Realization of the requirements for a safe operation of Wendelstein 7-X

J. Schacht, D. Naujoks, S. Pingel, A. Wölk, U. Herbst, S. Degenkolbe, A. Winter, R. Vilbrandt, H.-S. Bosch and the W7-X Team

***Abstract*—The Wendelstein 7-X superconducting stellarator is a fusion experiment designed for processing of plasma discharges in the range of some seconds up to 30 min in a quasi-steady state operation mode. The first plasma experiment was conducted in December 2015. Since this first plasma experiment, more than 100 experimental days with about 3500 plasma experiments were successfully performed within three operational phases. The operation of W7-X requires the handling of many different sources of hazards with different hazardous potentials for persons and for the device. To identify critical hazards, risk analyses and risk assessments are carried out at an early stage in the development process for all W7-X technical components and diagnostics, so that measures for risk mitigation can be taken into account already in the design. The main objective of this process is to ensure safe operation for the personnel and to protect the investment in the W7-X device.**

In this work, we present the safety model for W7-X operation. After a brief introduction to the architecture of the W7-X control system, the process of regarding the safety requirements will be discussed. In addition, the multi-shell safety model for the technical implementation of risk mitigation functions at the various levels of the W7-X control system is described. The experiences at W7-X during the previous operating phases obtained with the implemented safety concept will be described.

Finally, a preview of the enhancements and modifications of the safety systems for the next operation phase OP2, which will start in 2021, is given.

***Index Terms*—IEC 61511, functional safety, safety instrumented system (SIS)**

I. Introduction

THE superconducting fusion experiment Wendelstein 7-X (W7-X) is a stellarator with a capability for steady state plasma operation. Since commissioning of W7-X in December 2015, three operating phases have been carried out [1]. A total number of 4067 plasma discharges were conducted during 117 experiment operation days. The high availability and performance of the W7-X systems were the basis for the outstanding experimental physics results obtained [2]. Another important aspect is the safe operation of the experiment in all operation phases. The operation team of W7-X is legally obliged to ensure safe operation through adequate safety management. Fig. 1 shows the different impact factors for the operation of the W7-X device. However, these impact factors have also to be considered regarding safe operation with respect to occupational and device safety.

By various measures, such as through a safe design, using a Safety Instrumented Systems (SIS) and through organizational regulations, potential risks should be kept below an acceptable limit. These safety measures reduce the likelihood of accidents that could result in personal injury or death, destruction of the equipment, and environmental damage.

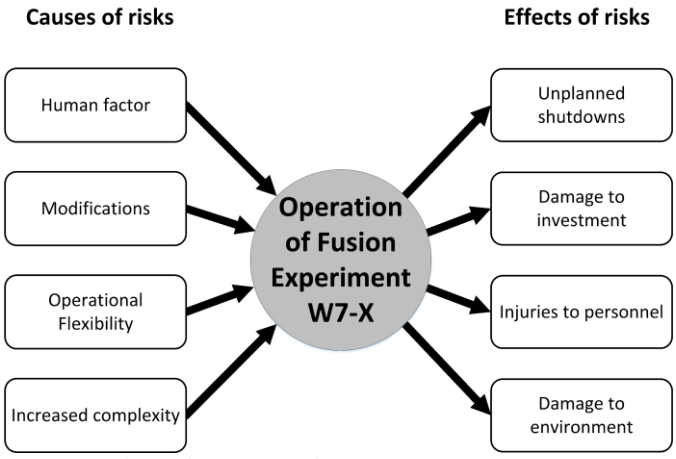

Fig.1. Impact factors for operation of the W7-X experiment.

This contribution is focused on risk reduction measures through the implementation of SIS functions, but this should not weaken the importance of the other two risk mitigation measures.
After a short description of the W7-X control system, the design and implementation of SIS functions for the multi-layer safety model of W7-X will be described.

II. Overview of the W7-X control system

The W7-X control system is designed to enable operation in all phases of W7-X operation. The operating phases include the commissioning of the device (pumping of plasma vessel

Manuscript received May 26, 2019.

J. Schacht, D. Naujoks, S. Pingel, A. Wölk, U. Herbst, S. Degenkolbe, R. Vilbrandt, A. Winter, H.-S. Bosch 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).

/cryostat, cool down of the magnet system), the preparation for the plasma operation (e.g. boronization, glow discharges, magnet field tests), the plasma operation and the standby mode (short standby mode, long standby mode).

