

This is a preview - click here to buy the full publication



IEC 61511-1

Edition 2.1 2017-08
CONSOLIDATED VERSION

INTERNATIONAL STANDARD



**Functional safety – Safety instrumented systems for the process industry sector –
Part 1: Framework, definitions, system, hardware and application programming requirements**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 25.040.01

ISBN 978-2-8322-4752-5

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

REDLINE VERSION



**Functional safety – Safety instrumented systems for the process industry sector –
Part 1: Framework, definitions, system, hardware and application programming requirements**

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	9
2 Normative references	12
3 Terms, definitions and abbreviations	13
3.1 Terms	13
3.2 Terms and definitions.....	13
3.3 Abbreviations	31
4 Conformance to the IEC 61511-1:2016	32
5 Management of functional safety	32
5.1 Objective	32
5.2 Requirements	33
5.2.1 General	33
5.2.2 Organization and resources	33
5.2.3 Risk evaluation and risk management.....	33
5.2.4 Safety planning.....	33
5.2.5 Implementing and monitoring.....	34
5.2.6 Assessment, auditing and revisions	34
5.2.7 SIS configuration management	37
6 Safety life-cycle requirements.....	37
6.1 Objectives.....	37
6.2 Requirements	38
6.3 Application program SIS safety life-cycle requirements	40
7 Verification	43
7.1 Objective	43
7.2 Requirements	43
8 Process H&RA.....	45
8.1 Objectives.....	45
8.2 Requirements	45
9 Allocation of safety functions to protection layers	46
9.1 Objectives.....	46
9.2 Requirements of the allocation process.....	46
9.3 Requirements on the basic process control system as a protection layer	49
9.4 Requirements for preventing common cause, common mode and dependent failures.....	50
10 SIS safety requirements specification (SRS).....	50
10.1 Objective	50
10.2 General requirements	50
10.3 SIS safety requirements.....	51
11 SIS design and engineering.....	53
11.1 Objective	53
11.2 General requirements	53
11.3 Requirements for system behaviour on detection of a fault	54
11.4 Hardware fault tolerance	55
11.5 Requirements for selection of devices.....	56

11.5.1	Objectives	56
11.5.2	General requirements	56
11.5.3	Requirements for the selection of devices based on prior use	56
11.5.4	Requirements for selection of FPL programmable devices (e.g., field devices) based on prior use	57
11.5.5	Requirements for selection of LVL programmable devices based on prior use	58
11.5.6	Requirements for selection of FVL programmable devices	59
11.6	Field devices	59
11.7	Interfaces	59
11.7.1	General	59
11.7.2	Operator interface requirements	59
11.7.3	Maintenance/engineering interface requirements	60
11.7.4	Communication interface requirements	60
11.8	Maintenance or testing design requirements	61
11.9	Quantification of random failure	61
12	SIS application program development	63
12.1	Objective	63
12.2	General requirements	63
12.3	Application program design	64
12.4	Application program implementation	65
12.5	Requirements for application program verification (review and testing)	66
12.6	Requirements for application program methodology and tools	67
13	Factory acceptance test (FAT)	68
13.1	Objective	68
13.2	Recommendations	68
14	SIS installation and commissioning	69
14.1	Objectives	69
14.2	Requirements	69
15	SIS safety validation	70
15.1	Objective	70
15.2	Requirements	70
16	SIS operation and maintenance	73
16.1	Objectives	73
16.2	Requirements	73
16.3	Proof testing and inspection	75
16.3.1	Proof testing	75
16.3.2	Inspection	76
16.3.3	Documentation of proof tests and inspection	76
17	SIS modification	76
17.1	Objectives	76
17.2	Requirements	77
18	SIS decommissioning	77
18.1	Objectives	77
18.2	Requirements	78
19	Information and documentation requirements	78
19.1	Objectives	78
19.2	Requirements	78

Bibliography.....	80
Figure 1 – Overall framework of the IEC 61511 series	8
Figure 2 – Relationship between IEC 61511 and IEC 61508	10
Figure 3 – Detailed relationship between IEC 61511 and IEC 61508.....	11
Figure 4 – Relationship between safety instrumented functions and other functions.....	12
Figure 5 – Programmable electronic system (PES): structure and terminology.....	24
Figure 6 – Example of SIS architectures comprising three SIS subsystems.....	26
Figure 7 – SIS safety life-cycle phases and FSA stages.....	38
Figure 8 – Application program safety life-cycle and its relationship to the SIS safety life-cycle	41
Figure 9 – Typical protection layers and risk reduction means	49
Table 1 – Abbreviations used in IEC 61511.....	31
Table 2 – SIS safety life-cycle overview (1 of 2).....	39
Table 3 – Application program safety life-cycle: overview (1 of 2)	42
Table 4 – Safety integrity requirements: PFD_{avg}	47
Table 5 – Safety integrity requirements: average frequency of dangerous failures of the SIF	47
Table 6 – Minimum HFT requirements according to SIL	55

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 1: Framework, definitions, system, hardware and application programming requirements

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.

This consolidated version of the official IEC Standard and its amendment has been prepared for user convenience.

IEC 61511-1 edition 2.1 contains the second edition (2016-02) [documents 65A/777/FDIS and 65A/784/RVD], its corrigendum 1 (2016-09) and its amendment 1 (2017-08) [documents 65A/844/FDIS and 65A/848/RVD].

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendment 1. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.

International Standard IEC 61511-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 2003. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

- references and requirements to software replaced with references and requirements to application programming;
- functional safety assessment requirements provided with more detail to improve management of functional safety.
- management of change requirement added;
- security risk assessment requirements added;.
- requirements expanded on the basic process control system as a protection layer;
- requirements for hardware fault tolerance modified and should be reviewed carefully to understand user/integrator options.

The text of this standard is based on the following documents:

FDIS	Report on voting
65A/777/FDIS	65A/784/RVD

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

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

A list of all parts in the IEC 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 publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

IMPORTANT – The “colour inside” logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this publication using a colour printer.

INTRODUCTION

Safety instrumented systems (SISs) have been used for many years to perform safety instrumented functions (SIFs) in the process industries. If instrumentation is to be effectively used for SIFs, it is essential that this instrumentation achieves certain minimum standards and performance levels.

The IEC 61511 series addresses the application of SISs for the process industries. The IEC 61511 series also addresses a process Hazard and Risk Assessment (H&RA) to be carried out to enable the specification for SISs to be derived. Other safety systems' contributions are only considered with respect to the performance requirements for the SIS. The SIS includes all devices necessary to carry out each SIF from sensor(s) to final element(s).

