IEC TR 61511-4

Edition 1.0 2020-02

TECHNICAL REPORT

Functional safety – Safety instrumented systems for the process industry sector – Part 4: Explanation and rationale for changes in IEC 61511-1 from Edition 1 to Edition 2

IEC TR 61511-4:2020-02(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC®

IEC TR 61511-4

Edition 1.0 2020-02

TECHNICAL REPORT

Functional safety – Safety instrumented systems for the process industry sector –
Part 4: Explanation and rationale for changes in IEC 61511-1 from Edition 1 to Edition 2

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110, ICS 25.040.01

ISBN 978-2-8322-7870-3

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

Part 4: Explanation and rationale for changes in IEC 61511-1 from Edition 1 to Edition 2

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a Technical Report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 61511-4, which is a Technical Report, has been prepared by subcommittee 65A: Systems aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this Technical Report is based on the following documents:

Draft TR	Report on voting
65A/911/DTR	65A/920A/RVDTR

Full information on the voting for the approval of this Technical Report can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the 61511 series, published under the general title *Functional safety – Safety instrumented systems for the process industry sector*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

IEC 61511 (all parts) addresses safety instrumented systems (SIS) for the process industry sector. It is written to use terminology that is familiar within this sector and to define practical implementation requirements based on the sector-independent clauses presented in the IEC 61508 basic safety standard. IEC 61511-1 is recognized as a good engineering practice in many countries and a regulatory requirement in an increasing number of countries.

Nevertheless, standards evolve with the application experience in the affected sector. The second edition of IEC 61511-1 was edited based on a decade of international process sector experience in applying the requirements of the first edition of IEC 61511-1:2003. The changes from Edition 1 to Edition 2 were initiated by comments from National Committees representing a broad spectrum of users of the standard worldwide.

In Edition 1:2003 (Ed. 1)[1], the requirements addressing the avoidance and control of systematic errors that occur during design, engineering, operation, maintenance and modification were adapted primarily to support independent safety functions up to a SIL 3 performance target. In contrast, Edition 2:2016 (Ed. 2) needed to address a prevailing trend of sharing automation systems across multiple safety functions.

Ed. 2 also needed to address the common misinterpretations of the Ed. 1 requirements that became evident to the IEC 61511 maintenance team (MT 61511) over the intervening years. For example, Ed. 2 reinforced the necessity to design for functional safety management rather than a narrow focus on a calculation and to manage the actual performance of the SIS over time.

IEC TR 61511-4 was created to provide a brief introduction of the above issues to a general audience, with the more detailed content remaining in the main parts of the IEC 61511 series. IEC TR 61511-4 describes the underlying rationale of the primary clauses in IEC 61511-1, clarifies some common application misconceptions, provides a listing of the main differences between the first and second editions of IEC 61511-1, and gives a brief explanation of the typical process sector approaches to the application of each primary clause.

[1] For ease of reading, "Ed. 1" and "Ed. 2" will be used in this document.

FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

Part 4: Explanation and rationale for changes in IEC 61511-1 from Edition 1 to Edition 2

1 Scope

This part of IEC 61511, which is a Technical Report,

- specifies the rationale behind all clauses and the relationship between them,
- raises awareness for the most common misconceptions and misinterpretations of the clauses and the changes related to them,
- explains the differences between Ed. 1 and Ed. 2 of IEC 61511-1 and the reasons behind the changes,
- presents high level summaries of how to fulfil the requirements of the clauses, and
- explains differences in terminology between IEC 61508-4:2010 and IEC 61511-1 Ed. 2.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050-192, *International Electrotechnical Vocabulary (IEV) – Part 192: Dependability* (available at http://www.electropedia.org)

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61511-1:2016, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements*
IEC 61511-1:2016/AMD1:2017

ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC Guide 51, IEC 60050-192, IEC 61508-4 and IEC 61511-1 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.2 Abbreviated terms

Abbreviated terms used throughout this document are given in Table 1. Also included are some common abbreviated terms related to process sector functional safety.

Table 1 – Abbreviated terms used in IEC TR 61511-4

Abbreviated term	Full expression
AIChE	American Institute of Chemical Engineers
ANSI	American National Standards Institute
BPCS	Basic process control system
CCPS	Centre for Chemical Process Safety (AIChE)
Ed.	edition
FAT	Factory acceptance test
FMEA	Failure mode and effects analysis
FMEDA	Failure modes, effects, and diagnostic analysis
FPL	Fixed program language
FSA	Functional safety assessment
FVL	Full variability language
HFT	Hardware fault tolerance
H&RA	Hazard and Risk Assessment
HAZOP	Hazard and Operability Study
HMI	Human machine interface
IEC	International Electrotechnical Commission
IPL	Independent protection layer
ISA	International Society of Automation
ISO	International Organization for Standardization
LOPA	Layers of protection analysis
LVL	Limited variability language
MOC	Management of change
MooN	“M” out of “N” channel architecture
MPRT	Maximum permitted repair time
MRT	Mean repair time
MTTR	Mean time to restoration
NP	Non-programmable
PE	Programmable electronics
PES	Programmable electronic system
PFD_{avg}	Average probability of dangerous failure on demand
RRF	Risk reduction factor
SAT	Site acceptance test
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SRS	Safety requirement specification

4 Background

The document structure chosen by the original IEC 61511 team did not provide sufficient details for clarity on the intent or rationale behind the creation or modification of a clause. There is a need to provide an explanation of the changes, provide the rationale behind each clause of the standard, and provide introductory information into functional safety in the process industry.

This document helps improve the implementation of the requirements contained within IEC 61511-1 Ed. 2 across the industry by providing an overview of “what”, “why”, and “how”. With this summary, newcomers to functional safety should find an easy way to understand the underlying concepts behind the clauses of the standard.

5 Management of functional safety (IEC 61511-1 Ed. 2 Clause 5)

5.1 Why is this clause important?

Management of functional safety addresses systematic failures, mostly caused by humans, that are not quantifiable as mathematical models. These activities, covering the whole safety lifecycle, are applied through processes and procedures.

Functional safety cannot be implemented without the involvement of humans as the personnel involved in the safety lifecycle activities of an operating company, engineering company, vendor or anybody who interacts with the safety system. In this multi-disciplinary environment, all the activities need to be clearly identified and assigned to people. This will increase the probability that nothing is left off the task list and ensure that there will be a responsible person for every task.

To increase the success rate in each task, IEC 61511-1 requires competency for all personnel in their assigned SIS safety lifecycle responsibilities. Both responsible and accountable people are included. The accountable person is the individual who is ultimately answerable for the activity or decision. Only one accountable person can be assigned to an action. The responsible person is the individual(s) who completes the task.

There is a distinction between FSA and functional safety audit. FSA is a detailed review of all the aspects of a specific stage of the safety lifecycle. The timing of the separate FSA-1, 2, and 3 aligned with different project milestones is based on where the work would be performed most cost-effectively, as opposed to a single FSA performed at the end of the project. Functional safety audit on the other hand, reviews information, documents, and records to determine whether the functional safety management system is in place.

5.2 Common misconceptions

There is a misbelief that the IEC 61511-1 management system and design requirement rigor for SIL 1 is less important than for SIL 3. The high-level functional safety management systems (such as qualification, management of change, assessment, and auditing) in IEC 61511-1 are the same and aim to avoid or control systematic errors. While not encouraging the implementation of safety and non-safety functions in the same system, some aspects of SIS functional safety management could be used favourably for critical non-safety systems like asset protection systems.

Project teams desire for readily implementable solutions sometimes results in a “checklist mentality” (creating a list of project deliverables to check off without ensuring effective content). Management systems are “living” systems that need ongoing upkeep to remain effective. The content of these systems is used to facilitate correct operation, maintenance, change management and auditing of the safety systems over time.

There is often a desire to defer consideration of performance monitoring and ongoing functional safety management to after project start-up. While these responsibilities ultimately fall upon the owner/operator, capabilities needed to sustain this activity are best incorporated into the project design through a multi-disciplined approach to ensure successful pre-start-up reviews and avoid costly rework after start-up.

The simple lifecycle example depicted in the standard is not sufficiently detailed for implementation directly in the plant. A company implementing a detailed lifecycle model will need to account for its unique organizational structure. The safety plan covering that facility should include the additional details necessary for sustainable installation within that organization, such as specific roles and responsibilities.

5.3 What was changed from Ed. 1 to Ed. 2 and why?

5.3.1 Existing systems

With Ed. 2, a new functional safety management requirement regarding the acceptability of existing systems implemented per Ed. 1 (or prior standards) was deemed necessary and appropriate for the scope of the standard. This concept is sometimes referred to as "grandfathering". Commonly this has been misunderstood to mean that nothing needs to be done to manage these systems. Thus, the terminology of "existing systems" was used in the new Subclause 5.2.5.4. Existing systems and practices are evaluated to ensure functional safety can be achieved. This necessitates at least a risk assessment and then evaluation of each IPL to prevent and mitigate the assessed risks. This new subclause also triggered a revision to Clause 17 regarding the modification of such existing systems.

