Enhancements of the central Safety System for Wendelstein 7-X operational phase OP2.4

J. Schacht, S. Pingel, U. Herbst, R. Vilbrandt, S. Degenkolbe, E. Scharff

***Abstract*—The Wendelstein 7-X (W7-X) Safety Instrumented System (SIS) ensures personal safety and investment protection. The development and implementation of the SIS are based on the international safety standard for the process industry sector, IEC 61511. The SIS is based on a distributed and hierarchically organized architecture consisting of a central Safety System (cSS) on the top and many local Safety Systems (lSS). Each technical component or diagnostic system potentially hazardous to staff or the device is equipped with an lSS, that is responsible for the safety of the component. Whereas the cSS ensures safety of the W7-X device as a whole and is part of the central control system of W7-X.**

For every operation phase of the W7-X experiment, hard- and software updates for the SIS are mandatory. New components with additional lSS functionality and additional safety signals have to be integrated. Already established safety functions must be adapted and new safety functions have to be implemented in the cSS. Finally, the safety programs of the central and local safety systems have to be verified for every development stage and validated against the safety requirement specification.

This paper focuses on the application of a model based simulation system for the whole SIS of W7-X. A brief introduction into the development process of the SIS and its technical realization will be given followed by a description of the design and implementation of the SIS simulation system using the framework SIMIT (Siemens). Finally, the first operational experience of this simulation system for the preparation of the SIS for the upcoming operation phase OP 1.2b of W7-X will be discussed.

***Index Terms*—IEC 61511, functional safety, safety instrumented system (SIS), simulation, PLC (Programmable Logic Controller), SIMIT**

I. Introduction

WENDELSTEIN 7-X is a fusion experiment based on the stellarator principle. Magnetic confinement is generated by a superconducting magnetic field. Since its first plasma operation in December 2015, W7-X has completed five scientific experimental phases. During this time, a wide variety of plasma scenarios were implemented by the W7-X experiment control system, such as short discharges in the range of 10–20 seconds with very high heating power (10–15 MW) as well as long plasma discharges lasting several minutes with a continuous heating power of, for example, 6 MW. The primary plasma heating methods used in these discharges are Electron Cyclotron Resonance Heating (ECRH) and Neutral Beam Injection (NBI), but Ion Cyclotron Resonance Heating (ICRH) is also employed.

The parameters for the magnetic field, plasma heating, fuel supply, and plasma density can be flexibly specified within a wide range in the experimental programs.

In addition to flexible plasma operation, the safe operation of all involved systems is a fundamental prerequisite for personal safety and plant safety.

Following an introduction to the tasks and structure of the W7-X safety control system, the modifications and enhancements to the Central Safety Control System for the new W7-X operational phase OP2.4 are presented. The key work packages for modifying the Central Safety Control System are described, and their implementation status is provided.

The paper concludes with a brief status and summary.

Overview of Functional Safety for the W7-X Fusion Experiment

Functional safety is responsible for ensuring the protection of people and the environment during the operation of a technical system. On the other hand, risks to the technical components of the system in question must be minimized to protect the system from damage or destruction.

Functional safety works in conjunction with organizational and design measures to ensure that the specified safety objectives are achieved (see Fig. 1).

In functional safety, safety functions—which have been defined as a result of a safety analysis—are implemented by electrical or electronic systems. To ensure that a safety system can perform its risk-reducing safety functions in an emergency, the processing chain—comprising sensors, processing logic, and actuators—must function reliably and be able to detect faults with certainty. The safety system must be able to detect its own faults and respond appropriately, e.g., by switching to a safe state in such cases. In cases of high risk potential or high availability, suitable measures—such as redundant and/or diverse structures—must be taken into account when implementing the safety functions (see IEC 61511 [1]).

The requirements for safe operation of W7-X are implemented through technical measures, organizational measures, and personal protective measures [2]. The functional safety systems at W7-X are divided into central and local

Manuscript received June 22, 2018; revised March 27, 2019.

J. Schacht, S. Pingel, U. Herbst, R. Vilbrandt, S. Degenkolbe, E. Scharff are with the Institute for Plasma Physics, Wendelsteinstraße 1, Greifswald, Germany, D-17491, telephone: +049(0)3834-882761, (e-mail: joerg.schacht@ipp.mpg.de).

safety-related systems, as shown in Fig. 1. The local safety-related systems implement the safety functions for a specific system, such as a technical system (e.g., gas inlet, plasma vessel valve control, plasma heaters) or for diagnostics (e.g., laser diagnostics). The systems responsible for the functional safety of the entire W7-X facility are referred to as central safety systems.

