EUROFUSION WPS1-CP(16) 15705

R Vilbrandt et al.

Application of the engineering standard for functional safety to the W7-X central safety 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.

Application of the engineering standard for functional safety to the W7-X central safety system

Reinhard Vilbrandt, Hans-Stephan Bosch, Georg Kühner, Dirk Naujoks, Jörg Schacht, Andreas Werner, Sven Degenkolbe, W7-X Team

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

This paper focuses on the application of a controlled process for W7-X to develop and implement the Safety Instrumented System (SIS) based on the international safety standard IEC 61511 for the process industry sector. The organization and the approach of the whole life cycle of the SIS are described. The definition of a risk graph and its calibration according to the W7-X-specifics were necessary to assess the required rating of availability and reliability as safety integrity levels according to the standard. The fixed verification and validation process is a prerequisite for the acceptance by the authority as well as the correct and complete documentation of the process and the test certificates.

Keywords: IEC 61511, functional safety, safety instrumented system (SIS), management system, verification, risk assessment

reinhard.vilbrandt@ipp.mpg.de

1. Introduction

Engineering, commissioning, and final validation of the central safety system (cSS) and the acceptance by the authority were very important steps immediately before the successful operation of the first plasma in Wendelstein 7-X in December 2016. Task of the cSS is to protect the personnel and the investment from hazardous situations in an adequate way.

Due to its complexness, the many interdependencies and limiting conditions, design and realization of the cSS must follow strict rules in all phases of the process. Responsibilities and competences have to be defined clearly; the documentation must be complete and traceable for acceptance reasons by the authorities and its assigned inspectors.

2. What is functional safety?

Safety means the absence of unacceptable risks. Functional safety is a part of the whole safety that depends on a system or equipment operating correctly in response to its inputs. In other words, functional safety is the detection of a potentially dangerous situation and the activation of a protective device with a mechanism to prevent this hazardous situation or a corrective device to mitigate the consequences of hazardous events. To fulfill these requirements, the system has to control all dangerous situations with high availability and reliability.

Because the term “functional safety" was used first in IEC 61508:1998 [1], sometimes it is reduced only to the area of programmable safety control. But "functional safety" covers indeed a wide spectrum of devices like sensors, actuators, safety relays, safety contactors, valves, etc.

It is important to recognize that functional safety is a system property like the application domain, but the SIS is fully independent from the process control system. This clear separation must be also emphasized to avoid safe but nuisance trips which might hinder experiments.

In W7-X the cSS with its local instances (local safety systems) represents the Safety Instrumented System (SIS) to realize the functional safety.

3. Which standard is the correct to use?

In recent years a lot of standards in the field of safety or functional safety were published. The generic standard IEC 61508 [1] can be regarded as the progenitor for a lot of specific standards for several industrial branches. Two of them are of special interest for complex experiment devices like W7-X. The first is the IEC 61511 “Functional safety - Safety instrumented systems for the process industry sector” [2] (very similar to ANSI/ISA 84 [3]), that is based mainly on the concept of the safety lifecycle and safety integrity levels (SIL). This guideline supports the approach (and gives some tools) to go a straight way from the assessment of risks to a properly working result. It guides trough all necessary steps and gives with the principle of SIL a tool to describe the requirement level and to verify it for all single function of the SIS.

The second standard is the ISO 13849 [4] which concerns the safety of machinery (safety-related parts of control systems). It can be applied to electrical, hydraulic, pneumatic and even mechanical systems. The methods are used are very similar to IEC 61511, but the rating of the availability and reliability uses the so called “performance level” (PL). Because some industries use this standard and give only certificates for the PL, this standard must be considered as well.

4. General Approach along IEC 61511

The safety life cycle according to IEC 61511 is defined as an engineering process consisting of all necessary steps to achieve the required functional safety. This common guideline was adapted to the real situation of the W7-X organization. The whole procedure and the responsibilities are laid down in a process instruction, the so called Project Safety Plan (PSP), and the related documents.

4.1 Project Safety Plan (PSP) - Personnel

The **project manager** (PM) defines and maintains the Functional Safety Management System (FSMS) according to IEC 61511 for W7-X (Fig. 1). He leads the safety project and appoints a qualified Safety Team. He assigns certain tasks to it and provides necessary resources and information. He needs basic knowledge in IEC 61511 and has to supervise the Safety Team.

