Technical Paper

Functional Safety Update

IEC 61511 Edition 2 Standards Update

Functional Safety Update

Table of Contents

IEC 61511 Edition 2 Standards Update

1.0 Introduction

Purpose

The purpose of this standards update is to provide a notification from ABB's Safety Lead Competency Centre (SLCC) in order to highlight the changes that have been agreed to be made to IEC 61511 Edition 1 as an Edition 2 version. It is a summary of what is considered by the ABB SLCC to be the most significant changes. Note that not all changes have been included and some changes, which are deemed significant for the SLCC, might not be considered as important as other updates in the revised standard.

Status of the standard

As on the date of this notification, IEC 61511 Edition 2 Part 1 has been published in February 2016. The IEC 61511 maintenance committee have also completed Parts 2 and 3. These two parts have now been published as of July 2016.

General

Changes have resulted from comments provided by National Committees and User Groups. The Edition 2 standard also clarifies the relationship with IEC 61508 Edition 2. IEC 61511 Edition 2 Part 1 contains normative requirements only. Part 2 provides guidelines for the application of Part 1. Part 3 provides guidance for the determination of the required safety integrity level (SIL). Note that this document focuses mainly on Part 1.

2.0 IEC 61511-1 changes

Management of functional safety
The second edition requires a formal procedure to be in place to manage the competence of all those involved within the safety instrumented system (SIS) lifecycle. Such competency assessment process shall be documented. Additionally, periodic assessments shall be carried out to document the competence of individuals.

It should be noted that if a supplier makes any functional safety claims for a product or service, then they shall have a compliant functional safety management system (FSMS) in place. End users should therefore seek assurances that this is the case for any safety related products or solutions being provided by the supply chain.

Also note that in support of FSMS, there are defined requirements to undertake a periodic functional safety assessment (FSA) which shall be performed during the 'operations and maintenance' lifecycle phase.

The SIS software, hardware and procedures used to develop and execute the application program shall be subject to configuration management and shall be maintained under revision control.

Process Hazard & Risk Assessment
A security risk assessment on the SIS and associated equipment is now required. It shall result in a description of the devices covered by this risk assessment and provide a description of the potential threats to security during the different phases of the design, operation and maintenance lifecycles, together with potential consequences resulting from such security events (including likelihood). Part of this assessment process is to identify requirements for additional risk reduction together with the measures to be taken to reduce or remove the potential threats.

Allocation of safety functions
The results of the allocation process shall be recorded. The safety instrumented functions (SIF) of the process shall be described, e.g., the actions to be taken, set points, reaction times, activation delays, fault treatment, valve closure requirements.

This description shall be in an unambiguous logical form and shall be referred to as the process requirements specification or the safety description. The process requirements specification is used as input information for the safety requirements specification (SRS) and shall be sufficiently detailed to ensure adequate specification of the SIS and its devices.

If it is intended not to qualify the basic control system (BPCS) to the IEC 61511 standard, then two BPCS functions may be given credit (RRF=<10) for the same hazardous event. They could be: a single BPCS protection function in the case of a demand caused by a BPCS control function or two BPCS protection functions in the case of a demand caused by a non BPCS element e.g. alarm function and control function. It shall be noted that BPCS functions designed to be separate and independent (sensors, input cards, processor, output cards and final element).

SIS safety requirements specification
Note that there are a number of additional requirements added to the list of requirements (now 29 topic areas) in the SRS content; and in particular:

- a list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification (e.g., field tag list);
- requirements relating to proof test implementation

There is also a modified bullet point from Edition 1 regarding bypass functionality and is as follows:

- the SRS shall also include requirements for which procedure (written procedure) is to be applied during the bypassed state

Application program safety requirements
Section 10.3.5 identifies a number of modified Edition 1 clause 12.2.2 content and grouped with additional requirements for application program as indicated below:

- acceptable real time performance in the presence of faults,
- program sequencing and time delays if applicable;
- the requirements for communication interfaces, including measures to limit their use and the validity of data and commands both received and transmitted;
- process dangerous states (for example closure of two valves at the same time that could lead to a dangerous state) generated by the application program that shall be identified and avoided;
- definitions of process variable validation criteria for each SIF.

