This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

Management of the Wendelstein 7-X Central Safety System Using a Requirement Engineering Tool

E. Scharff, S. Degenkolbe, J. Schacht, R. Vilbrandt, H.-S. Bosch, and the W7-X Team

***Abstract*— A safety instrumented system (SIS) is in place for the continuous safe operation of Wendelstein 7-X (W7-X). The central safety system (cSS) is part of this system. Prior to the last operation phase (OP) 2.1 in preparation for the steady-state regime, the cSS was fundamentally revised. A requirements engineering tool (RET) was introduced to support the development process. The SIS development plan, adapted to the W7-X, provides for fixed steps. All functional requirements derived from the W7-X risk analysis for the cSS and derived objects along the safety lifecycle are documented in the RET by means of work items. In this way, the requirements of the SIS standards and those of the approving authorities can be met. Dependency relationships have been established between the work items to allow the analysis of completeness, dependency, and explicitness, as well as the analysis of the impact of possible changes at any point in the process. The requests for adaptations and extensions to the cSS, derived from the experience with the SIS in OP2.1, are also organized with the RET.**

***Index Terms*— Documentation, functional safety, nuclear fusion reactor, requirement engineering tool, test management, traceability, Wendelstein 7-X (W7-X).**

I. Introduction

The Wendelstein 7-X (W7-X) fusion experiment can look back on four successful operation phases (OPs) until 2023 [1], [2]. The first three OPs were followed by an extended assembly period during which the device was converted to steady-state operation. In preparation for operation, the central safety system (cSS) was also thoroughly re-engineered. As part of the safety instrumented system (SIS), it contributes to reduce the risks arising from the device down to a tolerable residual risk in a controlled manner.

II. SIS of W7-X

The continuous safe operation of W7-X and its components is only possible if both personal safety and device safety are comprehensively taken into account. The protective measures implemented at W7-X can be divided into the following categories: A) Design measures; B) Automated control measures; and C) Organizational measures.

Manuscript received 7 September 2023; revised 8 January 2024; accepted 13 February 2024. This work was supported by the European Union via the Euratom Research and Training Program (EUROfusion) under Agreement 101052200. The review of this article was arranged by Senior Editor R. Chapman. *(Corresponding author: E. Scharff.)*

E. Scharff, S. Degenkolbe, J. Schacht, and the W7-X Team are with the Max Planck Institute for Plasma Physics, 17491 Greifswald, Germany (e-mail: erik.scharff@ipp.mpg.de).

R. Vilbrandt and H.-S. Bosch, retired, were with the Max Planck Institute for Plasma Physics, 17491 Greifswald, Germany.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TPS.2024.3366750.

Digital Object Identifier 10.1109/TPS.2024.3366750

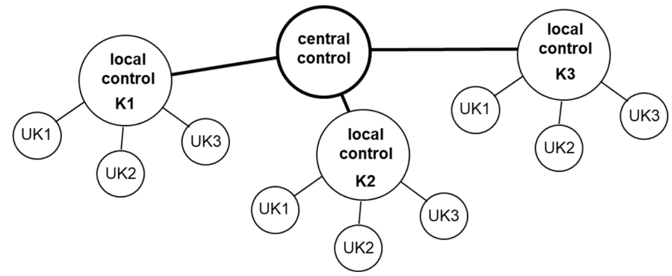


Fig. 1. Scheme of the centralized approach followed in the structure of safety systems at W7-X.

In order to achieve a defined protection level and to preserve it in any operating state, the measures of A)–C) can be weighted differently in the sense of a protection layer concept, so that, for example, additional organizational protection measures can serve to compensate for control technology monitoring systems that are temporarily out of operation. In general, however, the measures of A) should be given preference over the measures of B), and these in turn should be given preference over the measures of C).

The measures discussed in this article fall into category B, such as safety-instrumented functions (SIFs). SIFs are usually not performed by a single component, but by a chain of devices consisting of sensors, logic, and actuators (that are typically located in different subsystems). The totality of the control systems that implement SIF form the SIS of the device. The SIS represents the "functional safety" level of protection, which must be implemented independently of the "process control and monitoring" level in order to avoid the failures of common cause or common failure mode. Accordingly, the safety control of the W7-X operates autonomously. All control systems on the W7-X follow the clear hierarchical structure shown in Fig. 1. The safety system of W7-X thus consists of a central unit (cSS) and a number of local instances (lSS) at the component level.