The **functional safety manager** (FSM) or quality manager needs expert knowledge in IEC 61511 and good project management skills. He initiates the preparation of the PSP and the associated procedures like V&V-plan (verification and validation plan), Functional Safety Assessment Plan, Project Test plan, etc. He checks the compliance of all activities with the standards, carries out audits and takes care of an adequate training of the involved staff. He checks the conformity of test certificates and he monitors the handling of deviations and changes. He has the right to intervene and to initiate additional correction measures to eliminate faults w. r. t. to functional safety or in case of malfunctions.

The **safety team** (ST) is formed by the safety engineer in charge, the responsible for device safety and typically an experienced interdisciplinary team of methods engineers, specialists for safety assessment, safety commissioners, engineers for the safety control system and process control systems (PCS). This team is organized in the task force central safety system (TF cSS) and assesses the risks and hazards of all processes, allocates safety functions to protection layers, develops the safety requirement specification (SRS), and determines the required SIL for each safety instrumented function (SIF) of the SIS.

The **functional safety assessment team** (FSAT) acts as a design review board and consists of representatives

of the upper project management as well as responsible of important components like plasma heating, cryostat and plasma vessel, helium-cooling system, high voltage supply, head of project control, head of quality management. The project progress is reviewed critically according to the process instruction "Approach to Design and Development at W7-X". The FSAT intervenes and corrects the project if functional safety would not be handled correctly. For this task, technical expertise and operational experience is necessary as well as basic knowledge in functional safety. Note that at least one experienced and competent review board member must not be involved with the project development directly to ensure his independence.

The technical project management is the part of the **engineering manager** (EM). He is responsible for the realization of the requirements from the safety analysis and the implementation of the protective functions into the SIS. The **lead engineer** (LE) for hard- and software and the senior engineers together with their staff completes the team. They are responsible for the realization and testing of the SIS.

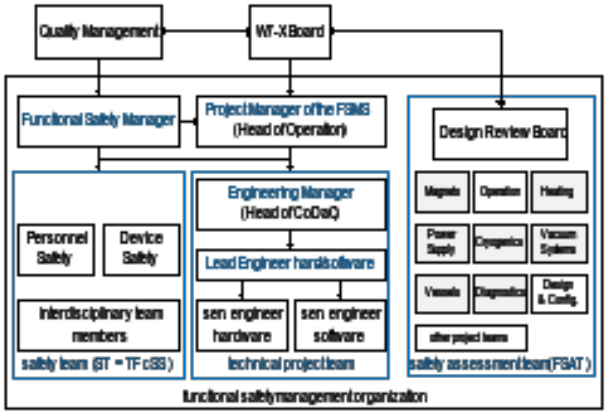


Fig. 1 Organizational structure for the FSMS

4.2 Project Safety Plan (PSP) – approach

4.2.1 Risk Analysis and Allocation of Safety Functions to the SIS – SIL-requirement

First the safety analyses of single components and systems use the "black box"-principle to reduce the complexity of the matrix of interactive impacts as far as possible. The following combined analysis of the entire W7-X device detects the additional risks resulting from their interactions.

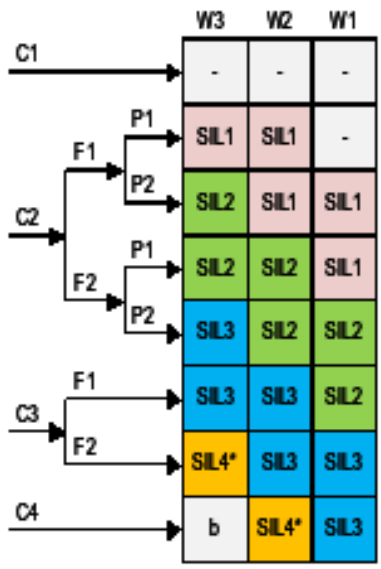
A combination of LOPA (Layer of Protection Analysis) and HAZOP (HAZards and OPerability studies) is used to identify the risks. The measures (safety functions) to control or eliminate the risks are allocated to the several protection layers. It results in the determination of "gaps" in safety, which must be "closed" by the SIS to mitigate the risks to an acceptable level. This process has to be performed very carefully to avoid a mixture of functional safety and experiment process layers. The latter remains the domain of the process control and in the case of W7-X the so called segment control.

For the determination of the necessary reliability and availability of each single SIF of the SIS a risk graph corresponding to IEC 61511 is used. But this risk graph must be adapted and calibrated according the real situation at W7-X to provide a proper SIL value. Fig. 2 shows this risk graph applied at W7-X with its calibrations for personnel safety and investment protection respectively.

