Fusion Engineering and Design 194 (2023) 113671

Contents lists available at ScienceDirect

Fusion Engineering and Design

journal homepage: www.elsevier.com/locate/fusengdes

Recent advances of the IFMIF-DONES central instrumentation and control systems engineering design

Mauro Cappelli [a,*], Francesca Ambi [b], Andrea Bagnasco [b], Enrico Botta [b], Zhe Chen [c], Javier Diaz [d], Victor Gutierrez [e], Piotr Goryl [f], Jorge Sousa [g], Angel Ibarra [e]

[a] *ENEA, Frascati Research Center, Rome, Italy*
[b] *Ansaldo Nucleare, Genova, Italy*
[c] *University of Aalborg, Aalborg, Denmark*
[d] *University of Granada, Granada, Spain*
[e] *CIEMAT, Madrid, Spain*
[f] *S2 Innovations, Krakow, Poland*
[g] *IPFN, Lisbon, Portugal*

ARTICLE INFO

Keywords:
Control system
DEMO
DONES
I&C
Protection
Safety

The International Fusion Materials Irradiation Facility-DEMO—Oriented NEutron Source (IFMIF-DONES) is an accelerator-based neutron source that generates high-energy neutrons via stripping processes by focusing a high-energy deuteron beam on a fast-flowing liquid lithium jet. The neutrons produced are used for the irradiation of materials foreseen in DEMO, thus providing relevant data for the design and licensing of the future fusion reactor. The complexity of such a plant is managed by a central control system that guarantees the safe supervision and control of all operations. This paper summarizes the most recent developments in the design of the IFMIF-DONES plant's Central Instrumentation and Control Systems (CICS) after the completion of the preliminary design phase. In particular, the architecture of two of the main CICS systems (namely, MPS and SCS) is described in detail, focussing on the specific design choices recently proposed. For each system, the current status of design is presented, as well as the existing and future plans for their integration in a unique control framework.

1. Introduction

In future fusion power plants the irradiation environment is defined by the presence of high-energy neutrons in the first-wall region [1]. For the DEMOnstration Fusion Reactor (DEMO), whose in-vessel materials will be exposed to neutron fluxes up to 5×10^{18} m^2 s^{-1} at a peak energy of 14.1 MeV, with a potential displacement damage in excess of 10 dpa per year of operation and a He production rate of 10^{-13} appm/dpa, the availability of a fusion-relevant neutron source is a first priority requirement for a safe design [2].

Yet such an environment cannot be replicated by the neutron sources that are now available. It has been widely accepted that an accelerator-based neutron source utilizing D-Li stripping processes (Li(d,nx)) is the best option for supplying the necessary neutron flux and spectrum for replicating the aforementioned irradiation conditions [3,4]. To this purpose, the EU provided funding through the EUROfusion Work Package Early Neutron Source (WPENS) in collaboration with the F4E Agency to develop a Li(d,nx) neutron source known as IFMIF-DONES (International Fusion Materials Irradiation Facility-DEMO Oriented NEutron Source), which is specified in the EU Roadmap [4–6].

In [7–9] the current IFMIF-DONES Plant design is widely described: Five primary systems—the accelerator systems, lithium systems, test systems, plant systems, and central instrumentation and control systems—are individuated to compose the experimental facility.

The Accelerator Systems (AS), which consists of a series of acceleration and beam transport stages, produces a 5 MW deuteron beam (125 mA, 40 MeV) with a rectangular cross section of [100, 200] mm x 50 mm that impinges on a free surface liquid lithium target (25 mm thick, 260 mm wide), cross-flowing at 15 m/s. The Lithium Systems (LS), which are in charge of lithium flow control, heat removal, and lithium purification, are in charge of the High Flux Test Module (HFTM), which is a portion of the Test Systems (TS) directly behind the lithium target housing the material samples from the stripping reactions.

The Instrumentation and Control (I&C) System, whose overall architecture has been extensively documented in [10–12], regulates all plant operations while being backed by general services known as Plant

[*] Corresponding author.
E-mail address: mauro.cappelli@enea.it (M. Cappelli).

https://doi.org/10.1016/j.fusengdes.2023.113671
Received 28 October 2022; Received in revised form 8 February 2023; Accepted 16 March 2023
Available online 17 April 2023

Systems (PS).