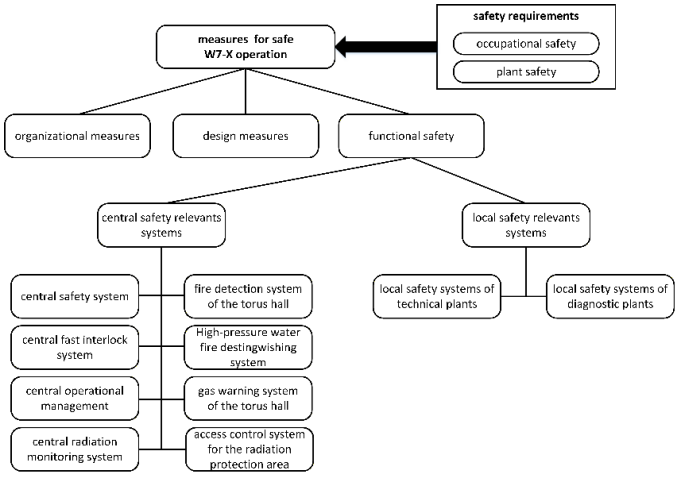

Fig. 1. The Functional Safety Architecture of the W7-X.

Fig. 1 shows the breakdown of the functional safety of the entire W7-X facility into central and local safety-related systems.

The central control system, with its safety-related subsystems—the Central Safety Control (cSS), the Central Interlock System (cFIS), and the Central Operations Management (cOPM)—is responsible for the safe operation of W7-X, including all technical systems and diagnostics. In addition to the central control system, there are other central safety-related systems that independently perform specific safety-related tasks, such as fire detection, fire suppression, or gas detection. These systems are connected to the central safety control system and the central operations management system via interfaces.

The main tasks of the local and central safety-related systems are summarized in Table 1.

The following functions of the central safety control (cSS) are fundamental to the safe operation of W7-X:

- Safety level logic,
- Safety functions,
- Special operating modes,
- Emergency stop safety logic, and
- Access logic to the radiation protection area.

The safety levels (Safety Level SL) are used to grant access to the radiation protection area in accordance with the degree of hazard. For the defined safety levels (see Fig. 7), the states of the enable signals for hazardous activities are assigned to the local systems. Furthermore, for each safety level, it is specified how access to the entire radiation protection area or parts thereof is regulated.

The safety functions are based on the safety chain: sensor, processing logic, and actuator. Safety-relevant states are detected via the sensors and then processed in the logic unit. The measures determined by the logic are then implemented via the actuators.

TABLE I
MAIN TASKS OF THE LOCAL AND CENTRAL SAFETY-RELATED SYSTEMS

Safety System	Safety-related tasks	Safety Integrity Level
Local safety control	Implementation of measures for personal and plant safety within the plant area that are defined and implemented as safety functions. The safety measures are triggered either by the system's own sensors or by signals from the cSS.	SIL 0 to SIL 2
Central safety control	Implementation of measures for personnel and plant safety for the entire W7-X facility in the radiation protection area, which are defined and implemented as safety functions. The cSS processes the safety signals from local systems in its safety logic and controls the safety behavior of the systems via the output of safety signals. In addition to the interfaces to the local systems, the cSS also has interfaces to other safety-related systems and processes their signals within the cSS safety logic.	SIL 0 to SIL 2
Local Fast Interlock System	Detection of plasma vessel overloads during plasma operation: Interlock diagnostics, Rapid shutdown of plasma heater power and stopping of gas inlet upon triggering of fast interlocks: Interlock functions.	SIL 0
Central Fast Interlock System	The Central Fast Interlock System processes the status information from the Fast Interlock Diagnostics in the Fast Interlock logic. Upon detection of plasma vessel overload conditions, the plasma heaters and gas inlet are quickly shut down.	SIL 0

Special operating modes are required when plant activities are necessary that cannot be implemented based on the normal safety functions. Here, authorizations for activities are enabled to, for example, allow commissioning and plant tests with specially trained personnel in the torus hall. In this context, technical protective measures are replaced by organizational measures.

The emergency stop safety logic is a critical safety function of the cSS that governs the behavior when the W7-X emergency stop condition is activated. The W7-X emergency stop safety function is triggered via a total of 38 emergency stop buttons distributed throughout the radiation protection area. In doing so, the emergency stop signal is activated at all safety interfaces of the local systems, causing the systems to activate their own emergency stop or emergency shutdown state. Furthermore, the evacuation signal is triggered in the radiation protection area. The emergency stop safety logic also handles the procedures for acknowledging and exiting the emergency stop state.

