EUROFUSION WPS1-CP(16) 16499

A Werner et al.

Development and Commissioning of the Wendelstein 7-X Safety Control System

Preprint of Paper to be submitted for publication in Proceedings of 29th Symposium on Fusion Technology (SOFT 2016)

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 under grant agreement No 633053. The views and opinions expressed herein do not necessarily reflect those of the European Commission.

Development and Commissioning of the Wendelstein 7-X Safety Control System

Andreas Werner, A.Wölk, S. Pingel, J. Schacht, G. Kühner, D. Naujoks, Reinhard Vilbrandt, H.-S. Bosch, S. Degenkolbe, P. van Eeten and the W7-X Team

Max-Planck-Institute for Plasma Physics, D-17491 Greifswald, Germany

The Wendelstein 7-X safety control system is one of the main central control entities and ensures personnel safety and investment protection. It has a distributed architecture comprising the central safety system with safety signal interfaces attached to components like the cryo plant, superconducting magnets, heating systems and many more. The development and commissioning process has been established according to the engineering standard for functional safety in industrial processes (IEC 61511). On the requirements level, the unified modelling language and finite state machine simulations (SysML) have been used for the formal specification of the desired functionality and validation plans of the safety instrumented functions. The safety software runs on a fault tolerant Siemens PLC with distributed interface to Profibus-Safe devices and has been implemented with the Siemens PCS7 programming environment. The commissioning was performed in two steps, one stage for the evacuation and cool-down of the cryostat and the final stage for the preparation of the first plasma. The safety programs had been verified for both development stages and finally validated against the safety instrumentation function specification.

Keywords: IEC 61511, functional safety, safety instrumented system (SIS), SysML, PLC, commissioning

1. Introduction

The commissioning of Wendelstein 7-X required a well validated safety control system according to safety standards. Since the beginning of construction phase in 2004, the major standard of machine safety has been renewed with the European Machinery Directive 2006/42/EC, which led to new engineering standards with respect to safety instrumented systems. With the end of the construction phase, these new standards had to be applied for the Wendelstein 7-X safety control system.

Figure 1 shows the overall architecture of the control system, which is a three tier system of hierarchies **Fehler! Verweisquelle konnte nicht gefunden werden.**[1]. The safety system, which is described here solely, resides on the safety layer and provides enabling signals for the operational management system and subsequently for the plasma control system.

Since Wendelstein 7-X is the most recent experiment, which has been put into operation, the applied procedures for development and commissioning of such a safety system is being reported.

2. Requirements

2.1 Early safety concepts

The conceptual work on the safety instrumented system has already been started in 2006. During this time, only a subset of the required safety functions could be gathered, since the project had to focus on the mechanical construction of the device. Nevertheless, the requirements were sufficient to define the architecture of

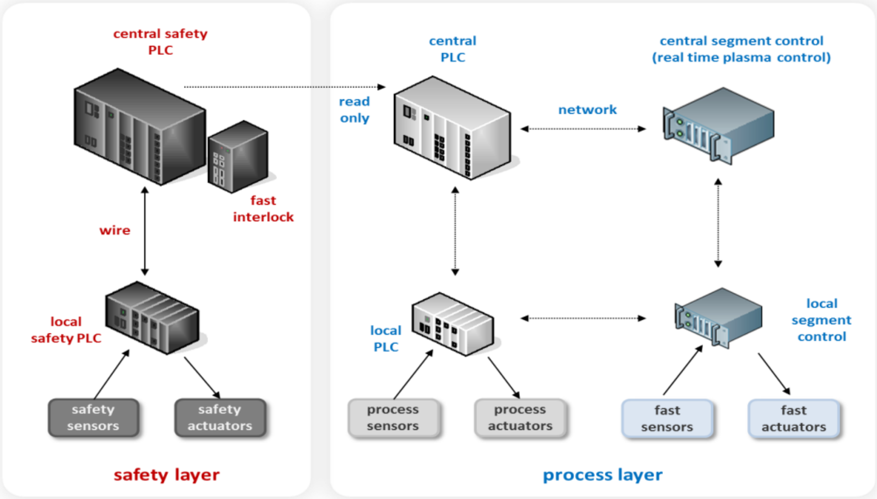

Figure 1: Architecture of the Wendelstein 7-X control system.

author's email: andreas.werner@ipp.mpg.de the control system and some basic safety functions like safety enabling for components and emergency stop. Regarding the architecture, it had been decided to choose the same distributed control system as for the operational management, a star like topology with central safety system (CSS) and local safety systems (LSS) attached within the components like heating systems, auxiliary systems (e.g. gas inlet) and diagnostics. A similar architecture can be found for the ITER control system [2].