This paper provides an overview of the current state of the overall design for the Central Instrumentation and Control Systems (CICS), with a focus on the key advances in the Machine Protection Systems (MPS) and Safety Control Systems (SCS).

2. The central instrumentation and control systems (CICS): general architecture

The DONES I&C System is designed with a hierarchical structure, from the top level Central Instrumentation and Control Systems (CICS), down to the Local Instrumentation and Control Subsystems (LICS) level, similar to other experimental plants (see for example the ITER case, as in [12–14], or other modern I&C tokamak designs [15]).

The DONES I&C System is made up of various systems that are capable of doing complex tasks on their own. It uses a distributed control technique to provide local independence while still providing overall I&C subsystem supervision and control from a central location. CICS are in charge of managing, monitoring, and regulating all plant parameters and variables, as well as of storing and visualizing data from a system perspective. They primarily rely on a collection of supervisory tools that ensure constant, two-way contact with LICS and real-time interaction with other subsystems via networking (Fig. 1).

It should be noted that sensors and actuators are here generic terms, the real implementation depending on the different system. They include simple instruments like thermocouples, flow meters, pressure gauges, or radiation monitors, up to more complex diagnostic instrumentation. Typical actuators are electromagnetic pumps, valves or motors. The detailed description of such instruments is out of the scope of this paper as it treated in specific papers on diagnostics. While the corresponding raw signal data acquired are processed and converted into process variables and then made available throughout the entire plant, LICS are responsible for controlling every subsystem and component to ensure that all process variables are kept inside the required range at a local level. The I&C Systems typically contain a Human-Machine Interface (HMI) and operational monitoring capabilities at each level of the hierarchy.

A real-time distributed control system based on open source software tools, libraries, and applications is used to construct the control architecture. Robust control hardware is used, including Field Programmable Gate Arrays (FPGA) and Programmable Logic Controllers (PLC). For regulating and monitoring the complete plant operation and status, the communication is based on multiple control and supervisory networks (Ethernet and fiber optic 10 Gigabit Ethernet) [11].

As for Fig. 1, three systems make up CICS from a functional standpoint: Control Data Access and Communication (CODAC) System, Machine Protection System (MPS), and Safety Control System (SCS). Through the utilization of specific networks and buses, each system at the central level is in continuous, bidirectional contact with the equivalent system at the local level. In [10–12], a thorough general description of the CODAC, MPS, and SCS is provided.

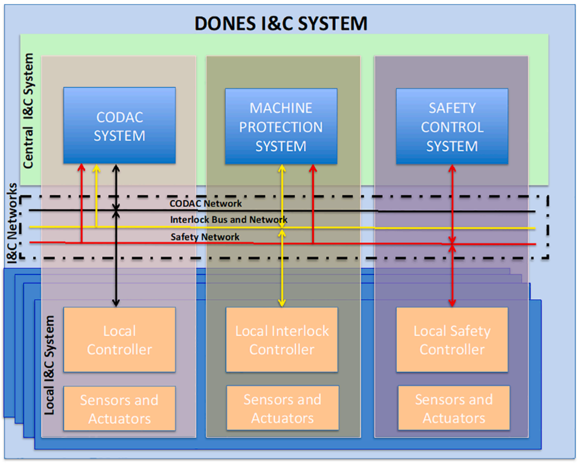

Fig. 1. DONES I&C Systems: General Top Level Architecture.

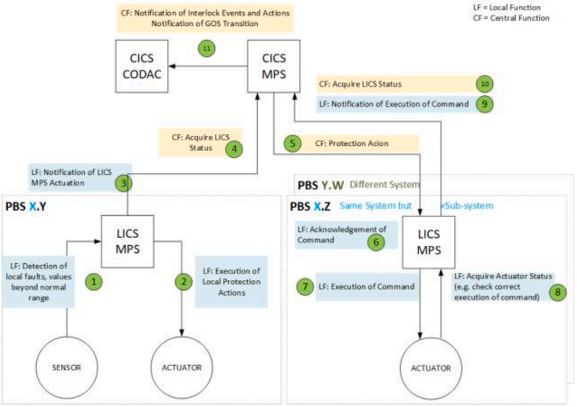
LF = Local Function
CF = Central Function
CF: Notification of Interlock Events and Actions
Notification of GOS Transition
11
CICS CODAC
CICS MPS
CF: Acquire LICS Status
10
LF: Notification of Execution of Command
9
CF: Acquire LICS Status
4
5
CF: Protection Acion
LF: Notification of LICS MPS Actuation
3
PBS Y.W Different System
PBS X.Y
PBS X.Z Same System but ≠Sub-system
LICS MPS
LF: Acknowledgement of Command
6
LICS MPS
LF: Detection of local faults, values beyond normal range
1
2
LF: Execution of Local Protection Actions
7
LF: Execution of Command
LF: Acquire Actuator Status (e.g. check correct execution of command)
8
SENSOR
ACTUATOR
ACTUATOR

Fig. 2. Local versus Central Protection Functions.

