ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-WEBR02

TOWARDS THE OPTIMIZATION OF THE SAFETY LIFE-CYCLE FOR SAFETY INSTRUMENTED SYSTEMS

B. Fernández*, G. De Assis, R. Speroni, T. Otto, E. Blanco,
CERN, Geneva, Switzerland

Abstract

The design and development of Safety Instrumented Systems (SIS) according to the IEC 61511 standard is a long and costly process. Although the standard gives recommendations and guidelines for each phase of the safety life-cycle, implementing them is not a simple task.

Access to reliability data, hardware and systematic safety integrity analysis, software verification, generation of reports, guarantee of traceability between all the phases and management of the project are some of the main challenges. In addition, some of the industrial processes or test benches of large scientific installations are in continuous evolution and changes are very common. This adds extra complexity to the management of these projects.

This paper presents an analysis of the safety life-cycle workflow and discusses the biggest challenges based on our experience at CERN. It also establishes the basis for a selection of the tools for some of the safety life-cycle phases, proposes report templates and management procedures and, finally, describes the roles of the different members in our functional safety projects.

INTRODUCTION

The design, development and maintenance of Safety Instrumented Systems (SIS) requires a lot of resources and time for a company or organization. It is not enough to develop a reliable SIS based on good engineering practices, it is necessary to prove that the Safety Instrumented Functions (SIF) reduce the existing risk to the tolerable region. The functional safety standards provide the guidelines to design and develop such systems and the methods to prove the compliance with the risk reduction target. For industrial processes, the IEC 61511 [1] is the most appropriate standard. It uses the same principles as the IEC 61508 standard with a more specific language and context.

The IEC 61511 Safety Life-Cycle

Figure 1 shows the so-called IEC 61511 safety life-cycle, whose requirements are specified in the Clause 6 of the IEC 61511-1:2016. This Clause defines the different phases, organizes the technical activities and ensures that adequate planning exists for the development of the SIS.

In order to claim conformance with the IEC 61511 standard, all requirements from Clause 5 to Clause 19 from the 61511-1:2016 have to be met and the corresponding reports have to be created. All these requirements are clearly specified, but how to implement them is the real challenge.

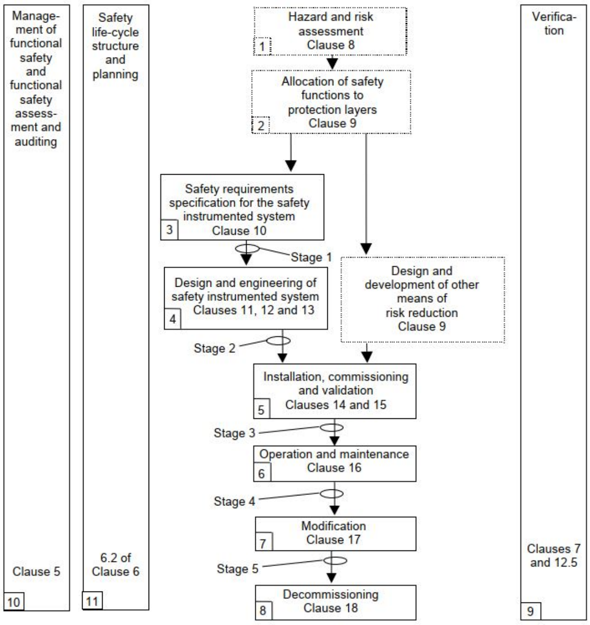

Management of functional safety and functional safety assessment and auditing
Clause 5
10
Safety life-cycle structure and planning
6.2 of Clause 6
11
Hazard and risk assessment
Clause 8
1
Allocation of safety functions to protection layers
Clause 9
2
Safety requirements specification for the safety instrumented system
Clause 10
3
Stage 1
Design and engineering of safety instrumented system
Clauses 11, 12 and 13
4
Design and development of other means of risk reduction
Clause 9
Stage 2
Installation, commissioning and validation
Clauses 14 and 15
5
Stage 3
Operation and maintenance
Clause 16
6
Stage 4
Modification
Clause 17
7
Stage 5
Decommissioning
Clause 18
8
Verification
Clauses 7 and 12.5
9

Figure 1: IEC 61511 safety life-cycle.