The IEC 61511 series has two concepts which are fundamental to its application: SIS safety life-cycle and safety integrity levels (SILs).

The IEC 61511 series addresses SISs which are based on the use of electrical/electronic/programmable electronic technology. Where other technologies are used for logic solvers, the basic principles of the IEC 61511 series should be applied to ensure the functional safety requirements are met. The IEC 61511 series also addresses the SIS sensors and final elements regardless of the technology used. The IEC 61511 series is process industry specific within the framework of the IEC 61508 series.

The IEC 61511 series sets out an approach for SIS safety life-cycle activities to achieve these minimum principles. This approach has been adopted in order that a rational and consistent technical policy is used.

In most situations, safety is best achieved by an inherently safe process design. However in some instances this is not possible or not practical. If necessary, this may be combined with a protective system or systems to address any residual identified risk. Protective systems can rely on different technologies (chemical, mechanical, hydraulic, pneumatic, electrical, electronic, and programmable electronic). To facilitate this approach, the IEC 61511 series:

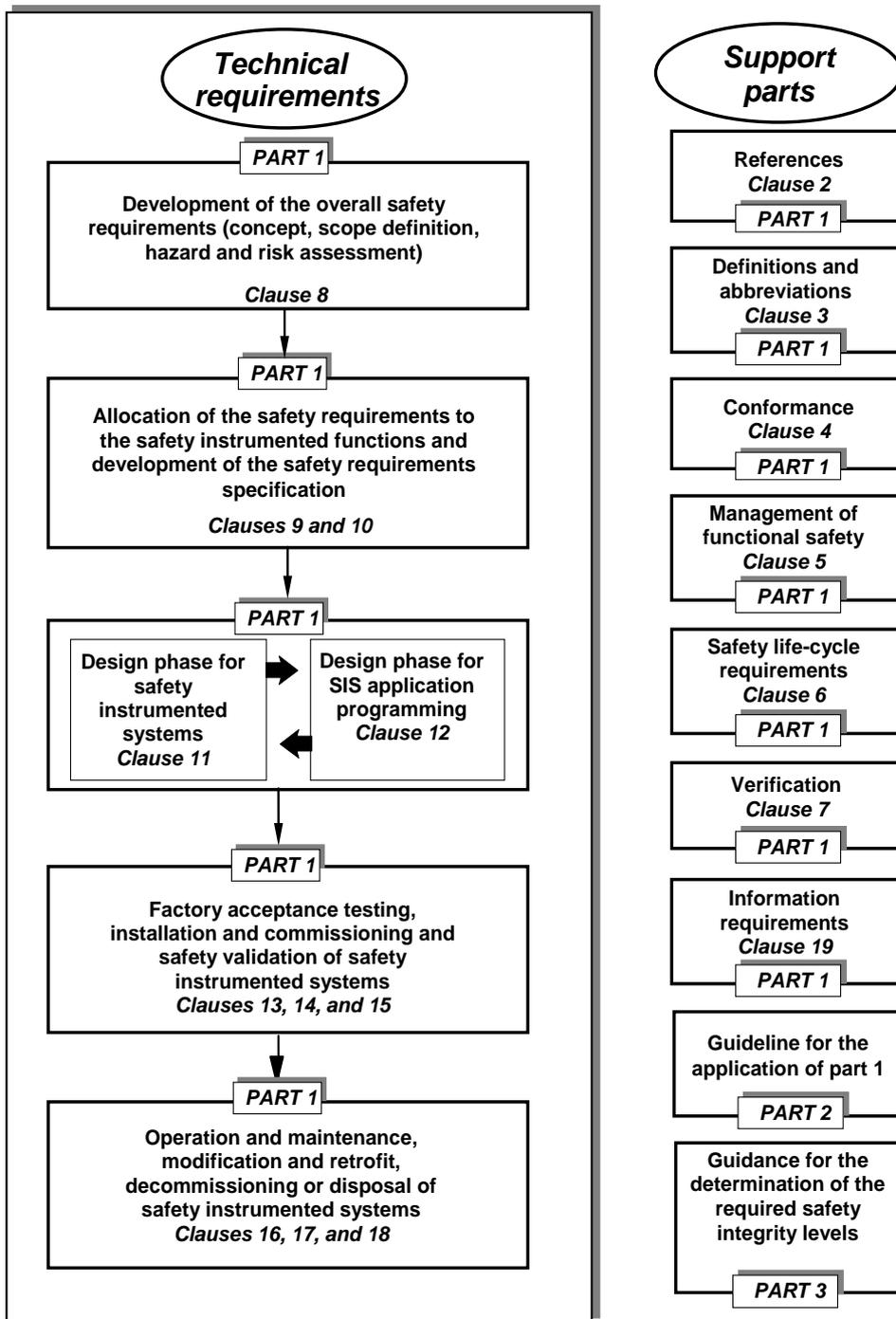
- addresses that a H&RA is carried out to identify the overall safety requirements;
- addresses that an allocation of the safety requirements to the SIS is carried out;
- works within a framework which is applicable to all instrumented means of achieving functional safety;
- details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.

The IEC 61511 series on SIS for the process industry:

- addresses all SIS safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
- enables existing or new country specific process industry standards to be harmonized with the IEC 61511 series.

The IEC 61511 series is intended to lead to a high level of consistency (e.g., of underlying principles, terminology, and information) within the process industries. This should have both safety and economic benefits. Figure 1 below shows an overall framework of the IEC 61511 series.

In jurisdictions where the governing authorities (e.g., national, federal, state, province, county, city) have established process safety design, process safety management, or other regulations, these take precedence over the requirements defined in the IEC 61511 series.



IEC

Figure 1 – Overall framework of the IEC 61511 series

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

Part 1: Framework, definitions, system, hardware and application programming requirements

1 Scope

This part of IEC 61511 gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system (SIS), so that it can be confidently entrusted to achieve or maintain a safe state of the process. IEC 61511-1 has been developed as a process sector implementation of IEC 61508:2010.