In 2008, proof of principle tests had been performed at the WEGA stellarator [3], in which the central safety control system was setup W7-X like but with component interfaces just realized over standard data networks. These tests revealed the appropriateness of the basic safety hard- and software concept, which allowed the determined setup of the safety hardware for W7-X in 2013 while the safety requirements specification was still in the definition phase.

2.2 Applied engineering standards

It has been found and confirmed by external reviewers, the German Technical Inspection Association (TÜV), that the EN/IEC 61511 standard [4] for the "functional safety – safety instrumented systems for the process industry sector" is the most appropriate one. The applied standard is also based on EN/IEC 61508 [5] for the functional safety of electronic, electrical and programmable safety related systems, in which the definition of the safety integrity levels (SIL), required hardware fault tolerance (HFT), self-diagnosis system and more are defined. For the distributed components itself and depending on their complexity, the ISO 13849 [6] can be applied alternatively, which defines the safety of machinery. The procedure for implementing the safety lifecycle of the safety instrumented system is described in [7], this conference.

2.3 Requirements on safety functions

The requirements on safety instrumented functions (SIF) were derived from the safety concept for the main device and infrastructural environment as well as from the risk assessment of all attached components. The functions have been separated into those belonging to personnel safety and those for protection of the investment (in the following device SIF). For the personnel safety, a risk assessment yields the required safety integrity level (SIL), which are typically SIL2 or SIL1 for W7-X. For the investment protection, the same procedure is being applied but can be less strict formal in order to cope with more complex SIFs.

All these requirements are summarized in the safety requirements specification (SRS), which contains 27 personnel related and 9 device safety related SIFs for the operation phase OP1.1. It is basically a catalog of SIFs describing sensors, logic, actors, dependencies to other SIFs and more. It also contains references to SIF datasheets with detailed descriptions of the function itself but also sensor/actor identification numbers, safety signals and the architectural design.

2.4 Safety instrumented functions

The 27 personnel SIFs for the first operation phase can be grouped in categories, namely to allow torus hall access only when the safety instrumented systems and sub components are working properly, emergency stop and shutdown, door locking of the torus hall and magnet operation, radiation protection and experiment stop as well as the door locking of the outer radiation protection zones.

The 9 device SIFs are mainly belonging to the operation of the cryostat and the magnet operation. Prominent examples are:

- to interrupt the liquid Helium or Nitrogen cryo supply when the water flow through the cooling lines on plasma vessel is perturbed to prevent freezing,
- to stop the cryo supply when the cryostat pressure increases to prevent high pressure blow-off,
- to block the magnet operation when the cryo supply is perturbed,
- to perform a soft ramp down of the magnets, even if an emergency stop is launched.

The latter two save the number of stressful fast magnet ramp-downs and prevent persons from hesitating to press the emergency stop button in unexpected dangerous situations. Even more, for the whole system, the soft magnet ramp-down is considered as a safer situation and less harmful than the fast ramp-down.

3. Development

3.1 Architecture and hardware setup

The basic non-functional requirement is the SIL attributed to the SIF. In order to achieve the required level, the hardware has to be setup with an appropriate architecture. For a given assumption on the setup for the chain of sensors, logics and actors, a strict calculation of the probabilities to fail for the whole system has to be performed and iterated until the required level can be achieved. This may lead to higher SIL requirements for individual parts, since a chain of many SIL3 certified elements sum up to a probability to fail, which belongs to the class of SIL2. In order to achieve the required SIL, the basic parameters for the architecture are the hardware fault tolerance HFT, which is the number of non-critical hardware failures, the safe failure fraction SFF and, induced by these numbers, the redundancy architecture. For sensors as an example 2oo3 means, 2 out of 3 sensors have to be functional for retaining at HFT=1 and therefore to keep the SIL.

The logic processor of the central safety system is built with a redundant pair of two Siemens PLCs of type S7-416-5FH, which comply to SIL3 already. Nevertheless, the system has a redundant setup to prevent failures which are caused by the system environment. Common cause failures by the overall system environment like a trip of the air conditioning are accepted, since the system enters the fail-safe state causing an emergency stop. The communication lines to the distributed interface cubicles are based on the Siemens Profibus-Safe system with a redundant ring topology leading to HFT=1 (damage of fibre cable), which is sufficient for SIL 3 when the SFF of the system is larger than 90%. The high SFF is achieved by a rich set of self-diagnosis functions, which lead to high fraction of critical but detected failures (according to λ_{DD} in IEC 61508).