The cSS combines all SIFs with a safety integrity level (SIL) assessment without high response time requirements, which can only be realized across all components. In contrast to the safety architecture of some other large research facilities (such as *ITER* [3], *ITER NBTF* [4], and *ESS* [5]), the protection objective of the cSS is both personnel and device/invest protection.

The main tasks of the cSS are as follows.

1) Realization of interlocks of corresponding components by the removal of the release signal according to the function matrix depending on the operating functions.

2) Implementation of shutdown measures (e.g., by the removal of releases) according to the status of the respective affected components. In some cases, a media supply (e.g., with cooling water, LN2, or LHe flow) is still required to maintain the safe state.

The cSS is built with SIL-rated hardware only. The details of the physical and logical architecture of the cSS are described in [6].

In addition to and independently of the cSS, the so-called fast interlock system (FIS) [7] operates, which is primarily designed to protect the components inside the plasma vessel and, in particular, implements all those functions for which a short reaction time (<10 ms) is required.

III. Ensuring Functional Safety at W7-X

In terms of functional safety, control systems that perform safety functions must have an availability and reliability commensurate with the hazard. The IEC 61511 formulates for SIS how these requirements can be met [8]. The standard is based on the safety life cycle, which divides the "life" of an object into the phases: 1) hazard and risk assessment; 2) specification of safety requirements; 3) design and engineering of the SIS; 4) installation, commissioning, and validation; 5) operation and maintenance; 6) Modification (hopefully after a long period of reliable operation); and finally 7) decommissioning.

The IEC61511 has been adapted to the real situation of the W7-X organization in a so-called *Project Safety Plan* (PSP) [9]. In the plan, measures are defined for each phase of the safety life cycle to ensure that the functional safety objectives are achieved. The verification (analysis or testing) of the achieved results to prove that they meet the objectives and requirements of the respective phase is essential. All development and implementation steps defined for the realization of the SIS are therefore assigned corresponding test activities in the V&V plan of the PSP (Fig. 2).

Werner et al. [10] describe the general procedure for the development and commissioning of the cSS as it has always been applied in the project. The starting point of the development process is the *safety requirements specification* (SRS), which contains the functional requirements with regard to personnel and device safety. All safety functions to be covered by the cSS are derived from the first stage, the hazard and risk assessment. Within this, for each subsystem or component (e.g., a diagnostic, supply, or heating system), a *safety analysis* had to be submitted by the *responsible officer* containing the risks and measures (including safety-related ones) for risk reduction. These safety analyses formed the basis for the overall safety analysis of W7-X, in which the additional risks resulting from the interaction of the individual subsystems or components were identified. For the measures assigned to the "functional safety" level, i.e., the SIS, the required SIL was determined from the required degree of risk reduction.

For special procedures that need to be performed in the preparation of plasma experiments (e.g., baking, boronization, glow discharge, test operation of lasers, or heating systems), the concept of special operation states has been introduced at W7-X. These states may be associated with increased hazards,

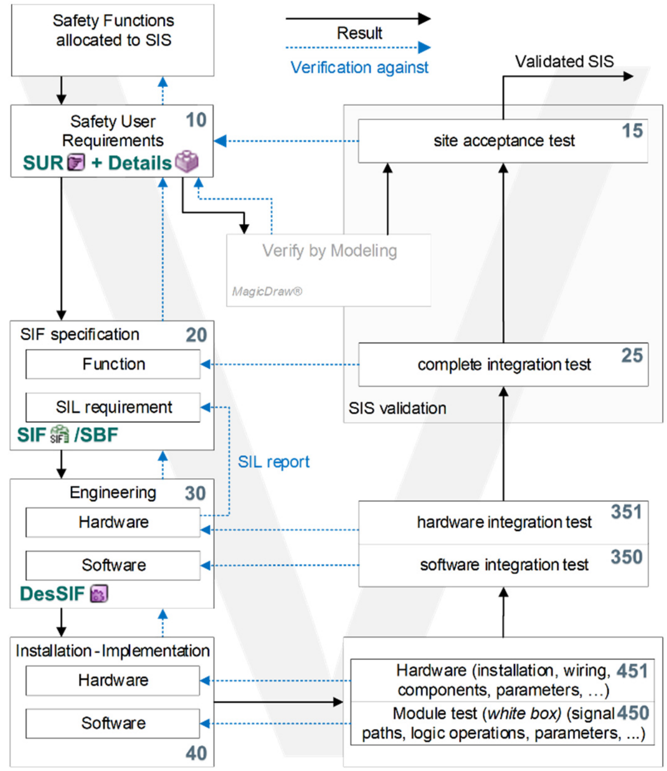


Fig. 2. Verification and validation plan for the SIS of W7-X; on the left the realization steps and on the right the test activities.

usually require certain preconditions and thus represent additional requirements for the SIS.

