus CPU), microTCA technology (FPGA based on Xilinx© CPU) is under consideration, while VME systems are being phased out due to their complexity and declining relevance.

The architecture of local control systems is designed to be highly compatible with either the PV Channel Access protocol or the OPC-UA protocol, enabling seamless data processing and transmission, regardless of the primary control SW employed, such as EPICS or WinCC-OA©. This adaptability highlights the integration of controllers that support OPC-UA (like Siemens© S7-1200 and S7-1500), within the more industrialized systems of IFMIF-DONES, as well as 'old' CPUs as Siemens© S7-400, still in use. Additionally, EPICS IOC servers are utilized for the accelerator group controllers. Experimental tests are ongoing to verify the interface between OPC-UA and EPICS protocols and the associated latency.

In both scenarios, information exchange takes place within a communication network where all LICS and the CICS can communicate with one another. They transmit messages that include metadata to enhance the value of the data, adhering to the PV Channel Access standard in the case of EPICS or utilizing OPC-UA for other communications (see figure 19).

All controllers within the CODAC system can generate three distinct types of data:

1. LICS status monitoring data: These messages are small to medium in size and are generated at a maximum frequency of 10 Hz. They are sent from all local control systems and represent synchronous data, which is required by all local control systems.
2. Control data: Whereas the term 'monitoring' refers to the operator's action that occurs approximately three seconds after receiving a notification on the HMI, 'control' data is directed towards automatic process management, allowing for much quicker responses.
3. Scientific data: This type consists of larger messages produced by a limited number of LICS, representing asynchronous data. Only those local control systems that specifically require such data will utilize it.

To ensure the timely transmission of this information without delays or collisions, and based on lessons learned from LIPAc, all local control systems will connect to the CDCS network through one dedicated port for monitoring data and one dedicated port for control data. An additional port will be provided for scientific data transmission as needed.

All data transmitted to the CICS must be timestamped using network time protocol (NTP), precision time protocol (PTP), or White-Rabbit (WR) as timing protocols (see section 7) to ensure sequential ordering for archiving and other purposes. Consequently, all LICS must be synchronized via the IFMIF-DONES timing network. The accuracy levels vary depending on the protocol employed:

1. NTP synchronization: This protocol will be used for systems that require low time precision, typically in the millisecond range. NTP synchronization will be implemented through the CDCS network to minimize the usage of ports on the controllers.
2. PTP synchronization: This protocol will be employed for systems needing higher time precision, around the microsecond range. Controllers requiring PTP synchronization will be directly connected to the timing network through an exclusive port designated solely for this purpose.
3. White-rabbit synchronization: This protocol will be utilized by selected accelerator group systems that demand extremely precise time accuracy (in the nanosecond range). Controllers needing White-Rabbit synchronization will also be directly linked to the timing network using a dedicated port reserved for this specific function.

While the timing network is part of the CODAC system, it is extended to the MPS and SCS systems, maintaining the same properties, including redundancy.

6.2. MPS LICS design

The main objectives of the LICS for the MPS system in IFMIF-DONES are to guarantee the protection of the machine. These systems must be monitored and configured for proper functionality. Designing the LICS architecture for the MPS system presents considerable challenges due to the diversity and quantity of sensors and actuators throughout IFMIF-DONES, as well as the timing responses required to stop the beam and prevent any potential damage.

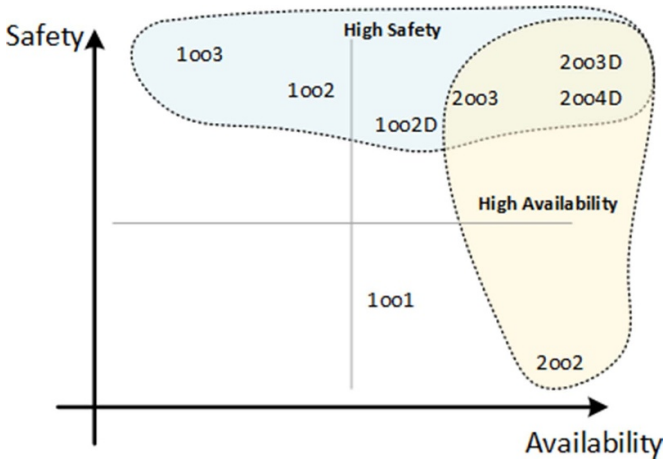

Figure 20. Safety versus availability in MPS LICS.

The operational availability target for IFMIF-DONES is set at an ambitious 87%, which introduces several challenges. Achieving a balance between availability and safety necessitates careful planning and meticulous attention to detail. Furthermore, maintaining a clear separation between the CODAC and MPS systems is crucial for the integrity of the entire system. Space constraints also pose challenges, sometimes requiring the reuse of I&C elements. Additionally, compliance with the IEC-61511 standard adds another layer of complexity to the design and implementation processes.

To tackle these challenges, a thorough analysis of LICS is crucial for identifying the optimal I&C configurations. In most cases, a 1oo2 architecture should be employed to enhance reliability and safety; however, a 1oo1 configuration may be suitable in certain situations (figure 20). Moreover, it is essential to avoid reusing I&C components from the CODAC system for the MPS to maintain the integrity of safety and control boundaries.

The sensors and actuators within the LICS for the MPS system exhibit considerable diversity, encompassing both slow devices, such as thermocouples and vacuum valves, and fast devices, like beam position monitors and beam loss monitors. These devices feature various signal interfaces, including both digital and analogue formats.

A hardwired signal topology similar to the CODAC one is desirable, even if a hardwired topology between the LICS and CICS is not currently planned, with the exception of TTL data exchanges for superfast interlocks, provided that the distance between the CICS and LICS allows for this configuration.

6.3. SCS LICS design

Safety is the primary objective of all LICS within the SCS system in IFMIF-DONES, and these systems must be monitored and configured to ensure correct functionality. The LICS of the SCS face significant challenges due to the wide variety and quantity of sensors and actuators present throughout IFMIF-DONES.

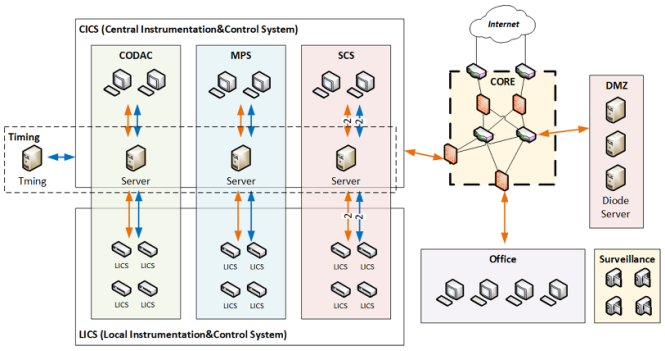

Figure 21. IFMIF-DONES CICS-LICS communication network general architecture.

The voting arrangement of sensors and actuators is a critical component for the LICS within the SCS. The architecture typically employs at least a 1oo2 voting scheme to ensure a balance between safety and availability. In some instances, a 2oo3 configuration may be necessary for specific systems to enhance reliability and fault tolerance.

Reusing the I&C from the CODAC or MPS systems for SCS purposes is strictly prohibited. The LICS of the SCS must utilize their own dedicated I&C, reinforcing the requirement that the SCS should be capable of operating autonomously and maintaining plant safety independently of the CODAC and MPS systems. SCS sub-systems should adhere to the IEC-61508, IEC-61511, and IEC-61513 standards on the basis of the categorization of the safety functions to be performed.