Challenges

The main challenges related to the implementation of the safety life-cycle are common to most industries. In our experience, proving the compliance with the standard and guaranteeing the traceability between all phases of the safety life-cycle are two of the most critical ones. Compliance is a very costly and time-consuming process, and lack of traceability most certainly would create discrepancies in the project documents, delays and potential errors.

In addition, at CERN (European Organization for Nuclear Research) and most probably in other large scientific installations, some of the industrial processes or test benches are in continuous evolution and changes that influence the safety of the installation are very common.

Objectives

Our goal is to overcome the technical and organizational challenges to optimize the allocated resources for the design, development and maintenance of SIS.

More specifically, we aim to:

- Create report templates that are necessary for the documentation and management of such projects.
- Reuse and integrate the existing tools we have at CERN that can be applied to any of the phases of the safety life-cycle.
- Discuss the management procedures and the roles of the different members in our functional safety projects.

[*] borja.fernandez.adiego@cern.ch

COMMERCIAL TOOLS

There are many commercial tools that offer solutions for one or several phases of the safety life-cycle. Table 1 presents some of the most relevant ones.

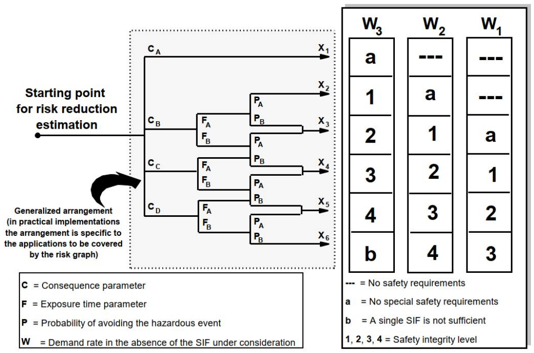
Exida's toolkit, exSILentia®, is one of the most popular tools. It covers all the phases of the life-cycle and certainly fulfils the requirements of most engineering teams to design and develop SIS in terms of reporting, management, traceability and reliability. This tool could certainly bring a lot of benefits to our workflow, especially traceability. There are however a few requirements that are not covered by this framework, to the best of our knowledge, regarding code generation and formal verification. At CERN, we have adopted alternative solutions, which are discussed in the following sections.

Another relevant tool is the Reliability Workbench provided by Isograph. It allows the creation of reliability models, such as FTA (Fault Tree Analysis) and RBD (Reliability Block Diagrams), and analyses their compliance with the IEC 61508 standard [2] in terms of random failures and architectural constraints. An example can be found in [3].

The rest of the paper analyses some of the most challenging phases of the safety life-cycle based on our experience and describes the adopted solutions.

HAZARD AND RISK ASSESSMENT, ALLOCATION OF SAFETY FUNCTIONS TO PROTECTION LAYERS AND SAFETY REQUIREMENTS SPECIFICATION

The hazard and risk assessment, allocation of safety functions to protection layers and Safety Requirements Specification are the first three phases of the safety life-cycle. The IEC 61511-1:2016 Clause 8 defines the requirements to perform the hazard and risk (H&R) analysis from the process and the BPCS (Basic Process Control System). Clause 9 defines the requirements for the allocation of safety functions to protection layers. Clause 10 provides all the requirements to produce the SRS (Safety Requirements Specification) document.


Starting point for risk reduction estimation
Generalized arrangement (in practical implementations the arrangement is specific to the applications to be covered by the risk graph)
C_A
C_B
C_C
C_D
F_A
F_B
P_A
P_B
X_1
X_2
X_3
X_4
X_5
X_6
C = Consequence parameter
F = Exposure time parameter
P = Probability of avoiding the hazardous event
W = Demand rate in the absence of the SIF under consideration
--- = No safety requirements
a = No special safety requirements
b = A single SIF is not sufficient
1, 2, 3, 4 = Safety integrity level

W_3	W_2	W_1
a	---	---
1	a	---
2	1	a
3	2	1
4	3	2
b	4	3

Figure 2: Risk graph: general scheme from IEC 61511-3:2016 Annex D.