In addition to the development process described in [10], a requirements engineering tool (RET) was introduced during the long modification phase in preparation for the first operating phase of W7-X with water-cooled high heat flux divertor. Together with other implemented systems engineering tools [11], the RET attempts to address the complexity of the device in the area of safety control systems. Specifically, the RET is used to document all SIS requirements and the associated verification and test activities in the development process and to manage them throughout their life cycle. In this way, the requirements for completeness, consistency, and permanent traceability resulting from the standard for SIS, as well as the requirements of the authorities and their assigned inspectors, can be fulfilled in an effective manner.

IV. Setup of RET

Ebert [12] sees the following advantages in supporting requirements management with specialized tools:

1) fast and consistent access to the project's requirements;
2) clear status control in the project;
3) consistent change management;
4) efficient linking with other project results;
5) easy filtering based on attributes; and
6) single source of truth for all relevant stakeholders.

The core idea of all RETs is to treat each requirement as an independent object. This allows for effective organization, representation, and management of requirements.

In the W7-X project, various commercial RETs were first compared in a selection process, from which the web-based product *Siemens Polarion*[1] was finally selected as a suitable tool to accompany the development process of the W7-X central safety control.

In *Siemens Polarion*,[1] all objects to be created in the safety lifecycle (requirements, SIF specifications, test cases, etc.) can be documented in the form of individually designed work items with attributes adapted to their specific nature. Work items can be structured in word-like documents. A key feature is the ability to link each type of work item, allowing dependencies to be defined between them to illustrate different aspects. Analysis and traceability are provided by *LiveReport-Pages*, which makes the linked structures visible.

Administratively, the different stakeholders (requesters, project developers, testers, etc.) are divided into roles with separate access rights to the RET according to their interests. The folder structure in the cSS project follows the hierarchy of the aforementioned V&V plan (Fig. 3). The development level represented by a folder is identified by its number. Starting with the number "1" as the first digit identifying the top level of requirements, all subsequent levels of SIS realization were identified by counting up. Specifications, analyses, and implementation documents of the individual levels, i.e., all steps on the right side of the V (see Fig. 2), are stored in the folders with a "0" as the second digit. The test documentation of the verification and validation steps on the opposite levels are located in the folders with a "5" as the second digit.

Each work item type is identified by its own icon (examples shown Fig. 2). Work items are grouped into controlled documents (e.g., functional requirements and their details form the SRS).

At regular intervals, especially after the completion of a realization step, baselines are created, which serve as a reference for the next step, freezing the status and documenting it for retrieval at any time.

V. Management of Realization Process

A. Item Documentation

The SRS is formed from the collected individually formulated functional requirements, the *safety user requirements* (SURs). SURs have the attributes of potential hazard, the safe state to be assumed, and the components that act as sensors or actuators (the safety signal scope can be derived from these). Each SUR also includes the SIL of the signal chain to be realized and, if applicable, permitted options for signal bridging (Fig. 4). In additional detailed requirements, aspects such as intervention options (e.g., necessary confirmation after triggering of the function) as well as reaction times or delays to be observed can be assigned to each SUR.

When formulating the SUR and the detailed requirements, special attention must be paid to correctness, unambiguousness, completeness, and verifiability in accordance with the established quality criteria for requirements documentation [13].

[1]Registered trademark.

