

INTERNATIONAL STANDARD



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

IEC 61511-1:2016

<https://standards.iteh.ai/catalog/standards/iec/361c0fa3-af20-46c6-aa33-02db10e53012/iec-61511-1-2016>



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 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 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: csc@iec.ch.

[IEC 61511-1:2016](https://standards.iteh.ai/catalog/standards/iec/361c0fa3-af20-46c6-aa33-02db10e53012/iec-61511-1-2016)

<https://standards.iteh.ai/catalog/standards/iec/361c0fa3-af20-46c6-aa33-02db10e53012/iec-61511-1-2016>



IEC 61511-1

Edition 2.0 2016-02
REDLINE VERSION

INTERNATIONAL STANDARD



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

[IEC 61511-1:2016](https://standards.iteh.ai/catalog/standards/iec/361c0fa3-af20-46c6-aa33-02db10e53012/iec-61511-1-2016)

<https://standards.iteh.ai/catalog/standards/iec/361c0fa3-af20-46c6-aa33-02db10e53012/iec-61511-1-2016>

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 25.040.01

ISBN 978-2-8322-3216-3

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

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	2
1 Scope.....	9
2 Normative references.....	14
3 Terms, definitions and abbreviations	15
3.1 Terms	15
3.2 Terms and definitions	15
3.3 Abbreviations	38
4 Conformance to the IEC 61511-1:2016.....	39
5 Management of functional safety.....	39
5.1 Objective	39
5.2 Requirements.....	39
5.2.1 General	39
5.2.2 Organization and resources.....	39
5.2.3 Risk evaluation and risk management.....	40
5.2.4 Safety planning	40
5.2.5 Implementing and monitoring.....	40
5.2.6 Assessment, auditing and revisions	41
5.2.7 SIS configuration management.....	44
6 Safety life-cycle requirements	44
6.1 Objectives.....	44
6.2 Requirements.....	45
6.3 Application program SIS safety life-cycle requirements	47
7 Verification	50
7.1 Objective	50
7.2 Requirements.....	50
8 Process H&RA.....	52
8.1 Objectives.....	52
8.2 Requirements.....	52
9 Allocation of safety functions to protection layers	53
9.1 Objectives.....	53
9.2 Requirements of the allocation process	54
9.3 Additional requirements for safety integrity level 4	56
9.3 Requirements on the basic process control system as a protection layer	56
9.4 Requirements for preventing common cause, common mode and dependent failures	58
10 SIS safety requirements specification (SRS).....	58
10.1 Objective	58
10.2 General requirements.....	58
10.3 SIS safety requirements	58
11 SIS design and engineering	60
11.1 Objective	61
11.2 General requirements.....	61
11.3 Requirements for system behaviour on detection of a fault.....	63
11.4 Requirements for Hardware fault tolerance	63

11.5	Requirements for selection of components and subsystems devices	65
11.5.1	Objectives	67
11.5.2	General requirements	67
11.5.3	Requirements for the selection of components and subsystems devices based on prior use	67
11.5.4	Requirements for selection of FPL programmable components and subsystems devices (e.g., field devices) based on prior use	69
11.5.5	Requirements for selection of LVL programmable components and subsystems (for example, logic solvers) devices based on prior use	69
11.5.6	Requirements for selection of FVL programmable components and subsystems (for example, logic solvers) devices	70
11.6	Field devices	70
11.7	Interfaces	71
11.7.1	General	71
11.7.2	Operator interface requirements	71
11.7.3	Maintenance/engineering interface requirements	72
11.7.4	Communication interface requirements	73
11.8	Maintenance or testing design requirements	73
11.9	SIF probability of failure Quantification of random failure	74
12	Requirements for application software, including selection criteria for utility software	
12.1	Application software safety life cycle requirements	
12.2	Application software safety requirements specification	
12.3	Application software safety validation planning	
12.4	Application software design and development	
12.5	Integration of the application software with the SIS subsystem	
12.6	FPL and LVL software modification procedures	
12.7	Application software verification	
12	SIS application program development	92
12.1	Objective	92
12.2	General requirements	92
12.3	Application program design	93
12.4	Application program implementation	94
12.5	Requirements for application program verification (review and testing)	95
12.6	Requirements for application program methodology and tools	96
13	Factory acceptance test (FAT)	76
13.1	Objective	96
13.2	Recommendations	96
14	SIS installation and commissioning	98
14.1	Objectives	98
14.2	Requirements	98
15	SIS safety validation	99
15.1	Objective	99
15.2	Requirements	99
16	SIS operation and maintenance	102
16.1	Objectives	102
16.2	Requirements	102
16.3	Proof testing and inspection	104
16.3.1	Proof testing	104
16.3.2	Inspection	105