The objectives of these phases are: (1) identify the hazards and risks of the industrial process and the BPCS, and evaluate the necessary risk reduction to the tolerable levels, (2) propose a risk mitigation strategy and (3) provide a detailed and unambiguous specification of the SIS. Annex A from IEC 61511-3:2016 describes the concepts of ”tolerable risk target”, the layers of protection and how to select the appropriate method to evaluate the risks.

In our case, in order to identify the dangerous hazards that can provoke a risk to operators, environment or asset loss (damage to the installations), we usually apply the FMEA (Failure Mode and Effect Analysis) method. To quantify the necessary risk reduction for each failure mode, we use

Table 1: Safety Life-cycle Tools and Software Suites.

Tool	Safety life-cycle coverage	Reference
exSILentia® (Exida)	All phases	`https://www.exida.com/`
Safeguard Profiler	Phases 1, 2, 3, 4 and 6 (Bowtie, LOPA analysis, SRS, SIS design, SIL verification, Proof test analysis)	`https://www.acm.ca/safeguard-profiler/`
SISsuite	All phases	`https://www.sissuite.com/`
SLM V2	All phases	`https://mangansoftware.com/slm-v2/`
Vertigo™	Phases 3 and 4 (Equipment failure rate database, SRS and SIL verification)	`https://www.kenexis.com/software/sis-lifecycle-management-and-sil-verification/`
SIL Solver®	Phase 4 (SIL verification)	`https://sis-tech.com/applications/sil-solver/`
Isograph's Reliability Workbench	Phase 4 (SIL verification)	`https://www.isograph.com/software/reliability-workbench/`
Siemens Safety Matrix Engineering Tool	All phases	`https://assets.new.siemens.com/siemens/assets/api/uuid:f18dcad1-9faf-4f33-8c20-c8390d176993/safetymatrixflyerfinal-300.pdf`
SILcet	Phase 4 (SIL verification)	`https://safetyandsis.com/sil-verification/`

ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-WEBR02

Table 2: Simplified FMEA Example

Subsystem	Failure Mode	Effects	Causes	Current mitigation measures
Water-cooled system	High temperature	Melting insulation, short circuit and electrocution	Water leak	None

Table 3: Example of Risk Evaluation for Personnel Using the Risk Graph Method from IEC 61511-3:2016 - Annex D

Consequence	Occupancy (Frequency of exposition	Possibility of avoidance	Base prob. of failure	SIL target
CC (1 fatality is possible)	FA (less than 10% of working time)	PB (no other system)	W1 (less than once every 10 years)	SIL1 (risk reduction bet. 10 and 100)

one of the methods proposed by the IEC 61511-3:2016, the calibrated risk graph (Annex D). Figure 2 shows the general scheme of this method.

Tables 2, 3 and 4 show a simplified example of the selected methods (FMEA and calibrated risk graph) applied to an industrial installation at CERN.

In Table 2, a failure mode, its effects and causes are described for a simple example of water-cooled cable subsystem, as part of a superconducting magnet test bench facility.

In Table 3, the calibrated risk graph method is applied to evaluate the necessary risk reduction to protect the operators of the installation for the failure mode example shown in Table 2. The risk reduction factor (RRF) is given by the target SIL (Safety Integrity Level). In this example, a SIL1 implies a RRF between 10 and 100.

In Table 4, the same method is applied for the same failure mode but evaluating the asset loss. In this case, the failure mode could provoke a serious damage on the water-cooled cable subsystem and weeks of delay in the test program.