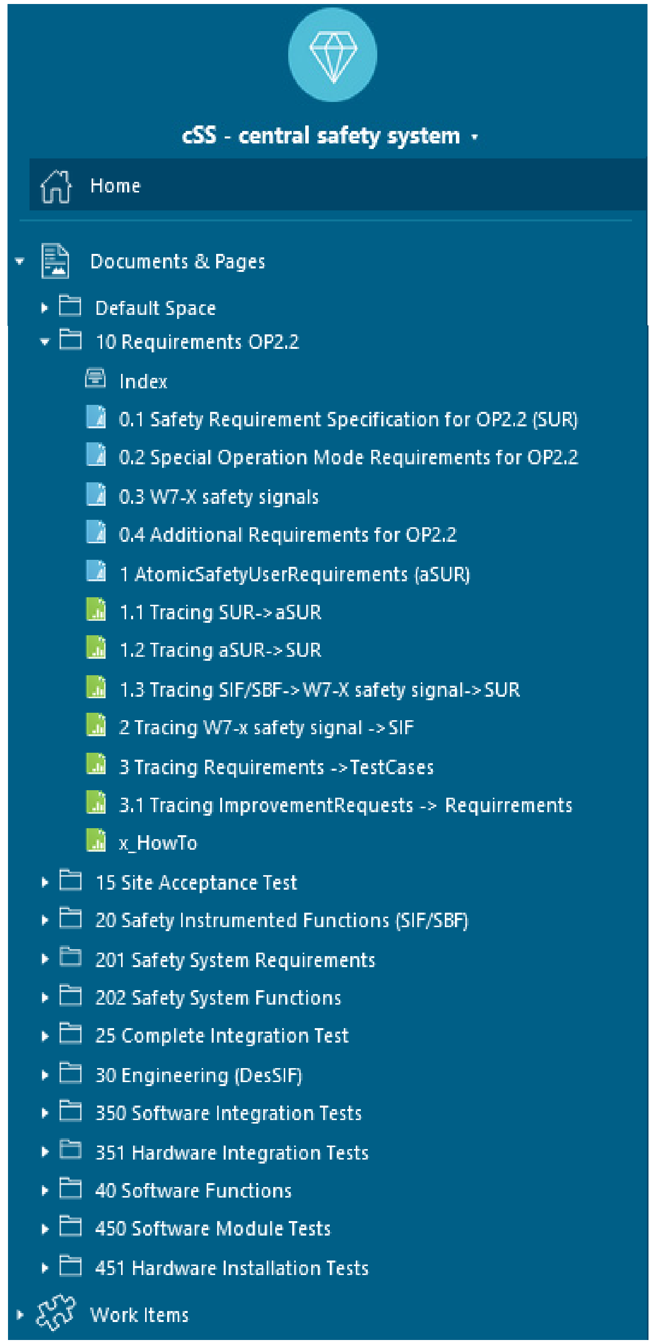
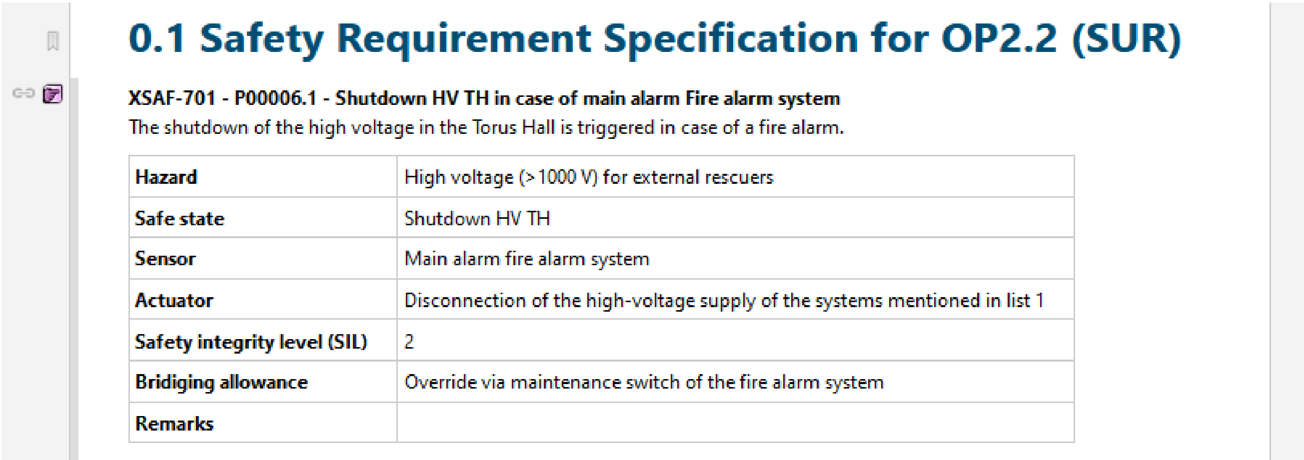


Fig. 3. Folder structure of the RET for the cSS; blue icon means *LiveDocDocument* and green means *LiveReportPage*.