Modified clause: 17.2.3.

New/rewritten clause: 5.2.5.4.

5.3.2 Change management

Since existing systems tend to be changed piece by piece, further clarity was needed on how to handle such changes using the functional safety management system, including change impact analysis and FSA, as part of change management. This includes changes that affect the requirements on an existing SIS.

New/rewritten clauses: 5.2.6.1.9, 5.2.6.2.5 (see also Clause 17 of this document).

5.3.3 Performance metrics and quality assurance

A common concern in SIS design is the use of overly optimistic data that is not applicable to the operating environment the SIS will be used in. However, even if data and assumptions appropriate for a given operating environment are used in the initial SIS design, variations in the performance of the process, operations, maintenance, and automation management systems over time can result in poor system performance and inadequate risk reduction. The primary practice specified in the standard for determining actual achieved risk reduction and restoring is to collect performance data on an ongoing basis, periodically assess for conformance to the H&RA and SRS requirements (that is, periodically perform FSA stage 4), and correct deviations as needed. The expectations of performance monitoring and quality assurance are consistent with basic process safety management regulations, such as the USA CFR 1910.119(j), UK Control of Major Accident Hazards (COMAH), Dangerous Substances and Explosive Atmospheres Regulations (DSEAR), and European Community Annex III to Council Directive 2012/18/EU, and international industry standards (e.g., ISO 14224).

Modified clauses: 3.2.51, 5.2.5.3, 16.2.2.

New/rewritten clauses: 5.2.6.1.10, 11.4.9, 11.9.4, 16.2.9.

5.3.4 Competency

SISs tend to be changed and interact less frequently than BPCSs. Without refresher training and ongoing practical experience, initial competency is likely to degrade over time. Particularly common areas where this has been an issue are the qualification of providers of SIS design services and the performance of H&RA and SRS development by personnel who lack training and demonstrated competence in both loss prevention and IEC 61511-1 requirements. Therefore, a competency management system is required.

Modified clauses: None.

New/rewritten clause: 5.2.2.3.

5.3.5 More requirements for functional safety product and service providers

To ensure functional safety products and service providers have the capabilities for achieving the required SIL and systematic capabilities, in addition to the quality management system, these providers are now required to have a functional safety management system.

Modified clauses: None.

New/rewritten clause: 5.2.5.2.

5.4 Summary on how

Every SIS project has clear roles and responsibilities. All involved parties are aware of their responsibilities and are competent to fulfil the related activities necessary for functional safety. Competencies are kept up to date. All necessary activities in a project are described in a safety plan which can be a project specific one or a general company specific document. For all relevant activities, an FSA is carried out to demonstrate that a SIF fulfils all requirements and is compliant with the agreed standards. Performance management during operation is done by collecting field data for SIS reliability and SIS process demand information. Functional safety audits are done at regular intervals to demonstrate that the involved organizations remain capable of fulfilling the defined functional safety requirements. Assessment and auditing activities are done by individuals independent of the project team. Meaningful documentation of the assessment and audit results is generated and recommendations tracked for effective closure.

6 Safety life cycle (IEC 61511-1 Ed. 2 Clause 6)

6.1 Why is this clause important?

To ensure functional safety can be achieved, several activities (most of the time by different stakeholders, e.g. end user, engineering company, vendors) need to be accomplished. All these activities are connected to each other like a chain and the strength of this chain will be only as strong as the weakest link. It is crucial to consider functional safety as a lifecycle which starts with hazard identification and ends with decommissioning of SISs, not as individual and separated activities. All activities in the safety lifecycle are impacted by upstream and downstream activities.

6.2 Common misconceptions

In addition to the need for organization-specific detailed content in the safety plan, project teams not experienced in the safety lifecycle often do not understand and plan for the iterative nature of H&RA, SRS development, and SIS design. This can potentially lead to unexpected re-work and increased costs. If individual project disciplines are trained too narrowly, necessary interactions can be overlooked.

6.3 What was changed from Ed. 1 to Ed. 2 and why?

The SLC clause was updated to address all activities, particularly application programming. Material was incorporated from Clause 12 into Clause 6 regarding application programming. See also 12.3 of this document for additional content regarding movement of application program related content.

6.4 Summary on how

During the planning phase, a high-level workflow SIS safety lifecycle is defined. In the next step, a detailed activity list including development of application software and other work processes are generated. The lifecycle includes inputs and outputs for each activity, procedures and processes on how to perform the activity and finally responsible organization/people for doing them.

7 Verification (IEC 61511-1 Ed. 2 Clause 7)

7.1 Why is this clause important?

Phase by phase review, analysis, and/or testing will reduce systematic errors and find possible problems and errors in time for cost effective correction. This clause defines the minimum aspects of verification planning. Specifically, verification using testing involves several detailed tasks to ensure the test will reveal any errors.

7.2 Common misconceptions

People might think verification and validation are the same thing, leading to one of them being omitted. Similarly, there is misunderstanding that verification is only done as part of the FAT or a pre-startup safety review, instead of being done consistently throughout the lifecycle.

7.3 What was changed from Ed. 1 to Ed. 2 and why?

Requirements for verification that involves testing, ensuring non-interference from non-safety functions is confirmed, and applying impact assessments to changes identified during verification were added. The updates also require modification carried out during testing to be re-verified.

Modified clauses: 7.2.1, 7.2.6 (was 7.1.1.2),

New/rewritten clauses: 7.2.2, 7.2.3 and 7.2.5,

7.4 Summary on how

A test and review plan for each activity, including development of an application program and of the safety lifecycle, is generated. This plan includes how to perform the test or review, and success criteria for meeting the requirement of each activity.

8 Hazard and risk analysis (IEC 61511-1 Ed. 2 Clause 8)

8.1 Why is this clause important?

The process H&RA evaluates the process design to identify the hazardous events, design limits, potential causes, and protection for these events. The H&RA develops the basis for the functional safety of the process. Hazard analysis is important in identifying the specific hazards of the process and identifying how much protection is needed for the specific events. Included in this clause is security analysis to address cyber and physical security.

The failure frequency related to failures originating in the BPCS, along with any risk reduction allocated to BPCS protection layers (see 9.3.1 of this document regarding BPCS protection layers), directly impact the risk reduction target and the mode of operation for an associated SIF. Therefore, IEC 61511-1 Ed. 2 limits (based on long-standing process industry consensus) what failure rate can be claimed for the BPCS.

8.2 Common misconceptions

Personnel executing H&RA via process hazards analysis methods (HAZOP, FMEA, What If?) often fail to recognize the requirement to specify the SIF mode of operation and the required SIL. Additionally, personnel often lack the skills to properly perform these tasks due to their lack of understanding of BPCS, SIS and SIL assignment methodologies (such as LOPA, Risk Graph, Risk matrix, as described in IEC 61511-3) often leading to poorly executed H&RA processes and allocation of instrumented protection layers.

One common misconception is that IEC 61511-1 does not include requirements for the H&RA or instrumented protection layers with an RRF of 10 or less. Because of the direct and unavoidable impact that the BPCS failures and other instrumented protection layers have on the SIF specification and design, these requirements were considered indispensable and were included in the H&RA and allocation clauses.

Another misconception is that the frequency limit for failures of a BPCS as an initiating source is specifically for the BPCS hardware (or even just the controller itself). A BPCS, as defined in IEC 61511-1 Ed. 2, includes all the devices necessary to ensure that the process operates in the desired manner, with the specific exception of the devices executing SIFs (that is, the SIS). In applying the frequency as intended (roughly once in ten years), it is important to understand that the failure rate performance of a BPCS is typically dominated by the frequency of human error (such as controllers being left in a manual mode, unmanaged change to program settings, or operating outside the limits assumed in the original process design).

H&RA teams that do not involve a person with competency in functional safety in the process typically underestimate the long-term costs and complexity of SIS lifecycle activities. This leads to a failure to consider other methods of risk reduction, resulting in additional SIFs or alarms instead of making the design inherently safer, using pressure safety valves, or using passive safeguards that would have a lower long-term cost of ownership. Also, the consequence of not performing the H&RA work at the right time is often underestimated.

H&RA is usually iterative work, which is often not understood or reflected in the project schedule and staffing plan. For example, projects using vendor packages commonly deliver functional safety information later than needed for the specific project activity or might not use H&RA approaches that are consistent with the safety philosophy of the facility. This can result in additional verification reviews and assessments (see Clause 5 of this document).