In our experience, the biggest challenge in these two phases is the risk graph calibration for asset loss. Calibration means assigning numerical values to the risk graph parameters in accordance with the corporate risk criteria. The calibration to define the tolerable risk level for personnel protection is relatively straight forward, following the examples given by the standard (e.g. table D.2 from the IEC 61511-3:2016 Annex D, or table E.1 from the IEC 61508-5:2016 Annex E). A bigger challenge is to calibrate the graph for asset loss. A failure in one of our industrial processes would normally provoke a delay in the physics program of one of our particle accelerators (e.g. the Large Hadron Collider) or in the test program of one of our test benches. We have calibrated the consequences in ”delay time”, which is a way for our process and accelerator experts to define the tolerable risk. It is, however, very hard to generalize and provide the same calibration for all the industrial processes we have at CERN. In Table 5, we show an example of the calibration for asset loss in one of our projects.

This calibration has a very big impact in the next phases of the project. It was a very time-consuming process, since it needed the consensus and approval of many members of the functional safety project. However, we have built a sound base for future projects.

Once the risks are identified and the necessary risk reductions (SIL) are calculated, the functional safety expert must propose a mitigation strategy for this risk. If the mitigation method is a SIF, the rest of the safety life-cycle should be completed and a detailed SRS document must be provided to proceed to the next phase. However, SIF is not the only option to mitigate a risk. Other protection layers that should be considered to mitigate a risk (see IEC 61511-1 Clause 9).

This exercise was performed by the functional safety engineer, the process expert, the automation engineer and the Departmental Safety Officer (in charge of evaluating and fixing the acceptable risk levels for the project). Report templates were created for the FMEA-based risk analysis, the risk assessment and the SRS.

SIS DESIGN AND ENGINEERING

The IEC 61511-1:2016 Clauses 11, 12 and 13 define the requirements of the phase 4 of the safety life-cycle: Design and engineering of the SIS.

The goal is to design an SIS compliant with the requirements defined in the SRS document. This phase is a very

Table 4: Example of Risk Evaluation for Asset Loss Using the Risk Graph Method from IEC 61511-3:2016 - Annex D

Consequence	Occupancy (Frequency of exposition	Possibility of avoidance	Base prob. of failure	SIL target
CC (several weeks of delay)	FB (max. occupancy)	PB (no other system)	W1 (less than once every 10 years)	SIL2 (risk reduction bet. 100 and 1000)

Table 5: Example of Risk Graph Calibration for Asset Loss

Consequence		Occupancy		Possib. of avoidance		Prob. of failure	
CA	delay < few hours	FB	always	PA	automatic system that detects and alerts the operators	W1	< 1 failure per 10 years
CB	few hours < delay < few days			PB	There is not	W2	< 1 failure per year
CC	few days < delay < few weeks					W3	> 1 failure per year
CD	delay > a month or cancellation of test program						

long and time consuming process. For each SIF specified in the SRS, four main analyses must be conducted: (1) the random hardware failures, (2) the architectural constraints, (3) the systematic failures or selection of the devices and (4) the application program.

SIF Random Hardware Failures and Architectural Constraints Analysis

In this analysis, the functional safety engineer performs the calculation of the probability of dangerous failure on demand (PFD_{avg}), when the SIF operation mode is low demand; or the probability of dangerous failure per hour (PFH), when the operation mode is high or continuous demand. For this purpose, the reliability data of the SIF components is needed (e.g. failure rate, mean time to failure, etc.). Once the data for the individual components (sensors, final elements and controller) is collected, a reliability model of the SIF must be created and the global PFD_{avg} or PFH is calculated. Table 6 shows the random hardware failure requirements in demand mode for each SIL.

Table 6: Safety Integrity Requirements for Random Hardware Failures from IEC 61511-1:2016 Clause 9.2.3

Demand Mode of Operation		
Safety Integrity Level (SIL)	PFD_{avg}	**Required risk reduction**
4	$\geq 10^{-5}$ to $< 10^{-4}$	$> 10^{4}$ to $\leq 10^{5}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$> 10^{3}$ to $\leq 10^{4}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$> 10^{2}$ to $\leq 10^{3}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$> 10^{1}$ to $\leq 10^{2}$

However, this analysis is not enough. It is also needed to evaluate the architecture of the SIF. For sensors and final elements, the IEC 61511-1:2016 Clause 11.4 provides the requirements for the minimum hardware fault tolerance (HFT) of each element of the SIF. Table 7 shows the HFT requirements for each SIL and operation mode.