7. Communication networks

Large-scale facilities like IFMIF-DONES depend on a robust network infrastructure to enable data exchange, system control, and security measures. The technical network at IFMIF-DONES consists of multiple interconnected networks that are essential for its operation, including the CODAC, MPS and SCS networks (figure 21). These networks play critical roles in facilitating efficient data transmission, ensuring system integration, and managing the overall facility effectively.

Designing and implementing a communication network for a scientific infrastructure like IFMIF-DONES presents several complex challenges. Key issues include ensuring high data throughput, maintaining low latency, achieving robust security, and enabling scalability:

- High data throughput: It is essential to manage the vast volumes of data generated by scientific experiments, necessitating networks capable of supporting multi-gigabit-per-second speeds. This has become more important than ever with the potential to incorporate AI techniques for data analysis and optimization.
- Low latency: Real-time control and monitoring systems require low latency, which calls for optimized routing and minimal network congestion.
- Security: Protecting sensitive experimental data and control systems from cyber threats is paramount. This requires the implementation of advanced firewall configurations, intrusion detection systems, and secure communication protocols.
- Scalability: The network must be highly scalable to accommodate future expansions and technological advancements without significant disruptions.

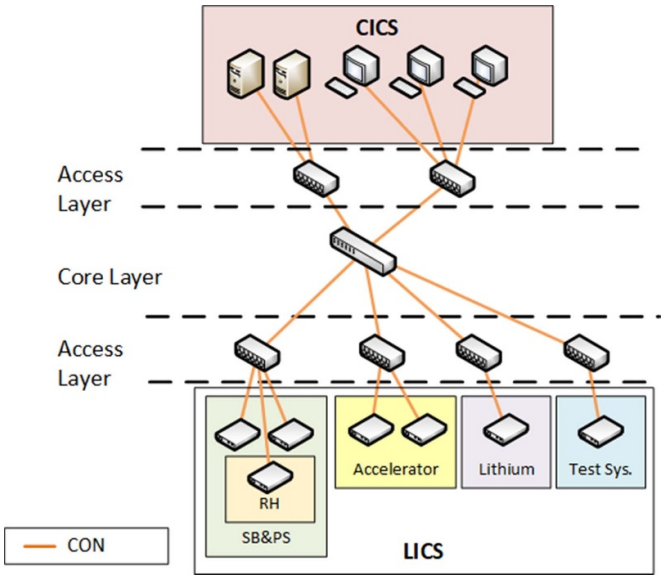

Figure 22. IFMIF-DONES CON network architecture.

These factors, along with the necessity for reliable maintenance, automated configuration management, and continuous monitoring, create a complex challenge that demands careful planning and execution to ensure the seamless operation of scientific research facilities.

7.1. CODAC network

The primary components connected to the CODAC include WSs in the central control room, all CODAC servers, and all LICS. This network group is utilized for transmitting monitoring data, configuration data, commands, and acquisition data between CICS and LICS. Additionally, it facilitates command and configuration for RH devices, as well as audio-visual signals.

The key network for CODAC is the controller operation network (CON): this network manages commands, system status, monitoring, and configuration data (figure 22).

In the framework of CODAC, additional specific purpose networks are needed, such as:

- DTN/massive data network: This network is responsible for transferring large volumes of asynchronous data, thereby reducing congestion on the CON and it is key for including AI-powered data analysis.
- Timing network: Dedicated to the TMS, it allows precise synchronization across the control systems. This network is described in more depth later.

Other specific purpose networks, not formally part of the CODAC system but strongly related to it are the following:

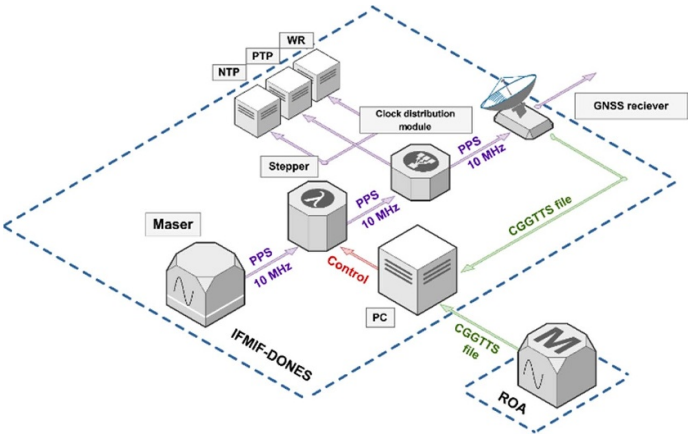

Figure 23. Time reference proposed for IFMIF-DONES.

- Audio–video network: This network manages audio and video communications in the areas under radiation, required for human safety.
- RH network: This is an exclusive network dedicated to supporting RH operations as required by the corresponding LICS. The RH system will feature a dedicated network for exchanging RH commands and data.

7.1.1. Timing network. The Timing Network is responsible for producing a global time reference for all the devices in the facility, providing the proper reference for triggering actions and event timestamping for all devices available in the CODAC Network. The timing subsystem is implemented based on an accurate time reference build on a low phase noise maser disciplined to national time lab (UTC-ROA) using a commune view technique. This is illustrated in figure 23. It allows to provide a unique time scale in the facility, useful also for RF dissemination.

Timing network supports three distinct levels of accurate time transfer solutions, ensuring precise synchronization across all the elements. While the network is part of the CODAC system, the timing synchronization it generates is propagated through a dedicated network that spans the three main systems: CODAC, MPS, and SCS, providing a reference 'point of presence' at each LICS level as well as recommendations and mechanisms for time handling inside each LICS (figure 24) [31].

This synchronization is essential for maintaining coherence and coordination between systems, especially for operations that require precise and coordinated operations or a commune frequency dissemination such as the RF elements of the accelerators. Three different time classes have been established for each individual LICS, with a corresponding time transfer protocol designed for each of them:

1. Information parameters (IPs) : NTP
2. Loose time-related parameters (LTPs) : PTPv2
3. Tight time-related parameters (TTPs) : IEEE-1588-2019 HA or WR.

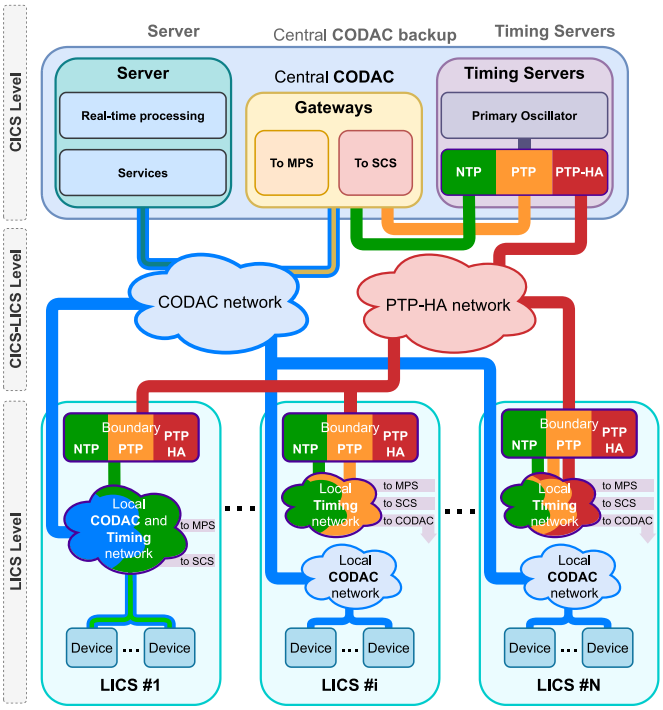

Figure 24. IFMIF-DONES timing subsystem network architecture. Reproduced from [31]. CC BY 4.0.

