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 It also gives information on projects, replaced and withdrawn publications.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 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

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.