Although these requirements can be relaxed if the parameter Safe Failure Fraction (SFF) is known for each element. In this case, it is possible to use the Route 1_H method provided by the IEC 61508-2:2010 Clause 7.4.4. Table 8 shows the HFT requirements for each SIL and the SFF ranges for type A elements (typically, devices without any processor, e.g. simple mechanical sensors or final elements). A similar table with more strict requirements for type B elements (e.g. controllers) can be found in Clause 7.4.4.

Table 7: Minimun HFT Requirements According to SIL from IEC 61511-1 Clause 11.4

SIL	Minimun HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode) or continuous mode)	1
4 (any mode)	2

Table 8: Maximum Allowable SIL for a Safety Function Carried Out by a Type A Safety-Related Element or Subsystem from IEC 61508-2:2010 Clause 7.4.4

SFF	HFT		
	0	1	2
$SFF < 60\%$	SIL1	SIL2	SIL3
$60\% \leq SFF < 90\%$	SIL2	SIL3	SIL4
$90\% \leq SFF < 99\%$	SIL3	SIL4	SIL4
$SFF \geq 99\%$	SIL3	SIL4	SIL4

In our case, Isograph is the selected tool for checking the architectural constraints and quantifying the random hardware failures. This tool is widely used at CERN for reliability calculations. It provides access to the reliability component data and supports the IEC 61508 standard (PFD_{avg} and PFH formulas are included, as well as the HFT tables from Route 1_H). The functional safety engineer can create the failure models, which allows to calculate the random hardware failures according to this standard. Figure 3 shows a diagram of a Fault Tree that models one of our SIFs within the Isograph's Reliability Workbench. The SIF components, to mitigate the risk from Table 2, are: a thermoswitch, the Programmable Logic Controller (PLC) and its input/output cards, and the final elements (in this case, the safety ”slow abort” and the ”main circuit breaker” of a power converter). In this diagram, Q represents the unavailability, which corresponds to the PFD. In addition, Qm represents the mean unavailability, which corresponds to the PFD_{avg}).

ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-WEBR02

By using this tool, we have minimized the time of creating the models and performing both analysis. The calculations performed by Isograph can be exported in CSV (comma-separated values) format and integrated in our reports.

When the SFF data is not available, the Route 2_H from the IEC 61508-2:2010 Clause 7.4.4 can be applied. It is based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels.

SIF Systematic Failures Analysis

Regarding the systematic failures analysis, the selection of the SIF components can be done by complying with the prior use approach from the IEC 61511-1:2016 Clause 11.5.3. In this case, it is necessary to gather sufficient evidence, showing that the dangerous systematic faults have been reduced to a sufficient low level compared to the required safety integrity. Another option is to apply the requirements for systematic safety integrity provided by the IEC 61508-2:2010 Clause 7.4 (Route 1_S, 2_S or 3_S).

SIF Application Program

The application program (AP), which contains the logic of all SIFs, is specified as part of the SRS and usually implemented in a PLC. The AP design and implementation requirements are defined in the IEC 61511-1:2016 Clause 12. In addition, the Annexes A and B from the IEC 61511-2:2016 provide guidelines and recommendations to produce an AP compliant with the standard. Most of our functional safety projects use Siemens Safety PLCs and, depending on the project, we work with Simatic Step7 or TIA Portal[1] programming environments.

According to the IEC 61511-1:2016, the AP development cycle is divided in three phases: (1) design, (2) implementation and (3) verification.

The first phase consists of specification of the SIS logic and its operation modes in a clear and precise way, free from ambiguity and free from design faults. This functional specification is part of the SRS. The IEC 61511-2:2016 Annexes A, B, D and E show examples of recommended specification methods that can be applied to define the functional logic of a SIF. They also recommend the usage of model-based approaches, for example, in Annex B section B.2, the standard states: ”The traditional text based approach of safety AP specification is not efficient enough to handle the advanced, complex safety requirements commonly found in SIF specifications. The most efficient tool to address these challenges is the Model-based design (MBD)...”. In the Annex B section B.4.3.4 the standard states: ”specification should be implemented in the graphical language of the model checking workbench environment...”.