In particular, IEC 61511-1:

- a) specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements (e.g., designers, suppliers, owner/operating company, contractor). This responsibility will be assigned to different parties according to safety planning, project planning and management, and national regulations;
- b) applies when devices that meets the requirements of the IEC 61508 series published in 2010, or IEC 61511-1:2016 [11.5], is integrated into an overall system that is to be used for a process sector application. It does not apply to manufacturers wishing to claim that devices are suitable for use in SISs for the process sector (see IEC 61508-2:2010 and IEC 61508-3:2010);
- c) defines the relationship between IEC 61511 and IEC 61508 (see Figures 2 and 3);
- d) applies when application programs are developed for systems having limited variability language or when using fixed programming language devices, but does not apply to manufacturers, SIS designers, integrators and users that develop embedded software (system software) or use full variability languages (see IEC 61508-3:2010);
- e) applies to a wide variety of industries within the process sector for example, chemicals, oil and gas, pulp and paper, pharmaceuticals, food and beverage, and non-nuclear power generation;

NOTE 1 Within the process sector some applications may have additional requirements that have to be satisfied.
- f) outlines the relationship between SIFs and other instrumented functions (see Figure 4);
- g) results in the identification of the functional requirements and safety integrity requirements for the SIF taking into account the risk reduction achieved by other methods;
- h) specifies life-cycle requirements for system architecture and hardware configuration, application programming, and system integration;
- i) specifies requirements for application programming for users and integrators of SISs.
- j) applies when functional safety is achieved using one or more SIFs for the protection of personnel, protection of the general public or protection of the environment;
- k) may be applied in non-safety applications for example asset protection;
- l) defines requirements for implementing SIFs as a part of the overall arrangements for achieving functional safety;
- m) uses a SIS safety life-cycle (see Figure 7) and defines a list of activities which are necessary to determine the functional requirements and the safety integrity requirements for the SIS;

- n) specifies that a H&RA is to be carried out to define the safety functional requirements and safety integrity levels (SIL) of each SIF;
NOTE 2 Figure 9 presents an overview of risk reduction means.
- o) establishes numerical targets for average probability of failure on demand (in demand mode) and average frequency of dangerous failures (in demand mode or continuous mode) for each SIL;
- p) specifies minimum requirements for hardware fault tolerance (HFT);
- q) specifies measures and techniques required for achieving the specified SIL;
- r) defines a maximum level of functional safety performance (SIL 4) which can be achieved for a SIF implemented according to IEC 61511-1;
- s) defines a minimum level of functional safety performance (SIL 1) below which IEC 61511-1 does not apply;
- t) provides a framework for establishing the SIL but does not specify the SIL required for specific applications (which should be established based on knowledge of the particular application and on the overall targeted risk reduction);
- u) specifies requirements for all parts of the SIS from sensor to final element(s);
- v) defines the information that is needed during the SIS safety life-cycle;
- w) specifies that the design of the SIS takes into account human factors;
- x) does not place any direct requirements on the individual operator or maintenance person:

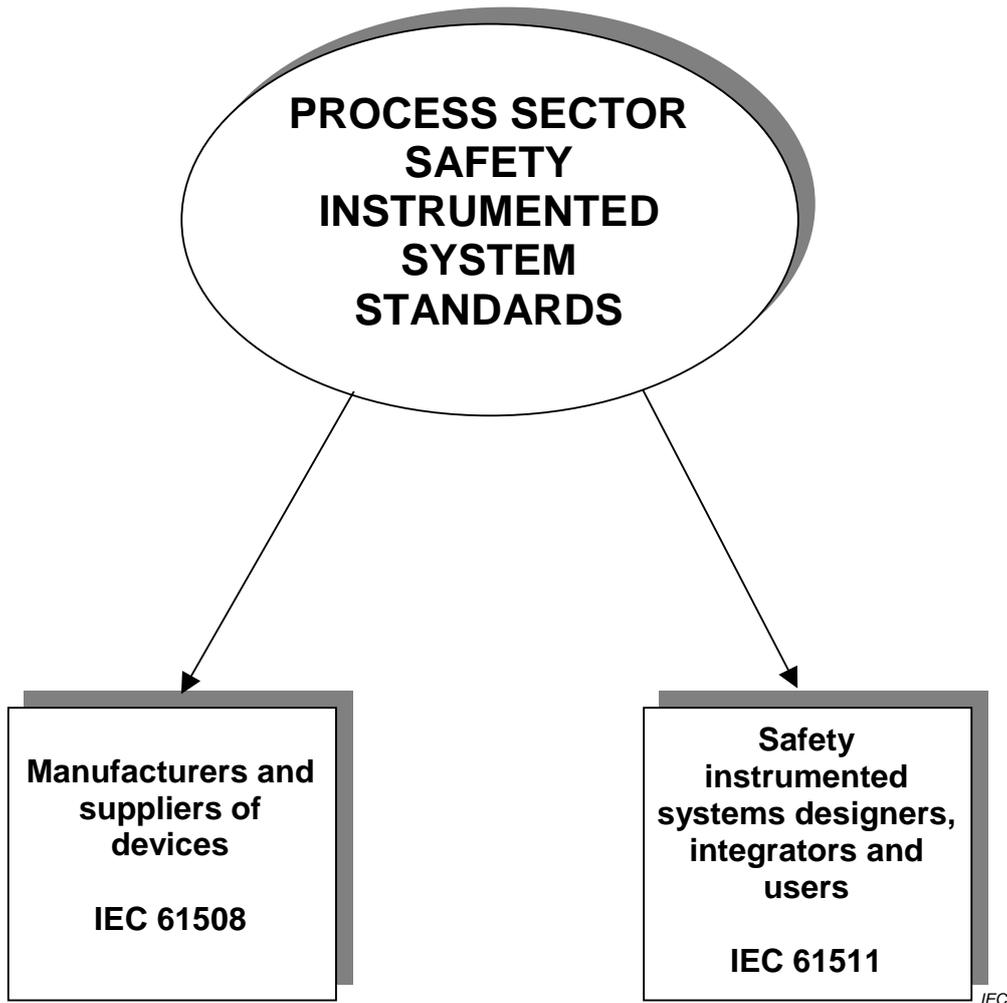


Figure 2 – Relationship between IEC 61511 and IEC 61508

NOTE 3 IEC 61508 is also used by safety instrumented designers, integrators and users where directed in IEC 61511.