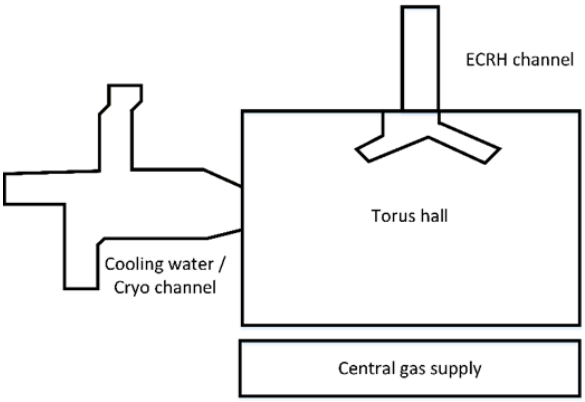

Fig. 2. Schematic of the sub-areas of the W7-X radiation protection area.

The access logic controls access to the radiation protection area for various operating situations. The radiation protection area at W7-X comprises a total of 4 separate sub-areas with their own access points that can be locked. Depending on the safety levels or on certain operating situations, sub-areas or the entire radiation protection area must be locked down and verified to be free of personnel.

The technical systems and diagnostics, hereinafter referred to as local systems, have local operational management and, depending on the specifications of the safety measures for plant operation, also local safety control and/or a local fast interlock system.

Various interface types are used for the exchange of information between the central safety systems and their counterparts on the local systems side, as shown in Fig. 3.

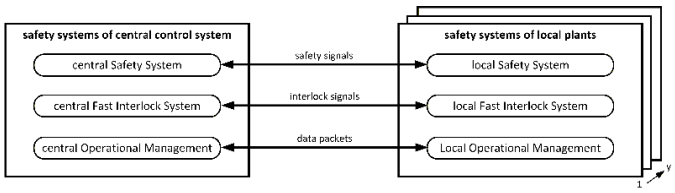

Fig. 3. The Functional Safety Architecture of the W7-X.

The connection between the central safety controller and the local safety controllers is established via safety signals. The cSS provides the necessary number of safe digital inputs and outputs via safe I/O modules of a decentralized peripheral unit (ET200). The standard safety interface transmits enable signals for hazardous activities and the W7-X emergency stop signal to the respective local system. The local system reports the status "safe state active/inactive" and the status "emergency stop of the system active/inactive" back to the cSS. Additional special safety signals (e.g., command to shut off media, release to open plasma vessel valves) expand the signal range of the cSS interfaces as needed.

The plasma interlock system also works with digital hardware signals to exchange request and release signals for heating in the plasma vessel and to exchange interlock diagnostic signals.

To handle the process safety functions, the central operating management system cOPM processes extensive data from the local systems. Data exchange takes place via a fieldbus of the Profinet or Profibus type or via standard Ethernet.

A. The hardware structure of the Central Safety Control (cSS)

The hardware structure of the central safety control system is shown in Fig. 4. The cSS is divided into the section for the automation system and the section for the human-machine interface (HMI) for operator control and monitoring.

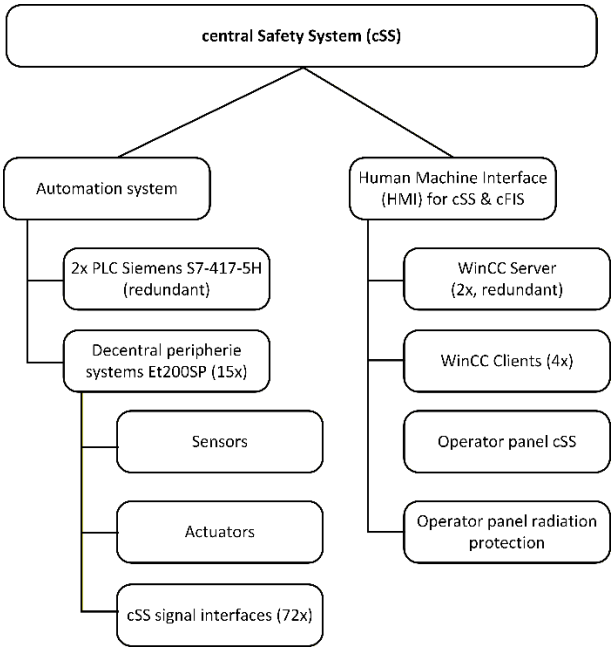

Fig. 4. Hardware structure of the cSS

The cSS automation system uses two redundant Siemens S7-417-5H PLCs to ensure high reliability and availability with high performance.

Fifteen decentralized ET200SP peripheral modules (from OP2.4) are connected to the PLCs via Profinet. The ET200 modules are equipped with I/O modules for processing safe or standard I/O signals.

The cSS hardware is housed in a total of 18 control cabinets for control and network technology and signal processing. The operator can control and monitor the cSS via the cSS itself, as well as via the radiation protection console and the operator and monitoring stations, using Siemens WinCC software.