The block diagram in Fig. 2 gives an overview about the main control components of W7-X.

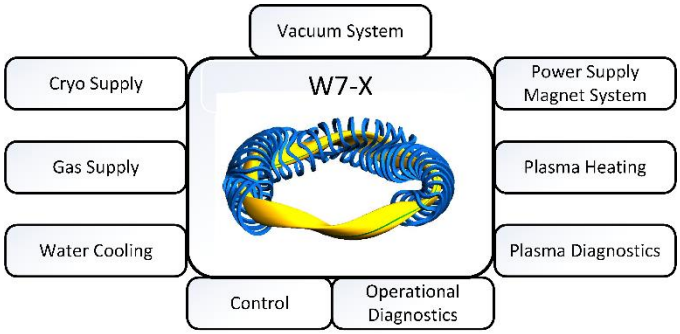

Fig. 2. Block diagram of main W7-X control components.

A general overview about the structure of W7-X control system is given in Fig. 3. The structure of the control system has a strict hierarchy. All central control systems are situated on the top of this control structure. This central group includes the central Operational Management (cOPM), the central Safety System, the central Fast Interlock System (cFIS), and the central Segment Control System (cSegCtrl).

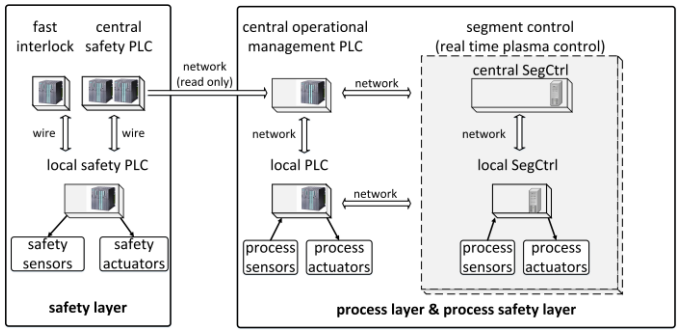

Fig. 3. Overview of the W7-X control system.

The technical systems (e.g. vacuum systems, plasma heating systems, gas supply and gas inlet systems, power supplies for the magnet systems) and diagnostic systems (operational diagnostics, plasma diagnostics) form the lower layer of the control structure. Normally, all sensors and actuators are part of the technical and diagnostic components. These components can be operated in a standalone mode or in a subordinated control mode. For processing of plasma experiments all mandatory control component have to be set in a subordinated mode. In this way, the cSegCtrl can start, monitor and stop experiment programs.

The main tasks of the central control systems are summarized in Table 1.

TABLE I
TASKS OF THE CENTRAL CONTROL SYSTEMS

Control system	Task	Description
cOPM	Operational states of device W7-X	Control and supervision of operational states according the state machine definition for operational states of W7-X,
	Components and W7-X device status	Collecting and processing of component and W7-X device data for visualization of their actual status,
	Data dispatcher	Distribution of important component data to one or more data receivers,
	Data archiving	Long term data saving of process data, operator inputs and messages (archives: W7-X data archive, cOPM process historian server),
	Operational functions of W7-X	Processing and supervision of operational function like glow discharge, baking, boronization, with cOPM as a master and more than one control components as slaves.
	Process safety functions	Collecting and visualization of infrastructure values like status of smoke detectors and temperatures inside electrical cabinets and in torus hall and status of all gas sensors of the gas warning system of W7-X.
	Infrastructure supervision	
cSS	Safety Functions	Processing of SIFs (personnel safety functions and device safety functions),
	Safety logic	Processing of safety logic for Emergency Stop system
		Control and supervision of access to the radiation protection area,
		Control and supervision of enable signals for hazardous activities of components according to the safety levels state machine,
cFIS	Interlock functions	Processing of I_SIFs (fast interlock functions for device safety during plasma experiments),
cSegCtrl	Experiment control	Processing and supervision of experiment program runs based on segment programs.

III. FUNCTIONAL SAFETY FOR W7-X

In this section a brief overview about the meaning of functional safety is given. Following, the functional safety lifecycle for W7-X is described. Finally, the implementation of the most important safety concepts for SIS of W7-X is presented.

A. *Functional safety*

The IEC61511 Functional Safety Standard [3] regards functional safety as part of the overall safety of a machine. It includes the safety required by the correct function of risk reducing system, e.g. safety-related electrical, electronic and programmable electronic systems. These systems, named as Safety Instrumented Systems (SIS), perform safety functions. In case of failures, they have to act with a pre-defined reliability. The reliability of a safety functions depends on the probability of occurrence of a hazard and the amount of its possible damage.