A detailed description of the main components of the CODAC System, namely Data Management (DM) System, the Human-Machine Interface (HMI) System, and the Timing System (TS), has been given in [16]. In what follows an overview about the current design of the MPS and SCS will be provided.

3. Machine protection system (MPS)

The Machine Protection System (MPS) is in charge of implementing all the investment protection strategies at the different plant levels, ensuring plant protection against:

- failures of the system or equipment components;
- failures of the central/local control systems;
- incorrect operation.

by means of dedicated sensors and actuators, and specific high integrity logic solvers.

It should be remarked that the MPS only deals with the investment protection, while all the strategies related to (environmental, occupational, human health) safety is handled by the Safety Control System, described in Section 4.

The MPS is designed as a two-level architecture (Fig. 2):

1 The Central Machine Protection System (CMPS), for the implementation of plant-wide protection actions;
2 The Local level Machine Protection System (LMPS), for handling local (i.e. at subsystem level) protection events. Communication among the CMPS and the LMPSs is performed through dedicated networks and buses.

The role of the Central Machine Protection System (CMPS) is to provide a reliable and uniform environment for the detection, processing, alarm handling, logging and display of interlock events occurring in the systems. Its main objective is the coordination of the different implemented local protection systems, as well as the safe execution of all the protection functions that involve several systems or subsystems. As an example, for the protection of the Target Assembly, a very fast shutdown of the beam is needed to avoid the meltdown of the Back Plate (BP) and resultant leakage of the lithium flow by detecting signals from hardwired interlock systems in the Lithium Target Systems and sending the beam shutdown signal directly to the Accelerator Systems.

The Local Machine Protection Systems (LMPSs) ensure the detection of failures and the implementation of all the investment protection functions within the scope of each subsystem. The LMPSs have direct interfaces with the Central Machine Protection System for parameter notification as well as for the exchange of critical information regarding the protection functions affecting other systems or subsystems. To better clarify the distinction between central and local protective functions, Fig. 2 shows the MPS actuation chain in case of local fault within system X.Y.

The CMPS is divided in three subsystems or architectures according to the different timing requirement that were defined for the interlock actuation.

- Slow interlocks (response time higher than 300 ms);
- Fast interlocks (response time lower than 300 ms);
- Hardwired interlocks (response time lower than 30μs).

Fig. 3 describes the MPS Fast and Hardwired architectures, respectively. It can be observed that the Hardwired Architecture simplifies the actuation of the protection function by bypassing the local controllers and directly connecting local sensors and actuators to the FPGA of the CMPS.

The CMPS is divided in different functional and hardware modules in order to allow flexible operation and maintenance as well as progressive integration and commissioning.

As shown in Fig. 4, the CMPS is divided in the following different functional modules:

- Supervisor module
- System Protection Modules (SPMs)
- CODAC Interface Module (EPICS Gateway)

This modularity allows integration of new LMPS to an existing and operating version of the CMPS with minimal modifications on the running components already installed; modification (up to disconnection) of a module while the other CMPS functions remain active; separation in different protection modules of interlock functions requiring different response time performance.

It should be underlined that the CMPS shall be based on a fail-safe design to guarantee the machine protection even in case of CMPS failure. As a consequence the “candidate technologies” have been chosen on the basis of such a requirement.