Furthermore, the cSS features a range of sensors (e.g., emergency stop switches, experiment abort switches, door sensors) and actuators (e.g., sirens, signal lights, display panels). The PLC CPUs and network technology are housed in three control cabinets. The exchange of safety signals, including the fast-interlock signals from the safety interfaces to the local systems, is implemented in the 14 interface control cabinets of the cSS.

B. The hardware architecture of the Fast Interlock System (cFIS):

The design and functionality of the Fast Interlock System are described in [3], [4], and [5].
An overview of the hardware structure of the central interlock system is shown in Fig. 5.

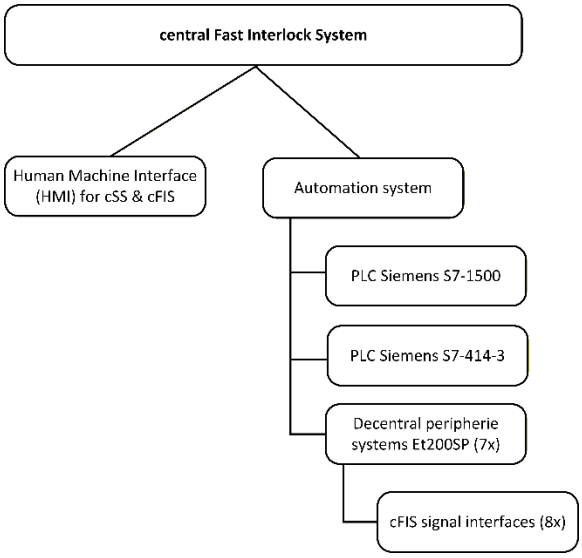

Fig. 5. Hardware structure of the central Fast Interlock System.

A high-speed Siemens S7-1500 PLC was selected to implement the interlock logic in order to achieve a response time of max. 100 ms. The response time encompasses the time from data acquisition in the interlock diagnostics to the reception of the Boolean interlock signal calculated in the cFIS at the inputs of the interlock actuators.

Decentralized ET200 peripheral units are used to acquire the signals from the interlock diagnostics and to output the interlock signals. The hardware of the cFIS signal interfaces is integrated into the cSS interface control cabinets.

II. CHANGES TO THE CSS AND CFIS FOR THE OPERATIONAL PHASE 2.4

The most important changes for operational phase OP2.4 to the central Safety Control System and the central Fast Interlock System are described below.

Changes to the cSS

A significant change concerns the operational sequence of the cSS in the context of W7-X operation. The operation of W7-X is divided into phases for the conversion and maintenance of the W7-X facility (MPx.y) and into phases for operation (OP x.y). The operational phase of W7-X is divided into three sub-phases: Commissioning Phase, Experimental Phase, and Decommissioning Phase. Fig. 6 illustrates the sequence of phases using the example of phases MP 2.4 – MP2.5 and OP2.4 through OP2.5.

Up to and including MP2.4, the cSS was shut down throughout the entire assembly phase of W7-X. Due to the shutdown of the cSS, no effective safety functions or special operating functions of the cSS were available during assembly.

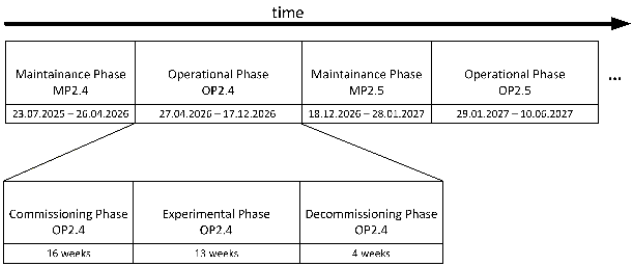

Fig. 6. Phases in the W7-X operational sequence.

The reasons for introducing the “Assembly” safety level are multifaceted. For certain events during the assembly phase, hazard reductions based on organizational measures are not possible or are only possible with significant effort.

The radiation protection system is connected to the cSS; for example, the radiation protection console is directly linked to the cSS, and the cSS exchanges safety signals and data with the radiation protection system. For displays and signaling in the radiation protection area, both systems use the same actuators (sirens, horns), which are, however, controlled by the cSS.

For future deuterium operation, regulatory requirements stipulate that radiation protection functions (with the exception of registered exemptions) must always be active.

Furthermore, experience from a transformer fire in the Torus Hall has shown that the use of hardware bridges to statically set enable signals is counterproductive in the event of a hazard. The cSS was not active during the fire scenario, and the enables issued via bridges could therefore not be revoked in the event of a fire. Consequently, the safe state of the affected W7-X systems could not be automatically restored. One conclusion drawn from this incident was the determination that the central safety control system should also be active during installation phases.

This requirement will be implemented with the upgrade of the cSS to OP2.4. During the assembly phases starting with MP2.5, the cSS may only be shut down for a maximum of 4 weeks to allow for internal modifications, expansions, and maintenance work on the cSS. Shutting down the cSS also requires approval from the Radiation Protection Office. For the remainder of the assembly phase, the cSS remains fully operational.