The objective of functional safety is twofold: minimizing hazards during operation of a machine (safe operation of a machine) and to set the safe state when certain hazards are identified.

The IEC 61511 defines all necessary activities of the engineering process for setting up the required functional safety.

B. Safety life cycle

The safety life cycle according the EN61511is implemented at W7-X.

In Fig. 4. a SysML activity diagram [4] shows the main action during the three phases of safety live cycle: analyze phase, implementation phase, and operation phase.

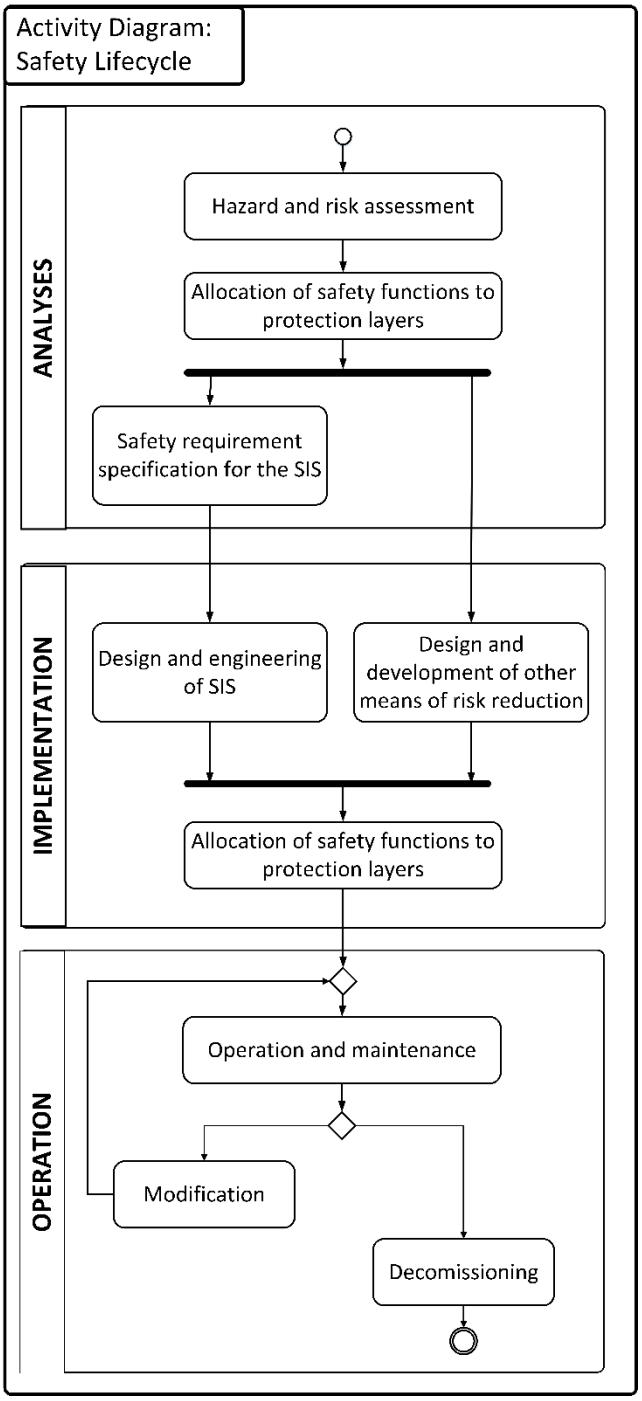

Fig. 4. SysML activity diagram for safety life cycle of W7-X.

The safety lifecycle applies to projects for the development of the technical and diagnostic systems as well as to the project for development and modification of W7-X as a complex technical system. Safety concepts have been developed based on the results of the individual safety analyses of the different technical components and the consideration of possible failure scenarios of the W7-X device. Required safety measures have been determined for implementation in order to meet the necessary level of risk mitigation. Fig. 5 shows the different types of such measures for risk mitigation ordered by their priority: 1. safe design, 2. instrumented control and monitoring and 3. organizational measures.