16.3.3	Documentation of proof tests and inspection.....	105
17	SIS modification	105
17.1	Objectives.....	105
17.2	Requirements.....	106
18	SIS decommissioning	106
18.1	Objectives.....	106
18.2	Requirements.....	107
19	Information and documentation requirements	107
19.1	Objectives.....	107
19.2	Requirements.....	107
	Bibliography	108

Figure 1	– Overall framework of the IEC 61511 series	8
Figure 2	– Relationship between IEC 61511 and IEC 61508.....	11
Figure 3	– Detailed relationship between IEC 61511 and IEC 61508 (see clause 1).....	12
Figure 4	– Relationship between safety instrumented functions and other functions.....	14
Figure 5	– Programmable electronic system (PES): structure and terminology.....	28
Figure 6	– Example of SIS architectures comprising three SIS subsystems	32
Figure 7	– SIS safety life-cycle phases and FSA stages.....	45
Figure 8	– Application program safety life-cycle and its relationship to the SIS safety life-cycle.....	48
Figure 9	– Typical protection layers and risk reduction methods found in process plants means	57
Figure 11	– Application software safety life cycle (in realization phase).....	
Figure 12	– Software development life cycle (the V-model).....	
Figure 13	– Relationship between the hardware and software architectures of SIS.....	

Table 1	– Abbreviations used in IEC 61511	38
Table 2	– SIS safety life-cycle overview (1 of 2).....	46
Table 3	– Application program safety life-cycle: overview (1 of 2).....	49
Table 4	– Safety integrity levels requirements: probability of failure on demand PFDavg	54
Table 5	– Safety integrity levels requirements: average frequency of dangerous failures of the SIF	54
Table 5	– Minimum hardware fault tolerance of PE logic solvers	
Table 6	– Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers	
Table 6	– Minimum HFT requirements according to SIL	66
Table 7	– Application software safety life cycle: overview	

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**FUNCTIONAL SAFETY –
SAFETY INSTRUMENTED SYSTEMS
FOR THE PROCESS INDUSTRY SECTOR –****Part 1: Framework, definitions, system,
hardware and ~~software~~ 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 redline version of the official IEC Standard allows the user to identify the changes made to the previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

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.

<https://standards.iteh.ai/catalog/standards/iec/361c0fa3-af20-46c6-aa33-02db10e53012/iec-61511-1-2016>

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.

The contents of the corrigendum of September 2016 have been included in this copy.

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 ~~requires~~ 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 ~~so that their contribution can be taken into account when considering with respect to~~ the performance requirements for the SIS. The SIS includes all ~~components and subsystems~~ 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 (~~see Annex A~~).

The IEC 61511 series sets out an approach for SIS safety life-cycle activities to achieve these minimum ~~standards~~ 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:

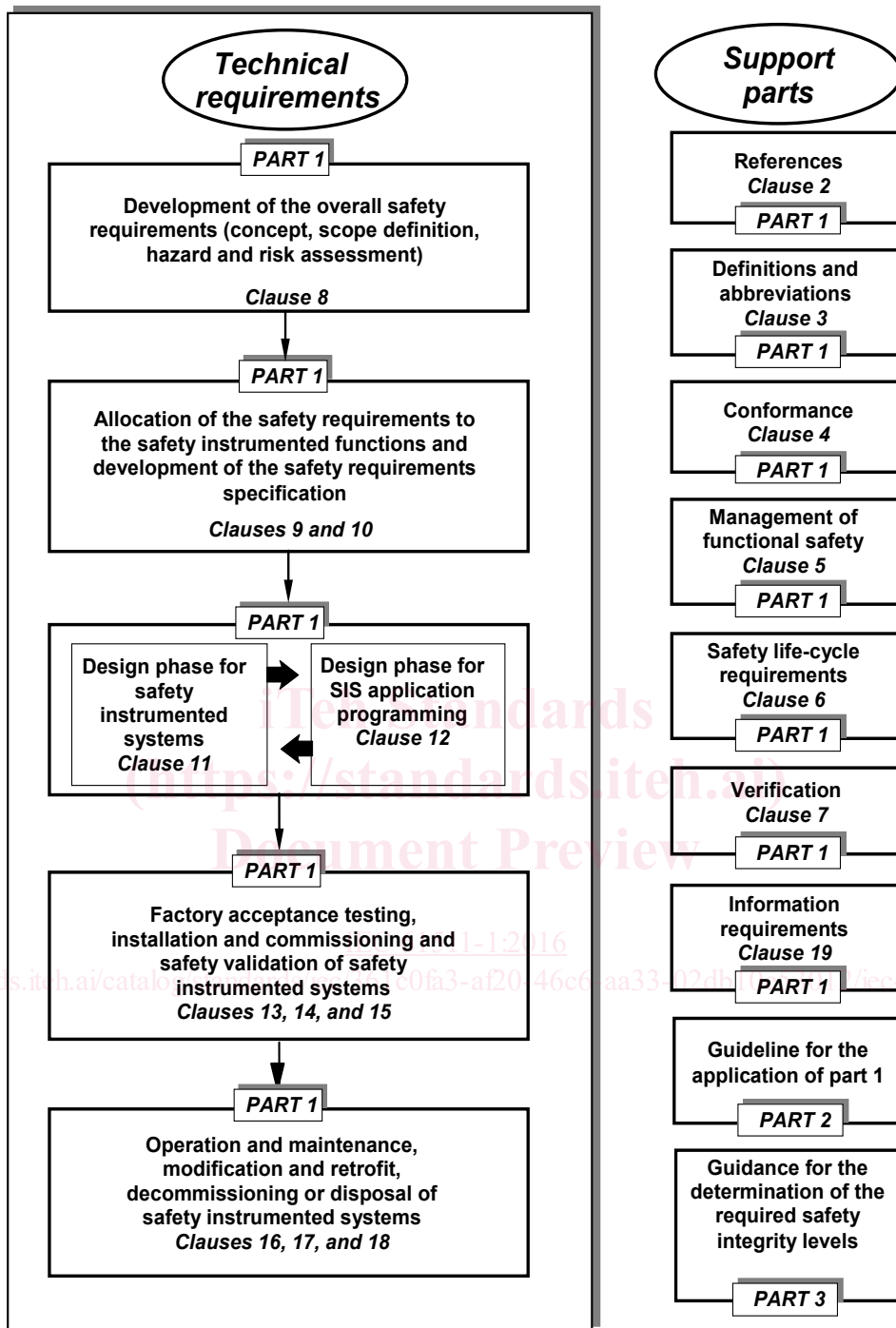
- ~~requires~~ addresses that a H&RA is carried out to identify the overall safety requirements;
- ~~requires~~ addresses that an allocation of the safety requirements to the SIS is carried out;
- works within a framework which is applicable to all instrumented ~~methods~~ means of achieving functional 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 ~~requirements~~ 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 ~~software~~ 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 ~~place and/~~ 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 ~~equipment~~ 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 ~~software is~~ programs are developed for systems having limited variability language or when using fixed ~~programmes~~ 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 refining~~, oil and gas ~~production~~, pulp and paper, pharmaceuticals, food and beverage, and non-nuclear power generation;
- NOTE 1 Within the process sector some applications, ~~(for example, off shore)~~, 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 ~~means~~ methods;
 - h) specifies life-cycle requirements for system architecture and hardware configuration, application ~~software~~ programming, and system integration;
 - i) specifies requirements for application ~~software~~ programming for users and integrators of SISs ~~(clause 12)~~.