At CERN, depending on the nature of the project, we use one of these two popular model-based specification methods: Logic Diagrams (LD) or Cause and Effect Matrix (CEM). In [4], an example of how the CEM was applied to one of our projects is shown and it also introduces the tool that supports this formalism: SISpec. In addition, another prototype tool has been developed to support LD-based specifications for SIF logic: Grassedit. Both tools have the capabilities of test and verification cases generation for the verification phase.

In the implementation phase, the functional specification is translated into the PLC AP. Siemens safety PLC programs must be written in LADDER or FBD (Functional Block Diagram) with several restrictions in the data types, operations, etc. in order to be compliant with the requirements for LVL (Low Variability Language) defined by the IEC 61511. In addition, PLC brands normally oblige the PLC programmer to manually write the PLC safety program on their own pro-

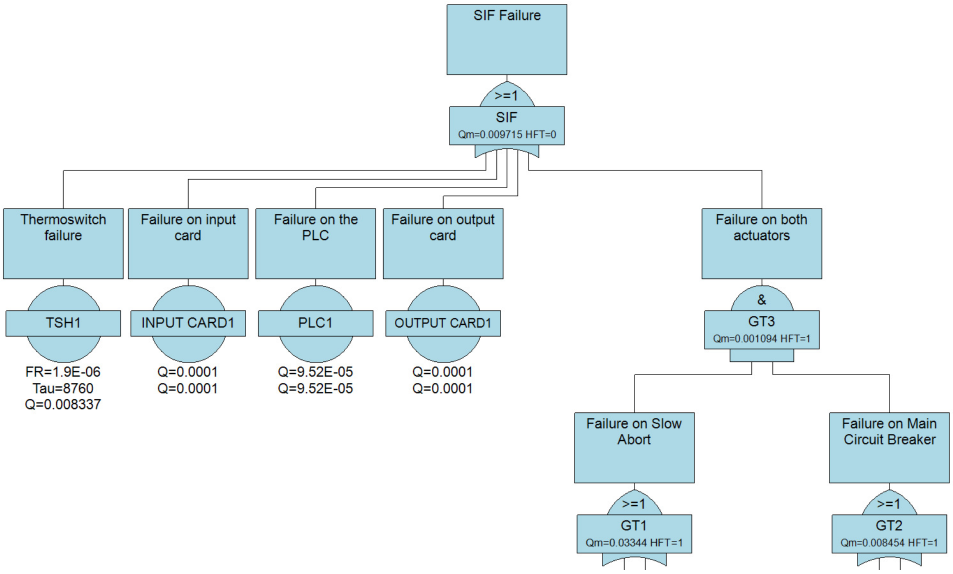


Figure 3: Fault Tree developed with the Isograph’s Reliability Workbench.

[1] https://new.siemens.com/global/en/products/automation/industry-software/automation-software/tia-portal/software.html

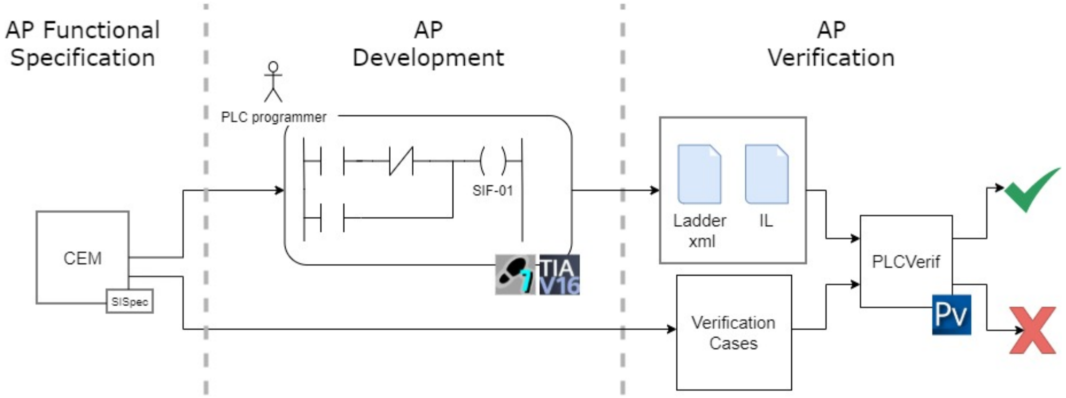


Figure 4: Specification, development and verification of the SIS AP.