The additional requirements for the cSS resulting from the special operating functions are defined as the so-called *special operating mode* in the RET in a separate specification document.

The realization process itself begins with an analysis step in which all the SUR formulated in the SRS, their detailed requirements and the special operation requirements are first broken down into *safety system requirements* (SSRs). From these, the *atomic SUR* (aSUR) can be derived, each of which represents an elementary functional chain from a sensor to an actuator that cannot be further subdivided. In the next step, the SSRs are synthesized by the software developer into

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.



0.1 Safety Requirement Specification for OP2.2 (SUR)

XSAF-701 - P00006.1 - Shutdown HV TH in case of main alarm Fire alarm system

The shutdown of the high voltage in the Torus Hall is triggered in case of a fire alarm.

Hazard	High voltage (> 1000 V) for external rescuers
Safe state	Shutdown HV TH
Sensor	Main alarm fire alarm system
Actuator	Disconnection of the high-voltage supply of the systems mentioned in list 1
Safety integrity level (SIL)	2
Bridging allowance	Override via maintenance switch of the fire alarm system
Remarks	

Fig. 4. Referable requirement *P00006.1* in the SRS for disconnection of high voltage in the event of a fire alarm.

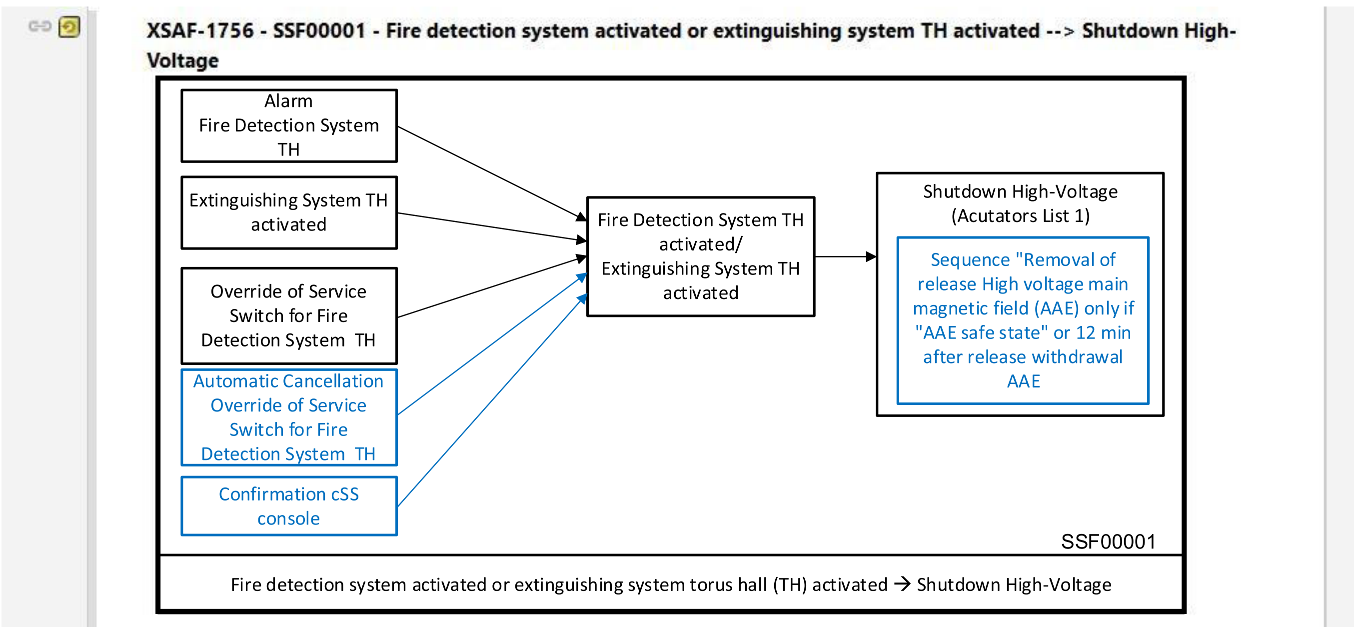


Fig. 5. Graphical description of *SSF00001* in the RET; resulting from requirement *P00006.1*.

functionally collapsible *safety system functions* (SSFs). The SSR and SSF are described graphically and documented in the RET (Fig. 5). Each SSF forms the functional template of an SIF to be implemented. In the RET, the SIF work item is assigned a large number of attributes that specify all the details necessary for the hardware and software implementation, such as bypassing, overriding, resetting SIF, and/or (ordered) restart. The SIF is documented in the software specifications of level 20.