Figure 25 shows the current network design for such a system, where each LICS is provided with the three-time transfer protocols (NTP, PTPv2 and WR). A further optimization based on the number of slaves can be implemented to reduce the number of time servers. It is also important to note that the master clock is redundant to avoid single point of failure on this critical feature for the facility operation.

One proposed technology currently under evaluation is TSN (time sensitive networking), which enables deterministic data delivery with low latency while supporting best-effort traffic over the same cable. This approach would simplify deployment without compromising flexibility or real-time operation.

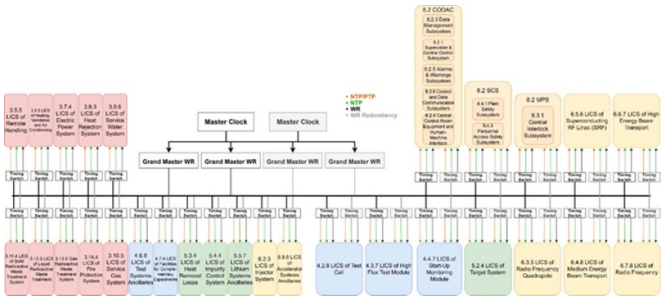

Figure 25. Final network design for the timing subsystem including the different LICS.

7.2. MPS network

The main components connected to the MPS include WSs in the central control room, MPS SCADA servers, and Central MPS controllers linked to dedicated controllers within the LICS. These components are organized on two distinct rings:

- A pure Ethernet ring: This ring is used to exchange all data except for interlock signals, primarily utilizing TCP/IP for communication.
- A mixed ring: This ring facilitates the exchange of Boolean interlock signals between the LICS and the central MPS. It mainly employs PROFINET and EtherCAT over an Ethernet layer, with some exceptions for 'wired' or FO connections used for superfast communication via dedicated TTL controllers.

These two networks primarily transmit monitoring data and configuration data between the CICS and LICS.

Both networks are isolated by the CODAC system, which continuously monitors their operational status. Communication is conducted through a dedicated gateway, with unidirectional data flow (i.e., UDP) from the MPS central servers to CODAC.

The primary Ethernet network must be sized to accommodate all 'service functions' of the MPS and can have the same architecture of the CODAC network. Conversely, the second network must be designed to support all interlock MPS functions, which requires adherence to dedicated criteria (e.g., very low PFH, low latencies, 'black channels') and standards (e.g., IEC-61508).

A dedicated engineering WS can be connected to both networks, depending on the required functions, such as remotely managing the MPS controllers in the LICS or performing advanced actions like interlock bypassing or overriding and controller programming.

The IDCS is the communication infrastructure dedicated to the MPS (figure 26).

The IDCS consists of the following components:

- Digital network infrastructure: This includes active components, such as switches, for both slow and fast interlocks. The design anticipates the potential for a shared physical infrastructure between the fast and slow sections to optimize costs and space. If implemented as a single infrastructure, it must accommodate communications for both types of interlocks, utilizing different protocols as needed.
- Directly wired connection: This link is designated for very fast interlocks, where the expected response time is in the order of tens of microseconds. It is specifically for signals, both inputs and outputs, that must be managed directly by the CIS fast logic device (e.g. FPGA).

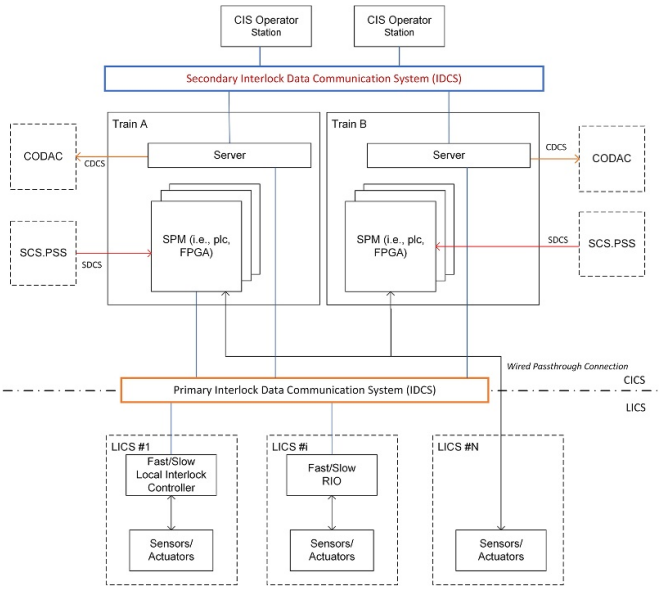

Figure 26. MPS networks.

All LICS are required to exchange at least a minimum set of signals with the CIS, that is the number of interlock nodes corresponds to the number of LICS. Additionally, the CIS will also connect to other CICS systems.

At the top of the MPS communication infrastructure, there exists an Ethernet layer that connects the MPS servers from both CIS Train A and CIS Train B to the CIS WS. The CODAC gateway should be directly linked to the CDCS. The CIS central controllers (i.e. SPMs) are linked to the IDCS. Communication with the CIS HMI is facilitated through the supervisor module. At the moment, the connections to the CR have been unified under the CCN for the CICS systems. However, the necessity for an independent communication channel from the CIS modules to the CIS HMI should be evaluated in the future, depending on the features of the CCN and whether critical functions (e.g., overrides) need to be executed by the HMI in the CR.

The IDCS serves as the connection between the CIS and LICS. Architecturally, no distinctions are made based on the characteristics of the LICS. Depending on the complexity of the protected system, the local implementation of the MPS can utilize either a programmable device (such as a fast or slow controller) or rely on hardwired logics. In the latter scenario, the required signals are exchanged through fast or slow remote I/O devices. Regardless of the method employed, field data are consistently exchanged through the IDCS.

Direct hardwired links are also planned for:

- Monitoring outputs originating from the SCS.PSS;
- Key-scram buttons located on the Interlock Desk and CIS SPMs, allowing operators to execute manual interlock actions where necessary.

7.2.1. Interlock signal categories. According to the specific requirements, three categories of interlocks signals to be exchanged over the IDCS have been identified:

- Slow interlocks over Ethernet network: Utilizing the Siemens S7 family for slow controllers, the ProfiNet protocol is the reference choice. It can satisfy the SIL requirements through the availability of ProfiSAFE as safety protocol to be built on the main layer.
- Fast interlocks over network infrastructure: This category is designated for fast interlocks utilizing the NI cRIO© platform. While it can be extended to the safety version FailSafe over EtherCAT (FSoE), at the time the initial requirements were set, the platform did not have full certification for safety applications. Therefore, integrity must be ensured through redundancy, fail-safe communications, and additional validation. This objective can be achieved either through the 'double-decker' reference configuration and/or by implementing dedicated redundancies within each control train.
- Very fast interlock via hardwired connection: This category involves direct hardwired connections for interlocks that require immediate action and response times in the order of tens of microseconds.

Some other relevant features should be remarked:

- Mixing protocols: The design allows for sharing the same physical infrastructure between fast and slow sections to optimize cost and space. While PROFINET and EtherCAT can be mixed on the same infrastructure, specific tests are required to evaluate communication performance under the project specific traffic conditions.
- Active components: The IDCS network will incorporate active components that support redundancy protocols for implementing network rings. The switches utilized must be compatible with both PROFINET and EtherCAT protocols.
- OPC UA support: The system must support the OPC UA protocols for communication between the supervisor module and the CODAC Gateway. This protocol can also facilitate communication between fast controllers and server applications (i.e., supervisor module), with support from commercial SW tools.
- Web protocols: For communication between the Central MPS Supervisor Module and MPS Operator Stations, web protocols like hypertext transfer protocol secure (HTTPS) and file transfer protocol (FTP) are planned for implementation.