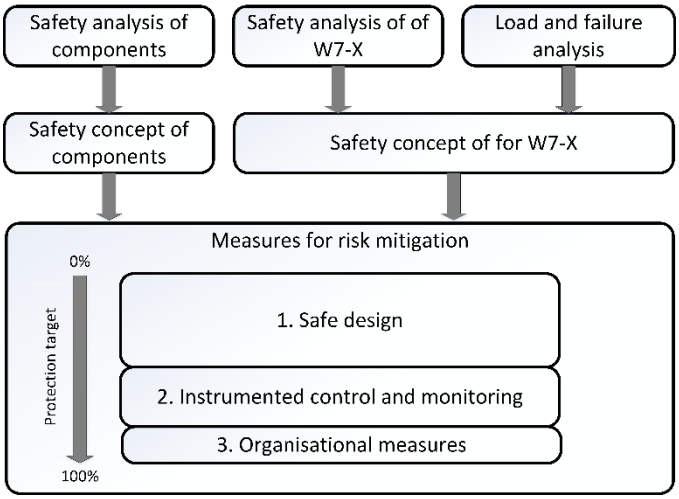

Fig. 5. Risk minimization process.

The task of the risk minimization is that after the application of all specified measures the remaining residual risk remains below the limit of the tolerable residual risk. The relation between the different types of risks is shown in Fig. 6.

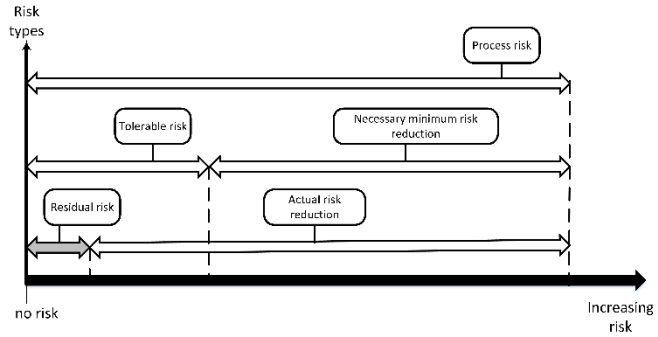

Fig. 6. Risk types.

A safety requirements specification (SRS) must be created for every safety instrumented system (SIS) at W7-X. These SRS documents describe all requirements for all safety functions and allocates a safety integrity level (SIL) for its implementation by the SIS. The SIL has 4 discrete levels for risk mitigation. The SIL 1 has the lowest level of risk mitigation and level 4 has the highest level of risk mitigation. For W7-X SIS the level of safety integrity has a range from SIL 1 up to SIL 2.

Safety relevant process functions (cOPM: central Operational Management of the central control system/lOPM: local Operational Management of the technical components and

diagnostics) and plasma interlock functions (cFIS: central Fast Interlock System/lFIS: local Fast Interlock System of the technical components and diagnostics) have not a SIL classification. These kind of functions are exclusively for investment protection of the W7-X machine. The process for setup of a SIS follows the V-model as shown in Fig. 7.

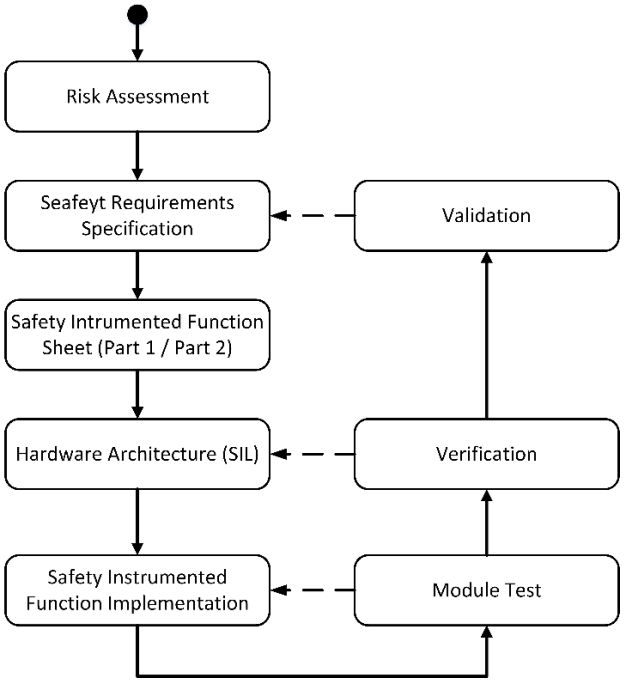

Fig. 7. V-model of W7-X SIS development process.

C. Implementation of safety concepts

The diagram in Fig. 8 shows different scenarios of the development of a process variable, such as the pressure in the plasma vessel of W7-X. Inside of the normal operation range of the pressure (section 1), the process control of the vacuum system set and controls the plasma vessel pressure according the set values. This pressure set value can be given either by the operator or can be given by automatic control processes.