Further work items documented by RET are as follows:

1) specifications of safety signals between lSS and cSS;
2) actuators and sensors from safety signals;
3) logic representations of the SIFs to be designed in software (DesSIF);
4) software module tests in the simulated test environment;
5) SIF integration tests in the simulated test environment;
6) hardware interface tests of the safety signals;
7) test steps, test cases, and test suites of site acceptance tests (see Section V-C); and
8) software changes (see Section VI).

B. Traceability Analyses

Due to the process, all objects created during the realization have different relationships to each other. Since the work items in RET are interactive, referable objects, dependencies can be explicitly modeled, in contrast to a purely document-based capture. Understandably, only certain relationships between the objects of different categories and different realization levels are meaningful and permissible (e.g., SIF is derived from requirements and uses safety signals. Test cases validate requirements).

Based on the relationships, RET offers the possibility to clearly represent the modeled aspects with the help of the so-called traceability tables. Completeness, dependency, uniqueness, and impact analyses can be performed at any time (example Fig. 6). Inconsistencies and multiple requirements are detected. At this point, it is important to model only those

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

1.3 Tracing SIF/SBF -> W7-X safety signal -> SUR

Overview of safety instrumented functions (SIF/SBF) including the functional description, sensors and actuators of the SIF/SBF and the related requirement (SUR) out of the specification of safety requirements.

Description of SIF of SBF	Signals and states addressed by SIF/SBF	related SUR
XSAF-2514 - The SIF00030 is active when a prerequisite for boronazation is not satisfied. **reqIF.Code:** DesSIF00030 **description:** The SIF00030 is active when A prerequisite for boronization is not satisfied (signals K5-10; K5-13; K5-14; K12-3; K12-4; K22-6; K22-7; K22-8; radiation protection area not free of persons). Operator alarm (at the cSS operating station) is only triggered if special boronazation mode (SB4-1) is activated.	XSAF-689 - SIF00030: No release for Diborane in gas supply **sensors:** K5-10, K5-13, K5-14, K12-3, K12-4, K22-6, K22-7, K22-8, state of radiation protection area " person-free inspected " **actors:** K9-2, Function: Alarm signalling via signal tower at the cSS operating station, Function: Alarm message requiring acknowledgement at the OS of the cSS.	XSAF-723 - P00040 - Release for Diborane supply **description:** Diborane gas may only be supplied if certain systems (vacuum system, fire alarm system) are working as intended. **hazard:** Leakage of Diborane **sensor:** The plasma vessel vacuum system reports the status diborane decomposition ok, Theplasma vessel vacuum system reports the status full inertisation ok, The fire alarm panel reports the status ready for use, The room air system LU40 reports normal operation no recirculation operation, The room air system LU40 reports normal operation (negative pressure in the torus hall). The exhaust system LU62 reports in operation without malfunction. The radiation protection area is tested free of persons. **actor:** Release Diborane supply in gas supply **safe_state:** Shut-off Diborane supply in gas supply **safety_integrity_level:** 1 **bridging:** not allowed **remarks:** The release is only withdrawn when the signal "Negative pressure in torus hall ok" is inactive (uninterrupted) for 60 minutes.
XSAF-2513 - The SIF00029 is active when... **reqIF.Code:** DesSIF00029 **description:** The SIF00029 is active when an unauthorised door opening occurs in an actively monitored radiation protection area The SIF leads to triggering of the SSB evacuation alarm. (The assignment of one effect per SSB is preparation for later implementation only in the affected SSB evacuation alarm)	XSAF-664 - SIF00029: Door opening in case of "actively blocked area" status --> Evacuation alarm SSB **sensors:** Status "Door locking actively monitored", status "Control access enabled", door contacts of the doors in the SSB **actors:** Function: Signalling evacuation in the radiation protection area (SSB), Function: Alarm signalling via signal tower at the operating station of the cSS, Function: Alarm message requiring acknowledgement at the OS of the cSS.	XSAF-716 - P00029 - Signalling evacuation in case of breach of actively monitored areas **description:** If an unauthorised opening of doors of an actively monitored area occurs, the signalling for evacuation of the radiation protection area is activated. **hazard:** Danger to persons due to radiation, magnetic field, HV **sensor:** Door contacts or css state "actively monitored" and state "control access enabled". **actor:** Signalling evacuation of torus hall **safe_state:** Signalling evacuation of torus hall **safety_integrity_level:** 1 **bridging:** not allowed **remarks:** For future development: Provide that radiation protection areas are also monitored and alarmed individually.