As discussed in section 7.2, TSN is under evaluation in particular for the MPS. A possible architecture for the

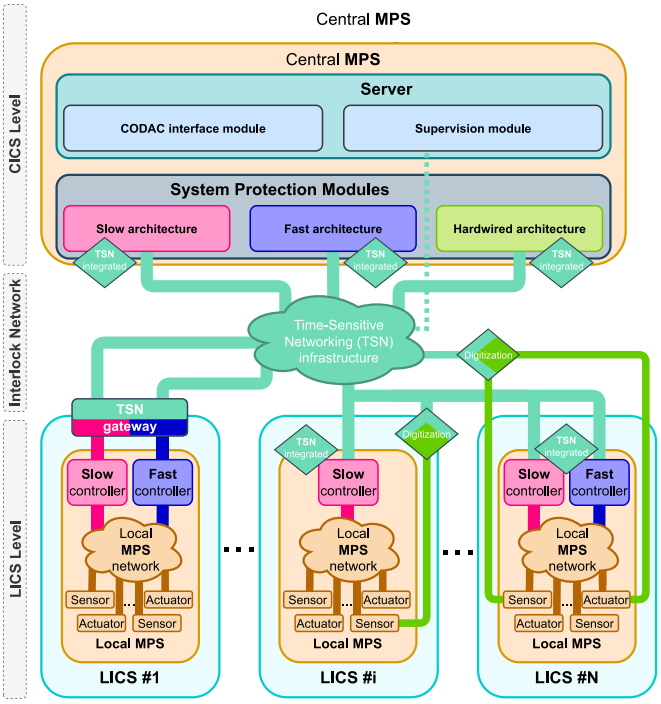

Figure 27. TSN-based MPS network (see [32]). The slow architecture is represented in pink, the fast architecture in dark blue and the hardwired architecture in light green. All parts related to TSN are represented in aquamarine.

TSN-based MPS architecture is shown in figure 27. The description of this specific TSN-based architecture is given in [32].

7.3. SCS network

The SCS is a multifaceted system made up of four primary functional subsystems, each with distinct sizing criteria and standards. These subsystems include also a large number of field components (sensors, DAUs and data collecting units) that must be interconnected and data routed to the assigned CICS cubicles.

To meet these needs, a specialized network called SDCS has been designed, not only for managing safety interlock signals but also as a protective barrier system, since it is designed by following the same standards used for the connected subsystems/components. The SDCS provides secure, asynchronous communication interfaces between SCS controllers located in the LICS and the central SCS system, supporting status monitoring and parameter configuration.

The SDCS is divided into four independent, redundant subnetworks, four assigned to a specific IFMIF-DONES safety subsystem (PSS, OSS, PASS, RAMSES) and one to connect the SCADA servers with the dedicated operator WSs in the control room and/or in the rooms required by the health physics office.

While the primary communication medium is Ethernet, the SDCS incorporates additional protocols such as PROFINET, EtherCAT, TCP/IP, and UDP, along with safety layers like

Table 3. Technology potentially involved in the SCS networks. For SCS.PSS the 'wired' option shall be evaluated, preliminary, as the more effective way to connect central SCS.PSS to plant system LICS. For SCS.PASS and SCS.RAMSES the 'wired' option should be limited to the on-field components.

Net branch tag	Ethernet	Field bus	Wired
SCS.SDCS.CR	Yes	No	No
SCS.SDCS.PSS	Yes	No	Yes
SCS.SDCS.OSS	Yes	No	No
SCS.SDCS.PASS	Yes	Yes	Yes
SCS.SDCS.RAMSES	Yes	Yes	Yes

ProfiSAFE, FSoE, and OpenSAFE. Field devices may also use other protocols, including MODBUS over TCP/IP.

Both PSS and PASS require the management of Boolean safety interlock signals. Based on the technology selected for the SCS controllers in the LICS and their respective categories, these signals may be 'hardwired' (e.g., a 24 V DC energized line) to maximize the PFH. Other communication methods are also under consideration.

The SDCS is responsible for connecting all equipment with a safety function and it is organized into different branches or segments:

1. SCS.SDCS.CR: safety data communication network for the control room
2. SCS.SDCS.PSS: safety data communication network for the plant safety subsystem
3. SCS.SDCS.OSS: safety data communication network for the occupational safety subsystem
4. SCS.SDCS.PASS: safety data communication network for the personal access safety subsystem
5. SCS.SDCS.RAMSES: safety data communication network for the radiation monitoring system

Each branch will meet the specific requirements for SIC, SIL, Seismic Class, and Electric Class as needed for the connected subsystems. Routers, hubs, and switches form an integral part of this network, while gateways (if necessary) will be part of the CICS and housed within its cubicles.

Table 3 shows the technologies potentially involved.

The SCS.SDCS.CR network branch is tasked with connecting all data servers housed within the CICS cubicles, linking each part of the SCS to its corresponding specialized operator terminal and the CODAC Gateway. This network is configured as a redundant Ethernet-based ring, leveraging either copper cabling or FO.

A portion of this Ethernet network is categorized based on the components connected:

- SIC-2/Non-SIC, Category C, and Class 3 for critical safety systems
- Non-SIC/Not Classified for less critical or non-classified components

This modular design ensures redundancy, reliability, and fault tolerance.

The SCS.SDCS.PSS network branch will consist of at least three main sub-networks:

1. Double redundant Ethernet network: This network will connect the SCS.PASS and SCS.RAMSES cubicles to ensure redundancy for the safety interlock system.
2. Dedicated safety interlock network: This network will handle direct connections between the Central SCS.PSS, LICS controllers, and the devices they control. It will transfer Boolean signals characterized by specific cabling standards:

   - 4–20 mA for analog input signals, though not recommended by vendors.
   - 0–30 V DC for DI/DO signals, with a reference of 24 V DC.
   - Low impedance ($<$50 pF m^{-1}) for TTL signals, if applicable.

   The central SCS.PSS does not generate analog outputs and is not directly connected to the devices it controls.

3. Ethernet network for safety alarms: This network will connect all LICS controllers generating safety alarms to the SCS.PSS CICS, enabling the real-time transfer of the numerical values associated with the generation of safety interlock alarms.

Each LICS controller or train will execute safety logic independently. A double voting mechanism will check the processing results for any discrepancies, ensuring system integrity. Segregation between the two safety trains will be enforced by defining two separate installation paths, in line with safety protocols.

To comply with SCS.PSS requirements, particularly those classified as SIC-1 (IEC 61226 Category A or B) or SIC-2 (IEC 61226 Category B or C), the following criteria are mandatory:

- All safety interlock signals received or generated by the SCS.PSS must be discrete.
- Safety interlock processing logics for the SCS.PSS must be Boolean (i.e., DI, DO, relays).
- Signals received by the central SCS.PSS must be duplicated at the LICS level, allowing a minimum of 1oo2 logic (with a target of 2oo3 based on RAMI results).
- Signals processed by the central SCS.PSS will be handled by two separate trains, identified as Train A and Train B.
- Safety commands generated by the central SCS.PSS must be duplicated and transmitted to separate actuators.