SIS design & engineering

In terms of hardware fault tolerance (HFT) requirements, the revised requirements are now based only on the type of device (A or B type) and the target SIL. The safe failure fraction (SFF) concept has been abandoned in IEC 61511 Edition 2. The new requirements for architectural constraints can be seen in Table 1 below. The route now developed within IEC 61511 has been derived from 'Route 2H' of IEC 61508-2:2010.

SIL	Minimum required HFT
1 (Any mode)	0
2 (Low demand)	0
2 (High and continuous demand)	1
3 (Any mode)	1
4 (Any mode)	2

Table 1. Hardware Fault Tolerance – IEC 61511 Edition 2

Also note that clause 11.9 now improves the clarity on the relationship between random failure and the SIF probability of failure calculation and specifically focuses on both probability of failure on demand (PFD) and architectural constraints as there may have been a misconception that the calculation of SIF probability of failure (dependent only on random failure) was directly related to the calculated failure rate only.

In other words, it now clarifies that the quantification of random failure is not just the PFD calculation alone, but architectural constraints and the additional requirements for systematic capability aspects also need to be considered (refer to Clause 11.5.2.1).

A "systematic capability" concept has been included within IEC 61511 Edition 2 and has been further aligned to IEC 61508 Edition 2 requirements. The main intent of the 'prior use' evaluation has also been better expressed i.e. 'is to gather evidence that the dangerous systematic faults have been reduced to a sufficiently low level compared to the required safety integrity'. The previous edition was not clear in this area.

A safety manual is required for elements that are proven by 'prior use'. This now means all SIS devices shall have a safety manual. A safety manual shall cover operation, maintenance, fault detection and constraints associated with the SIS, the intended configurations of the devices and the intended operating environment.

Quantification of random failure

The reliability data used when quantifying the effect of random failures shall be based on field feedback from similar devices used in a similar operating environment. The reliability data uncertainties shall be assessed and taken into account when calculating the failure measure. Additional requirements have been added for what to be considered when calculating the failure measure of a SIF e.g. the requirement for proof test coverage which should be identified with the compliant device safety manual i.e. the assumption of 100% proof test coverage.

SIS application program development

The term "application software" has been replaced by "application programs" (AP). Requirements have been streamlined and made more relevant for LVL and FPL rather than FVL. Many of the AP requirements content has been relocated from clause 12 into those lifecycle clauses that the AP addresses (mainly clause 6 and 10). Many AP requirement clarifications have been added during this process.

The application program (AP) shall be designed in such a way as to ensure that once the SIS has placed the process in a safe state, the process remains in the safe state, including under loss of power conditions and on power restoration, until a reset has been initiated unless otherwise directed by the SRS.

Factory Acceptance Test (FAT)

A dedicated Factory Acceptance Test shall take place. New requirements have been added for FAT planning.
A FAT is required to perform:

- performance tests (to determine if the system meets timing, reliability and availability, integrity, safety targets and constrains)
- internal checks (Internal data flow checks can be carried out to that the SIS is processing input data and generating output response as specified.)
- environmental tests (EMC life- and stress-testing)
- testing for safe reaction in case of power failure (including restart after power restored)

There are also additional requirements that sensor and final element configurations shall be checked for appropriateness during this stage of the design & engineering lifecycle (Note Edition 1 referred to the logic solver only.)

It is now also required to consider the hazards posed by testing especially dealing with stored energy and to record results and observations whilst the test is being conducted.

SIS operation and maintenance

Persons responsible for operations and maintenance shall review the hazard and risk analysis, allocation and design to ensure the assumptions made are valid e.g. assumptions on occupancy and corrosion protection.

A new requirement is added for those responsible persons (this could be either the duty holder or their nominated supply chain partners) to identify spare parts in order to minimise the 'bypass duration' due to the potential non-availability of the hardware parts of the SIS.

A new requirement has been introduced to highlight the need for additional measures or constraints to be applied if a non-fault tolerant subsystem is taken offline during maintenance. This is consistent with the requirements when failures in non-fault tolerant systems are detected. The maximum time the SIS is allowed to be in bypass (for repair or testing), while safe operation of the process is continued, shall be defined. Continued process operation with a SIS device in bypass shall only be permitted if a hazards analysis has determined that compensating measures are in place and that they provide adequate risk reduction.

The compensating measures required depend on: SIL, the tolerable risk associated with the hazardous event, the hardware fault tolerance of the SIS, the anticipated mean repair time (MRT) and the availability of any other layers of protection etc. In some cases, it can be adequate for an action to be taken to ensure repair of the dangerous failure within the assumed maximum permitted repair time (MPRT) in the calculation of the PFDavg, but in other cases it can be deemed necessary to provide other measures to compensate for the reduced risk reduction until the SIS is fully restored.