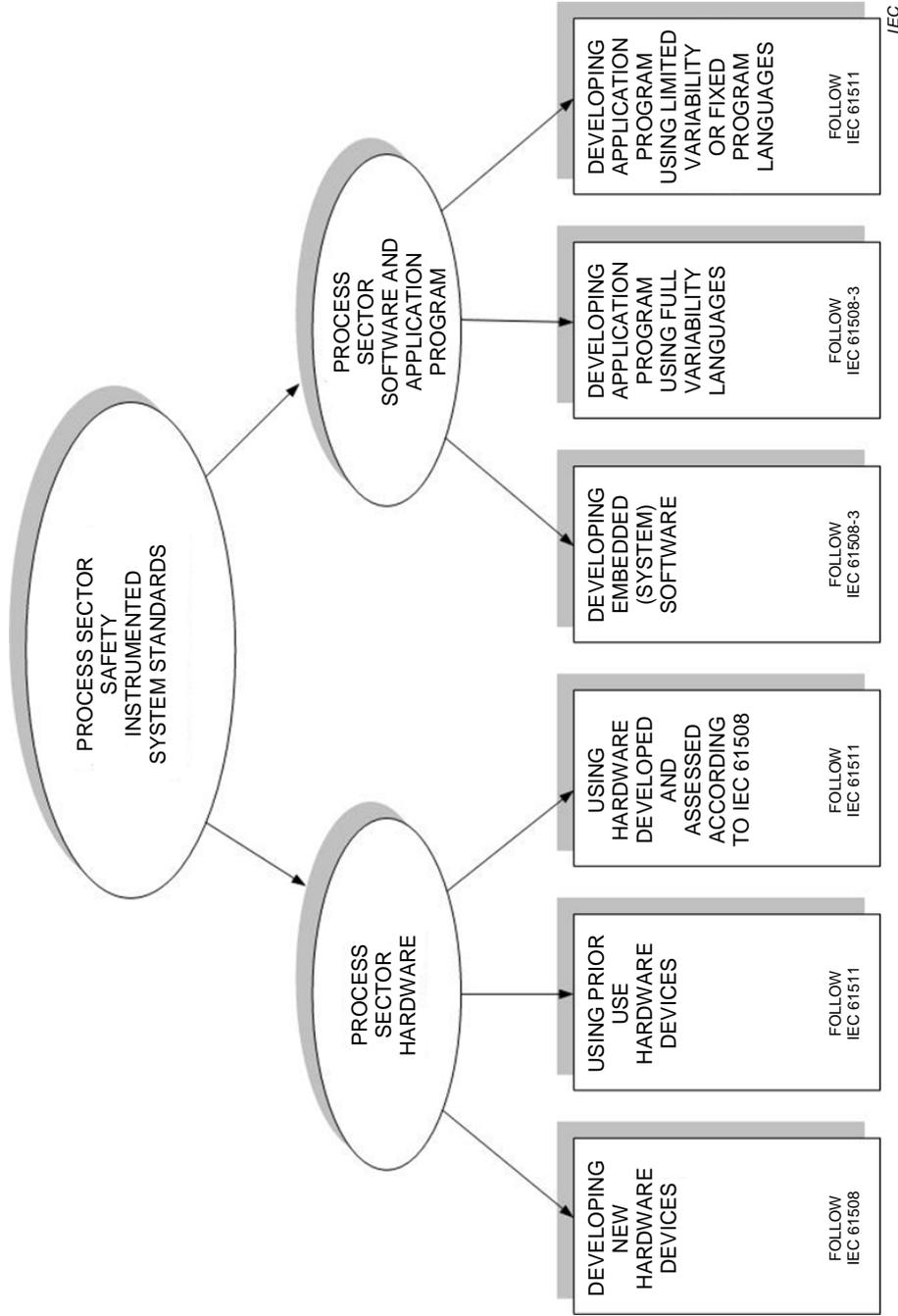
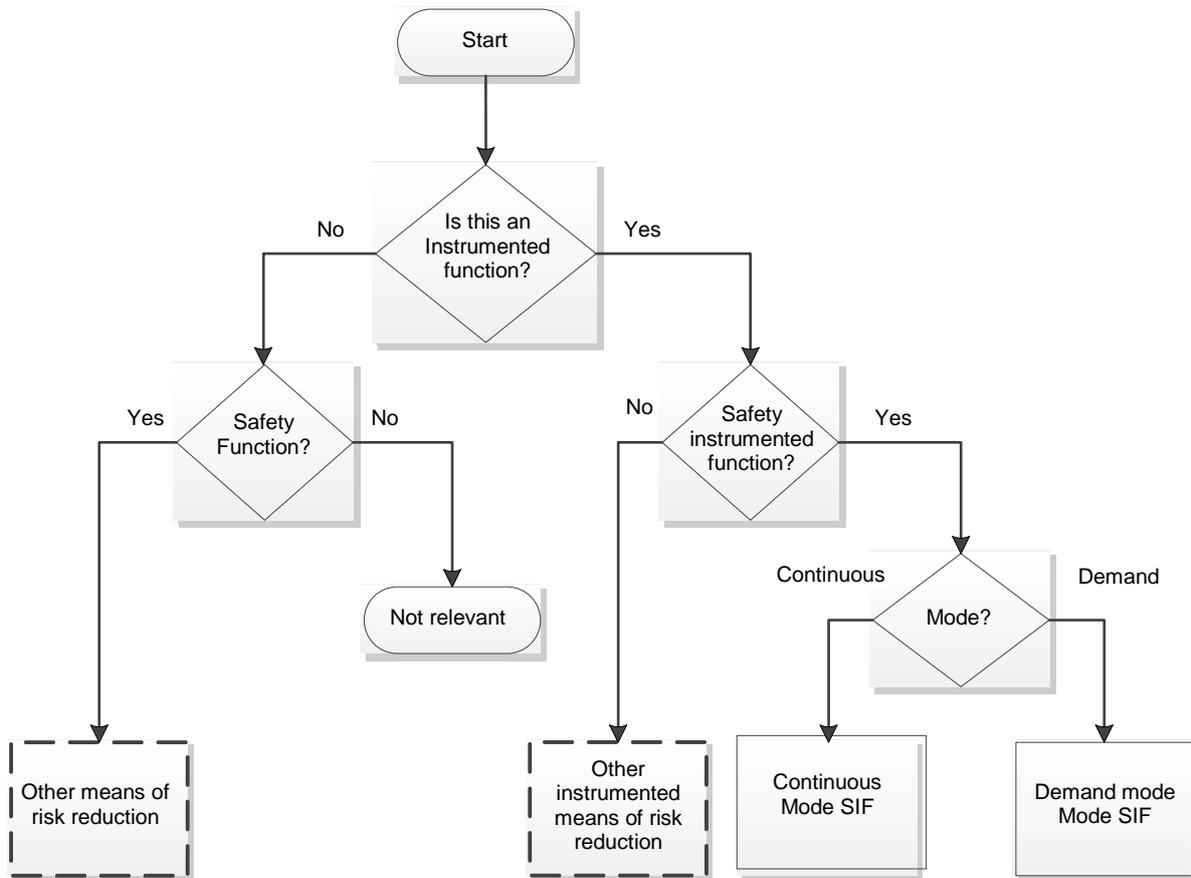


Figure 3 – Detailed relationship between IEC 61511 and IEC 61508

NOTE 4 Subclause 7.2.2 in IEC 61511-1:2016 and A.7.2.2 in IEC 61511-2:2016 contain guidance on handling integration of sub-systems that comply with other standards (such as machinery, burner, etc.).