The SCS.SDCS.OSS network branch will consist of:

a) Direct connections (field bus or Ethernet) DI/DO involving:
   a. LICS inside the main building to SCS.OSS
   b. LICS outside the main building to SCS.OSS
   c. SCS.OSS to SCS.PASS direct connection

b) Ethernet connections among SCS.OSS CICS and SCS.PASS and SCS.RAMSES CICS to exchange numerical values associated to alarms.
c) Ethernet connections among SCS.OSS and monitoring devices outside the main building.

The SCS.SDCS.PASS network branch has several key functions:

1. Connect access controllers to peripheral devices: This includes communication with door lockers, card readers, door position sensors, CAMs, and interphones.
2. Connect SCS.PASS CICS via Ethernet: The SCS.PASS CICS communicates with the other three SCS subsystems to exchange metadata, as well as with CODAC for centralized control.
3. Integration with the MPS: The SCS.PASS is linked to the MPS, providing the necessary inputs for authorizing plant operation changes.
4. Local room alarms: It is responsible for the connection to local emergency systems, such as visual and audio alarms, to signal alerts.
5. Ensure beam mode safety: It allows safety shutdown of the acceleration process in beam mode to prevent accidents, including the risk of 'man burn' incidents.

The main communication methods are:

a) Peripheral devices: Door lockers, card readers, and door position sensors connect to access controllers via RS-485 in a daisy-chain configuration. This method is widely adopted for its reliability and cost-effectiveness. If needed, RS-485 I/O can be adapted to Ethernet.
b) CAMs and interphones: These devices communicate over Ethernet, primarily for voice and video data. Their connections are directly linked to the server.

The SCS.SDCS.RAMSES network branch connects the RAMSES servers to radiation monitoring devices deployed throughout the plant. Its architecture includes:

a) RS-485 daisy chain and Ethernet: Devices are connected through RS-485 and RS-485/Ethernet terminal servers or directly through Ethernet (TCP/IP) in a star or Ethernet ring topology.
b) Radiation monitoring equipment: Most RAMSES devices are COTS, and the manufacturers are not constrained by communication protocols, except for ensuring that:
   a. Devices must include RS-485 and/or Ethernet connectors.
   b. If proprietary protocols are used, the manufacturers must provide the technical specifications to enable integration with RAMSES systems.
c) RSUs Type 2: Gateways such as RSU2 are used to unify protocols from different vendors to ensure compatibility with RAMSES CICS servers.

The SCS.SDCS.RAMSES architecture includes:

1. Sensors/DAUs: Distributed across the plant, these are connected to RSU2 via RS-485 or Ethernet media.
2. Hardwired SIC-1 sensors: Some sensors are directly connected to RSU1 via hardwired logic (0–1, 0–24 V DC), especially those classified SIC-1 and interfacing with SCS.PSS.
3. SCS.PSS integration: Selected SIC-1 sensors are hardwired to SCS.PSS, and RSU1 connects to SCS.PSS via similar hardwired logic.
4. RSU Type 2 and RAMSES CICS: RSU2 communicates with RAMSES CICS over Ethernet.
5. Metadata exchange: SCS.OSS and SCS.PASS CICS are connected to the RAMSES cubicle via Ethernet to exchange metadata, ensuring system-wide integration of data and safety measures.

7.4. Service networks

In addition to the technical networks at IFMIF-DONES, several other networks support various operational and administrative functions within the facility:

- General purpose network (GPN): This network facilitates the daily operations of non-technical systems, connecting office devices such as laptops, desktop computers, printers, phones, and a wireless network. It also includes a dedicated network for visitors (figure 28).
- DMZ network: The DMZ network serves as a secure zone connecting general-purpose servers, such as email servers, file exchange servers, web servers, and printer servers. It provides controlled access while maintaining separation between internal and external systems to enhance security.
- Surveillance network: This network is responsible for monitoring the security of the IFMIF-DONES facility perimeter, ensuring continuous surveillance and protection against potential threats.

These networks provide critical infrastructure, supporting both the technical and administrative needs of the facility.

7.5. Management network

The management network oversees the entire IFMIF-DONES infrastructure, including both the technical and general purpose networks. Each switch and router within the system is equipped with a dedicated port connected to this network, allowing for several key functions:

- Maintenance: The network streamlines routine maintenance, troubleshooting, and diagnostics, ensuring optimal performance across the infrastructure.
- Automated configuration: It facilitates dynamic adjustments of switches and routers based on predefined

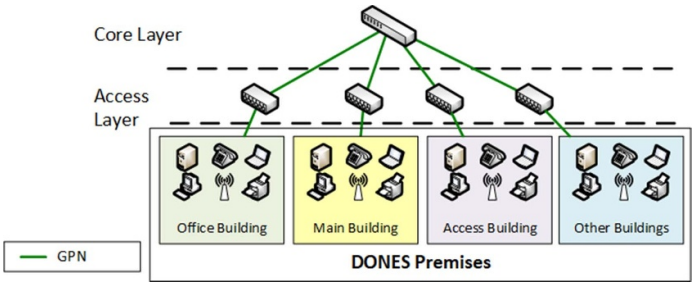

Figure 28. IFMIF-DONES GPN network architecture.

security policies, reducing misconfigurations and enhancing security.
- Firmware updates: Automated firmware updates ensure that vulnerabilities are addressed in a timely manner and that overall performance remains high, maintaining strong network security.
- Network monitoring: Continuous monitoring of network activity detects and addresses anomalies or breaches, safeguarding the integrity of the entire system.

This comprehensive approach to network management ensures that the IFMIF-DONES infrastructure remains secure, efficient, and resilient to potential threats. The extensive network architecture, encompassing CODAC, MPS, and SCS networks, provides a solid foundation for efficient operations and effective data management. By addressing potential challenges and implementing robust solutions, IFMIF-DONES ensures optimal performance and security in its research and experimentation. Ongoing R&D efforts will continue to enhance the network capabilities, allowing it to adapt to the evolving demands of fusion materials research.

8. Protection and safety considerations

In the previous sections, the design of the machine protection systems (MPS) and safety control systems (SCS) was presented based on the system requirements envisaged by the project. More generally, it is useful to make some design considerations on the reasons and purposes that in this activity were the basis of the choices currently made and those that will be made in the future both to correct the limitations of the current design and to consider new inputs coming from the natural evolution of the project. In this section we will therefore describe these protection and security issues from a more transversal point of view.

Functional safety is defined in the IEC 61508 standard as the 'part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures' [33]. IEC 61508 primarily addresses the structure of a company's quality system in relation to the functional safety of products (i.e. the so-called functional safety management system), the methods for determining PFD, PFH and SIL, and the reliability of components, equipment, and systems in safety applications.

Typically, safety systems consist of sensors and transducers, a logic solver (potentially including security SW), and final elements (such as actuators or safety function drives). PFD (or PFH) represents the probability that a device or system will fail to perform its required safety function. This probability correlates with a SIL level, which ranges from 1 to 4, to indicate the integrity level of the safety device or system in question.

Higher-risk safety systems demand higher SIL values. The evaluation of a system reliability and the certification of its components under IEC 61508 is an effective, internationally recognized method to ensure and verify the reliability of any device, system, or process involving safety considerations, such as risks to people, the environment, or property.

There are essentially three types of certifications that are possible and often required by the market:

1. HW certification according to IEC 61508.
2. HW certification with 'Proven in use' considerations compliant with IEC 61508/61511.
3. Full certification in compliance with IEC 61508.

On the other hand, SIL certification is increasingly becoming a contractual requirement in major tenders for both mechanical and electrical/electronic products or systems.