4. Safety control system (SCS)

The Safety Control System (SCS) is a dedicated safety grade protection system devoted to the implementation of all the identified protection functions regarding the personnel and/or the environment. It is implemented in an independent and dedicated architecture, minimizing the interactions with the conventional system. The SCS is mainly composed by the following subsystems:

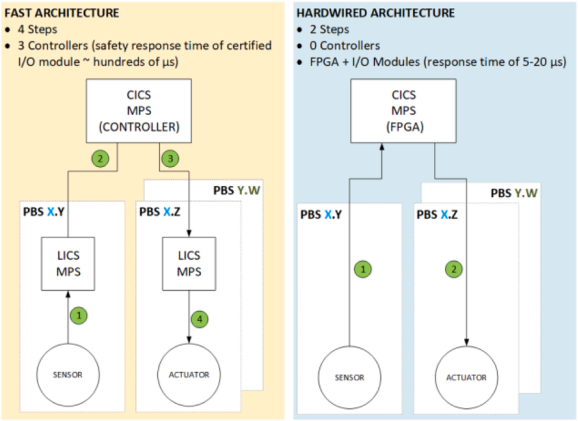

Fig. 3. Description of Fast and Hardwired architectures for the Machine Protection System.

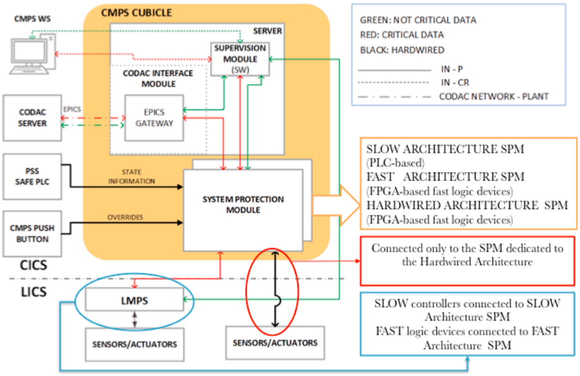

Fig. 4. Machine Protection System: Central versus Local data flow. It is also shown that each system utilizes different hardware based on the timing requirements.

- Plant Safety Subsystem (PSS)
- Occupational Safety Subsystem (OSS)
- Personal Access Safety Subsystem (PASS)
- Radiation Monitoring System for the Environment and Safety (RAMSES).

The SCS coordinates the individual protections provided by the Safety Procedures, enables manual control by the operator and displays data required for the operator supervision and control. Each part of the SCS has a different Safety Important Component (SIC) classification (on the basis of the safety functions implemented), and all the subsystems may be accessed from the operators as a single system. For these reasons, the lower part of the architecture consists of four separate legs that are different in terms of performance, configuration, and physical means. On the contrary, the upper part of the architecture has the duty of the seamless integration of the safety data to be accessed by the operator and by the CODAC gateway. The separation between the different levels of the networks is always mediated by the servers to guarantee a separation layer between the operators and the safety controllers. An additional degree of separation is created toward the interfacing CODAC system (not safety-classified system) by means of the CODAC gateway (Fig. 5).

4.1. Plant safety subsystem (PSS)

The Plant Safety Subsystem (PSS) guarantees the application of the principle of defense-in-depth by actuating technological safeguards designed to prevent or mitigate the consequences of “postulated accidents” versus the people (workers and public) and the environment.

The main characteristics of the PSS are:

- Two independent parallel trains (cubicles) for signal acquisition, elaboration and generation, based on safe controllers or logic solvers;
- Each Train (cubicle) has inside (at least):
  - 5 Hardwired Safety Controllers (up to 100 I/O signals in total);
  - A OPC UA Server to manage /monitor the Hardwired Safety Controllers (HSCs);
- Hardwired connections between HSCs and field;
- Double redundant communication channels with LICS;
- Two independent input signals from/to each LICS;
- Minimum of 1-out-of-2 (1oo2) safety actuation logics (similarly for alarm conditions);
- Redundant Ethernet connections on the Safety Network;