Standard specifies activities which are to be carried out but requirements are not detailed

IEC

Figure 4 – Relationship between safety instrumented functions and other functions

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General Requirements*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

FINAL VERSION

**Functional safety – Safety instrumented systems for the process industry sector –
Part 1: Framework, definitions, system, hardware and application programming requirements**



CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	9
2 Normative references	12
3 Terms, definitions and abbreviations	13
3.1 Terms	13
3.2 Terms and definitions.....	13
3.3 Abbreviations	31
4 Conformance to the IEC 61511-1:2016	32
5 Management of functional safety	32
5.1 Objective	32
5.2 Requirements	33
5.2.1 General	33
5.2.2 Organization and resources	33
5.2.3 Risk evaluation and risk management.....	33
5.2.4 Safety planning.....	33
5.2.5 Implementing and monitoring.....	34
5.2.6 Assessment, auditing and revisions	34
5.2.7 SIS configuration management	37
6 Safety life-cycle requirements.....	37
6.1 Objectives.....	37
6.2 Requirements	38
6.3 Application program SIS safety life-cycle requirements	40
7 Verification	43
7.1 Objective	43
7.2 Requirements	43
8 Process H&RA.....	45
8.1 Objectives.....	45
8.2 Requirements	45
9 Allocation of safety functions to protection layers	46
9.1 Objectives.....	46
9.2 Requirements of the allocation process.....	46
9.3 Requirements on the basic process control system as a protection layer	49
9.4 Requirements for preventing common cause, common mode and dependent failures.....	50
10 SIS safety requirements specification (SRS).....	50
10.1 Objective	50
10.2 General requirements	50
10.3 SIS safety requirements.....	51
11 SIS design and engineering.....	53
11.1 Objective	53
11.2 General requirements	53
11.3 Requirements for system behaviour on detection of a fault	54
11.4 Hardware fault tolerance	55
11.5 Requirements for selection of devices.....	56

11.5.1	Objectives	56
11.5.2	General requirements	56
11.5.3	Requirements for the selection of devices based on prior use	56
11.5.4	Requirements for selection of FPL programmable devices (e.g., field devices) based on prior use	57
11.5.5	Requirements for selection of LVL programmable devices based on prior use	58
11.5.6	Requirements for selection of FVL programmable devices	59
11.6	Field devices	59
11.7	Interfaces	59
11.7.1	General	59
11.7.2	Operator interface requirements	59
11.7.3	Maintenance/engineering interface requirements	60
11.7.4	Communication interface requirements	60
11.8	Maintenance or testing design requirements	61
11.9	Quantification of random failure	61
12	SIS application program development	63
12.1	Objective	63
12.2	General requirements	63
12.3	Application program design	64
12.4	Application program implementation	65
12.5	Requirements for application program verification (review and testing)	66
12.6	Requirements for application program methodology and tools	67
13	Factory acceptance test (FAT)	68
13.1	Objective	68
13.2	Recommendations	68
14	SIS installation and commissioning	69
14.1	Objectives	69
14.2	Requirements	69
15	SIS safety validation	70
15.1	Objective	70
15.2	Requirements	70
16	SIS operation and maintenance	73
16.1	Objectives	73
16.2	Requirements	73
16.3	Proof testing and inspection	75
16.3.1	Proof testing	75
16.3.2	Inspection	76
16.3.3	Documentation of proof tests and inspection	76
17	SIS modification	76
17.1	Objectives	76
17.2	Requirements	77
18	SIS decommissioning	77
18.1	Objectives	77
18.2	Requirements	78
19	Information and documentation requirements	78
19.1	Objectives	78
19.2	Requirements	78

Bibliography.....	80
Figure 1 – Overall framework of the IEC 61511 series	8
Figure 2 – Relationship between IEC 61511 and IEC 61508	10
Figure 3 – Detailed relationship between IEC 61511 and IEC 61508	11
Figure 4 – Relationship between safety instrumented functions and other functions.....	12
Figure 5 – Programmable electronic system (PES): structure and terminology	24
Figure 6 – Example of SIS architectures comprising three SIS subsystems.....	26
Figure 7 – SIS safety life-cycle phases and FSA stages.....	38
Figure 8 – Application program safety life-cycle and its relationship to the SIS safety life-cycle	41
Figure 9 – Typical protection layers and risk reduction means	49
Table 1 – Abbreviations used in IEC 61511.....	31
Table 2 – SIS safety life-cycle overview (1 of 2).....	39
Table 3 – Application program safety life-cycle: overview (1 of 2)	42
Table 4 – Safety integrity requirements: PFD_{avg}	47
Table 5 – Safety integrity requirements: average frequency of dangerous failures of the SIF	47
Table 6 – Minimum HFT requirements according to SIL	55

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 1: Framework, definitions, system, hardware and application programming requirements

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.

This consolidated version of the official IEC Standard and its amendment has been prepared for user convenience.

IEC 61511-1 edition 2.1 contains the second edition (2016-02) [documents 65A/777/FDIS and 65A/784/RVD], its corrigendum 1 (2016-09) and its amendment 1 (2017-08) [documents 65A/844/FDIS and 65A/848/RVD].

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted is available in this publication.

International Standard IEC 61511-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 2003. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

- references and requirements to software replaced with references and requirements to application programming;
- functional safety assessment requirements provided with more detail to improve management of functional safety.
- management of change requirement added;
- security risk assessment requirements added;.
- requirements expanded on the basic process control system as a protection layer;
- requirements for hardware fault tolerance modified and should be reviewed carefully to understand user/integrator options.

The text of this standard is based on the following documents:

FDIS	Report on voting
65A/777/FDIS	65A/784/RVD

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

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

A list of all parts in the IEC 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 publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

INTRODUCTION

Safety instrumented systems (SISs) have been used for many years to perform safety instrumented functions (SIFs) in the process industries. If instrumentation is to be effectively used for SIFs, it is essential that this instrumentation achieves certain minimum standards and performance levels.

The IEC 61511 series addresses the application of SISs for the process industries. The IEC 61511 series also addresses a process Hazard and Risk Assessment (H&RA) to be carried out to enable the specification for SISs to be derived. Other safety systems' contributions are only considered with respect to the performance requirements for the SIS. The SIS includes all devices necessary to carry out each SIF from sensor(s) to final element(s).

The IEC 61511 series has two concepts which are fundamental to its application: SIS safety life-cycle and safety integrity levels (SILs).