3.2 Design and Implementation

After the definition of the SIF architecture and the verification against the SIL requirements, a detailed logic plan has been developed for each SIF. At this stage, the functional architecture determines the combination of several SIFs, which are quite often driven by other SIFs having the same sensor or the same actor. This logic plan gets all its Boolean input values from the input fail-safe digital inputs (F-DI) including the diagnosis signals. The logic result is connected to the fail-safe digital outputs (F-DO), which configured not to keep the state in failures (SIL3 precondition). The safety software has been developed using the PCS7 technology and the logic plans are implemented using the CFC view (continuous function chart). The CFC view is valuable for the verification of the implementation against the logic plan. A major fraction of the logic has been implemented by employing the Siemens safety matrix. With this tool, a matrix like assignment of input and output logic signals can be embedded in the CFC plan, which improved the implementation efficiency in particular for SIFs with partly common functionality. Furthermore, several verification steps of the IEC 61511V-shaped lifecycle model can be saved according due to the vendors guarantee for this software block.

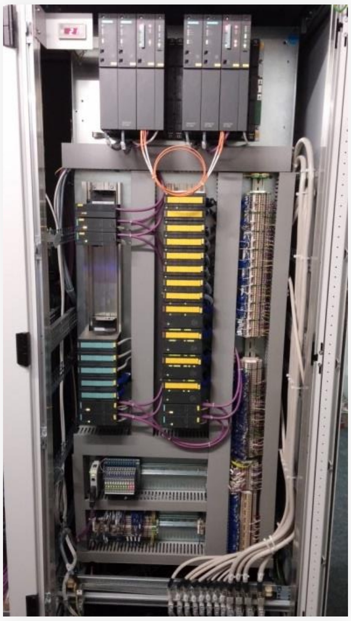

Figure 2: Redundant safety PLC (top) and Profibus-Safe fibre ring lines

3.3 Modelling support for SIFs

The requirements on the SIFs for radiation protection and the locking of the radiation protections zones became more complex than originally expected. This is mainly attributed to different use cases of magnet and heating test operations, the normal experiment operation and the personnel clearance procedures. In order to prevent too many implementation and test cycles, SysML has been applied for the formal specification of functional requirements. In particular finite state machine (FSM) simulations were useful to clarify and verify all the requirements by simulating the different states and transitions.

For the challenge for door locking, personnel clearance and radiation protection, three FSMs have been developed. One describes the state of the door safety supervision (SIL3 contacts) and the state of the door locking itself (no SIL). A second one is dedicated to the state of the radiation protection system, which is equipped with Gamma and Neutron detectors and the signaling of the radiation zone status (free, control, blocked). The two FSMs have been coupled to the FSM of the CSS by sending and receiving signals.

With these simulations (MagicDraw with Cameo Simulation Plugin [8]), different paths through possible states of more than 20 sub-FSMs were tested, corrected and finally verified. The main FSMs could be implemented in the CFC plan in a straight forward manner and, even more, could be used to derive directly the validation test sequences.

3.4 Verification and Validation

As required by IEC 61511, many verification steps have to be taken. At the end of the implementation task, module tests of the individual function blocks (clustering of SIFs) have been performed and documented. Additionally, verification has been performed for all the attached sensors and actors with respect to the correct wiring to the connector blocks of the F-DI/O modules, the correct function of the diagnosis signals like wire breaks and the correct software configuration of these modules.

The final functional tests against the SRS were recorded in the validation test plans. These test plans describe the test strategy, the test environment, the test cases as well as the sequence of the detailed test tasks and their expected values. For SIL2 rated SIFs, the tests have been performed by non-experts from other project divisions. The test strategy, in particular, describes how the system can be modified in order perform the tests while preventing too many harsh shutdowns or emergency stops. Nevertheless, as a minimum requirement, at least one test of the unmodified system was mandatory. Disconnections of signal lines have been only performed at certified parts like safety relais by testing against this interface from both the driver and actor side.

The validation plans have been finally tagged with a CRC (cyclic redundancy check) sum of the whole safety program. This checksum would change, if any of the CFC sub plans or a single parameter of the F-DI/O would change. With this procedure it could be ensured, that the software version and last validation tests were synchronized.