One of the misconceptions about H&RA is to only focus on normal process operating mode, forgetting about other operating modes such as, start-up, shutdown, maintenance, process upset, and emergency shutdown. Experience shows that most incidents arise outside normal operating modes.

8.3 What was changed from Ed. 1 to Ed. 2 and why?

With continued occurrences of cyber security events within industrial automation control and safety systems throughout the industrial world and more frequent installations of SIS with digital communication capability to other devices, high level security requirements have been added to Ed. 2. It is not the scope and intention of IEC 61511-1 to put additional detailed requirements on the security lifecycle model. IEC 61511-1 clarifies that safety can only be achieved, considering security threats, by close coordination between concerned disciplines under general engineering management. Ed. 2 clarifies which minimal security activities are to be performed to ensure security for the SIS is addressed without duplicating the necessary security means or objectives as this is the scope of dedicated documents such as IEC 62443 (all parts). The new clauses include a security risk assessment including the SIS to be performed and that the SIS be designed to provide the necessary resilience against, and ongoing management of, security risks (see also Clause 10 of this document).

New/rewritten clause: 8.2.4.

8.4 Summary on how

An H&RA on the process should be performed during front-end engineering and re-validated after detailed engineering. Clauses 8 and 9 work together to define the risk reduction required and the protection layers to close any gaps between the risk inherent in the process and the tolerable risk established by the authority having jurisdiction. Examples of how this might be performed are provided in IEC 61511-3. A security analysis including the SIS is also performed as defined in 8.2.4. The notes in 8.2.4 provide examples of how to perform the analysis. Gaps identified during these analyses are documented and resolved before start-up of the new or modified process.

9 Allocation of safety functions to protection layers (IEC 61511-1 Ed. 2 Clause 9)

9.1 Why is this clause important?

Not all safeguards will be adequate to provide the risk reduction required for a given hazardous event. Lack of independence between protection layers can result in significant gaps in risk reduction. This clause defines some requirements for safety functions and how they are allocated to protection layers, including an evaluation of common causes, limitations on BPCS layers, and understanding the impact of diversity, separation, and independence.

9.2 Common misconceptions

Dependency between the protection layers and the initiating source is often assumed to be negligible. This is often related to insufficient functional safety documentation or H&RA process. Similarly, limitations of existing equipment such as devices being in an inaccessible location or having known performance problems are often not considered during assignment of risk reduction targets to safeguards. Finally, teams often overlook the potential lack of independence of BPCS protection layer’s and overestimate the risk reduction from the BPCS.

Another misconception is that a BPCS protection layer and the BPCS are terms that can be used interchangeably. The BPCS is the total system of devices (such as field instruments, controllers, auxiliary systems and HMIs) that are used to safely operate the plant, except for the SIS. A BPCS protection layer would be the specific independent mechanism (BPCS device or set of BPCS devices) within the BPCS to implement a safety function. With sufficient independency between the BPCS protection layers, the BPCS can support up to two such BPCS protection layers.

It is frequently thought that IEC 61511-1 only applies to preventive safeguards. The lifecycle requirements of IEC 61511-1 apply also to protection layers which mitigate the consequence of a hazardous event and are based on instrumented functions with a specified requirement of SIL 1 or above in the process hazard analysis. Some examples include fire and gas detection systems and initiation of water curtains. Risk reduction verification for these systems includes analysis of detector coverage and mitigation effectiveness in addition to the sensor, logic solver, final element, and auxiliary system hardware contributions to failure. Performance of mitigating safeguards beyond a risk reduction of 10 is relatively difficult to achieve.

9.3 What was changed from Ed. 1 to Ed. 2 and why?

9.3.1 Limits on BPCS protection layers

The failure frequency claimed for initiating sources related to the BPCS control loop failure and the risk reduction allocated to BPCS protection layers, such as typical safety alarms, directly impact the risk reduction target and the operating mode for an associated SIF. Experience using Ed. 1 revealed that the previously existing two clauses (Ed. 1 Subclauses 9.4.2 and 9.4.3) were not sufficiently clear in expressing the following limitations intended by the committee:

- maximum risk reduction that could be claimed for a protection layer within the BPCS,
- maximum number of independent protection layers that could be executed within the BPCS for a given hazardous event,
- requirements for independence for protective layers executed within the BPCS.

These limitations reflect the overall performance impact associated with the less rigorous design, implementation, and management practices typically applied to the BPCS (as compared to those used to manage the SIS). The values provided in Ed. 2 for each of these limitations are consistent with evolving best practice as documented in other recent process industry consensus publications such as the CCPS Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis published in 2014.

Key points to remember are:

a) If a BPCS protection layer is being claimed for an RRF > 10, all the relevant requirements of IEC 61511-1 apply to the subsystem executing that protection layer (that is, the safety function is a SIF).

b) If a particular hazardous event involves two BPCS functions (whether as initiating source or protection layer(s)), the systems executing those functions would either be independent or the shared subsystems would follow the requirements of IEC 61511-1 appropriate for the total reduction in consequence frequency (that is, the shared subsystem is actually a SIS subsystem).

Modified clauses: 3.2.3, 8.2.2, 9.3.2, 9.3.3.

New/rewritten clauses: 9.3.4, 9.3.5.

9.3.2 Requirements for claiming RRF > 10 000 in total for instrumented safeguards

The underlying reason for the change is that while Ed. 1 provided requirements for a single function of SIL 4, it was felt that Ed. 2 should address overall risk reduction of 10 000 regardless of whether this was for a single function, or multiple functions in different protection layers. When a high level of risk reduction (RRF > 10 000) is identified to be provided by the SIS or SIS in conjunction with BPCS, the H&RA team should reconsider inherently safer design or other layers of protection (e.g. relief valves, passive barriers, administrative access controls) to reduce the risk. While a SIL 4 function or an overall RRF of 10 000 can be mathematically achieved, experience in the process sector is that the systematic aspects of implementing such high levels of risk reduction make it extremely difficult (and very expensive) to achieve and even more difficult to maintain. Even when the risk reduction allocation is spread over multiple protection layers with independent primary safety system devices (sensors, logic solvers, final elements), common personnel are often used to program, operate and maintain the instrumented safeguards. If RRF > 10 000 remain after the inherently safer analysis for instrumented protection functions, more advanced analyses for random and systematic error are needed.

Modified clauses: 9.2.5.

New/rewritten clauses: 9.2.6, 9.2.7.

9.4 Summary on how

A risk analysis on the hazardous events (see examples in IEC 61511-3) is performed to meet the tolerable risk requirements established by the appropriate authority or legal framework.

One output of this is to select the safety functions and allocate them to protection layers to reduce the risk to a tolerable level. An analysis on the safety functions and protection layers is used to verify the overall risk reduction is credible and sustainable. This analysis includes many factors, such as the independence, diversity, common cause, integrity provided, auditability, testability, and separation between layers. If the overall risk reduction allocated to instrumented safeguards exceeds 10 000, a careful analysis should be made of the assumptions relating to the efficiency and independence of the IPL's (of each other and the initiating event). An overall quantitative analysis should include the impact of dependency if this is identified. This analysis should be performed at the time of the H&RA as well as at the end of the detailed design of the functions.

10 SIS safety requirements specification (IEC 61511-1 Ed. 2 Clause 10)

10.1 Why is this clause important?

Every SIF needs a clear and traceable requirement specification as a basis for the development of the SIS. Performance requirement elements that are documented in the SRS, including bypass philosophy, testing philosophy, approved device criteria, and response time of the SIF, provide crucial inputs for efficient SIS design. The SRS describes the required functionality and reliability as well as the requirements for the application program.

The purpose of the SRS is to serve as baseline documentation for the development of the SIS and specifies the functional and safety integrity requirements for all SIFs that are to form part of the SIS. The SRS is used for transposing requirements into SIS hardware design and application program development. It is also used for SIS validation purposes and can facilitate the preparation of procedures for SIS operation, maintenance, proof testing, and operator response on SIF failure. The SRS is living documentation which is to be updated if any modification to the SIS arises. In order to support future change management and other functional safety management activities, the intent and approach used to derive the SRS specification details will also be needed.

10.2 Common misconceptions

While key items in SRS are derived from the H&RA and risk allocation documentation, it would be a misinterpretation to understand that all the content of the SRS comes from H&RA documentation. For example, IEC 61511-1 Ed. 2, 9.2.9 requires the functional needs of the plant process to be specified and documented. This process requirement specification is later used as an input for the SRS preparation.