4.2.2 Safety Requirement Specification (SRS)

The SRS set-up is one of the most important activities during the life-cycle. It collects all important and detailed information necessary to design and realize the SIS. Therefore the SRS includes much more information as resulted from the risk analysis, namely also requirements for reliability, availability, security, general design and architecture, human machine interface, systems environment, testing, maintenance, etc. [9] The SRS is also the reference for personnel dealing with the validation process later.

	Par.	Personnel safety	Investment protection
		Consequence	
	C1	Minor injury	Damage < 100 k€ or Down time < 1 week
	C2	Serious irreversible injury of some people or death of single person	Damage < 1 Mio € or Down time < 1 month
	C3	2-5 deaths	Damage < 10 Mio € or Down time < 1 year
	C4	> 5 deaths	Damage > 10 Mio € or Down time > 1 year
		Frequency & exposure time	
	F1	Up to 10 % of regular attendance	Up to 10% of operating time
	F2	More than F1	More than F1



- no special safety requirements
* avoid SIL4 (if possible)
b single SIS not sufficient

	Possibility of avoiding the hazardous event - without consideration of other protective measures	
P1	Sometimes possible	Sometimes possible
P2	Almost impossible	Almost impossible
	Probability of unwanted occurrence - under consideration of other protective measures	
W1	Once in the operating time of W7-X (30 years)	Once in the operating time of W7-X (30 years)
W2	Between W1 and W3	Between W1 and W3
W3	More often than every 3 years	More often than every 3 years

Fig. 2 W7-X risk graph and calibration

4.2.3 SIF specification

The SIF specification details the SRS for each single SIF and has two sections. First the corresponding requirements from the SRS must be adopted; that means the operational behavior, set values, triggers, trips, and the control modes like reset, restart, override, bypassing, etc. are defined. In the second step the first appointment of the requirements to rough functional blocks like sensors, processing, and actors is tried with the appointment of minimal to fulfilled SIL of each. This gives a guess about the possibility to realize the function.

4.2.4 Design & Engineering of the SIS

In the engineering process the function blocks are assigned to the hard- and software. Designing the architecture, specifying hard- and software, selecting tools to be used and choosing hardware are the first steps.

It is natural, that the central hardware equipment like SPC, its network and external components must fulfill the SIL. But also the software including its tools often must have a certificate from the supplier.

An important intermediate result is the SIL report. From the SIL of the chosen elements the resulting SIL must be calculated and compared with the SIF spec. If there are inconsistencies another way of realization must searched already in this stage. If for the components there are SIL given by the manufacturer, this is relatively easy. In other cases (Fig. 3) the performance level of some devices only can be calculated or transformed to SIL calculations. The given values for the average frequency of a dangerous failure per hour PFH are valid for typical integrated circuit structures.

Safety Integrity Level (SIL)	Performance Level (PL)	Average frequency of a dangerous failure per hour (PFH)
no correspondence	a	$10^{-4} > PFH \geq 10^{-5}$
1	b	$10^{-5} > PFH \geq 3 \times 10^{-6}$
1	c	$3 \times 10^{-6} > PFH \geq 10^{-6}$
2	d	$10^{-6} > PFH \geq 10^{-7}$
3	e	$10^{-7} > PFH \geq 10^{-8}$

Fig. 3 relation between SIL and PL

More difficult is the situation in cases of special sensors or “self-made” diagnostics used as such. Here one must indeed calculate the reliability with the help of the single probability of failure for the single elements of the sensor, e.g. by calculations with Markov-Chains.

4.2.5 Installation, Commissioning & Validation

The engineered parts of the SIS are realized subsequently. Each must be checked against its single specifications in so called factory acceptance tests; and all results must be recorded carefully as basis of the following more and more integrated tests. At the end stays the validation of the complete SIS.

4.2.6 Operation & Maintenance

The safe operation of the SIS is allowed only by qualified personnel and only with documented rules and adjustments. Specified periodic recurring examinations must be adhered. Repair actions must be carried out only by specialists, followed by the specified test. All activities must be recorded well.

4.2.7 Modification

Of course Modifications and extensions of the SIS in the future are foreseeable. This process is regulated along the process instruction “handling of changes at W7-X” principally. A modular system design is the guarantee that changes do not become a nightmare. Single changes can be verified and validated modularly too, and the consistence of the unchanged parts can be proven easily in this case.