The IEC 61511 series addresses SISs which are based on the use of electrical/electronic/programmable electronic technology. Where other technologies are used for logic solvers, the basic principles of the IEC 61511 series should be applied to ensure the functional safety requirements are met. The IEC 61511 series also addresses the SIS sensors and final elements regardless of the technology used. The IEC 61511 series is process industry specific within the framework of the IEC 61508 series.

The IEC 61511 series sets out an approach for SIS safety life-cycle activities to achieve these minimum principles. This approach has been adopted in order that a rational and consistent technical policy is used.

In most situations, safety is best achieved by an inherently safe process design. However in some instances this is not possible or not practical. If necessary, this may be combined with a protective system or systems to address any residual identified risk. Protective systems can rely on different technologies (chemical, mechanical, hydraulic, pneumatic, electrical, electronic, and programmable electronic). To facilitate this approach, the IEC 61511 series:

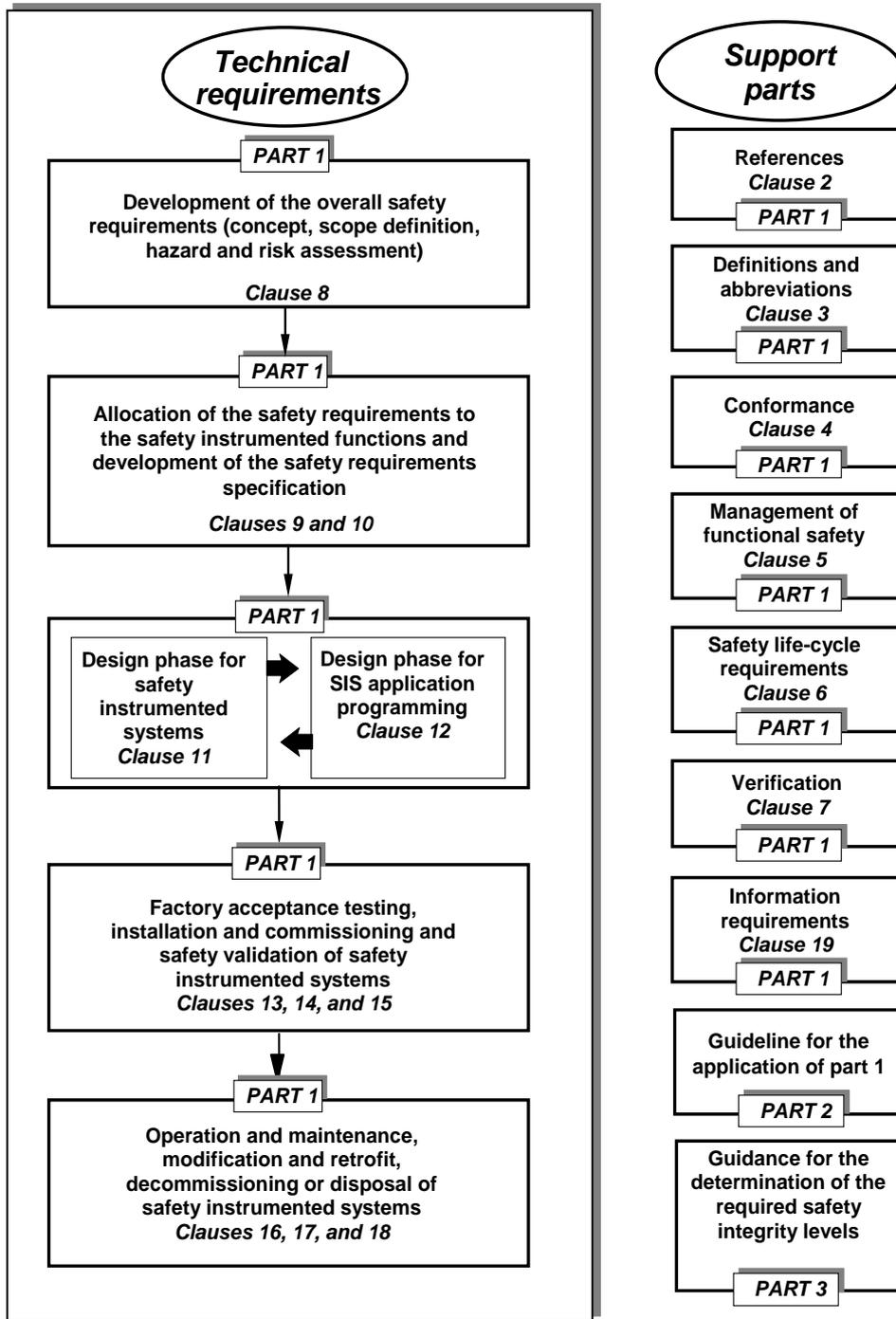
- addresses that a H&RA is carried out to identify the overall safety requirements;
- addresses that an allocation of the safety requirements to the SIS is carried out;
- works within a framework which is applicable to all instrumented means of achieving functional safety;
- details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.

The IEC 61511 series on SIS for the process industry:

- addresses all SIS safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
- enables existing or new country specific process industry standards to be harmonized with the IEC 61511 series.

The IEC 61511 series is intended to lead to a high level of consistency (e.g., of underlying principles, terminology, and information) within the process industries. This should have both safety and economic benefits. Figure 1 below shows an overall framework of the IEC 61511 series.

In jurisdictions where the governing authorities (e.g., national, federal, state, province, county, city) have established process safety design, process safety management, or other regulations, these take precedence over the requirements defined in the IEC 61511 series.



IEC

Figure 1 – Overall framework of the IEC 61511 series

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

Part 1: Framework, definitions, system, hardware and application programming requirements

1 Scope

This part of IEC 61511 gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system (SIS), so that it can be confidently entrusted to achieve or maintain a safe state of the process. IEC 61511-1 has been developed as a process sector implementation of IEC 61508:2010.

In particular, IEC 61511-1:

- a) specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements (e.g., designers, suppliers, owner/operating company, contractor). This responsibility will be assigned to different parties according to safety planning, project planning and management, and national regulations;
- b) applies when devices that meets the requirements of the IEC 61508 series published in 2010, or IEC 61511-1:2016 [11.5], is integrated into an overall system that is to be used for a process sector application. It does not apply to manufacturers wishing to claim that devices are suitable for use in SISs for the process sector (see IEC 61508-2:2010 and IEC 61508-3:2010);
- c) defines the relationship between IEC 61511 and IEC 61508 (see Figures 2 and 3);
- d) applies when application programs are developed for systems having limited variability language or when using fixed programming language devices, but does not apply to manufacturers, SIS designers, integrators and users that develop embedded software (system software) or use full variability languages (see IEC 61508-3:2010);
- e) applies to a wide variety of industries within the process sector for example, chemicals, oil and gas, pulp and paper, pharmaceuticals, food and beverage, and non-nuclear power generation;

NOTE 1 Within the process sector some applications may have additional requirements that have to be satisfied.