To ensure that plant and personnel safety requirements are met during the assembly phase, the cSS assembly safety level (SL) has been newly introduced.

There are two types of installation phases in W7-X operations: long installation phases lasting approximately 5–6 months and short installation phases lasting only 6–8 weeks.

Any necessary conversion or modification of the cSS will only be carried out during the longer installation phases at W7-X. The maximum duration of the cSS conversion phase must not exceed 4 weeks, as specified. During this time, the cSS must be completely shut down. Therefore, no hazardous activities

may be carried out at W7-X during this period unless equivalent organizational safety measures have been implemented. However, the gas detection system in the TH and the fire alarm and fire suppression systems remain active during this phase of the cSS conversion.

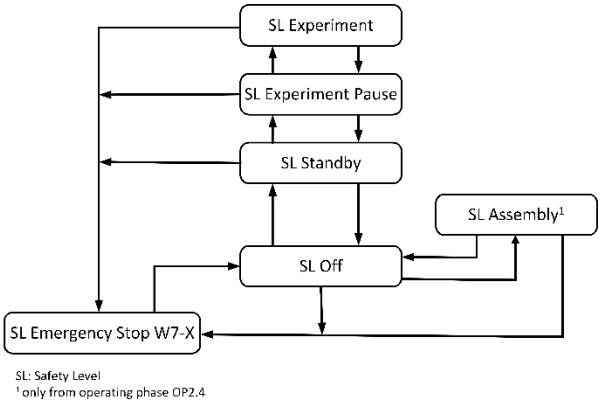

Fig. 7. Finite State Machine of the cSS safety levels.

The transition to the "Assembly" safety level occurs only from SL OFF. When SL ASSEMBLY is activated, all enable signals for the connected systems are reset, and no emergency stop signal to the systems is active. A specified set of safety functions is bypassed and therefore inactive. All safety functions not bypassed in SL Assembly remain active.

Enable signals for hazardous activities are provided exclusively by special operating modes, which are activated by the operator on the instructions of the technical supervisor on duty. In the cSS program, it was specified which of the existing special operating modes receive an enable for the SL Montage. Additionally, 10 new special operating modes were defined for the SL Montage. To activate certain special operating modes, a bypass of safety functions may still be necessary.

In the SL Assembly area, the safety functions for W7-X Emergency Stop, Fire Alarm, and Gas Alarm are always active, and no bypass is possible here.

During assembly, the large radiation shielding door in the Torus Hall will be open. Therefore, for certain special operations (e.g., when testing lasers), the doors of the adjacent pre-assembly hall must also be monitored to ensure that the Torus Hall area remains closed and that the absence of personnel in this area can be monitored.

It should be noted that, in the case of special operations, part of the risk mitigation responsibility is transferred from the technical level to the organizational level.

A. Extensions and modifications to special operating functions

Additional special operating functions were defined for the Assembly Safety Level, and existing special operating functions were modified.
The new special operating functions were defined to temporarily permit certain system activities during the assembly phase, specifically within the Assembly Safety Level, by setting approvals. These activities include, for example, testing system functions under assembly conditions (e.g., laser alignment).
For existing special operating modes, the activation conditions were expanded so that these special operating functions can also be activated in the Assembly Safety Level.

Table 2 summarizes the modified and new special operating modes by special operating mode type for OP2.4.

TABLE II
OVERVIEW OF MODIFIED OR NEW SPECIAL OPERATING FUNCTIONS (SOF) FOR OP2.4

Type of SOF Type	Description	Number of SOF	Changes to OP2.4
SOF0	Non-exclusive special operations (may be authorized alongside other special operations) "General" personnel permitted in TH	22	19 SOF0 are permitted for SL Assembly
SOFM	Special operations exclusively for SL Assembly	11	11 SOFM have been defined for SL Assembly
SOF1	Only “special” personnel permitted in TH Exclusive special operations.	10	8 SOF1 were modified. 5 SOF1 can be run in SL Assembly.
SOF2	Non-exclusive special facilities (may be licensed alongside other special facilities) No personnel permitted in the radiation protection area.	3	2 SOF2 were new defined.
SOF3	No personnel permitted in TH Exclusive.	1	1 SOF3 can be run in SL
SOF4	No personnel permitted in the radiation protection area SSB, excluding special operations.	1	1 SOF4 has been modified.

B. Modified safety functions for OP2.4

No new safety functions will be introduced in the cSS for OP2.4. Changes will take effect for 9 existing safety functions due to the inclusion of the Assembly safety level. These changes may involve either the possibility of bypassing the respective SIF at the Assembly safety level or the safety function being actively executed at the Assembly safety level as well. Further changes to the safety functions result from the inclusion of safety signals from newly integrated systems (e.g., Impurity Powder Dropper, Heavy Ion Beam Probe diagnostics).