Fig. 6. Extract from a multilevel traceability table generated in RET based on dependency relationships in order to verify completeness and consistency of SIF descriptions (left column) with all SUR (right column).

relationships that are of interest for the intended analyses, as the effort involved can be immense.

C. Test Management

In order to achieve a consistent development process, additional verification steps between the individual development steps ensure that the achieved results meet the respective requirements.

All test activities performed as part of the step-by-step commissioning, which prove the correct functioning of the software (through module tests, etc.), the correct structure of the hardware (interface tests, etc.), and their correct interaction (various integration tests), are recorded in the RET together with the test results achieved.

The validation of the SIS is executed at the end of the process. It must demonstrate that the SIS has been implemented in compliance with the requirements. Accordingly, each requirement must be matched by a corresponding test case. Test cases consist of individual test steps and have been combined into test suites. Linking the test cases to the aSUR in the RET, analogous to the procedure described in Section V-B, allows a convenient check of the test coverage. The elementary test steps to be performed in a test case and how individual test cases are combined into validation test suites cannot be determined by the RET. This depends on criteria for the different operating states and/or the availability of components at the time of validation, requires the expertise of the validation designers, and has been generated practically with the help of other modeling tools [11].

Since sensors and actuators are often not only far apart but also have different responsibilities, a large number of people (responsible officer for the connected components and diagnostics) are involved in the validation process at the same time. A coordinated, efficient validation is therefore essential.

Since the introduction of RET, the process has been supported by transferring the developed test suites to RET and running the test suites online via RET using a shared screen for all participants. In this way, the progress of the test plan can be monitored by all participants under the guidance of an internal SIL tester. Upon completion of the test suite, the test result and any actions taken are unalterable in RET and stored in a tamper-proof manner.

If nonconforming SIF characteristics are found during testing, they must be corrected immediately. Any software changes in the logic plans also change the software version checksum. By assigning the checksum to the validation plans in the RET and visualizing it, the complete history of logic changes and any software update can be traced at any time by external authorities in accordance with the standard.

VI. Management During Operation

With the successful validation of all parts of the SIS in July 2022, the W7-X with water-cooled divertor could be put into operation. The IEC61511 for SIS requires functional tests for each SIF (proof tests) also during operation in order to maintain the required level of probability of dangerous failure on demand.

During OP2.1, changes and enhancements to the cSS were proposed and collected in the RET. The new work item type *Improvement Request* was introduced for this purpose. Due to the short time until the next operational phase, all proposals had to be prioritized with regard to the need for change and the urgency of implementation. After identifying new hazards, it is generally necessary to go through the V&V process recursively after changes. The necessary changes were included in the RET as a modified requirement at the appropriate location (SRS, SIF specification, hardware or software module, etc.). Using the tool of baselining, different states of documents in the RET can be compared with each other, making all changes visible. The required test effort after the change is derived from the existing links in the RET, in order to finally be able to prove (again) a tested and validated overall system.

Due to the increased scope of enhancements by the implementation of improvements, integration of new sensors as well as diagnostics, a complete validation is essential for OP2.2. The new development cycle will be accompanied by the RET as described above.

VII. Lesson Learned

It is easy to underestimate the effort required to actually implement RET after initial selection and procurement. For example, a four-digit number of links between work items had to be created manually. It is recommended that the switch to RET should not be made during an ongoing development cycle, but only with sufficient lead time. In addition, initial skepticism and operating hurdles must be expected from future users, which must be overcome. A five-day intensive training course for all potential users minimized these issues.