4. Commissioning

In early stages of the development phase, it was envisaged to perform the V-shaped development lifecycle. The project, however, encountered the situation, that the development and commissioning phases were overlapping. The challenge was then to proceed with the development of the safety control system while keeping a subset of SIFs and, hence, the CSS in operation.

For this purpose, a staging of the SRS has been introduced. The first stage included basic SIFs for the commissioning of the vacuum system, the cryostat, the cryo supply and the torus hall signaling. For continuation of the development, the basic idea was to keep the safety during working days by organizational means. A typical development day started with bridging of the signal line with the highest commissioning impact, e.g. emergency stop for the cryo system. The validated software has been unloaded from safety PLC, the new version has been loaded for development. At the end of the day, the validated software had been reloaded, checksum verified and the bridges removed with help of checklists to ensure the correct system setup.

With this procedure, the development of the safety program with respect to door locking and magnet tests could be continued. With the inclusion of the radiation protection, the development was a few times slowed down by modification of the requirements. This was induced by parallel running clarifications of operation permit issues running in parallel. In between, tests have been supervised by the technical supervisory association, in particular for the radiation protection system, the personnel clearance procedure in combination with safety system and the heating emergency shutdown via the high voltage supply switches.

4.1 Final validation and operation

The final validation of the full set of SIFs for the first operation phase OP1.1 took about two weeks. During that time, 36 validation test plans have been performed. A major challenge was the first integrated action of many W7-X components. The validation procedure, in fact, proved capable to reveal some misbehavior in local safety control systems mostly due to bridges and simulations in the local safety systems, which could be corrected in a timely manner.

After successful validation of the system, a procedure for bridging of SIFs and signals (hard- and software) has been established. These bridges have been defined in the SRS for the reason of maintenance and for device safety related SIFs, which rely on new systems where no operation experience existed. One example is the shutdown of the magnets, where the coil current exceeds the critical current. This function was heavily perturbed by malfunctioning cryo sensors, finally bridged and compensated by organizational measures. All bridging had to be recorded, the CRC checksum had to be checked and the records had to be signed by the technical leader of the device operation.

After the final inspection of the validation, the software release management (checksums) and the bridging procedure, the project received the operation permit. Since then, the safety control system has been operated without any faults. The operation of the panels, the daily experiment operation procedure and the enabling logic for operation of components could be well established.

5. Outlook

Although the system has already a large set of SIFs, many additional organizational safety procedures are necessary to operate W7-X in the future. For the next operation phase, more heating systems, auxiliary systems (e.g. pellet injector) and diagnostics will be engaged for operation. Therefore more SIFs for minimizing the organizational safety measures and more component releases are required. As a simplification for setting up the experiment safety states, a finite state machine of safety levels will be introduced, which manages the release states of all attached components with a single operator action.

Acknowledgments

The authors are grateful to I. Müller for setting up robust fibre communications, D. Aßmus and M. Wallis for implementing in a very fast and structured manner the required changes in the electro-technical setup, U. Herbst for the setup of a solid radiation protection system, G. Hemmann for supporting us with CFC programming and M. Köppen, who showed us how to apply the engineering standards and how to perform the calculations of the IEC 61508. Thanks also to H. Braune, K. Rahbarnia, E. Pasch and K. Küttler for performing the SIL2 rated SIF validations.

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 under grant agreement No 633053. The views and opinions expressed herein do not necessarily reflect those of the European Commission.

References

[1] J. Schacht et al., Overview and status of the control system of WENDELSTEIN 7-X, Fusion Engineering and Design 82 (2007) 988-994

[2] L. Scibile et al., the ITER safety control systems—Status and plans, Fusion Engineering and Design 85 (2010) 540–544

[3] J. Schacht et al., Stellarator WEGA as a test-bed for the WENDELSTEIN 7-X control system concepts, Fusion Engineering and Design 83 (2008) 228-235

[4] DIN EN 61511:2005-05, Functional safety - Safety

instrumented systems for the process industry sector, (VDE 0810-1:2005-05; IEC 61511:2003)

[5] DIN EN 61508:2010, Functional safety of electrical/ electronic/programmable electronic safety-related systems - Part 1 to 7 (IEC 61508:2010, VDE 0803:2011)

[6] ISO 13849-1:2015, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

[7] R. Vilbrandt et al., Application of the engineering standard for functional safety to the W7-X central safety system, this conference

[8] https://en.wikipedia.org/wiki/MagicDraw