C. Modifications to the cSS interface hardware

The most complex work package for preparing the cSS for the OP2.4 operational phase is the retrofit of the cSS interface hardware. The previously used Siemens ET200M decentralized peripheral modules for processing safety signals

and standard signals are to be completely replaced with ET200SP modules. The motivation for this replacement is that the manufacturer Siemens has discontinued the ET200M modules, meaning that long-term spare parts procurement could no longer be guaranteed.

The ET200M modules used to date have already been in service for a long time, so a higher failure rate for these components is to be expected in the future. This would mean that the required high availability of the cSS could no longer be guaranteed, and replacing these ET200M modules with modules of the same type would have become very costly according to the manufacturer's specifications.

A key decision-making criterion for the conversion was that sufficient time was still available in the current MP2.4 assembly phase, which is no longer the case for future assembly phases with a maximum cSS shutdown duration of 4 weeks.

The ET200SP module intended as a replacement for the ET200M features a wide range of non-safety and safety I/O modules. The design of these ET200SP I/O modules is significantly more space-efficient than that of the ET200M modules, and the distribution of I/O channels per module also differs from that of the ET200M. Consequently, a simple switch from the ET200M to the ET200SP decentralized peripheral module was not possible; instead, a new electrical design had to be created for each control cabinet of the central safety controller as well as for the Fast Interlock system. In total, the electrical engineering for 17 control cabinets had to be redesigned, and the retrofit subsequently implemented.

Fig. 8 shows the configuration of a decentralized ET200SP peripheral unit, including the specified I/O modules.

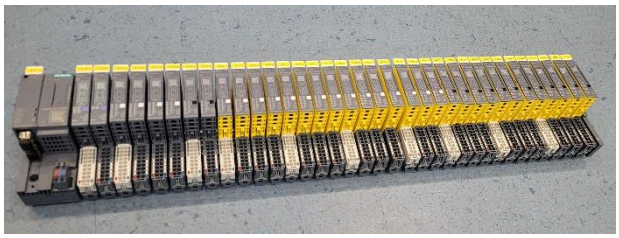

Fig. 8. ET200SP decentralized peripheral module with various I/O modules.

In addition to replacing the decentralized peripheral modules, extensive signal wiring had to be carried out in the control cabinets, which involved the following signal scope:

- Fail-safe digital input signals FDI: 1056
- Fail-safe digital output DO: 614,
- Standard digital input signals DI: 1024,
- Standard digital output signals DI: 384,
- Standard analog input signals (AI): 120.

The use of ET200SP modules also necessitated a transition from the previously used Profibus fieldbus to Profinet. The installation of a total of 26 new Siemens Scalance Profinet switches had to be planned and implemented. The new network topology was selected to achieve S2 redundancy. The ET200SP I/O devices with S2 system redundancy enable uninterrupted process data exchange with the redundant S7-417-5H system even if one of the two CPUs fails.

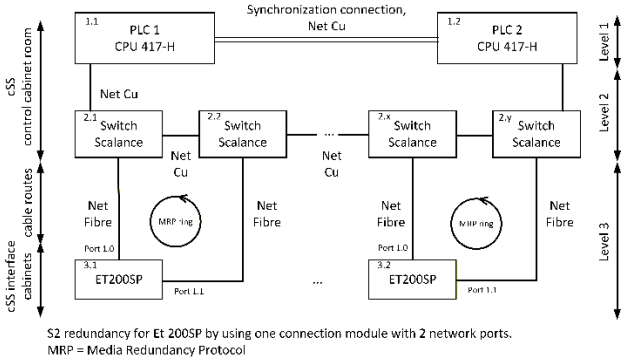

Fig. 9. ET200SP decentralized peripheral module with various I/O modules.

D. Replacement of safety relays

The hardware upgrade also included the replacement of safety relays. The cSS central safety controller currently uses 258 Pilz Type 7.1 safety relays; of these, more than 100 safety relays were replaced during the MP2.4 phase. The replaced safety relays had either been identified as defective during a functional test or had been in use prior to 2014.

The preventive replacement of the safety relays is a measure to maintain high availability and reliability of the central safety control system. The increase in detected hardware faults in these Pilz safety relays was attributed to contact problems in the switching contacts resulting from the functionally very low number of switching cycles / switching requirements in combination with only low operating currents.

cSS control panel retrofit:

Another modification involved the cSS control panel. A pushbutton and an indicator light were added to the panel to activate the Safety Level Montage.