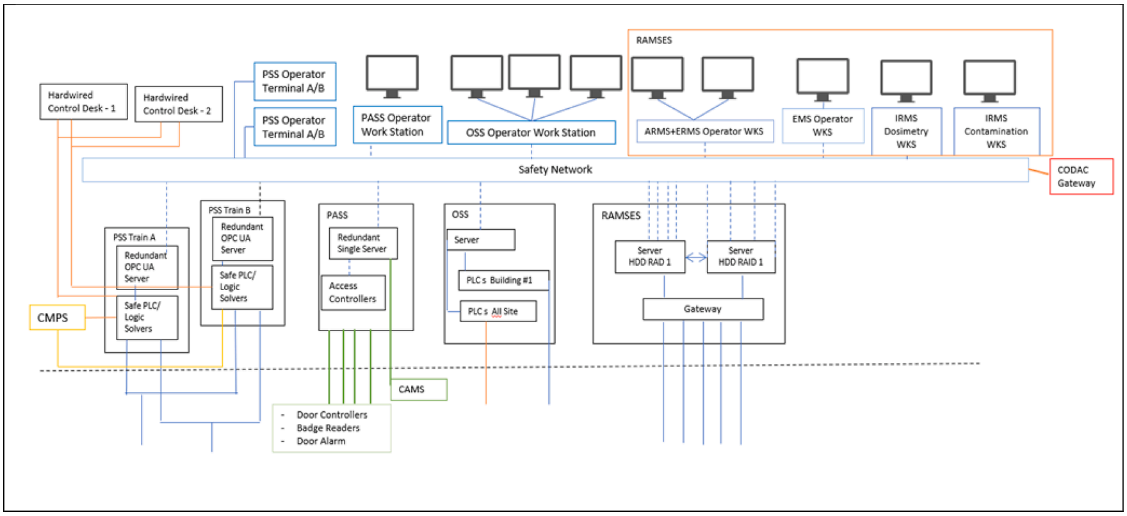

Fig. 5. Functional architecture of the Safety Control System.

- Two operator terminals (for OPC UA servers);
- Two hardwired control desks to force safety actuation on HSCs;

The other three SCS subsystems are devoted to the direct protection of people and their living environment, and are therefore considered here in a specific way.

4.2. Occupational safety subsystem (OSS)

The Occupational Safety Subsystem (OSS) provides safety functions for the protection of the people (i.e., worker and public) against all possible non-radiological hazards (toxicological, physical, electrical, cryogenic or other), which may be produced inside the plant in normal and abnormal circumstances. The foreseen safety functions can be implemented either locally or centrally by means of different protection systems (local passive systems, local hardwired systems, local programmable systems, central programmable systems).

The system is based on the personnel and zone classification with respect to the level of not radiological hazard. The subsystem is in tight connection with PASS and PSS since no active actuations or direct actions are associated to this subsystem.

OSS also keeps track of each worker operating in the plant of its total exposure to the risks and of each single contribution:

a) Radiation exposure produced by radioactive materials;
b) Chemical exposure produced by radioactive materials;
c) Chemical exposure produced by non-radioactive materials;
d) Electromagnetic exposure produced by induced magnetic fields.

The status of each worker will be communicated on a daily basis (or after each shift) to the PASS to get working permission to the single worker for a specific area or for a special activity.

The main characteristics of the OSS are:

- Safe controllers (Safe PLCs) with hot stand-by backup;
- Double redundant communication channels;
- Input from single sensors accepted;
- Single actuation logics acceptable for local alarms;
- Only bus-based connections;
- Real-time communication with PSS and PASS through a dedicated safety network, which has the function to actuate safety logics;
- A single server (not redundant) is accepted.

4.3. Personnel access safety subsystem (PASS)

The Personnel Access Safety Subsystem (PASS) has the objective to implement all the actions oriented to the safety of the people (i.e., workers and the public) in some specific areas that generate prompt risks (both radiological and non-radiological). PASS controls the access of the people to specific areas and enclosures inside the plant. Its function is more important where simple mechanical means are not sufficient or available, like in the case of a door opening, stop plant system equipment to remove the source of safety risks, or in very specific cases, ban access to an area, if there is the risk that people may not be protected from this hazard.

PASS implements the following access safety functions:

1) stopping hazardous equipment or devices in case of intrusion;
2) banning access on detection of a risk;
3) controlling access to safety airlocks by personnel;
4) interlocking safety access with the same or other safety subsystems.

A fundamental function of this system is the remote control of door opening and bypass of the interlock bars, according to the plant status and to the level of hazard (radiological and conventional) in the area to be accessed.

The PASS system is mainly based on COTS platforms with proven installation history in plants with similar characteristics. The doors/gates for the access to the critical areas shall be equipped with independent sensors (mechanical position switches) to be acquired directly by PASS. The others SCS systems (PSS, OSS, RAMSES) shall communicate the alarm status necessary to actuate PASS logics in real-time.

The independent sensors shall be interfaced to the relevant safety system by direct hardwired connections, to preserve the SIC level of the safety chain. Local I&C systems associated to PASS are:

- COTS sensor on doors
- COTS alarm and warning
- COTS interphones
- COTS CAMs
- PASS local controllers.

In the PASS cubicle, the following devices are present:

1 A single server: a server with redundant critical components (two power supplies hot swap, two HDD Raid 1 Hot Swap, two Ethernet cards on PCI Express (PCIe) bus).