Concerning MPS, where safety is not directly involved but rather the prevention of damage to equipment or systems, the SIL defined in IEC 61508 can be interpreted as interlock integrity level (IIL). The MPS ensures that the equipment is safely transferred to a controlled state when specific conditions are met, such as an operational anomaly or parameter breach.

MPS, which is designed using complex electronic devices like PLCs, FPGAs, or other programmable electronics, should be categorized as a Type B subsystem according to IEC 61508–2. A Type B system involves components whose failure modes are less well-defined, often involving SW or complex logic circuits that cannot be fully tested via traditional means.

Since the interlock function is only required when a deviation or anomaly occurs, but with the likelihood of more than one activation per year, MPS is classified as operating in high-demand mode. In this mode, the system is expected to frequently engage, moving the EUC into a specified 'safe state' (in this case, a protected or controlled state). The target failure measures for a safety function (here interlock function) operating in high demand mode of operation or continuous mode of operation are defined in table 4 following IEC 61508–1 [28].

Table 4. Safety integrity levels—target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation (from [IEC 61508–1]).

Safety integrity level	Low demand mode of operation (Average PFH to perform its design function on demand)	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	10^{-5} to $<10^{-4}$	10^{-9} to $<10^{-8}$
3	10^{-4} to $<10^{-3}$	10^{-8} to $<10^{-7}$
2	10^{-3} to $<10^{-2}$	10^{-7} to $<10^{-6}$
1	10^{-2} to $<10^{-1}$	10^{-6} to $<10^{-5}$

Table 5. Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem (from [IEC 61508–2]).

	Hardware fault tolerance		
Safe failure fraction of an element	0	1	2
<60%	Not allowed	SIL 1	SIL 2
60%–<90%	SIL 1	SIL 2	SIL 3
90%–<99%	SIL 2	SIL 3	SIL 4
⩾99%	SIL 3	SIL 4	SIL 4

The highest integrity level that can be claimed for a function is limited by the HW fault tolerance (HFT) and the SFF. The architectural constrains on type B components are defined in table 5 following IEC 61508–2 [34].

To achieve the desired IIL for the MPS, designers must carefully consider:

1. PFH: Set according to IEC 61508–1 table 3 for the high-demand mode.
2. SFF and HFT: Defined in IEC 61508–2 table 3, limiting the maximum possible IIL for the interlock function.
3. Type B subsystem classification: Ensuring the system architecture adheres to the required fault tolerance and reliability.

By aligning the MPS design with these guidelines, the system can achieve the appropriate IIL needed for reliable and effective interlock functionality.

It should be noted that the discussion regarding SIL for the MPS raises several important points regarding the application of the IEC 61508 standard and its implications for safety in complex systems like the IFMIF-DONES design.

The existing SIL-3 requirement for the MPS is acknowledged as an arbitrary target rather than a necessity dictated by a comprehensive risk analysis. While IEC 61508–1 specifies that the average PFH for an interlock function should be less than 10^{-7} h, it allows for a PFH between 10^{-8} and 10^{-7}. Thus, adopting a target of SIL-3 without substantiated risks could lead to unnecessary complexity in the system design.

It is important to note that SW compliance (such as CPU firmware, SCADA systems, and CPU programming tools) often represents the true bottleneck in implementing IEC 61508, rather than the HW itself. The very rapid actuation times (on the order of microseconds) of the MPS raise questions about the practicality of achieving a SIL-3 rating across the entire control chain. If certain components in the control chain (like sensors, actuators, and the communication networks) do not support the same integrity level, assigning a higher SIL to the MPS may lead to a misleading perception of safety.

Drawing on return experiences from other facilities, there is skepticism about the applicability of a high SIL requirement, particularly when the system's performance may not consistently align with such standards. The realization that various safety instrumented functions within the risk assessment scenarios had a broad distribution of safety requirements—ranging from no SIL to SIL-4—emphasizes that a one-size-fits-all approach to SIL assignment may not be suitable.

The SCS requirements described in section 5 form a robust framework for the SCS architecture, prioritizing safety and reliability while allowing for effective communication and monitoring across the subsystems. The emphasis on Boolean logic for connections and safety logics, the role of dedicated hardwired consoles, and the structured approach to HMI connections are all aimed at enhancing the operational integrity and safety of the facility.

By adhering to these guidelines, the SCS ensures a comprehensive safety approach, capable of effectively managing the complex interactions and requirements of the various subsystems while safeguarding personnel and the environment.

9. Conclusions and future work

In the future, the ENS project will advance by further refining the current engineering design of the IFMIF-DONES facility. Building on the definition design, the focus will shift toward completing the engineering blueprint, carrying out experimental validation, performing transversal analyses, and preparing technical specifications for upcoming construction tenders.

As mentioned in the introductory part, the final decision on which control framework to implement may strongly depend on the specific needs of the accelerator, including the complexity of the control tasks, budgetary considerations, and economic scale.

Modern ASs often adopt a hybrid approach, combining multiple control frameworks to achieve an optimal balance of flexibility, real-time performance, and ease of use—an approach reflected in the design of the IFMIF-DONES control system here described. This hybrid system addresses the

unique demands of the project while accommodating in a modular way future revisions driven by evolving technical, scientific, or management needs.

It is important to acknowledge that the project being in its definition phase, design choices may be adjusted as new technologies emerge or project requirements shift. Therefore, the IFMIF-DONES control system design reflects a versatile and adaptive approach tailored to meet both present and future demands. This leads to a continuous update and improvement of the project, starting from the control framework itself.

Due to the advances in technology and also to be aligned with new industry standards, nowadays some modern SCADAs have been introduced in other large scientific facilities as NASA [35], CERN [36, 37] or ITER [38]. Probably the most illustrative example of an industrial SCADA used in a large research facility is the implementation of WinCC OA© at CERN. There, this SCADA is the base for the supervisory system of their two main industrial control frameworks (JCOP and UNICOS) [39]. As another example, at the Karlsruhe Research Accelerator, WinCC OA© is working as the overall SCADA for all beamlines and it allows the interconnection between different systems controlled by TANGO and EPICS respectively, providing the GUI too [40]. And it is also worth mentioning the Sirius (the Brazilian 4th generation synchrotron light source). Here WinCC Unified© is planned to be used as general supervisory system for all the scientific facilities [41], to coordinate the data generated by different equipment, some controlled by EPICS and others using industrial protocols as OPC-UA provided by commercial automation systems.

In the scope of the IFMIF-DONES project some comparative studies have been performed to analyze the feasibility of different control frameworks to the plant scope. The main conclusions may show that:

- Unifying the CICS control framework with an industrial SCADA for all systems is a possible solution and might improve practicality, operability, and functionality.
- License cost of proprietary solutions is not the only key decision factor.
- If meeting SIL3 qualification remains a key requirement for MPS and/or SCS, an indutrial SCADA might be a necessary choice.

Based on these results, an update to the CODAC architecture is currently under evaluation. This update might lead to a unified industrial SCADA framework for all CICS systems (CODAC, MPS, and SCS), while EPICS remains an important control framework, though primarily focused on local control within certain LICS. This revised architecture would also facilitate the management and integration of other LICS using industry-standard protocols, distinct from EPICS. Various technologies for enabling communication between the two proposed control frameworks (EPICS and an industrial SCADA) through a gateway are being investigated, and a performance comparison will be conducted.