Modification of safety interfaces:

A total of 3 new cSS safety interfaces with 33 new safety signals were set up:

- Heavy Ion Beam Probe Diagnostics Interface: This interface comprises a total of 8 safety signals and remains deactivated in OP2.4 because the system will not go into operation until OP2.5.
- Impurity Powder Dropper Interface: This interface comprises a total of 5 safety signals,
- Access Control System Interface for the Radiation Protection Area: 20 signals
- Multi-channel Interferometry Interface: 4 safety signals, reactivated

Three existing safety interfaces were modified:

- X-ray pulse height analysis: 2 safety signals added (Emergency Stop + Emergency Stop status feedback),
- Mateo Divertor Manipulator: 5 safety signals; interface remains in OP2.4 but is deactivated,
- ECRH: 3 additional signals (High Voltage (HV) Enable, HV Safe Feedback, W7-X ECRH Operation without cFIS during adjustment).
- cSS console: Pushbutton and indicator light for SL assembly,
- Door monitoring for pre-assembly hall: additional monitoring of 3 doors in the pre-assembly hall.

E. Sensors for access monitoring of the pre-assembly hall

During the assembly phase, the large radiation shielding door to the Torus Hall is open. For this reason, access to the upstream pre-assembly hall must be monitored during certain special operational functions (e.g., laser calibrations of diagnostic equipment). The three entrances to the pre-assembly hall have been equipped with door sensors, and the signals have been connected to the cSS. The new status information is processed in the extended access logic.

F. PCS7 V10 software update

The phase for the cSS hardware upgrade was used to transition to the latest version of the software for the Process Control System PCS7-V10 (programming of the PLCs and the Human Machine Interface (HMI)). The use of PCS7 V10 was necessitated by the switch to the Windows 11 operating system for the engineering stations and the HMI servers and client computers.

For the migration of the cSS project to PCS7 V10, a new central engineering station, 3 additional engineering stations, 2 operator stations (OSs), and 3 operator station clients (OS clients) were first set up. Subsequently, the migration of the cSS software project from PCS7 V9 to PCS7 V10 was carried out without major issues.

G. cSS simulation system SIMIT

An extension and modification of the cSS simulation system (SIMIT) was necessary to ensure that the simulation environment processes the same scope of safety signals and uses the same PLC program version as the cSS production system for OP2.4.

Using the SIMIT simulation system, all software integration tests were successfully conducted between November and December 2025.

H. Extensions and modifications to the cSS software

The adaptation and expansion of the cSS software resulted from changes to the cSS hardware as well as from the implementation of requirements for the new safety level "Assembly" and the associated special operations.

- New I/O drivers for the new or modified safety interfaces,
- Expansion of the safety logic for the safety levels to include the new "Assembly" safety level.
- Modification of some existing safety functions
- Expansion of the logic for access monitoring to the radiation protection area through the integration of 3 door sensors in the pre-assembly hall,
- Extension of the scope of some safety functions and special operations to include the “Assembly” safety level.
- Eleven new special operating modes of the type “Assembly Special Operation” (SBM) were introduced for the assembly safety level. These new SBMs include, for example, the test operation of the Steady State Pellet Injector and the enablement of high voltage for heaters.

For Special Operation Type 1 (only “special” personnel permitted in the technical hall, excluding special operations), a new special operation SB1-5.1 – Heavy Ion Beam Probe – Analyzer Operation was defined. Furthermore, modifications were made to 33 existing special operations. These special operations are intended to enable specific activities for selected facilities following organizational approval.

I. Changes to the central Fast Interlock System (cFIS)

The planned changes for the cFIS can be summarized as follows:

- Integration of the Powder Dropper into the cFIS with a shutdown function. The release of powder into the plasma vessel is terminated by the Powder Dropper’s cFIS within 100 ms. Reason: To prevent unwanted release of powder from the Impurity Powder Dropper into the PG when no plasma is present, as the powder would interfere with subsequent discharges.
- Expansion of the range of predefined cFIS parameter sets beyond what was previously available. These parameter sets are used to set the threshold values for interlock diagnostics, enabling easy adaptation of cFIS behavior to different plasma scenarios.

III. Status of the modification and expansion of the cSS and cFIS for OP2.4

The schedule for the modification of the central safety control system and the central Fast Interlock System was planned so that all major work packages could be implemented during the MP2.4 assembly phase. Delays in implementation could have resulted in a postponement of the commissioning of W7-X.

Table 3 lists key work packages of the cSS modification project along with their current implementation status. During the MP2.4 assembly phase, all planned modifications to the cSS hardware and cSS software were completed in time before the start of the planned cSS validation. The planned changes to the cFIS hardware have also been implemented. The cFIS software is currently being expanded, and the planned cFIS validation will take place during the plasma test operation of W7-X in September 2026.