2 Access controllers, managed by the server, in order to acquire data from badge readers, to command the doors lock/unlock and to activate local alarm/warning.

The remote operator workstation (in the control room) through redundant Ethernet connections on the safety network allows the monitoring of the safety actuation logics.

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

The Radiation Monitoring Subsystem for the Environment and Safety (RAMSES) contributes to the protection of people by permanent monitoring the dose rates in areas with a risk of exposure to ionizing radiation. The comparison of the measured dose levels to the alarm levels triggers the activation of alarms and interlocks, in case of excessive dose levels. The integration with PASS provides the access control in function of the radiation levels. This prevents personnel from entering the areas in which an unacceptable exposure to ionizing radiation is measured.

The RAMSES system is organized on three different levels:

- Instrumentation distributed in the plant (essentially COTS);
- Radiological synthesis units to manage/generate localized alarms and routing data versus centralized server;
- Centralized servers and the associated Human Machine Interface (HMI) in the Central Control Room.

The RAMSES system is based on COTS platforms with proven installation history in plant with similar characteristics (when available). Each monitoring device is connected to the RAMSES supervisor for the ordinary tasks (configuration, historical data acquisition, warning alert, etc.). Each monitoring device is also equipped at least with a couple of redundant digital outputs (state logic 0–1) to be connected hardwired to the RAMSES itself and/or to the other relevant safety system (e.g. PSS or PASS).

The main features composing the (local or on-the-field) RAMSES are:

- Single sensor/monitor for non-safety functions;
- Duplicated sensors/monitors for safety-related functions;
- COTS detectors /monitor whenever possible;
- Radiological Synthesis Unit (RSU) Type 1 (RSU-1) to collect prompt information (state logic 0–1 output) to transfer it both to RAMSES servers and actuate area alarm in real time;
- Radiological Synthesis Unit Type 2 (RSU-2) to collect both digital data from detectors (on bus) and RSU-1 status in order to get a common protocol in output;
- Area Alarm Units.

The main features composing the (central) RAMSES data networking are (Fig. 6):

- Two mirroring servers with redundant components (i.e. HDD);
- Gateways (and/or switches);
- Redundant bus-based connection with RSU-2 (on the field);
- Redundant connection on the safety Ethernet network;
- Operator workstations in control room with several monitors and graphical pages to cover all the functions;
- Two independent servers in the same cubicle with functional redundancy;
- Only digital connection between the central system and the field.

5. Conclusions

In this paper, the architecture of two of the main DONES CICS systems (namely, MPS and SCS) have been described in detail, focussing on the specific design choices recently proposed. The design of an I&C system must follow a transversal approach for the success of a future implementation and should adhere to the plant design evolution. As a