The current MPS design could be revised by taking into account recent technological advancements and components (e.g., Siemens© S7-1518 HF CPUs, NI CRIO 9048 main chassis, Intel© Quartus FPGA, μTCA), updating communication protocols (e.g., Profinet I-Device, EtherCAT, OF wired, etc), and opting to exclude servers or embedded PCs from managing interlock signals. Additionally, certain design choices, such as the 'double decker' configuration—originally used to synchronize components available 10 years ago to achieve high PFH—could also be revised and simplified. Classifying MPS interlock parts as SIL2, SIL3, or SIL4 according to IEC 61508 should not be a design requirement, but rather a result of the system's compliance with response time requirements and PFH evaluation over its expected lifetime (e.g., 20 years) and minimum time between two planned maintenance periods (e.g., 1 year).

The current design of SCS.PSS and SCS.PASS is evolving toward a more detailed and refined approach, where safety interlock loops (based on Boolean signals) are physically separated from safety data management. Safety interlock signals need to be managed in the most reliable and fastest way possible, using certified technologies, which are currently still reliant on hardwired systems to interface with LICS and CICS. However, within the CICS, other technologies such as TwinSafe© and FSoE can be used for faster response times in processing logic. On the other hand, safety data management, which differs from Boolean-based interlock signals, can still utilize newer technologies (e.g. EtherCAT, PROFINET) that do not necessarily support safety protocols but are sized according to IEC 61226/IEC 61513, with SIL requirements relaxed to the same level as those of the MPS.

One of the main problems on which future development will have to focus is that of the LICS design. Potential challenges for LICS include communication latency or loss between LICS and CICS, actuator or sensor failures, and SW bugs that could disrupt control operations. Additionally, issues such as inadequate data preprocessing, HW degradation, or inadequate fault detection could affect system performance and safety. Handling these risks requires robust design, regular maintenance, and fail-safe mechanisms.

Other future improvements will deal with real-time control, safety interlocks, and communication protocols. As explained in the different sections above, IFMIF-DONES may require strict time constraints: delays or failures to act within the required time can lead to significant issues, so that a higher performant real-time system may be needed. This will lead to improve precise timing and response through the advanced design of a specific timing system and network introduced in section 7; improve the level of determinism by using devices like FPGAs or advanced programmable devices; reduce latency to maintain real-time performance; improve the integration with sensors and actuators in RT.

In the MPS section (see section 5), the importance of the safety interlocks design was seen to prevent dangerous or improper actions in automated systems. Future work on safety interlocks will focus on improved fail-safe mechanisms, physical and SW-based interlocks to ensure comprehensive safety coverage and optimized redundancy.

In section 7 it has been clearly shown how communication protocols govern the exchange of information between different system components, allowing them to work together

effectively. In control systems, reliable and efficient communication is crucial, especially in distributed systems with numerous multiple interconnected parts (e.g., sensors, controllers, actuators). Future work on communication protocols will include an optimized standardization and interoperability, a lower latency and higher reliability, the integration with the security to protect systems from cyberattacks, unauthorized access, or data tampering.

One key area of development will be the integration of the control system with instruments and diagnostics. This integration will be enhanced by AI tools, which will significantly increase the facility's reliability, efficiency, and safety (see [42] for a recent study on this subject). AI will provide operators with advanced tools for proactive system management, enabling them to optimize performance in real-time, especially in particle ASs (as shown in many ASs' applications as in [43–48]).

By incorporating AI-driven diagnostics, future operators will be able to extract more detailed insights from real-time data. Machine learning algorithms will analyze long-term operational data to enable predictive maintenance, allowing potential issues to be addressed before they escalate [49, 50]. This capability will reduce downtime and improve operational efficiency.

AI will also enhance the control systems by dynamically adjusting parameters in response to changing conditions, ensuring the system adapts in real-time and learns from operational data. Furthermore, AI will strengthen safety protocols through advanced anomaly detection, enabling operators to respond quickly to deviations and implement stronger preventive measures.

In conclusion, the future integration of AI into the control and diagnostic systems of IFMIF-DONES will lead to a highly adaptive, data-driven facility that prioritizes safety, efficiency, and optimized performance throughout its operations.

Acknowledgment

This work has been carried out within the framework of the EUROfusion Consortium, funded by the European Union via the Euratom Research and Training Programme (Grant Agreement No. 101052200—EUROfusion). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them.

This work would not have been possible without the unwavering support and collaboration from all team members, whose commitment and professionalism were instrumental in navigating the challenges we encountered. We would like to express our sincere gratitude to all the collaborators who contributed to the success of the I&C area throughout the years.

ORCID iD

M. Cappelli https://orcid.org/0000-0002-4344-6067

References

[1] Stork D. *et al* 2014 Materials R&D for a timely DEMO: key findings and recommendations of the EU roadmap materials assessment group *Fusion Eng. Des.* **89** 1586–94
[2] Stork D., Heidinger R., Muroga T., Zinkle S.J., Moeslang A., Porton M., Boutard J.-L., Gonzalez S. and Ibarra A. 2017 Towards a programme of testing and qualification for structural and plasma-facing materials in fusion neutron environments *Nucl. Fusion* **57** 092013
[3] Knaster J. 2018 An assessment of the available alternatives for fusion relevant neutron sources *Nucl. Fusion* **58** 095001
[4] Goland N., Snead C.L., Parkin D.M. and Theus R.B. 1975 Use of Li(d, n) neutrons for simulation of radiation effects in fusion reactors *IEEE Trans. Nucl. Sci.* **22** 1776–9
[5] Grand P., Batchelor K., Blewett J.P., Goland A., Gurinsky D., Kukkonen J. and Snead C.L. 1976 An intense Li(d,n) neutron radiation test facility for controlled thermonuclear reactor materials testing *Nucl. Technol.* **29** 327
[6] Stork D. *et al* 2014 Developing structural, high-heat flux and plasma facing materials for a near-term DEMO fusion power plant: the EU assessment *J. Nucl. Mater.* **455** 277–91
[7] Federici G., Biel W., Gilbert M.R., Kemp R., Taylor N. and Wenninger R. 2017 European DEMO design strategy and consequences for materials *Nucl. Fusion* **57** 092002
[8] Federici G. *et al* 2018 DEMO design activity in Europe: progress and updates *Fusion Eng. Des.* **136** 729–41
[9] Ibarra A., Heidinger R., Barabaschi P., Mota F., Mosnier A., Cara P. and Nitti F.S. 2014 A stepped approach from IFMIF/EVEDA toward IFMIF *Fusion Sci. Technol.* **66** 252–9
[10] Donné A.J.H. 2019 The European roadmap towards fusion electricity *Philos Trans A Math Phys Eng Sci.* **377** 2141
[11] Ibarra A. *et al* 2018 The IFMIF-DONES project: preliminary engineering design *Nucl. Fusion* **58** 105002
[12] Ibarra A. *et al* (the full IFMIF-DONES Team) 2019 The European approach to the fusion-like neutron source: the IFMIF-DONES project *Nucl. Fusion* **59** 065002
[13] Królas W. *et al* 2021 The IFMIF-DONES fusion oriented neutron source: evolution of the design *Nucl. Fusion* **61** 125002
[14] Bernardi D. *et al* 2022 The IFMIF-DONES project: design status and main achievements within the EUROfusion FP8 work programme *J. Fusion Energy* **41** 1–26
[15] Cappelli M., Centioli C., Neri C., Monti C. and Ibarra A. 2019 IFMIF-DONES central instrumentation and control systems: general overview *Fusion Eng. Des.* **146** 2682–6
[16] Cappelli M. *et al* 2019 Preliminary engineering design of the Central Instrumentation and Control Systems for the IFMIF-DONES plant *Proc. ICALEPCS2019* (*New York, NY, USA*) (available at: https://accelconf.web.cern.ch/icalepcs2019/papers/frapp02.pdf)
[17] Cappelli M., Bagnasco A., Diaz J., Sousa J., Ambi F., Campedrer A., Liuzza D., Carvalho B. and Ibarra A. 2021 Status of the engineering design of the IFMIF-DONES Central Instrumentation and Control Systems *Fusion Eng. Des.* **170** 112674
[18] Cappelli M., Ambi F., Bagnasco A., Botta E., Chen Z., Diaz J., Gutierrez V., Goryl P., Sousa J. and Ibarra A. 2023 Recent advances of the IFMIF-DONES Central Instrumentation and Control Systems engineering design *Fusion Eng. Des.* **194** 113671
[19] Cappelli M. (ed) 2023 *Instrumentation and Control Systems for Nuclear Power Plants* (Woodhead Publishing-Elsevier)
[20] 2025 Experimental Physics and Industrial Control System (EPICS) - EPICS 7.0 Release Series (available at: https://epics.anl.gov/base/R7-0/index.php) (3 April 2025)