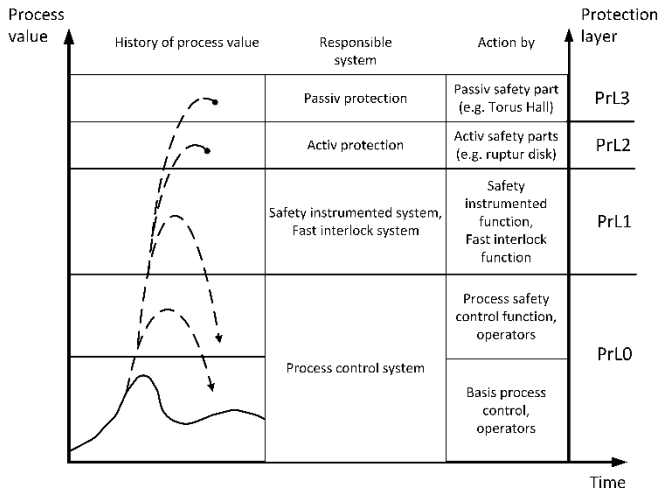

Fig. 8. Protection layer.

In the event of deviations from the setpoint, the controller as a part of the local Operational Management (lOPM of the vacuum system) reacts or the operator can actively influence the setpoint via the user interface. If the pressure continues to increase (section 2), the process safety control function for the pressure responds (Pr-SIF of lOPM of vacuum system). The pressure can be reduced e.g. by increasing the pumping capability of the running pumps or by switching on an additional pump system. An operator action is also possible. If the pressure still increases, then the SIS of W7-X (cSS) will intervene by activation of dedicated SIFs. One possible reaction of a SIF would be e.g. the closing of all gate valves of the plasma vessel except the pumping gate valves. While pressure continues to increase with the active SIF (Sections 4 and 5), the overpressure protection of the plasma vessel will be ensured by an activation of the installed rupture disks.

These staggered reactions of the various risk mitigation measures can meet the risk reduction requirements specified in the safety analysis.

In the following, important concepts of functional safety are described using the example of the central Safety System (cSS) and the central Fast Interlock System (cFIS).

1) central Safety System (cSS)

The structure of cSS is shown in Fig. 9. The hardware of the cSS was chosen according to fulfill the requirements for a high availability system and a failsafe system. The used Siemens PLC hardware (CPU: 2x S7-414, 13x decentral periphery devices: ET200M, fail safe PLC I/O devices) can process safety instrumented function up to SIL 3. The safety related software is written by using F-Systems software (Siemens) [5] and SIMATIC Safety Matrix [6].

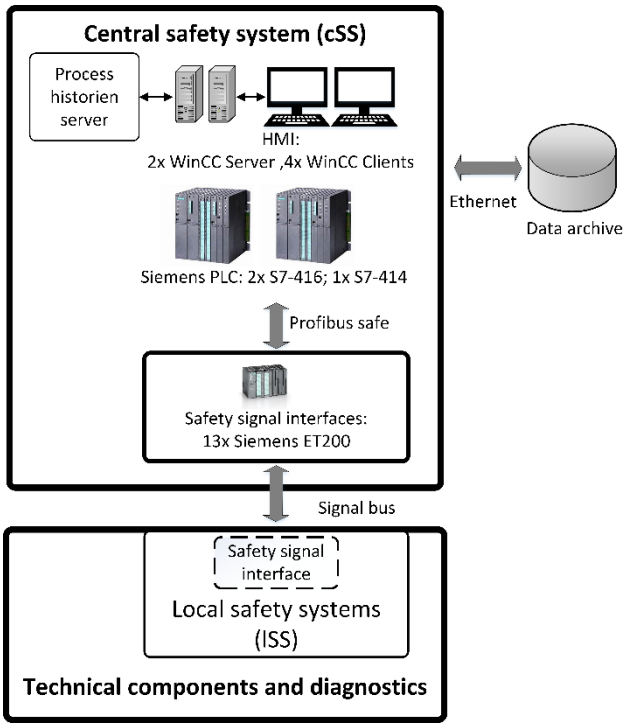

Fig. 9. Structure of SIS.