In addition, new requirements have been added for suitable management procedures to be applied to review deferrals and prevent significant delay to proof testing

Modification

A new requirement has been added. Modification activities shall not begin until a functional safety assessment is completed in accordance with clause 5. The FSA (Stage 5) shall be done by an independent person. It should be noted that every change to the SIS (covering the subsystem and/ or components, hardware and software (application program) is a modification unless a 'like for like' replacement in kind is performed.

Also there is a new clause covering the requirements that an FSA shall also be carried out periodically during the operations and maintenance phase to ensure that maintenance and operation are being carried out according to the assumptions made during design and that the requirements within IEC 61511 for safety management and verification are being met.

3.0 IEC 61511-2 changes

Part 2 remains as an informative part of the standard. However, significant additions have been made to a number of content sections. Note that some of the informative text originally found in Part 1 of the standard has been moved into Part 2. This section of the standard also consists of more examples and general explanations and therefore the number of pages have increased from 80 to 190.

4.0 IEC 61511-3 changes

A number of new annexes have been added. The content has been reworded to achieve improved clarity. A new clause (4.6) has been added to explain the commonly used terms in general use within Part 3.

A figure below is intended to illustrate the difference between the terms by showing the progression from hazard to abnormal situation on loss of control through hazardous event after protection measures failed to hazardous situation if a person is in the hazardous zone and to the occurrence of harmful event if a person is unable to escape consequences.

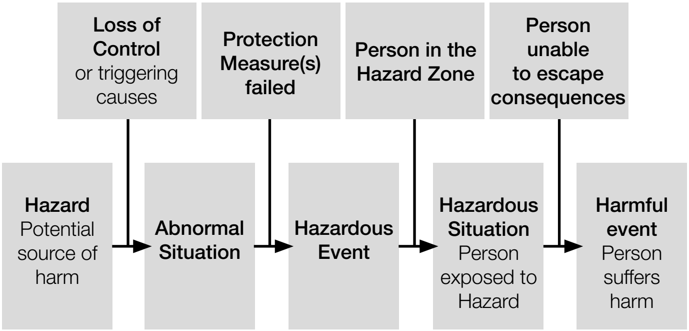
Loss of Control or triggering causes
Protection Measure(s) failed
Person in the Hazard Zone
Person unable to escape consequences
Hazard Potential source of harm
Abnormal Situation
Hazardous Event
Hazardous Situation Person exposed to Hazard
Harmful event Person suffers harm

Figure 1. Harmful event progression

5.0 IEC 61511 Edition 2 and impact on FSMS - summary

In the SLCC's opinion many significant changes have been agreed for the issue of IEC 61511 Edition 2.

The changes are primarily aimed at improving the quality of all lifecycle activities. In doing so, the wording of numerous clauses within the standard has been changed to achieve additional clarity and many of the previous contents comprising "should" have now been changed to "shall" within this new edition.

The second edition also puts more emphasis on the 'competency of persons' and introduces additional clarity for the systematic capability concept. Hardware fault tolerance requirements have been simplified and the safe failure fraction concept has been abandoned. The requirements for hardware reliability calculations are now more robust in terms of the quality of input data which is required and as such, aims at a more conservative approach of the failure rate calculation methods to be utilised.

It is also recognised that a functional safety cyber security lifecycle process must also be implemented for SIS.

The revised standard also requires the persons 'responsible for operations and maintenance' to review all design assumptions and to ensure they are valid. This is in addition to implementing an FSA by an independent person (to be performed periodically) during the operation lifecycle phase and before each SIS modification is actually implemented.

It is envisaged that the changes make the standard simpler in interpretation, but more exacting in requirements.

6.0 References

1. IEC 61511-1 Edition 2.0 2016-02 Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements
2. IEC 61511-1 First edition 2003-01 Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements

ABB SLCC July 2016.
Rafal Selega ABB, SLCC Functional Safety Consultant

Contact us

ABB Limited
Howard Road, Eaton Socon
St Neots
Cambridgeshire
PE19 8EU
Phone: +44 (0)1480 475321
E-Mail: oilandgas@gb.abb.com

www.abb.com

Notes:
We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

Printed in UK (10.2016)