- f) outlines the relationship between SIFs and other instrumented functions (see Figure 4);
- g) results in the identification of the functional requirements and safety integrity requirements for the SIF taking into account the risk reduction achieved by other methods;
- h) specifies life-cycle requirements for system architecture and hardware configuration, application programming, and system integration;
- i) specifies requirements for application programming for users and integrators of SISs.
- j) applies when functional safety is achieved using one or more SIFs for the protection of personnel, protection of the general public or protection of the environment;
- k) may be applied in non-safety applications for example asset protection;
- l) defines requirements for implementing SIFs as a part of the overall arrangements for achieving functional safety;
- m) uses a SIS safety life-cycle (see Figure 7) and defines a list of activities which are necessary to determine the functional requirements and the safety integrity requirements for the SIS;

- n) specifies that a H&RA is to be carried out to define the safety functional requirements and safety integrity levels (SIL) of each SIF;
NOTE 2 Figure 9 presents an overview of risk reduction means.
- o) establishes numerical targets for average probability of failure on demand (in demand mode) and average frequency of dangerous failures (in demand mode or continuous mode) for each SIL;
- p) specifies minimum requirements for hardware fault tolerance (HFT);
- q) specifies measures and techniques required for achieving the specified SIL;
- r) defines a maximum level of functional safety performance (SIL 4) which can be achieved for a SIF implemented according to IEC 61511-1;
- s) defines a minimum level of functional safety performance (SIL 1) below which IEC 61511-1 does not apply;
- t) provides a framework for establishing the SIL but does not specify the SIL required for specific applications (which should be established based on knowledge of the particular application and on the overall targeted risk reduction);
- u) specifies requirements for all parts of the SIS from sensor to final element(s);
- v) defines the information that is needed during the SIS safety life-cycle;
- w) specifies that the design of the SIS takes into account human factors;
- x) does not place any direct requirements on the individual operator or maintenance person:

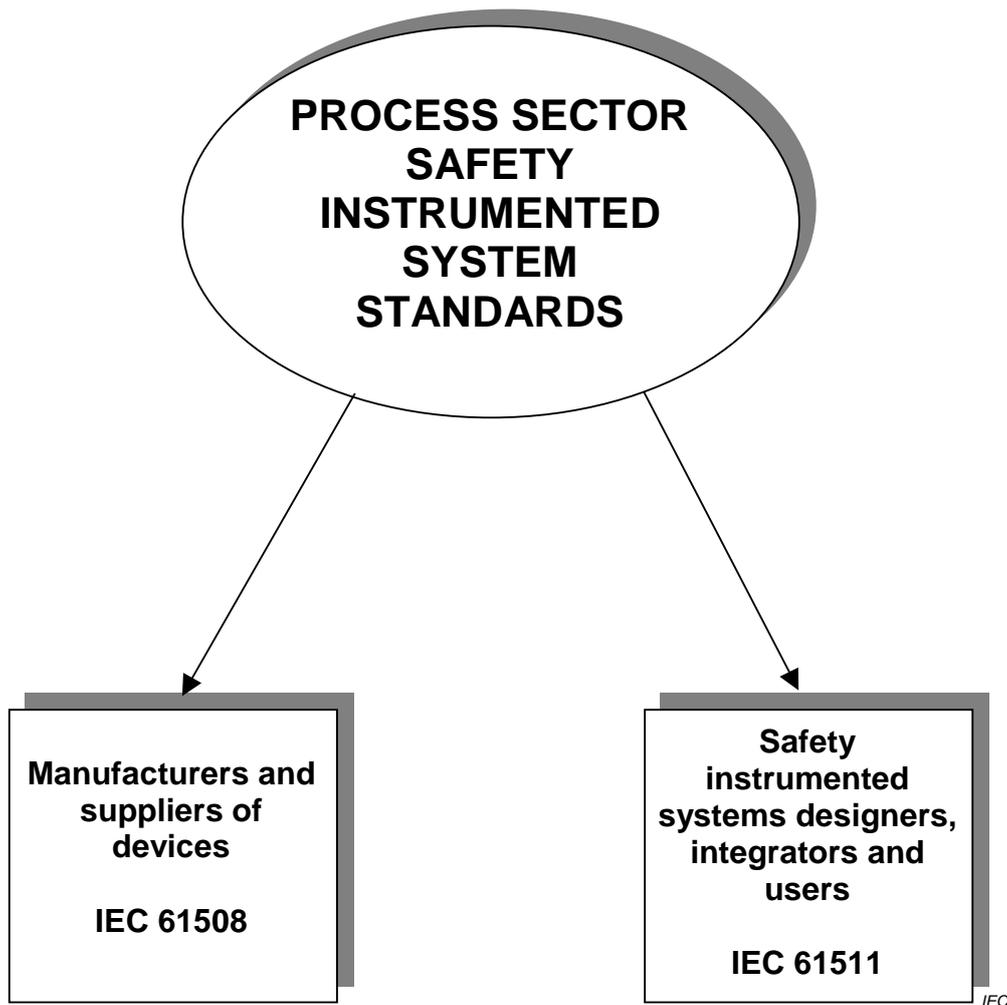


Figure 2 – Relationship between IEC 61511 and IEC 61508

NOTE 3 IEC 61508 is also used by safety instrumented designers, integrators and users where directed in IEC 61511.