The cSS own sensors and actuators as well as the signals of the safety interfaces to the control systems of W7-X are connected via the I/O signal modules in the ET200M devices. The cSS program processed a number of about 2200 input signals (thereof 980 safety inputs) and 1000 output signals (thereof 600 safety outputs) in operational phase OP1.2b. These safety signals connect the cSS to the sensor and actuator signals of the central system and are also used as interface signals between cSS and 60 control components with a local safety system (lSS). In the last case, the cSS can only indirectly access the sensors and actuators of the control components via the local SIS (lSS). The signalization interface cSS/lSS has normally a standardized signal set.

An overview about the signals of a safety interface and the meaning of the dedicated safety signals are given in Table II.

TABLE II
SIGNALS OF A STANDARD SAFETY SIGNALIZATION INTERFACE.

Signal name	Direction	Function
Enable	cSS→ lSS	Enables or disenables activities with a potential hazard,
Safe state	lSS→ cSS	Indicates the safe or unsafe state of a component,
Emergency stop W7-X	cSS→ lSS	Indicates an active or inactive emergency stop W7-X status of the cSS,
Emergency stop state	lSS→ cSS	Indicates an active or inactive emergency stop status of the component,
Fault (optional)	lSS→ cSS	Indicates an active or inactive status of a fault condition, detected by the component.

The cSS is responsible for processing of following safety related functions:

- Control of safety levels of W7-X,
- Processing of safety functions,
- Gas warning system,
- Access control system of radiation protection area and radiation protection system,
- Signalization system of the experiment area,
- Standard safety signalization interfaces (Emergency Stop, enable signals, status signals).

The so-called safety levels of W7-X operation is a very important basis concept of the cSS. The safety levels allow enabling of dedicated activity levels of potential hazardous components according planned W7-X operation scenarios and the closing status and person free status of radiation protection area.

The Finite State Machine (FSM) for the cSS safety levels is shown in Fig. 10.

Every safety states defines a set of enable signals for activities of control components of W7-X. By choosing a safety level by the cSS operator via the safety interface all components will be informed by the signal status of their enable signals, if a dedicated activity is allowed or inhibited. Only the "Emergency Stop W7-X" state is initiated by pushing one of the 33 emergency stop buttons located in the experiment area and the cSS control panel.

The processing of safety functions are another important task of the cSS. Based on the requirements specified in the SRS, the safety functions describe actions to be performed when defined events occur. The safety functions follow the reaction chain Sensor - SIS - Actuator. A safety function has the aim to prevent a hazardous situation for personnel or for the W7-X device, or, if this impossible, to reduce the damage consequences within an acceptable range. The sensors and the actuators can be both part of the cSS and part of the via the safety interfaces connected local safety systems of the components.

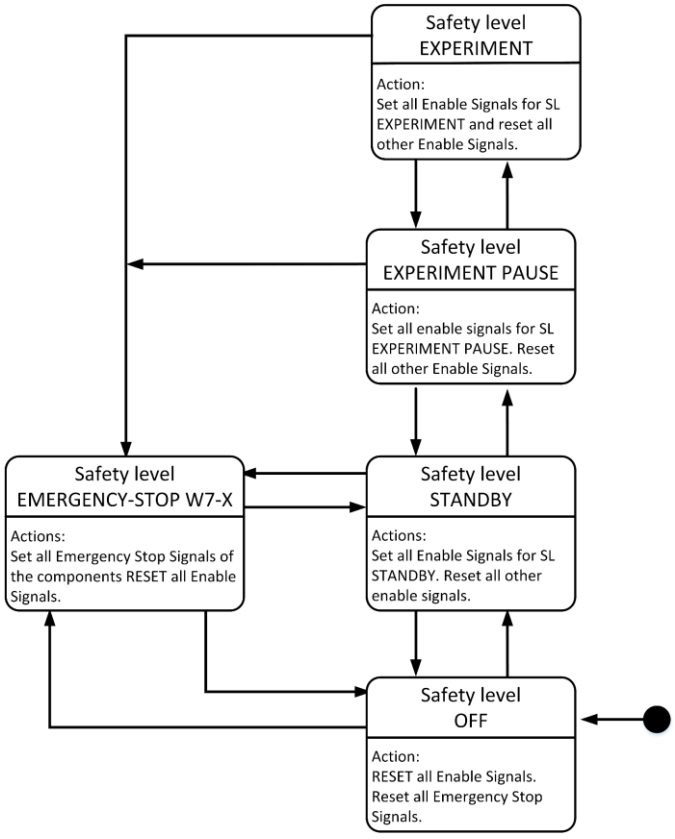

Fig. 10. FSM of safety states of cSS.

Table III shows the development of the safety functions over the previous operational phases of W7-X.

