



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

CONTENTS	2
FOREWORD	5
INTRODUCTION	7
1 Scope	8
2 Normative references	8
3 Terms, definitions and abbreviated terms	8
3.1 Terms and definitions	8
3.2 Abbreviated terms	9
4 Background	10
5 Management of functional safety (IEC 61511-1 Ed. 2 Clause 5)	10
5.1 Why is this clause important?	10
5.2 Common misconceptions	10
5.3 What was changed from Ed. 1 to Ed. 2 and why?	11
5.3.1 Existing systems	11
5.3.2 Change management	11
5.3.3 Performance metrics and quality assurance	11
5.3.4 Competency	12
5.3.5 More requirements for functional safety product and service providers	12
5.4 Summary on how	12
6 Safety life cycle (IEC 61511-1 Ed. 2 Clause 6)	12
6.1 Why is this clause important?	12
6.2 Common misconceptions	12
6.3 What was changed from Ed. 1 to Ed. 2 and why?	13
6.4 Summary on how	13
7 Verification (IEC 61511-1 Ed. 2 Clause 7)	13
7.1 Why is this clause important?	13
7.2 Common misconceptions	13
7.3 What was changed from Ed. 1 to Ed. 2 and why?	13
7.4 Summary on how	13
8 Hazard and risk analysis (IEC 61511-1 Ed. 2 Clause 8)	13
8.1 Why is this clause important?	13
8.2 Common misconceptions	14
8.3 What was changed from Ed. 1 to Ed. 2 and why?	14
8.4 Summary on how	15
9 Allocation of safety functions to protection layers (IEC 61511-1 Ed. 2 Clause 9)	15
9.1 Why is this clause important?	15
9.2 Common misconceptions	15
9.3 What was changed from Ed. 1 to Ed. 2 and why?	16
9.3.1 Limits on BPCS protection layers	16
9.3.2 Requirements for claiming RRF > 10 000 in total for instrumented safeguards	16
9.4 Summary on how	16
10 SIS safety requirements specification (IEC 61511-1 Ed. 2 Clause 10)	17
10.1 Why is this clause important?	17
10.2 Common misconceptions	17
10.3 What was changed from Ed. 1 to Ed. 2 and why?	18

10.4	Summary on how	18
11	Design and engineering (IEC 61511-1 Ed. 2 Clause 11)	18
11.1	Why is this clause important?	18
11.2	Common misconceptions	18
11.3	What was changed from Ed. 1 to Ed. 2 and why?.....	19
11.3.1	Hardware fault tolerance.....	19
11.3.2	Security risk requirements	20
11.3.3	Safety manual	20
11.3.4	Requirements for system behaviour on detection of a fault	20
11.3.5	Limitations on field device communication design	21
11.4	Summary on how	21
12	Application program development (IEC 61511-1 Ed. 2 Clause 12)	21
12.1	Why is this clause important?	21
12.2	Common misconceptions	22
12.3	What was changed from Ed. 1 to Ed. 2 and why?.....	22
12.4	Summary on how	22
13	Factory acceptance test (IEC 61511-1 Ed. 2 Clause 13)	22
13.1	Why is this clause important?	22
13.2	Common misconceptions	23
13.3	What was changed from Ed. 1 to Ed. 2 and why?.....	23
13.4	Summary on how	23
14	Installation (IEC 61511-1 Ed. 2 Clause 14)	23
14.1	Why is this clause important?	23
14.2	Common misconceptions	24
14.3	What was changed from Ed. 1 to Ed. 2 and why?.....	24
14.4	Summary on how	24
15	Validation (IEC 61511-1 Ed. 2 Clause 15).....	24
15.1	Why is this clause important?	24
15.2	Common misconceptions	24
15.3	What was changed from Ed. 1 to Ed. 2 and why?.....	24
15.4	Summary on how	24
16	Operation and maintenance (IEC 61511-1 Ed. 2 Clause 16)	25
16.1	Why is this clause important?	25
16.2	Common misconceptions	25
16.3	What was changed from Ed. 1 to Ed. 2 and why?.....	26
16.3.1	Fault detection, bypassing, and compensating measures.....	26
16.3.2	Proof testing after repair and change	26
16.4	Summary on how	26
17	Modification (IEC 61511-1 Ed. 2 Clause 17)	26
17.1	Why is this clause important?	26
17.2	Common misconceptions	26
17.3	What was changed from Ed. 1 to Ed. 2 and why?.....	27
	Planning for and completing change	27
17.4	Summary on how	27
18	Decommissioning (IEC 61511-1 Ed. 2 Clause 18).....	27
18.1	Why is this clause important?	27
18.2	Common misconceptions	27

18.3	What was changed from Ed. 1 to Ed. 2 and why?.....	28
18.3.1	Planning for and completing change	28
18.4	Summary on how	28
19	Documentation (IEC 61511-1 Ed. 2 Clause 19).....	28
19.1	Why is this clause important?	28
19.2	Common misconceptions	28
19.3	What was changed from Ed. 1 to Ed. 2 and why?.....	28
19.4	Summary on how	28
20	Definitions (IEC 61511-1 Ed. 2 Clause 3).....	29
20.1	Why is this clause important?	29
20.2	Common misconceptions	29
20.3	What was changed from Ed. 1 to Ed. 2 and why?.....	29
20.4	Summary on how	37
	Bibliography.....	38
	Table 1 – Abbreviated terms used in IEC TR 61511-4	9
	Table 2 – Rationale for IEC 61511-1 Ed. 2 terms and definitions.....	29

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*