The SRS provides functional and safety integrity requirements for all SIFs of the SIS. Meeting the minimum content requirements of the SRS provides a specification requirement document, not a detailed design document. In this case, more documentation will be needed to generate a sufficient design. For example, lack of additional application programming requirement documentation can result in a program that does not meet the defined SRS functional requirements such as the behaviour needed under device fault conditions. Additional requirements for SIS hardware design and application program development might be addressed in the safety manuals, operating manuals for logic solver and SIS devices, SIS design practices, instrument installation guidelines, regulatory requirements, and relevant general industry standards. It should also be noted that SIS design documentation includes those requirements for non-safety functions which are part of the SIS (not addressed by the SRS).

There are common misunderstandings regarding who is supposed to develop SRS content (wrongly thought to be the responsibility of a single discipline) and by when, frequently resulting in missing content or documentation of the SRS as an as-built (reversing the intended order of design basis development and the implementation).

A misperception that the SIS will always work can result in insufficient planning in the sections of the SRS addressing manual stop, survival of a serious event, or compensating measures.

10.3 What was changed from Ed. 1 to Ed. 2 and why?

Experience using Ed. 1 revealed that the SRS and the instrument selection justification are sometimes written in highly technical language that might not be maintainable, verifiable, or understandable by operations and maintenance, but which was considered compliant with Ed. 1. For example, it could not always be determined that the information used in the instrument selection and system design was even relevant to the operating environment for that installation. As the clarity and applicability of this information is essential to achieving and maintaining the expected performance of the safety function, further recommendations and requirements were provided. For example, requirements relating to proof test implementation and coverage, range and accuracy of SIS process measurements, leakage rate for valves, written procedures for managing bypasses, and application program safety requirements were added.

Modified clauses: 7.2.1, 10.2, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6.

New/rewritten clauses: 11.5.2.2, 11.9.2, 11.9.3, 16.2.13.

10.4 Summary on how

Defining the requirements of a SIF is one of the most important activities. Only a complete and measurable SRS guarantees the proper design, implementation and testing of a SIF. A complete SRS covers all functional, safety and reliability aspects as well as testing and diagnostics requirements. This can be done in different formats, but a form based on a checklist format has proven itself. The main input in an SRS comes from the process/technology department and operations and is predominantly an outcome of the H&RA phase.

11 Design and engineering (IEC 61511-1 Ed. 2 Clause 11)

11.1 Why is this clause important?

Designing a SIS involves controlling the effects of random hardware failures and avoiding or controlling systematic failures. The activity can mainly be summarized to the following four parts:

i) Select devices appropriately (based on prior use or in accordance with IEC 61508-2).

ii) Ensure minimum redundancy determined by HFT, either in accordance with the process sector approach defined in IEC 61511-1 or per IEC 61508-2.

iii) Design the architecture and application program to meet the requirements of the SRS and verify the specified performance objectives for integrity, reliability, and systematic error control have been met (including aspects such as human capabilities, bypass management, diagnostic coverage, common cause failures, proof test interval, MTTR).

iv) Ensure adequate demarcation between the SIS and the BPCS for both hardware and application program so that the overall risk reduction performance is achieved.

Clause 11 gives the design and engineering requirements for SIS hardware, whereas Clause 12 gives the corresponding requirements for the application program.

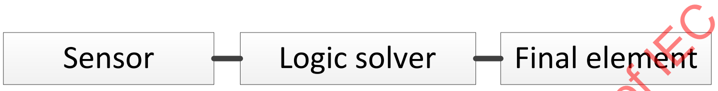
11.2 Common misconceptions

There are multiple requirements to fulfil in SIS design. Teams commonly focus on the SIL calculation and pay insufficient attention to the predicted reliability of the system and the systematic design requirements such as the importance of using field devices with successful prior use in a similar operating environment and meeting the specified HFT requirements. In performing the SIL verification, lack of understanding of how device diagnostics will be used can result in optimistic calculations.

In addition, teams can incorrectly use reliability parameters from safety manuals without considering the impact of the application on how that data should be used. Some differences that can influence the correct use of the safety manual information include fail-open versus fail-closed designs, use of diagnostics in the architecture, and the performance impacts of process or environmental effects. Similarly, there is a misunderstanding that the use of an IEC 61508 device eliminates the requirement for the facility to assess the suitability of the device in the operating environment. For this reason, new/modified clauses explicitly require the collection of reliability data based on field feedback from similar operating environments.

Teams often incorrectly correlate the SIL of the individual devices, such as the logic solver, to the achieved SIL. The SIL performance requirement applies to the entire function, not to individual devices. While all devices used in the SIS are selected as being appropriate for use in an application of that SIL (otherwise referred to as “fit for purpose”), the achieved SIL of the function will be dependent on many factors, such as fault tolerance, reliability, and desired test interval.

Example: Two alternate designs are being evaluated for a SIS specified to meet SIL 2 requirements based on the risk reduction allocated to the SIF. In both cases, each subsystem PFD_{avg} contribution falls within the SIL 2 or better range. However, in case 1, the total value exceeds the upper limit, resulting in an overall SIL 1 performance.



	Sensor		Logic solver		Final element			
Case 1	4E-3	+	5E-4	+	8E-3	=	<u>12.5E-3</u>	(> 1E-2)
Case 2	2E-3	+	5E-4	+	4E-3	=	6.5E-3	(< 1E-2)

Designers also should keep in mind that for devices selected based on IEC 61508 conformance, the associated safety manual might require additional redundancy beyond the minimum necessary to achieve the SIL.

11.3 What was changed from Ed. 1 to Ed. 2 and why?

11.3.1 Hardware fault tolerance

Prescriptive HFT limits were created in Ed. 1 to mitigate some of the more common design and implementation systematic failures:

- using overly optimistic reliability parameter assumptions,
- maintenance error such as leaving a root valve closed or a bypass jumper in place.

In Ed. 1, field devices and logic solvers had different requirements for HFT because field devices were low complexity devices and logic solvers were high complexity devices. However, there were some issues experienced with implementing HFT using Ed. 1 (such as reducing HFT based on “safe-failure-fraction”).

Ed. 2 allows for three different methods to determine HFT:

- Use IEC 61511-1 Ed. 2, Table 6 in conjunction with requirements under IEC 61511-1 Ed. 2, Subclauses 11.4.5 to 11.4.9.
- Use Route 1_H of IEC 61508-2:2010, based on FMEDA analysis and conformance with related clauses in IEC 61508-2:2010.
- Use Route 2_H of IEC 61508-2:2010, based on product returns to the manufacturer and conformance with related clauses in IEC 61508-2:2010.

IEC 61511-1 Ed. 2, Table 6 and Subclauses 11.4.5 to 11.4.9 were derived from IEC 61508-2:2010 route 2_H and present simplified HFT requirements, based on SIL and mode of operation of the SIF. For example, 11.4.9 specifies an upper bound statistical confidence limit of no less than 70 % instead of the 90 % required by Route 2_H on the basis that failure rates are justified by sufficient evidence from prior use in a similar environment and an existing system of maintenance, repair and renewal practices.

IEC 61511-1 Ed. 2, Table 6 was developed with the intention that it could be used for determining minimum HFT, regardless of the process used to approve the use of devices (Subclause 11.5). It is important to note that use of IEC 61511-1 Ed. 2, Table 6 is only appropriate if Subclauses 11.5 to 11.9 of IEC 61511-1 Ed. 2 (such as Subclause 11.5.2.2 confirming that the device is suitable for the environment) are also followed. For example, a minimum diagnostic coverage was established for devices using LVL software or FVL software. Given the conformance with these other clauses, a separate table for programmable devices (such as logic solvers) was no longer needed. Likewise, designs for SIL 4 application are addressed in Ed. 2, but have specific additional requirements provided in Clauses 9 and 12.

In addition, clauses were added indicating when certain faults may be excluded from the HFT analysis. If an element of a system has a very low probability of random failure due to properties inherent to its design and construction, then it might not be necessary to constrain the safety integrity of the function based on redundancy of that element. For example, for a redundant logic solver input card and redundant processor arrangement, the single channel terminals connection might not be a significant contributor to dangerous failures. Another example might be a cabinet being shared between redundant channel IO cards or logic solver processors.

Modified clauses: 11.4.3, 11.9.3 to 11.9.5.

New/rewritten clauses: 11.4.1, 11.4.2, 11.4.4 to 11.4.9, 11.9.2.

11.3.2 Security risk requirements

With increasing security concerns surrounding SISs, a security risk assessment clause was added, with the corresponding requirement to add resilience against the identified security risk into the design. (see also Clause 7 of this document).

New clause: 11.2.12.

11.3.3 Safety manual

In Ed. 1, the necessity of developing a safety manual was determined in a complicated way based on the SIL of the application, the type of devices (with application program or not) and the type of the programming language (FPL, LVL, or FVL). The content addressing operation, maintenance, fault detection, and implementation constraints was needed for all systems. This requirement was simplified in Ed. 2, which necessitates a safety manual for the SIS, regardless of the technology or SIL involved.