TABLE III
OVERVIEW SAFETY FUNCTIONS FOR OPERATIONAL PHASES OF W7-X

Operational phases	cOPM: Pr_SIF	cSS: SIF_P	cSS: SIF_A	cFIS: I_SIF
Commissioning OP1.1: cool down	0	16	4	0
Commissioning OP1.1: magnet field tests	0	27	9	0
Plasma operation: OP1.1	0	27	9	0
Plasma operation: OP1.2a	0	32	12	0
Plasma operation: O1.2b	18	31	13	6

[1]Pr-SIF: Process Safety Function (investment protection function, SIL0),
[2]SIF_P: Safety Function (personnel safety function, SIL1-2),
[3]SIF_A: Safety Function: (investment protection function, SIL0-2),
[4]I_SIF: Interlock Safety Function: (investment protection function, SIL0, response time < 10ms).

2) central Interlock System (cFIS)

The protection of the plasma vessel components during plasma discharges is the main function of the Fast Interlock System (FIS). The FIS reacts in cases, if the plasma build-up phase is not completed within the pre-defined time-window, the plasma density or energy are too low or if the microwave stray radiation is too high. The reaction consists in switching off the plasma heating systems (electron cyclotron resonance heating (ECRH), neutral beam injection heating (NBI) and for OP2.0 also the ion cyclotron resonance heating (ICRH)) within a reaction time of 50 ms.

The FIS acts as a safety system as part of the protection layer 1 (see Fig.8). The structure of the Fast Interlock System (FIS), as shown in Fig.11, is formed by connection of the central Fast Interlock System (cFIS) with local Fast Interlock Systems (lFIS) via optical signal connections. The cFIS is an independent part of the central control system. All lFIS are integrated into the control and data acquisition system of selected components. A fast interlock function follows the pattern: Sensor(s) (part of lFIS) – Fast Interlock Instrumented System FIIS (cFIS) – Actuator(s) (part of lFIS). The functions of the Fast Interlock System are not classified to a SIL due to the sensors and actuators for the defined fast interlock functions are special developments for plasma physics application.

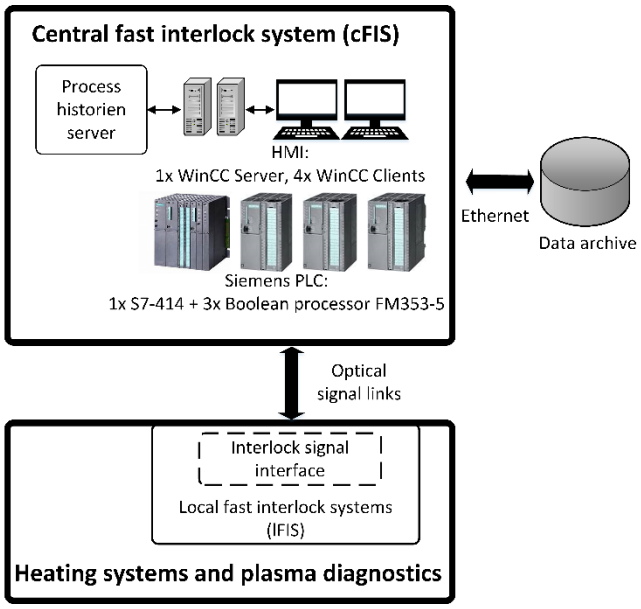

Fig. 11. Structure of Fast Interlock System.

During OP1.1 only the sniffer probes of the ECRH had been used as an interlock diagnostic. This interlock signals have been processed directly inside the control system of the ECRH, because the whole FIS was only available from operational phase OP1.2b. In Op1.2b the FIS was equipped with 6 FIS function (I_SIFs). The following interlock diagnostics were used:

- Sniffer probes for detection of the ECRH-stray radiation,
- Diamagnetic loops for determination of the plasma energy, and
- Single interferometer for determination of the electron density.

When activated, all interlock functions realizes the same reaction: stop immediately the plasma heating by switching off the OP1.2b plasma heating systems ECRH and NBI.

IV. Results

All systems relevant to safety could be designed, set up and put into operation in accordance with the requirements for the different operation phases of W7-X. The introduction of the safety lifecycle process was very demanding but necessary for a successful design and operation of the safety systems for the first three operation phases of W7-X. The chosen hardware and software concepts have proven their worth in 117 experiment days with overall 3052 plasma discharges. In addition, the conditioning of the plasma vessel by a boron-coating using diborane gas was introduced in OP2.1b. This function placed particularly high safety demands, since diborane is a very toxic and explosive gas.