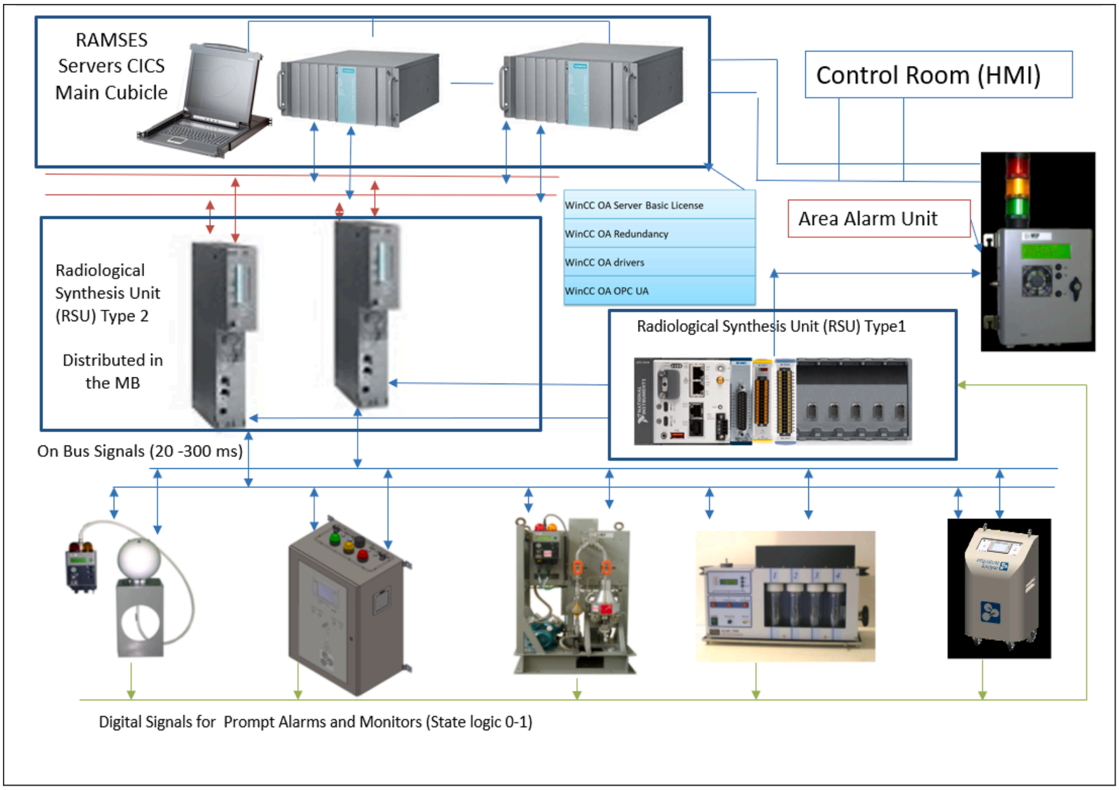

Fig. 6. The RAMSES data networking.

result, design choices need to be integrated with the parallel development of all systems and subsystems. Next activities will then focus on the completion and integration of control and operation activities, the improvement of CICS-LICS integration, and the overall (software and hardware) control system integration.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

Acknowledgements

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.

References

[1] D. Stork, et al., Towards a programme of testing and qualification for structural and plasma-facing materials in fusion neutron environments, Nucl. Fusion 57 (2017).
[2] G. Federici, et al., DEMO design activity in Europe: progress and updates, Fus. Eng. Design 136 (2018) 729–741.
[3] The IFMIF/EVEDA Integrated Project Team, "IFMIF Intermediate Engineering Design Report", 2013, available on request at ifmif@ifmif.org.
[4] A. Ibarra, et al., A stepped approach from IFMIF/EVEDA toward IFMIF, Fusion Sci. Technol. 66 (2014) 252–259.
[5] F. Romanelli, et al.. Fusion Electricity: A Roadmap to the Realisation of Fusion Energy, EFDA, 2012, ISBN 978-3-00-040720-8.
[6] T. Donné, et al., European Research Roadmap to the Realisation of Fusion Energy, EUROfusion Consortium, 2018. ISBN 978-3-00-061152-0.
[7] A. Ibarra, et al., The IFMIF-DONES project: preliminary engineering design, Nucl. Fusion 58 (2018), 105002.
[8] D. Bernardi, et al., The IFMIF-DONES Project: design Status and Main Achievements Within the EUROfusion FP8 Work Programme, Journal of Fusion Energy 41 (2) (2022) 1–26, n.
[9] W. Królas, et al., The IFMIF-DONES fusion oriented neutron source: evolution of the design, Nucl. Fusion 61 (2021), 125002, https://doi.org/10.1088/1741-4326/ac318f.
[10] M. Cappelli, et al., IFMIF-DONES Central instrumentation and control systems: general overview, Fus. Eng. Design 146 (Part B) (2019) 2682–2686.
[11] M. Cappelli, et al., Preliminary engineering design of the central instrumentation and control systems for the IFMIF-DONES plant, in: Proceedings of ICALEPCS2019, New York, NY, USA, 2019.
[12] M. Cappelli, ENS-3.6.1.1-T15-11-N1, 2017, available on request to the corresponding author.
[13] ITER Instrumentation and Control System – PRIMER (ITER_ID: 32J454 v1.1), 2010.
[14] W. Davis, et al., Current status of ITER I&C system as integration begins, Fus. Eng. Design 112 (2016) 788–795.
[15] M. Park, et al., Overview of KSTAR Integrated Control System, Nucl. Eng. Tech. 40 (6) (2008).
[16] M. Cappelli, A. Bagnasco, J. Diaz, J. Sousa, F. Ambi, A. Campedrer, D. Liuzza, B. Carvalho, A. Ibarra, Status of the engineering design of the IFMIF-DONES Central Instrumentation and Control Systems, Fus. Eng. Design 170 (2021), 112674. ISSN 0920-3796.