New clause replacing multiple prior ones: 11.2.13.

11.3.4 Requirements for system behaviour on detection of a fault

Ed. 1 provided three clauses, each describing specific cases involving fault tolerance, no fault tolerance and continuous demand, all of which still achieved a common objective. These three cases do not cover all possible cases, so in Ed. 2 this was simplified to two clauses where the specific objectives are defined, which would apply to any SIF implementation.

New/rewritten clauses: 11.3.1 and 11.3.2.

Deleted clause: 11.3.3 (merged into 11.3.1 and 11.3.2).

11.3.5 Limitations on field device communication design

The Ed. 1 clause requiring dedicated wiring for field devices was removed based on improvements in instrumentation and communication technology (such as the development of safety fieldbuses) and to avoid technology-specific prescriptive requirements.

Deleted clause: 11.6.3.

11.4 Summary on how

The design process is intended to ensure that the SIF functionality defined in the SRS is met. This process also ensures conformance with any requirements from device safety manuals, independence requirements, and the ability for SIFs to be tested.

The design decisions, such as device/technology selection, subsystem interconnection information, how faults are detected, how the architecture meets HFT requirements, how SIFs are tested, how systematic errors are addressed, and how the design will meet or exceed the target integrity requirements, are clearly documented. For example, how detected faults are to be enunciated, how they should be responded to (such as whether there will be an automated response or a manual one), and what system(s) are used to execute this response would be explicitly documented. This documentation is used in the verification of the design prior to implementation, the verification and validation of the implementation prior to the hazard being present, and the periodic assessment of performance during operation. One of the key output documents from the design process is the safety manual which addresses the specific operation and maintenance requirements for the SIS to be implemented.

Unchanged from the first edition of IEC 61511, prior use (such as adequate experience based on logic solver complexity and considering other factors like installation environment) can be used to approve the use of safety-configured general-purpose logic solvers up to SIL 2 (but not SIL 3). Due to the level of performance required, SIL 3 (or higher) logic solver capability analysis requires more specific practices that are provided in IEC 61508 (all parts).

12 Application program development (IEC 61511-1 Ed. 2 Clause 12)

12.1 Why is this clause important?

The paradigm of IEC 61511 versus IEC 61508 is to put requirements on the goals to be achieved instead of requiring the application of methods and techniques to achieve the same goals. In IEC 61511-1 there is no gradation of the application program design objectives as the standard is designed to consistently produce a compliant application program for functions up to and including SIL 3.

IEC 61511-1 is thus designed to be efficient within the defined constraints. These constraints include:

- use of LVL,
- use of simple applications for which it is expected that LVL technology will provide reasonable protection against systematic errors that can occur during application program development.

These limits are detailed in IEC 61511-2:2016, Annex E and G.

It is necessary to have a procedure for consistently developing the application program. Depending on the complexity of the software, including the degree of flexibility of the programming language and the familiarity of the application programming and operations teams with that language, different steps might be included in the application program development procedure. The minimum steps are application program specification, realization, and verification.

While IEC 61511-1 Ed. 2 includes SIL 4, the application programming requirements for this SIL are referred to IEC 61508 (all parts) to avoid duplication of the requirement details.

12.2 Common misconceptions

A common misunderstanding is that verification of a SIS is limited to a check of the hardware or simple tests of functionality. Application program/configuration verification is also required, which might involve more complex activities such as dynamic versus static behaviour analysis and proof of absence of dangerous variable combinations.

12.3 What was changed from Ed. 1 to Ed. 2 and why?

In Ed. 1, the provisions related to SIS application programming were gathered in Clause 12. With the rest of the document being structured in the order of the safety lifecycle, this led to confusion regarding when the application programming activities were to take place during the execution of a project. In addition, some of these activities would have an impact on both the hardware and application program design or implementation.

In Ed. 2, Clause 12 was revised significantly for many reasons, one of which was to better facilitate the required verification activities and FSA. Some provisions have been relocated from Clause 12 to provide clearer guidance on when the activity should be executed. For example, application program safety requirements have been incorporated into the main SRS requirements to emphasize the need for a close relationship between the SIS SRS and the application program safety requirements.

Other clauses include requirements that the application program be designed in a way that facilitates traceability to the requirements of the standard (including the SRS), which results in a program that is easy to read and understand.

Modified clauses: 6.2.1, 7.2.1, 10.3.2, 17.2.3.

Relocated clauses (with or without additional modification): 5.2.7.2, 6.3.1 to 6.3.3, 7.2.2 to 7.2.3, 7.2.5, 10.3.3 to 10.3.6.

12.4 Summary on how

Much like Clause 11, the application program design process is intended to ensure that the design meets the SIF functionality defined in the SRS, any requirements from device safety manuals, independence requirements including both safety and non-safety systems, and any specific application software requirements from the SRS.

The design decisions, such as language selection, modularity of the application program, application program flow, variable definitions, how the application program is to be verified, and how systematic errors are addressed should be documented so that the design can be verified against the SRS prior to implementation. The application program is documented to provide traceability back to the SRS and to support maintainability for the operational phase of the lifecycle.

13 Factory acceptance test (IEC 61511-1 Ed. 2 Clause 13)

13.1 Why is this clause important?

Historically, FATs have been a contractual part of capital projects in the process industry. Therefore, when a FAT is required per safety planning, Clause 13 provides requirements to establish a consistent structure for performing a FAT. A FAT is a way of achieving some elements of verification and validation (Clauses 7 and 15) in a more controlled factory environment where it is easier and more cost effective to correct failures or errors, rather than addressing them after the system has been delivered and installed in the field.

13.2 Common misconceptions

It is not always understood that a FAT is only required if it has been specified as part of the testing activities identified in the safety planning.

Misunderstanding the limited scope of a FAT, some teams can confuse this activity with validation and attempt to eliminate the latter from the schedule. FATs can be part of validation but cannot meet all of the validation requirements.

Another misconception is that there is no purpose in FATs for modification projects. In some cases where SIFs are being added to an existing SIS, it might not be possible to conduct a comprehensive system FAT. However, it can be possible to test individual components prior to validation testing. The advantage of a FAT for system components/subsystems in this scenario is to minimize down time and/or risk of spurious trips during validation testing prior to placing the new or modified SIF in service.

A FAT might not always be a single activity. Multi-stage FATs are becoming more common in larger projects. An application FAT can be conducted separately from a hardware test. Similarly, communication integration testing is commonly performed separately.

13.3 What was changed from Ed. 1 to Ed. 2 and why?

In principle, the intent between Ed. 1 and Ed. 2 regarding FATs has not changed. However, in Ed. 1, since in planning you could decide to or not to perform a FAT, Clause 13 was written as informative. In Ed. 2, the decision was to make more explicit that the Clause 13 content for performing the FAT is required if the FAT is chosen by planning. Therefore, all the subclauses have been changed from “should” to “shall”.

Minor edits to 13.1, 13.2.1 to 13.2.7.

13.4 Summary on how

The FAT procedure documents the scope of the FAT, including the tools necessary to execute the procedure. In addition, the functional safety plan developed per Clause 5 will document the location of the FAT and the resources allocated to the execution of the FAT. The project schedule will typically document when it is executed. A final approved report documents the execution of the FAT, including findings and the evidence of correction.

14 Installation (IEC 61511-1 Ed. 2 Clause 14)

14.1 Why is this clause important?

This clause addresses the handling of SIS components from the point of their arrival on site, to installation, and commissioning to confirm that the components are ready for validation testing. Systematic errors during installation can result in SIF failure. For example, incorrectly installed winterization measures can lead to plugging of impulse lines or tubing. SIS components are typically installed according to design and installation drawings; however, there are times when changes need to be made in the field. For example, the instrument air supply to the valve needs to be routed to another instrument air manifold. These changes should be reviewed by a competent person who can assess the impact of the change on the SIF and the SIS.

Commissioning of intelligent field devices is an important activity as it verifies that the device has been properly calibrated and configured. Process parameters, for example specific gravity of the service fluid, are critical for correct operation of the field device and the intended operation of the SIF.

14.2 Common misconceptions

The terms commissioning and mechanical completion for a SIS are often misunderstood and misrepresented in the project schedule. For example, do loop checks occur before or after mechanical completion? The requirements in this clause provide a list of typical commissioning activities.

14.3 What was changed from Ed. 1 to Ed. 2 and why?

There are no significant changes to this clause. Minor edits to 14.1, 14.2.2 to 14.2.5.