gramming environment. This is the case for Simatic Step7 from Siemens. However, in their latest programming environment tool, TIA portal, it is possible to generate the AP source code from external tools, import it in TIA portal, compile it and produce a safety AP. This feature opens the door to automatic code generation of the PLC APs.

The verification phase consists of testing and reviewing the AP in order to confirm that the AP implementation corresponds to the AP design, and that there are no unintended states. In our case, in addition to the FAT (Factory Acceptance Test) activities (requirements defined in 61511-1:2016 Clause 13), we apply model checking to our Safety PLC programs, as recommended in Annex B (section B.4.3). By applying model checking, all combinations of the AP are checked to guarantee that the SIF logic from the specification (CEM for example) is respected in the implementation. For that purpose, we use the open-source tool PLCverif[2], developed at CERN [5]. An example of how PLCverif is applied to a safety PLC program can be found in [6].

Figure 4 illustrates these three phases and associates them with the software tools we use in the development.

SISpec, Grassedit, PLCverif and Isograph can contribute to improve the reliability of the SIS. They are also compliant with the IEC 61508-3:2010 Clause 7.4.4.2 ”Software offline support tools shall be selected as a coherent part of the software development activities”. Therefore, it is certainly in the best interest of CERN to use these already available tools.

MANAGEMENT OF THE FUNCTIONAL SAFETY PROJECT

Management of functional safety projects is probably the most critical activity based on our experience. The requirements are described in IEC 61511-1 Clause 5. At CERN, typically the following roles are defined for each functional safety project:

- A functional safety expert: person with a deep knowledge and experience in applying the functional safety standards. The main activities of this role are the specification, design and validation of the SIS to be compliant with the risk reduction stated in the risk assessment. This person also participates in the risk analysis phase.
- A process expert: person with an excellent knowledge of the industrial process. The main activities of this role are to provide the operational requirements, contribute to the risk analysis and participate in the commissioning and validation of the SIS.
- The Departmental Safety Officer (DSO): person in charge of defining the tolerable risk levels and provide support to the project members in any safety matter. The main activities of this role are to conduct the risk analysis, define the tolerable risk level, as well as participate in the validation of the SIS.
- Health & Safety and Environmental Protection (HSE) unit representative: person that normally participates in the most safety-critical systems at CERN in coordination with the DSO and provides support in safety matters.
- Instrumentation and control experts: people in charge of selecting the hardware equipment for the SIS (sensors, final elements and controller), according to the SRS document, as well as implementing the AP.

In addition, for the Functional Safety Assessment (FSA), an external person to the project must be included in the FSA team. Moreover, an independent person to the project must conduct the Safety Audit.

Reporting

Documentation is an important part of the management of these projects. At CERN, report templates were created to cover different phases of the safety life-cycle. One of the most important and problematic aspects of the documentation is to keep the traceability between the documents of the project. For example, when a SIF specification is modified in the SRS, the proof testing document should be updated. We have created templates for the following reports: Hazard and risk assessment, SRS, FSA, proof testing and the safety manual. Traceability is currently maintained manually by the functional safety expert, but this is a topic taken into consideration for future work.

[2] https://gitlab.com/plcverif-oss/cern.plcverif

Table 9: Tools, Methods and Report Templates for Our Functional Safety Projects

Safety life-cycle phase	Tools	Methods	Report templates
H&R assessment	-	FMEA and calibrated risk graph	Risk assessment report
SRS	SISpec and Grassedit	CEM and Logic Diagrams	SRS report
Design and engineering	Isograph, PLCverif and UNICOS (future work)	FTA, RBD, model checking and FAT	Design and verification report
Validation	-	-	Proof test
Management	-	-	FSA and safety manual

CONCLUSIONS

This paper shares our experiences in the design, development and management of functional safety projects that are based on the IEC 61511 standard.