Before the actual productive system is set up, there should be sufficient time to familiarize oneself with the entire range of functions. Play projects help here. In particular, finding a suitable documentation structure, the right scope of *work items* and associated attributes took a lot of time. The constructs also have to be checked again and again for meaning and usefulness. The quasi-inflationary creation of new object constructs quickly leads to confusion, ambiguity, and ultimately to different treatment.

It has also proven to be useful to have the actual creation of these objects done by one and the same person (admin). Adequate human resources must also be planned for ongoing support and maintenance. Last but not least, the licensing system has to be adapted in such a way that peak times of tool use (validation times) can be realized.

VIII. Conclusion and Outlook

In many respects, the use of an RET is proving to be a valuable means of addressing complexity at various points in the life cycle of the W7-X cSS. Implementing the RET requires a careful and planned approach.

OP 2.1 identified potential for optimization in some areas of the SIS, which is currently being implemented through a new development iteration of the cSS in preparation for OP 2.2.

Currently, lifecycle management with RET is limited to the cSS. Given the benefits of RET in supporting the SIS lifecycle phases, it is planned to extend its use to the local safety systems of the W7-X components.

Acknowledgment

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

References

[1] H.-S. Bosch et al., "Preparing the operation of Wendelstein 7-X in the steady-state regime," *Fusion Eng. Design*, vol. 193, Aug. 2023, Art. no. 113830, doi: 10.1016/j.fusengdes.2023.113830.

[2] H.-S. Bosch, "Wendelstein 7-X in the steady-state regime, assembly, commissioning and operation," in *Proc. 30th IEEE Symp. Fusion Eng.* New York, NY, USA: Oxford, 2023.

[3] L. Scibile, J.-Y. Journeaux, W.-D. Klotz, I. Yonekawa, and A. Wallander, "The ITER safety control systems—Status and plans," *Fusion Eng. Design*, vol. 85, nos. 3–4, pp. 540–544, Jul. 2010, doi: 10.1016/j.fusengdes.2010.03.028.

[4] S. D. Bello et al., "Safety systems in the ITER neutral beam test facility," *Fusion Eng. Des.*, vol. 146, pp. 246–249, Sep. 2019, doi: 10.1016/j.fusengdes.2018.12.037.

[5] A. Sadeghzafeh, F. Plewinski, A. Nordt, E. Lund, and Sweden, "An overview of safety control system for ESS target station," in *Proc. 11th Int. Top. Meeting Nuclear Appl. Accel. (AccApp)*, Bruges, Belgium, 2013, p. 5.

[6] J. Schacht et al., "Realization of the requirements for a safe operation of Wendelstein 7-X," *Fusion Eng. Design*, vol. 152, Mar. 2020, Art. no. 111468, doi: 10.1016/j.fusengdes.2020.111468.

[7] S. Degenkolbe et al., "The requirements for the fast interlock system of Wendelstein 7-X," in *Proc. 30th IEEE Symp. Fusion Eng.*, 2023.

[8] *Functional Safety-Safety Instrumented Systems for the Process Industry Sector—Part 2*, Standard IEC 61511-1:2016, 2016.

[9] R. Vilbrandt et al., "Application of the engineering standard for functional safety to the W7-X central safety system," *Fusion Eng. Design*, vol. 123, pp. 632–636, Nov. 2017, doi: 10.1016/j.fusengdes.2017.02.066.

[10] A. Werner, J. Schacht, A. Wölk, S. Pingel, G. Kühner, and H. S. Bosch, "Development and commissioning of the Wendelstein 7-X safety control system," in *Proc. 29th Symp. Fusion Technol.*, 2016, p. 5.

[11] E. Scharff, S. Degenkolbe, G. Kuehner, and H.-S. Bosch, "Benefits of using model-based systems engineering at Wendelstein 7-X," *IEEE Trans. Plasma Sci.*, vol. 50, no. 11, pp. 4245–4250, Nov. 2022, doi: 10.1109/TPS.2022.3206411.

[12] C. Ebert, *Systematisches Requirements Engineering*, 7th ed. Heidelberg, Germany: Dpunkt, 2022.

[13] *IEEE Recommended Practice for Software Requirements Specifications*, IEEE Standard 830-1998, Inst. Electr. Electron. Eng., 1998, doi: 10.1109/IEEESTD.1998.88286.