14.4 Summary on how

Installation is typically done by contractors; hence it is critical to clearly communicate commissioning and change management procedures for SIS components. It is essential to install SIS components based on design and installation documents as a significant number of systematic failures of SIS occur due to improper installation of SIS components. Any deviations should be reviewed by a qualified person to confirm that the changes do not impact functional safety requirements specified in the SRS.

Commissioning plans should be developed in conjunction with the other project disciplines. For example, SIS components can be impacted by hydro testing of pipes. Commissioning of smart field devices should include verification of configuration parameters, such as the specific gravity of the process fluid for a differential pressure level transmitter. Resource plans should include expertise in communication with other systems as interfaces to other systems are typically tested for the first time during commissioning.

15 Validation (IEC 61511-1 Ed. 2 Clause 15)

15.1 Why is this clause important?

Validation testing is the last activity to occur prior to putting the SIS and associated SIFs into service in an operating environment. SIF validation testing is an end-to-end testing that verifies that all components, including application program, are functioning in a manner that meets the intent of the SRS. This is also the last opportunity to detect any failures prior to putting the SIS in service.

15.2 Common misconceptions

Partial credit can be taken for FATs as part of validation testing; however, validation testing cannot be eliminated from the schedule based on a FAT. A FAT typically tests one or more SIS components in a factory environment; however, it is not a substitute for validation testing which verifies that the integrated system is functioning satisfactorily in the field.

Another misunderstanding is that the safety lifecycle activities end at validation (which might be referred to as a SAT) or plant start-up. As per Ed. 1, Figure 8 and Ed. 2, Figure 7, the lifecycle does not stop here, but moves into operations, maintenance, and decommissioning.

15.3 What was changed from Ed. 1 to Ed. 2 and why?

No new subclauses have been added. Additional bullets were added under 15.2.1 relating to the equipment required to facilitate periodic testing, and 15.2.2 for validating documents for accuracy, consistency and traceability.

Minor edits to clarify intention to 15.2.1, 15.2.2, 15.2.4 to 15.2.8.

15.4 Summary on how

Validation testing tends to get rushed if other project disciplines are running behind schedule; however, it is important to allow sufficient time to validate the installed and commissioned SIS.

Credit can be taken for FATs; however, aspects of the integrated system that cannot be tested during a FAT are included in the validation test plan. Examples include overall function response time, correct connectivity and configuration of the individual devices in the production system, and confirmation that non-interferences were not compromised in the as-built system.

Validation plan should take into consideration changes made during installation and commissioning. For example, a robust validation procedure should reveal systematic errors such as the hydraulic system used for a SIS valve actuation being operated at a lower pressure than design specification. Any changes to the SIS during validation testing should be reviewed by a qualified person to confirm that the changes do not impact functional safety requirements specified in the SRS and all changes are tested.

Pre-start-up safety reviews (including FSA stage 3) should verify that all SIFs are operational, including ensuring that bypasses/forces have been removed and instrument isolation or sampling valves are in the correct position.

16 Operation and maintenance (IEC 61511-1 Ed. 2 Clause 16)

16.1 Why is this clause important?

Clause 16 addresses the operational and maintenance aspects of safety lifecycle and their impacts on SIL during operation as well as maintenance to ensure the required safety integrity is sustained with operational time and is managed accordingly during maintenance time.

16.2 Common misconceptions

Maintenance is not just about performing a full functional test. Nor does executing full functional tests ensure that overall safety performance is satisfactory. Inspection and preventive maintenance are essential to achieving the expected performance from the SIS devices. Periodic performance monitoring and corrections of identified discrepancies are used to ensure the functional safety objectives are achieved.

The operation and maintenance plan cannot be standardized independently of SIL and related maintenance features of each SIF. The operations and maintenance plan, procedure and reliability data gathering are incorporated in a new or modified design to ensure these tasks can be done without inconsistencies, re-work, or excessive cost.

Another point of confusion regarding maintenance is related to facilities desiring a long test interval. SIS devices that are not able to be proof tested at the design frequency due to production availability requirements are not fit for purpose. An existing system that cannot be tested to achieve the design SIL needs redesign. Automated diagnostic testing and reporting can help but are not a replacement for proof testing and recommissioning after testing. Devices for which imperfect proof testing cannot be avoided are replaced or rebuilt as new at an interval determined to be necessary to achieve the specified SIL.

Another common misconception is that management procedures are not needed for replacement-in-kind maintenance or that management of change is not needed for minor instrument changes or changes to SIS operations and maintenance procedures. Indeed, both are necessary to sustain the achieved performance over time. For example, analysis of the risk reduction lost when a maintenance bypass is used is performed to address any potential degradation using compensating measures.

Many misconceptions exist regarding proof testing devices or subsystems following repair of a broken device, modification of the installation, or when there is some amount of diagnostic or partial testing being done. In all these cases, proof testing is still a necessary part of ensuring that dangerous undetected failures, both random and systematic, are detected and corrected in a timely manner.

16.3 What was changed from Ed. 1 to Ed. 2 and why?

16.3.1 Fault detection, bypassing, and compensating measures

One common underlying SIS design assumption is that a SIS device will be out of service due to bypass or detected failure for a limited time and that compensating measures will be used to manage any gap in risk reduction during that time. Experience since Ed. 1 has exposed a lack of clarity regarding these basic expectations of managing known periods of SIS unavailability or degraded performance. To ensure operational response to faults and failures and the use of bypasses will be sufficient and timely, these actions need to be accounted for in the hazard analysis, design, and operations and maintenance planning, such as the spare parts program. Likewise, basic mechanical integrity principles indicate that data needs to be collected on the reliability parameters so that performance can be evaluated. Evaluation of this data can identify installations that need correction or possible opportunities to improve the installation costs. Operations and maintenance need procedures on how to perform these activities.

Modified clauses: 16.2.1, 16.2.3, 16.2.6, 16.2.9 and 16.2.10.

New/rewritten clauses: 3.2.7, 11.3.1, 11.3.2, 11.8.4, 11.8.5, 16.2.4, 16.2.7, 16,2,12 and 16.2.13.

16.3.2 Proof testing after repair and change

To address the common misconceptions noted above, clauses were modified to reinforce the expectations of testing after repair and modification of either the device or the application program, and that procedures for the process of approving deferrals were needed.

Modified clauses: 16.3.1.3, 16.3.1.4 and 16.3.1.6.

New clause: 16.3.1.7.

16.4 Summary on how

The operation and maintenance of a SIS are planned in the design phase before the operation of the SIS. For the safety systems to remain effective and risks to be managed, operation and maintenance personnel are expected to clearly understand the hazards that exist in the facility and to perform the activities required of them per the defined safety planning, such as being prepared to perform activities necessary to implement compensating measures when the SIS has a detected failure or bypass. The operators and maintenance personnel are given the necessary information in written procedures and are trained to keep the safety integrity of all the functions in the specified level. The procedures are made for them to carry out operation and maintenance activities per the safety plan, including compensating measures that ensure continued safety while the SIS is disabled or degraded due to bypass, repair or testing.

17 Modification (IEC 61511-1 Ed. 2 Clause 17)

17.1 Why is this clause important?

If modification is not planned, assessed, reviewed, approved and documented, there is a higher likelihood of negative impacts on the performance of the SIS and on other aspects of the safety lifecycle.

17.2 Common misconceptions

The objectives of Clause 17 clarify that, prior to making a change impacting the SIS, a functional safety impact analysis is done and safety planning is developed for implementing the change. This impact analysis is not only with SIS and/or facility engineers who will make the modification, but also with applicable H&RA team members, which might include additional roles such as operation personnel, process engineers, and instrumentation engineers. If there were to be an impact on functional safety, the assessment of the change and the management of change procedures would further identify the appropriate safety-lifecycle phase(s) and activities to be redone before the change is implemented. A change impact analysis should also be performed during the project design and implementation phases if changes are being proposed to approved deliverables from prior project phases.

Some facilities mistakenly believe that H&RA and SRS documents only need to be updated for an audit or other safety review, instead of as part of ongoing change management. In addition, MOC practices might be omitted for changes made to the application program after successful verification is complete, such as changing trip points or diagnostic settings. Similarly, replacement of a field device with a device not fully meeting the SRS requirements and thereby not meeting the “replacement in kind” criteria, can be missed by some MOC programs. The analysis of the change can also mistakenly focus on the SIF being changed without evaluating the impact of changes to other safeguards or critical control loops.

17.3 What was changed from Ed. 1 to Ed. 2 and why?

Planning for and completing change

To address the above misconceptions, clauses were modified and created to ensure that proactive planning for modification exists, that the change impact on safety is understood before the change is executed, and that documentation is fully updated with the change (see also Clause 4 of this document).

Modified clauses: 17.2.3 and 17.2.6.