The cycle times for processing of the safety functions (see Table IV) were within the expected range.

TABLE IV
CYCLE TIMES FOR PROCESSING PR-SIFS, SIFS, AND I_SIFS.

Type of safety function	Average cycle time: central SIS	Range of total cycle time: Sensor-SIS-Actor
Pr-SIF	cOPM: 1000ms	2s - 5s
SIF_P/A	cSS: 500ms	1s - 3s
I-SIF	cFIS: 0,1ms	500µs – 1s

The PLC fail safe hardware (Siemens) used for the cSS and for large number of lSS of components works very reliably. Since start of operation in 2015 only one I/O module of a decentralized periphery device ET200 (Siemens) had to be replaced due to an internal error.

The emergency stop function was triggered several times during operation because access to the torus hall was released too early due to an operator error. This error will be eliminated by a better software design and a new interface between cSS and the access control system.

The sensors of the gas warning systems works not as stable as needed. This led to a series of false alarms with an activation of dedicated SIFs. The causes of this sensor behavior must still be clarified together with the manufacturer.

The implementation of a simulation system for the safety system based on framework SIMIT (Siemens) was extremely helpful for the development of the SIS software, for integration tests, and for training of the cSS operators [7] [8].

A model-based generation of test plans for the acceptance tests of the safety systems was very helpful for an efficient preparation and execution of the extensive tests.

The interlock system required a lot of time until the algorithms for the evaluation of the measured values of the sensors of the interlock functions worked without errors.

The Pr-SIFs of the cOPM could be set in operation without any serious problems.

V. Status and Outlook

W7-X has successfully concluded three operation phases. The last experiment campaign ended in October 2018. The next

operation phase, starting in 2021, is in preparation. Beside the installation of a new water cooled divertor and cryo pumps, already established diagnostics will be modified and new diagnostics and technical systems will be setup for W7-X.

Due to new requirements for the safety systems for OP2, the definition of new safety functions as well as the modification of established safety functions must be realized in the current completion phase CP2 of W7-X. Plasma experiments with deuterium as working gas planned for OP2 requires special efforts, in particular, in the field of radiation protection functions.

The integration of plasma heating system ICRH and other technical systems and diagnostics in the safety functions of the central safety systems requires new safety interfaces between cSS and these components.

The interlock functions for plasma heating have to be adapted so that the new ICRH heating system and the extension of the NBI heating system can be integrated. The requirements for the interlock system for the tasks of protecting the water-cooled divertors are currently still under discussion.

Finally, also the adaption of the SIMIT testbed for the safety control system for using in CP2/OP2 is planned. This is to support the module and integration test of the cSS software. Another important point is the training and education of the cSS operators for the new operating phase OP2.

ACKNOWLEDGMENTS

This work has been carried out within the framework of the EUROfusion Consortium and has received funding from the Euratom research and training programme 2014-2018 and 2019-2020 under grant agreement No 633053. The views and opinions expressed herein do not necessarily reflect those of the European Commission.

REFERENCES

[1] H.-S. Bosch et al., "Transition from Construction to Operation Phase of the Wendelstein 7-X Stellarator", IEEE Trans. on Plasma Science., vol. 42, no. 3, pp. 432-438, Feb. 2014.

[2] R. Wolf et al., "Major results from the first plasma campaign of the Wendelstein 7-X stellarator", accepted for Nucl. Fusion.

[3] Functional safety-Safety instrumented systems for the process industry sector–Part 2, IEC 61511-1:2016 + COR1:2016 + A1: 2017,

[4] L. Balmelli, "An Overview of the Systems Modeling Language for Products and Systems Development", Journal of Object Technology, vol. 6, no. 6, pp. 149-177, July–August 2007.

[5] https://w3.siemens.com/mcms/simatic-controller-software/en/programming-options/s7-f-fh-systems/s7-f-systems/Pages/Default.aspx

[6] https://w3.siemens.com/mcms/simatic-controller-software/en/programming-options/s7-f-fh-systems/safety-matrix/Pages/Default.aspx

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

[8] J. Schacht, et al., Simulation System for the Wendelstein 7-X Safety Control System, IEEE Transactions on Nuclear Science On page(s): 1-3 Print ISSN: 0018-9499 Online ISSN: 1558-1578 Digital Object Identifier: 10.1109/TNS.2019.2913797.