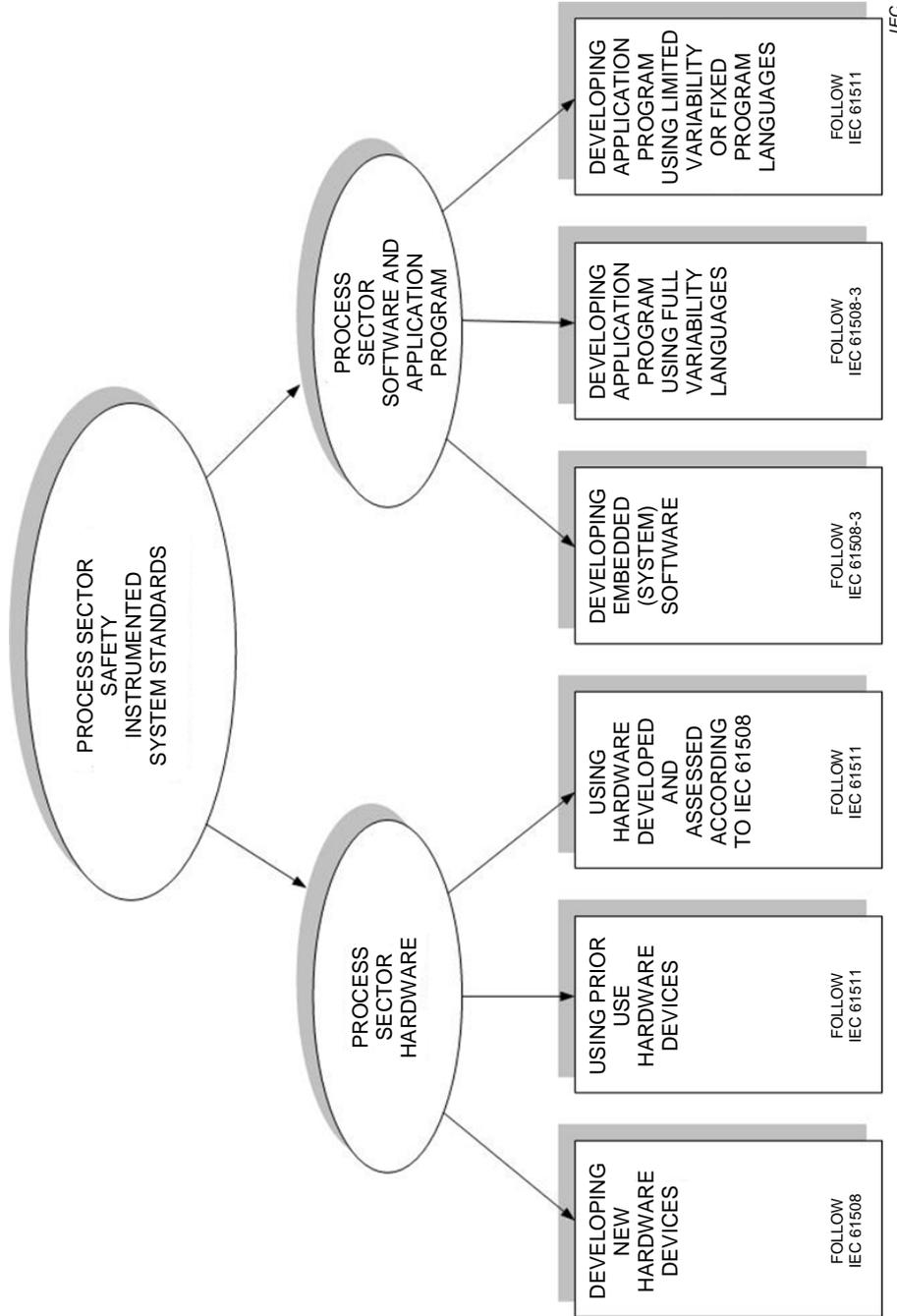
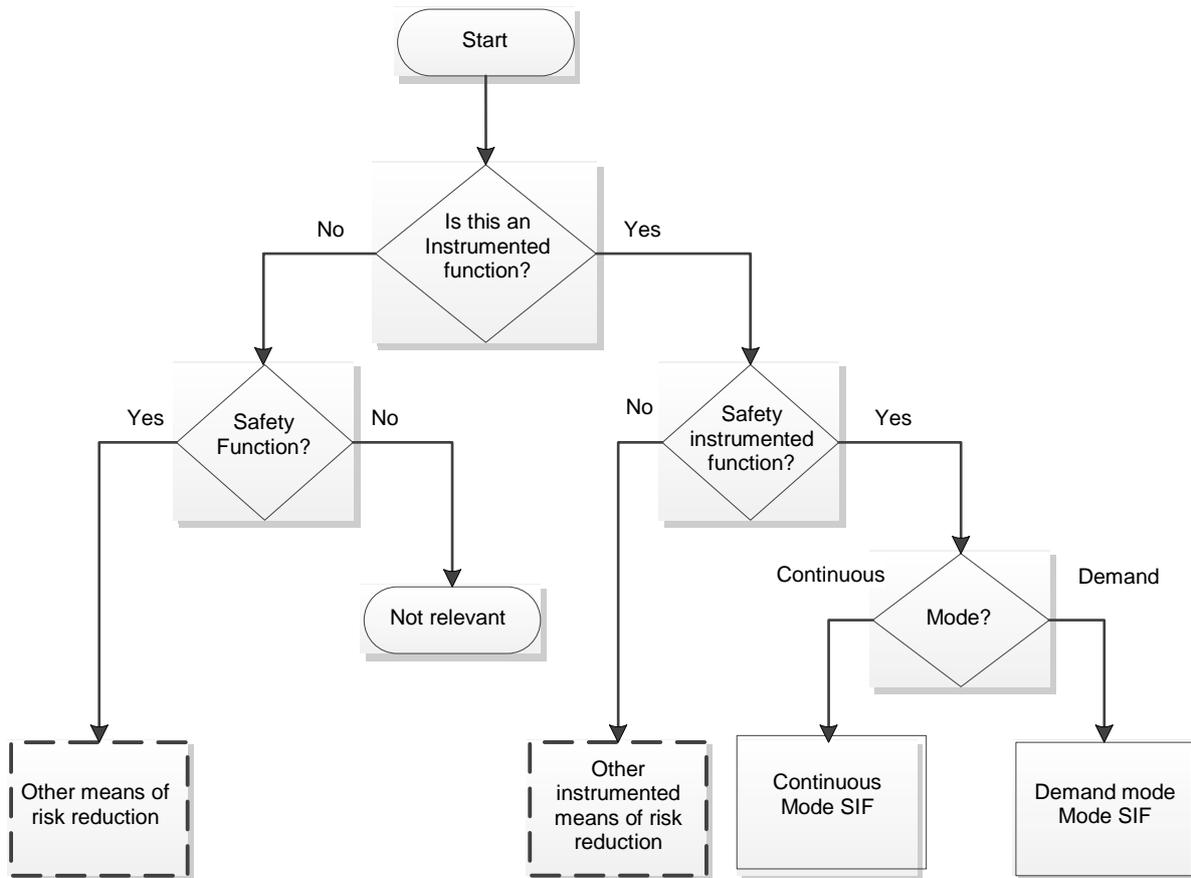


Figure 3 – Detailed relationship between IEC 61511 and IEC 61508

NOTE 4 Subclause 7.2.2 in IEC 61511-1:2016 and A.7.2.2 in IEC 61511-2:2016 contain guidance on handling integration of sub-systems that comply with other standards (such as machinery, burner, etc.).



Standard specifies activities which are to be carried out but requirements are not detailed

IEC

Figure 4 – Relationship between safety instrumented functions and other functions

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General Requirements*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*