New/rewritten clauses: 17.2.4 and 17.2.5.

17.4 Summary on how

Modifications are carried out in accordance with an authorization procedure. The scope of modification is developed, along with a related safety plan that addresses the functional safety impact of the proposed change, including risk assessment, impacts on other functions and personnel, safety integrity before and after modification, SRS modifications, and documentation. The safety plan is documented, reviewed, and approved prior to authorization. Modification is performed by qualified people. Appropriate information is kept and related documentation updated. The above activities are also carried out for simple changes to ensure that no risks arise from the change. For simple changes, the effort for the assessment will usually be small.

18 Decommissioning (IEC 61511-1 Ed. 2 Clause 18)

18.1 Why is this clause important?

If decommissioning is not planned, assessed, reviewed, approved, and documented, there is a higher likelihood of negative impacts on the performance of the SIS and on other aspects of the safety lifecycle.

18.2 Common misconceptions

As part of the ongoing change management, one common misconception would be to omit decommissioning changes made only to the application program, such as deleting the program for a decommissioned SIF while leaving the field devices in place for other uses. The analysis of the change can also mistakenly focus on a SIF being decommissioned without evaluating the impact on the SIS design caused by decommissioning other safeguards or critical control loops. For example, decommissioning utility control or safety functions in one plant can have a functional safety impact on plants sharing that utility.

Another common misconception regarding decommissioning is that it is suitable to only partially perform the work of removing the SIS. Examples might include simply converting subsystems to energize-to-trip and then de-energizing them, removing the devices in the field while leaving them in the engineering documentation, or by removing the function and devices from hazard analysis and engineering/configuration documents without removing the devices from the field, HMI, or control cabinet. This incomplete work can create potential new sources of failure and impair the effectiveness of future management of change efforts.

18.3 What was changed from Ed. 1 to Ed. 2 and why?

18.3.1 Planning for and completing change

To address the above misconceptions, clauses were modified and created to ensure that proactive planning for decommissioning exists, that the change impact on safety is understood before the change is executed, and that documentation is fully updated with the change (also see Clause 4 of this document).

Modified clauses: 18.2.1, 18.2.3, 18.2.4 and 18.2.5.

18.4 Summary on how

Decommissioning is carried out in accordance with an authorization procedure. Scope of decommissioning is developed, along with a related safety plan that addresses the functional safety impact of the proposed change, including risk assessment, impacts on other functions and personnel, SRS modifications, and documentation. This safety plan is documented, reviewed, and approved prior to authorization. Decommissioning is performed by qualified people. Appropriate information is kept and related documentation updated.

19 Documentation (IEC 61511-1 Ed. 2 Clause 19)

19.1 Why is this clause important?

Across the safety lifecycle, there are several stakeholders involved that are responsible for performing different activities. These activities need some information from previous activities. Flow of information and availability of documentation is essential for success of each activity. Upon completion of activities, records need to be retained for future access and traceability.

19.2 Common misconceptions

A common misconception about documentation is that SIS information should be in a single document, a single folder, or in a single document management system. The key requirement is traceability to the SIS functional and integrity requirements.

19.3 What was changed from Ed. 1 to Ed. 2 and why?

Some of the requirements for documentation became normative (using “shall” instead of “should”). In addition, the safety manual was added to the list of documents.

Modified clauses: 19.2.2, 19.2.9.

19.4 Summary on how

Several disciplines and departments are involved in developing “SIS related” information during the different phases of the SIS lifecycle, and the information can be stored in different document management systems. A common method is to have a document that outlines the structure of the SIS related information and provides a link/pointer to the location where the relevant information is stored. For example, the SRS can be in the SIS folder on the site document management system, and the proof test records are available in the site maintenance management system.

20 Definitions (IEC 61511-1 Ed. 2 Clause 3)

20.1 Why is this clause important?

It is critical that users of the standard understand the terminology used and why definitions sometimes differ from other standards, such as IEC 61508 (all parts).

20.2 Common misconceptions

One common misconception is that the definitions in IEC 61511 (all parts) are required to be identical to those in IEC 61508 (all parts). In general, the definitions in IEC 61511-1 Ed. 2 should be equivalent to those in IEC 61508-4:2010. However, due to the significant difference in context between IEC 61511 (all parts) and IEC 61508 (all parts), there are situations where a difference in the definition or the terminology within the definition was deemed necessary to be suitable to the process sector.

The definitions within IEC 61508-4:2010 are at times necessarily written at a high conceptual level or using generic technical terminology. This is to ensure the content remains applicable to all the sectors that fall under the scope of this basic safety standard. As a result, some of the definitions in IEC 61508-4:2010 use language that is not sufficiently common in the process sector. This leads to confusion for the IEC 61511 target process sector audience. To prevent misunderstanding, IEC 61511-1 Ed. 2 modified or added notes to these terms.

Some terms used in IEC 61511-1 Ed. 2 were not defined in IEC 61508-4:2010.

Where deviation from IEC 61508-4:2010 was deemed necessary, the committee preferentially used applicable definitions from material in the ISO/IEC Guide 51:2014, IEC 60050-192 (dependability section of IEC 60050), or similar standards.

20.3 What was changed from Ed. 1 to Ed. 2 and why?

Table 2 lists all the terms defined in IEC 61511-1 Ed. 2. The third column of this table indicates whether one or more changes were made to the technical terminology in the definition from IEC 61511-1 Ed. 1. The fourth column describes the basic safety standard alignment approach taken for each term, including why the definition differs from the referenced source definition. As the rationale for definitions in IEC 61511-1 Ed.2 is in the context of the source definitions that are being aligned to, no further explanation is provided here regarding changes between IEC 61511-1 Ed. 1 and Ed. 2.

Table 2 – Rationale for IEC 61511-1 Ed. 2 terms and definitions

IEC 61511-1 Ed. 2 Term number	Term	Definition different between IEC 61511-1 Ed. 1 and Ed. 2?	Rationale for IEC 61511-1 Ed. 2 Definition
3.2.1	architecture configuration	Yes	Same as IEC 61508-4:2010, but informative Note 1 is added as a sector specific clarification – see discussion on component versus element.
3.2.2	asset protection	Yes	Definition added for clarity in process sector. The term is not used in IEC 61508-4:2010.
3.2.3	basic process control system BPCS	Yes	"EUC control system" defined in IEC 61508-4:2010 is too broad for use in the process industry sector (also, "EUC" is not commonly used in the process sector). Synonym in IEC 61511-1 Ed. 2 is "basic process control system".
3.2.4	bypass	New	Definition added for clarity in process sector. IEC 61508[a] uses the term "inhibited", but provides no definition.

IEC 61511-1 Ed. 2 Term number	Term	Definition different between IEC 61511-1 Ed. 1 and Ed. 2?	Rationale for IEC 61511-1 Ed. 2 Definition
3.2.5	channel	Yes	Equivalent to definition in IEC 61508-4:2010 – see discussion on device versus element. The IEC 61511-1 Ed. 2 usage is not limited to safety functions.
3.2.6	common cause	<not a separate definition>	<not a separate definition>
3.2.6.1	common cause failures	Yes	Definition broadened in IEC 61511-1 Ed. 2 from IEC 61508-4:2010 beyond applicability just to channels of a SIS, clarifies that the failures are not consequences of each other, restricts the common cause of the failures to a single event, and does not specify that system failure is the result.
3.2.6.2	common mode failures	Yes	Definition added for clarity in process sector. Term is used in IEC 61508, but not defined.
3.2.7	compensating measure	New	Definition added for clarity in process sector. The term is not used in IEC 61508.
3.2.8	component	Yes	Definition added for clarity in process sector. Term is used in IEC 61508, but not defined.
3.2.9	configuration management	Yes	Same as IEC 61508-4:2010, with exception of the Note referring to software requirements.
3.2.9.1	conservative approach	New	Definition added for clarity in process sector. Term is used in IEC 61508, but not defined.
3.2.10	control system	No	Equivalent to the definition in IEC 61508-4:2010, but IEC 61511-1 Ed. 2 uses the process sector terminology. The term "EUC" is not commonly used in the process sector.
3.2.11	dangerous failure	Yes	Technically similar to the definition in IEC 61508-4:2010, but IEC 61511-1 Ed. 2 uses the process sector terminology.
3.2.12	dependent failure	Updates to notes only	Equivalent to the definition in IEC 61508-4:2010. Notes were added to further clarify the concepts.
3.2.13	detected revealed overt	Yes	Similar to the definition in IEC 61508-4:2010, but IEC 61511-1 Ed. 2 definition was extended to include software. Notes were added to further clarify the concepts.
3.2.14	device	Yes	The term "element" from IEC 61508-4:2010 is not used in IEC 61511-1 Ed. 2. This term is confusing in IEC 61508-4:2010 since the definition of "element" refers to the "element safety function" whose definition refers in turn to "element". This circular reference cannot be considered as constituting a proper definition of either term. The term is only used in IEC 61511-1 Ed. 2 as part of the term "final element". Synonym in IEC 61511-1 Ed. 2 is "device". The definition of "device" is similar to that of "functional unit" in IEC 61508-4:2010, but is more consistent with process sector terminology.
3.2.14.1	field device	New	Definition added for clarity in process sector. The term is not used in IEC 61508.