TABLE III
WORK PACKAGES FOR MODIFICATION OF CSS

Working package	Content	Status
Modification of the cSS hardware	Design of control cabinets, Procurement of materials, Assembly of mounting plates with decentralized Et200SP peripherals, Assembly of cable harnesses, Conversion of cSS control cabinets, Conversion of cSS console,	Completed
Tests, inspections, and commissioning of the hardware	ET inspection following completion of cSS control cabinet retrofit, Signal tests after completion of the cSS conversion, Update of cSS module parameters, cSS interface tests with the systems, Maintenance of the cSS / cFIS control cabinets,	Completed
Modification of cSS software	cSS software design and programming for OP2.4, Updating the SIMIT software test system for the cSS,	Completed
Conducting tests of the cSS software	Conducting software module tests, performing integration testing of the cSS software for Op2.4 on the cSS SIMIT test system,	Completed
Testing of cSS hardware and software	Validation of the cSS for operation in OP2.4,	Completed

IV. SUMMARY

For the OP2.4 operating phase, a comprehensive modification of the central Safety Control (cSS) and the central Fast Interlock System (cFIS) was carried out. The discontinued ET200M decentralized peripheral modules (Siemens) had to be replaced with ET200SP devices. This resulted in a very high level of effort for the planning and retrofitting of the cSS/cFIS control cabinets. Furthermore, new systems were connected to the cSS and the cFIS.

To ensure safe operation even during the assembly phase at W7-X, the safety level “Assembly” was added to the finite state machine of safety levels. This ensures that the cSS’s safety functions remain active and effective during the upcoming assembly phases. System operations within the radiation protection area can be selectively enabled or disabled using the new special operating functions (SOFs) of the safety level “Assembly”.

Safety functions (SIFs) and the logic for granting clearances for hazardous system operations have been expanded.

Access monitoring in the radiation protection area had to be expanded for assembly phase to include three entrances to the pre-assembly hall, as the large radiation protection door of the torus hall is open during the assembly phase and the absence of personnel during, for example, laser tests in the torus hall must be ensured via the upstream entrances to the pre-assembly hall.

The extensive modification and programming work on the cSS for OP2.4 was completed on time and to a high standard. The validation of the cSS is the final work package to be completed before the cSS begins mid of June 2026 operation for the W7-X’s operational phase OP2.4.

The modification work on the cFIS control cabinets has been completed. Software work is currently underway to integrate the Impurity Powder Dropper system into the interlock system. Commissioning of the cFIS, including validation of the interlock functions, is planned as part of the W7-X plasma commissioning for OP2.4 in July 2026.

ACKNOWLEDGEMENT

This work has been carried out within the framework of the EUROfusion Consortium, funded by the European Union via the Euratom Research and Training Program (Grant Agreement No. 101052200 — EUROfusion). The 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] Functional Safety-Safety Instrumented Systems for the Process Industry Sector—Part 2, Standard IEC 61511- 1:2016, 2016, p. 2016.

[2] J. Schacht, D. Naujoks, S. Pingel, A. Wölk, U. Herbst, S. Degenkolbe, A. Winter, R. Vilbrandt, H.-S. Bosch, „Realization of the requirements for a safe operation of Wendelstein 7-X”, Fusion Engineering and Design, Volume 152, March 2020, 111468.

[3] J. Schacht, “Enhancements of the fast interlock system for Wendelstein 7-X operational phase OP2.1,” IEEE Trans. Nucl. Sci., vol. 70, no. 6, pp. 1124–1130, 2023.

[4] S. Degenkolbe et al., "The Requirements for the Fast Interlock System of Wendelstein 7-X," in IEEE Transactions on Plasma Science, vol. 52, no. 9, pp. 3622-3627, Sept. 2024, doi: 10.1109/TPS.2024.3391509.

[5] R. Vilbrandt, J. Schacht, U. Herbst et al., The fast Interlock system of W7-X – First experience, Fusion Engineering and Design, Volume 151, 2020, 111380, ISSN 0920-3796.

[6] J. Schacht, R. Vilbrandt, S. Degenkolbe, O. Grulke, A. Winter, U. Herbst, A. Wölk, S. Pingel, and H.-S. Bosch, “Enhancements of the Fast Interlock System for Wendelstein 7-X Operational Phase OP 2.1,” IEEE Transactions on Nuclear Science, Volume: 70, Issue: 6, June 2023.

[7] J. Schacht, A. Wölk, S. Pingel, U. Herbst, D. Naujoks and the W7-X Team, „ Simulation System for the Wendelstein 7-X Safety Control System, IEEE Transactions on Nuclear Science, Volume: 66, Issue: 7, July 2019.

[8] SIMIT V7-open simulation platform for virtual commissioning, Siemens, Available: https://www.industry.siemens.com/datapool/industry/industrysolutions/services/en/SIMIT-V7-en.pdf.