The challenges and the adopted solutions for some of the most critical phases of the safety life-cycle have been discussed. Table 9 summarizes the current solutions adopted for our functional safety projects. In general, we have worked in two main topics:

1. The creation of report templates compliant with the standard. For example, the risk analysis and assessment, the SRS, the proof tests, etc. These templates help us to standardize our projects and speed up the creation of the necessary reports.

2. The integration of external tools that can contribute to improving the reliability of the final SIS and speed up the development, maintenance and verification time. This is the case of the CERN tools, PLCverif, SISpec and Grassedit and the commercial tool, Isograph.

Future Work

In general, we have faced the optimization challenge individually for each of the phases of the safety life-cycle. As mentioned previously in this paper, an unsolved challenge is to be able to keep traceability in an automatic way. We will explore the possibility of using commercial tools (e.g. exSILentia®) that tackle the problem of traceability and management of changes. We will also evaluate the possibility of developing our own tool that would be able to integrate all our templates, generate automatically an important part of our reports, integrate our existing tools and guarantee the traceability of the project.

In terms of management, we are currently working on the optimization of the workflow of our projects, defining more precisely the different roles and responsibilities of the different groups involved in a functional safety project.

Finally, we want to go a step further in the design and development of the SIS AP. At CERN, we have a large number of control and safety systems and we are always looking for the standardization of our PLC programs and supervision interfaces. For that purpose, we will aim to create a new component of the UNICOS[3] framework that is able to generate automatically the SIS AP from a formalized specification, respecting the IEC 61511 guidelines.

[3] https://unicos.web.cern.ch

REFERENCES

[1] "Functional safety - safety instrumented systems for the process industry sector," International Electrotechnical Commission, Geneva, CH, International Standard, 2016. https://webstore.iec.ch/publication/24241

[2] "Functional safety of electrical/electronic/programmable electronic safety-related systems," International Electrotechnical Commission, Geneva, CH, International Standard, 2010. https://webstore.iec.ch/publication/5515

[3] S. K. Hurst, H. Boukabache, and D. Perrin, "Overview of a Complete Hardware Safety Integrity Verification According to IEC 61508 for the CERN Next Generation of Radiation Monitoring Safety System," 5 p, Oct. 2020. http://cds.cern.ch/record/2771471

[4] B. F. Adiego *et al.*, "Cause-and-Effect Matrix Specifications for Safety Critical Systems at CERN," in *Proc. ICALEPCS'19*, (New York, NY, USA), ser. International Conference on Accelerator and Large Experimental Physics Control Systems, JACoW Publishing, Geneva, Switzerland, Aug. 2020, pp. 285–290, ISBN: 978-3-95450-209-7. DOI: 10.18429/JACoW-ICALEPCS2019-MOPHA041.

[5] E. B. Viñuela, D. Darvas, and V. Molnár, "PLCverif Re-engineered: An Open Platform for the Formal Analysis of PLC Programs," in *Proc. ICALEPCS'19*, (New York, NY, USA), ser. International Conference on Accelerator and Large Experimental Physics Control Systems, JACoW Publishing, Geneva, Switzerland, Aug. 2020, pp. 21–27, ISBN: 978-3-95450-209-7. DOI: 10.18429/JACoW-ICALEPCS2019-MOBPP01.

[6] B. Fernández Adiego, I. D. Lopez-Miguel, J.-C. Tournier, E. Blanco Vi nuela, T. Ladzinski, and F. Havart, "Applying model checking to highly-configurable safety critical software: the SPS-PPS PLC program," presented at the 18th International Conference on Accelerator and Large Experimental Physics Control Systems (ICALEPCS 2021), Shanghai, China, Oct. 2021, paper WEPV042, this conference.