[21] 2023 TANGO Developer's Guide (available at: https://tango-controls.readthedocs.io/en/latest/development/index.html) (3 April 2025)
[22] Wallander A. *et al* 2010 ITER instrumentation and control—Status and plans *Fusion Eng. Des.* **85** 529–34
[23] Davis W., Wallander A. and Yonekawa I. 2016 Current status of ITER I&C system as integration begins *Fusion Eng. Des.* **112** 788–95
[24] Ravensbergen T., Zabeo L., de Vries P., Pangione L., Treutterer W., De Tommasi G., Lee W.-R., Tak T. and Zagar A. 2023 Strategy towards model-based design and testing of the ITER plasma control system *Fusion Eng. Des.* **188** 113440
[25] De Vries P.C. *et al* 2024 Strategy to systematically design and deploy the ITER plasma control system: a system engineering and model-based design approach *Fusion Eng. Des.* **204** 114464
[26] Park M. *et al* 2008 Overview of KSTAR integrated control system *Nucl. Eng. Technol.* **40** 451–8
[27] Torregrosa-Martin C. *et al* 2023 Overview of IFMIF-DONES diagnostics: requirements and techniques *Fusion Eng. Des.* **191** 11355
[28] IEC 61508–1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems—part 1: general requirements (available at: https://webstore.iec.ch/en/publication/5515)
[29] US Department of Labor OSHA 3071 OSHA guidelines 2002 (available at: www.osha.gov/sites/default/files/publications/osha3071.pdf)
[30] Martín-Fuertes F. *et al* 2022 Implementation of Safety Aspects in IFMIF-DONES Design *J. Nucl. Eng.* **3** 373–84
[31] Megías C., Vázquez V., Ros E., Cappelli M. and Díaz J. 2023 Ethernet-based timing system for accelerator facilities: the IFMIF-DONES case *Comput. Netw.* **233** 109897
[32] Megías C., Sánchez-Garrido J., Vázquez V., Ros E., Cappelli M. and Díaz J. 2023 Time-sensitive networking for interlock propagation in the IFMIF-DONES facility *Fusion Eng. Des.* **191** 113774
[33] IEC 61508–4:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems—part 4: definitions and abbreviations (available at: https://webstore.iec.ch/en/publication/5518)
[34] IEC 61508–2:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems—part 2: requirements for electrical/electronic/programmable electronic safety-related systems (available at: https://webstore.iec.ch/en/publication/5516)
[35] McNelis A., Beach R., Soeder J., McNelis N., May R., Dever T. and Trase L. Simulation and control lab development for power and energy management for NASA manned deep space missions *12th Int. Energy Conversion Engineering Conf.* (*Cleveland, OH*, *28–30 July 2014*) (https://doi.org/10.2514/6.2014-3835)
[36] Golonka P., Fabian W., Gonzalez-Berges M.L., Jasiun P. and Varela-Rodriguez F. 2014 FwWebViewPlus: integration of web technologies into WinCC OA based human-machine interfaces at CERN *J. Phys.: Conf. Ser.* **513** 012009
[37] Ledeul A., Millan G.S., Savulescu A., Styczen B. and Ribeira D.V. CERN supervision, control and data acquisition system for radiation and environmental protection *12th Int. Workshop on Personal Computers and Particle Accelerator Controls (PCaPAC)* (*Hsinchu, Taiwan*, *16–19 October 2018*) p FRCC3
[38] Dal Bello S., Battistella M., Grando L., Luchetta A., Moressa M., Breda M., Svensson L., Paolucci F. and Labate C.V. 2019 Safety systems in the ITER neutral beam test facility *Fusion Eng. Des.* **146** 246–9
[39] Golonka P. and Varela-Rodríguez F. Consolidation and redesign of CERN industrial controls frameworks *17th Biennial Int. Conf. on Accelerator and Large Experimental Physics Control Systems (ICALEPCS)* (*New York, United States*, *5–11 October 2019*) p WEDPL04
[40] Mexner W., Aydt B., Hofmann D., Bründermann E., Blomley E., Schuh M., Müller A.-S. and Marsching S. Control system virtualization at Karlsruhe research *Accelerator 17th Biennial Int. Conf. on Accelerator and Large Experimental Physics Control Systems (ICALEPCS)* (*New York, United States*, *5–11 October 2019*) p MOMPL009
[41] Arruda L.C., Barreto G.T., Canova H.F., Franca J.V.B. and Calcanha M.P. Supervisory system for the Sirius scientific facilities *18th Int. Conf. on Acc. and Large Exp. Physics Control Systems ICALEPCS2021* (*Shanghai, China*, *14–21 October 2021*)
[42] Cappelli M., Torregrosa-Martin C., Diaz J. and Ibarra A. 2024 The IFMIF-DONES diagnostics and control systems: current design status, integration issues and future perspectives embedding artificial intelligence tools *J. Fusion Energy* **43**
[43] Emma C., Edelen A., Hogan M.J., O'Shea B., White G. and Yakimenko V. 2018 Machine learning-based longitudinal phase space prediction of particle accelerators *Phys. Rev. Accel. Beams* **21** 112802
[44] Arpaia P. *et al* 2021 Machine learning for beam dynamics studies at the CERN Large Hadron Collider *Nucl. Instrum. Methods Phys. Res.* A **985** 164652
[45] Edelen A.L., Biedron S.G., Chase B.E., Edstrom D., Milton S.V. and Stabile P. 2016 Neural networks for modeling and control of particle accelerators *IEEE Trans. Nucl. Sci.* **63** 878–97
[46] Kain V., Hirlander S., Goddard B., Velotti F.M., Zevi Della Porta G., Bruchon N. and Valentino G. 2020 Sample-efficient reinforcement learning for CERN accelerator control *Phys. Rev. Accel. Beams* **23** 124801
[47] Edelen A., Neveu N., Frey M., Huber Y., Mayes C. and Adelmann A. 2020 Machine learning for orders of magnitude speedup in multi-objective optimization of particle accelerator systems *Phys. Rev. Accel. Beams* **23** 044601
[48] Ivanov A. and Agapov I. 2020 Physics-based deep neural networks for beam dynamics in charged particle accelerators *Phys. Rev. Accel. Beams* **23** 074601
[49] Oluwasegun A. and Jung J.-C. 2020 The application of machine learning for the prognostics and health management of control element drive system *Nucl. Eng. Technol.* **52** 2262–73
[50] Garcia H.E., Aumeier S.E., Al-Rashdan A.Y. and Rolston B.L. 2020 Secure embedded intelligence in nuclear systems: framework and methods *Ann. Nucl. Energy* **140** 107261