4.3 Project Safety Plan (PSP) – the Verification and Validation Process

The Verification & Validation plan (V&V plan) fixes, what result is verified against which specification, when and by whom.

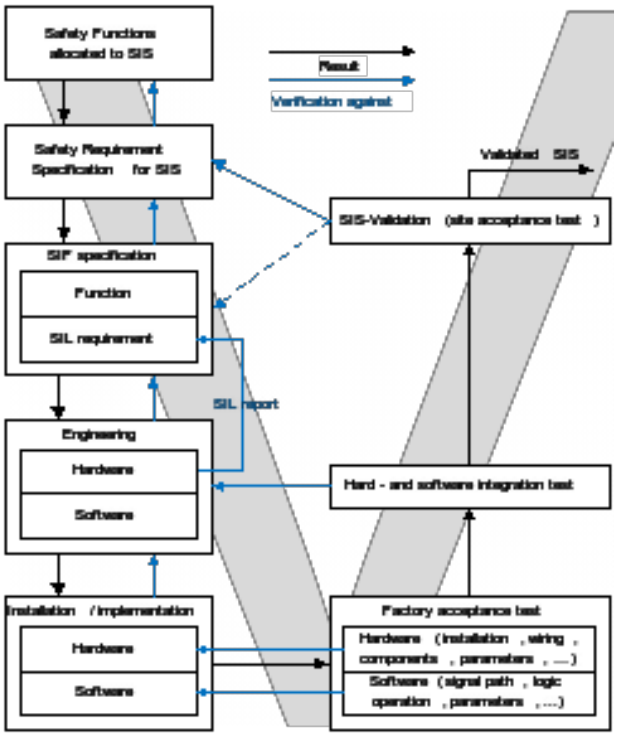


Fig. 4 V&V-Plan from the SRS to the validated SIS

The specified phases with their own results are contrasted with the corresponding test activities. This treatment leads to high test coverage, because the specification of each development step is the basis for the test of this step.

As shown in Fig. 4 the SIS must be validated against the requirements of the SRS at the end. Additional checks take place between subsequent steps verifying the

product specification against the requirements before realization (left side).

4.4 The Fast interlock system specifics

In the past fast interlock systems (FIS), which are used commonly in such experiments like W7-X, were handled as separate systems sometimes. But the FIS has properties of functional safety definitely for the device protection. The PSP is therefore applied for the FIS in all steps. The proof of the SIL is certainly difficult from case to case. But it offers the opportunity to complete a very fast FIS with limited SIL by a safe, but slow SIF to close the gap in safety or to mitigate the risks of disastrous damages. And one can calculate it in advance.

Summary

The quality management in all stages of the lifetime of the central safety system is a key issue to protect both the personnel and the W7-X machine by functional safety. Applicable standards were chosen and rules were defined for the organizational and technical approach, beginning with the risk analysis and proceeding with validation procedures, operation and maintenance, and necessary modifications. The whole process and the results of each step must be documented well for the project as well as for the acceptance by the authority and recurring examinations.

Acknowledgments

All work as described above was done in close cooperation between the departments of W7-X, physicist, engineers and operators, the CoDaC-team, and the QM-department. The good collaboration between these various partner, sometimes subject to strong time pressure, is gratefully acknowledged.

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

[2] DIN EN 61511:2005-05, Functional safety - Safety instrumented systems for the process industry sector, (VDE 0810-1:2005-05; IEC 61511:2003)

[3] ANSI/ISA-84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector

[4] ISO 13849-1:2015, Safety of machinery – Safety-related parts of control systems

[5] Angela E. Summers, IEC 61511 and the capital project process - A protective management system approach, Journal of Hazardous Materials 130 (2006) 28–32

[6] LuiginScibile, Jean-Yves Journeaux, Wolf-Dieter Klotz, Izuru Yonekawa, Anders Wallander,ITER Organization, An overview of the ITER Interlock and safety systems, Proc. of ICALEPCS 2009, Kobe, Japan

[7] Himanshu Tyagi, Jignesh Soni, Ratnakar Yadav, Mainak Bandyopadhyay, Chandramouli Rotti, et. al., Preliminary design of safety and interlock system for indian test facility of diagnostic neutral beam, Fusion Eng. Des., Available online 20 May 2016, ISSN 0920-3796,

[8] International Electrotechnical Commission (IEC), IEC Functional Safety, Geneva, 2015

[9] Johan Hedberg, Safety Requirements Specifications – Guidline, SP Swedish National Testing and Research Institute, 2005