IEC 61511-1 Ed. 2 Term number	Term	Definition different between IEC 61511-1 Ed. 1 and Ed. 2?	Rationale for IEC 61511-1 Ed. 2 Definition
3.2.15	diagnostic	New	Definition added for clarity in process sector. Term is used in IEC 61508, but not defined.
3.2.15.1	diagnostic coverage	Yes	The IEC 61511-1 Ed. 2 definition is similar to that in IEC 61508-4:2010. The second sentence in the IEC 61508-4:2010 definition was replaced by Note 2, since it was neither a definition nor an exclusion. A second sentence was added to the IEC 61511-1 Ed. 2 definition to clarify what diagnostic coverage is not – to prevent misuse of the term. This definition was extended to apply for non-constant failure rates.
3.2.16	diversity	Yes	Same as IEC 61508-4:2010, with modification to notes to include programming techniques.
3.2.17	error	No	Conforms with IEC 60050-192:2015, 192-03-02. Same as IEC 61508-4:2010.
3.2.18	failure	Yes	Conforms with IEC 60050-192:2015, 192-03-01 with modification to notes for clarity in the process sector.
3.2.18.1	failure mode	New	The definition was added for clarity in the process sector. Term is used in IEC 61508, but not defined. Conforms with IEC 60050-192:2015, 192-03-17.
3.2.19	fault	Yes	Conforms with IEC 60050-192:2015, 192-04-01, modified – Some notes to entry have been changed, others have been deleted.
3.2.20	fault avoidance	Yes	Equivalent to the definition in IEC 61508-4:2010, but IEC 61511-1 Ed. 2 uses the process sector term SIS.
3.2.20.1	fault exclusion	New	Definition added for clarity in process sector. Term is used in IEC 61508, but not defined.
3.2.21	fault tolerance	Yes	Equivalent to the definition in IEC 61508-4:2010, but IEC 61511-1 Ed. 2 uses the “item” instead of “unit” per the working group direction.
3.2.22	final element	Yes	Definition added for clarity in the process sector. The term is used in IEC 61508 but not defined.
3.2.23	functional safety	Eliminated note	Equivalent to the definition in IEC 61508-4:2010. “EUC control system” defined in IEC 61508-4:2010 is too broad for use in the process industry sector (also, “EUC” is not commonly used in the process sector).
3.2.24	functional safety assessment FSA	Yes	Equivalent to the definition in IEC 61508-4:2010, but IEC 61511-1 Ed. 2 uses terminology consistent with process sector usage.
3.2.25	functional safety audit	No	Same as IEC 61508-4:2010
3.2.26	hardware safety integrity	Yes	Equivalent to the definition in IEC 61508-4:2010, but IEC 61511-1 Ed. 2 uses terminology consistent with process sector usage.
3.2.27	harm	Yes	Conforms with ISO/IEC Guide 51:2014, 3.1. Equivalent to the definition in IEC 61508-4:2010.

IEC 61511-1 Ed. 2 Term number	Term	Definition different between IEC 61511-1 Ed. 1 and Ed. 2?	Rationale for IEC 61511-1 Ed. 2 Definition
3.2.27.1	harmful event	New	Equivalent to the definition in IEC 61508-4:2010, but IEC 61511-1 Ed. 2 developed a more concise definition making use of the term “hazardous event” to which “harmful event” and “hazardous situation” are related (see Note 1 to entry).
3.2.28	hazard	Updates to notes only	Conforms with ISO/IEC Guide 51:2014, 3.2, modified – Note 1 to entry has been added. Same as IEC 61508-4:2010.
3.2.28.1	hazardous event	New	Conforms with ISO/IEC Guide 51:2014: 3.3, modified – see Note 1. Equivalent to the definition in IEC 61508-4:2010.
3.2.28.2	hazardous situation	New	Conforms with ISO/IEC Guide 51:2014, 3.4. Same as IEC 61508-4:2010.
3.2.29	human error	Yes	Definition added for clarity in process sector. Term is used in IEC 61508, but not defined.
3.2.30	impact analysis	No	Equivalent to the definition in IEC 61508-4:2010. Note removed from entry due to differences in scope between IEC 61508 and IEC 61511-1 Ed. 2.
3.2.31	independent organisation	Yes	Equivalent to the definition in IEC 61508-4:2010, but IEC 61511-1 Ed. 2 uses the process sector term SIS.
3.2.32	independent person	No	Equivalent to the definition in IEC 61508-4:2010, but IEC 61511-1 Ed. 2 uses the process sector term SIS.
3.2.33	input function	No	Sector specific definition added to clarify the importance of the architecture used in the process sector. The term is not used in IEC 61508.
3.2.34	instrument	Note made into term 3.2.34.1	Definition added for clarity in process sector. Term is used in IEC 61508, but not defined.
3.2.34.1	instrumented system	New	Definition added for clarity in process sector. The term is not used in IEC 61508.
3.2.35	logic function	No (second phrase that was not an allowable part of definition was moved into a note)	Sector specific definition added to clarify the importance of the architecture and logical I/O transformations used in the process sector. The term is not used in IEC 61508.
3.2.36	logic solver	No	Sector specific definition added to clarify the family of controllers used in the process sector. Term is used in IEC 61508, but not defined.
3.2.36.1	safety configured PE logic solver	Yes	Sector specific definition added to clarify the importance of the two types of logic solvers used in the process sector for safety applications. The term is not used in IEC 61508.
3.2.37	maintenance/engineering interface	No (second phrase that was not an allowable part of definition was moved into a note)	Definition added for clarity in process sector. These terms are not used in IEC 61508.
3.2.37.1	mean repair time MRT	New	Same as IEC 61508-4:2010.
3.2.37.2	mean time to restoration	New	Definition added to be the same as

IEC 61511-1 Ed. 2 Term number	Term	Definition different between IEC 61511-1 Ed. 1 and Ed. 2?	Rationale for IEC 61511-1 Ed. 2 Definition
	MTTR		IEC 61508-4:2010, along with relationship to MPRT. Note: IEC 61508-4:2010 added this definition, which is aligned with the latest international definitions (IEC 61703), to clearly identify the constituent parts of the MTTR.
3.3.37.3	maximum permitted repair time MPRT	New	Definition added for clarity in process sector. The term is not used in IEC 61508.
3.2.38	mitigation	Updates to notes only	Definition added for clarity in process sector. Term is used in IEC 61508, but not defined.
3.2.39	mode of operation (of a SIF)	Yes	Equivalent to the definition in IEC 61508-4:2010, but IEC 61511-1 Ed. 2 uses the process sector terminology.
3.2.39.1	demand mode SIF	Yes	Definition added for clarity in process sector. Term is used in IEC 61508, but not separately defined.
3.2.39.2	continuous mode SIF	Yes	Definition added for clarity in process sector. Term is used in IEC 61508, but not separately defined.
3.2.40	module	Yes	Similar to the definition in IEC 61508-4:2010, but with minor technical changes to: i) introduce better precision in the definition since a module should be ''self-contained'', ii) recognize that IEC 61511-1 Ed. 2 focuses only on LVL and FPL programming, iii) update dates for standards indicated in notes, iv) add note on one potential benefit of utilizing a modular approach.
3.2.41	MooN	No	Definition added for clarity in process sector. Term is used in IEC 61508, but not defined.
3.2.42	necessary risk reduction	Yes	Equivalent to the definition in IEC 61508-4:2010, but IEC 61511-1 Ed. 2 uses the process sector terminology.
3.2.43	non-programmable system (NP) system	No	Definition added for clarity in process sector. The term is not used in IEC 61508.
3.2.44	operating environment	New	Similar to ''environment'' in IEC 61508-4:2010, but IEC 61511-1 Ed. 2 definition is more specifically defined to limit to the process operating environment.
3.2.45	operating mode process operating mode	New	Definition added for clarity in process sector.
3.2.46	operator interface	Yes	Definition added for clarity in process sector.
3.2.47	output function	Yes	Sector specific definition added to clarify the importance of the architecture used in the process sector.
3.2.48	performance	New	Definition added for clarity in process sector. Term is used in IEC 61508, but not defined.
3.2.49	phase	Yes	Definition added for clarity in process