~~In particular, requirements for the following are specified:~~

- ~~— safety life-cycle phases and activities that are to be applied during the design and development of the application software (the software safety life-cycle model). These requirements include the application of measures and techniques, which are intended to avoid faults in the software and to control failures which may occur;~~
- ~~— information relating to the software safety validation to be passed to the organization carrying out the SIS integration;~~

~~— preparation of information and procedures concerning software needed by the user for the operation and maintenance of the SIS;~~

~~— procedures and specifications to be met by the organization carrying out modifications to safety software;~~

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) ~~requires~~ 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 ~~methods~~ means.

o) establishes numerical targets for average probability of failure on demand (in demand mode) and average frequency of dangerous failures ~~per hour for the safety integrity levels (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;

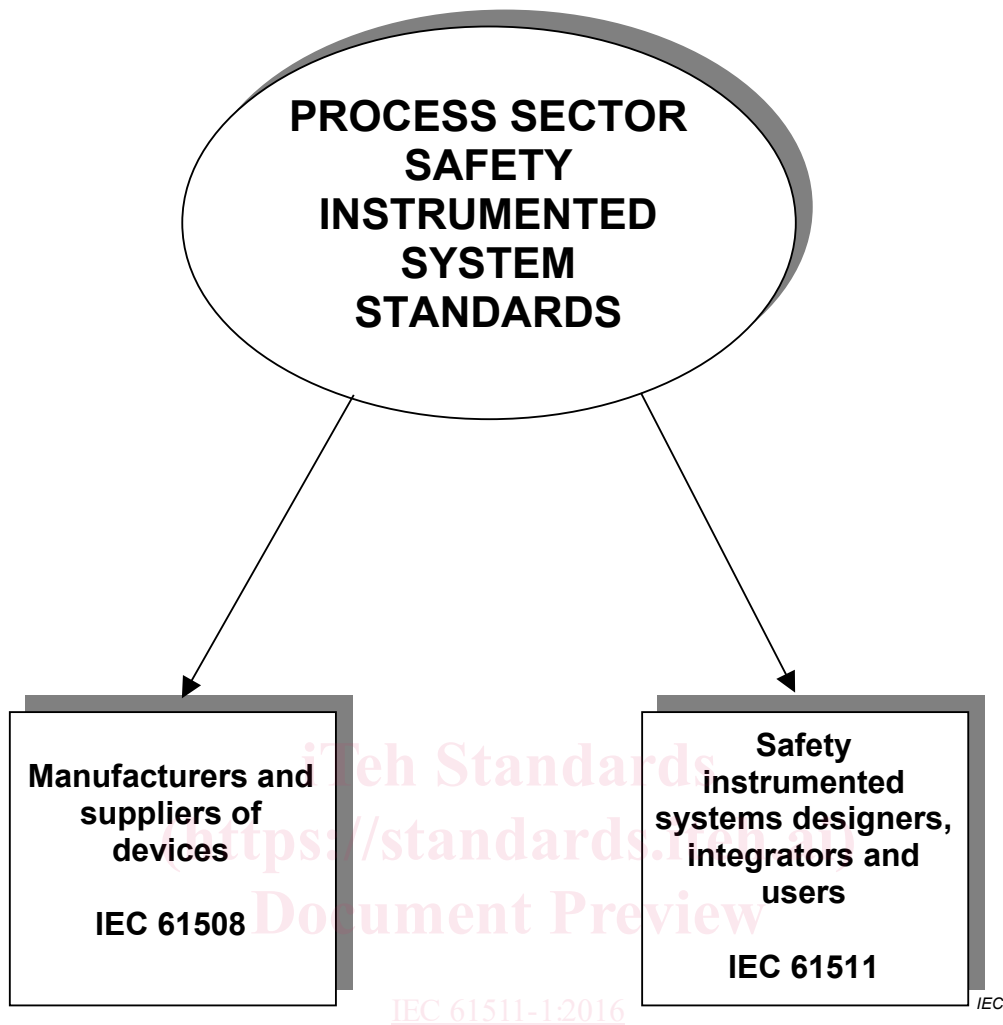
t) provides a framework for establishing the SIL but does not specify the SIL required for specific applications (which should be established based on knowledge of the particular application and on the overall targeted risk reduction);

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) ~~requires~~ 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:



<https://standards.iteh.org/standards/iec-61511-1-2016> Figure 2 – Relationship between IEC 61511 and IEC 61508 [2/iec-61511-1-2016](https://standards.iteh.org/standards/iec-61511-1-2016)

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

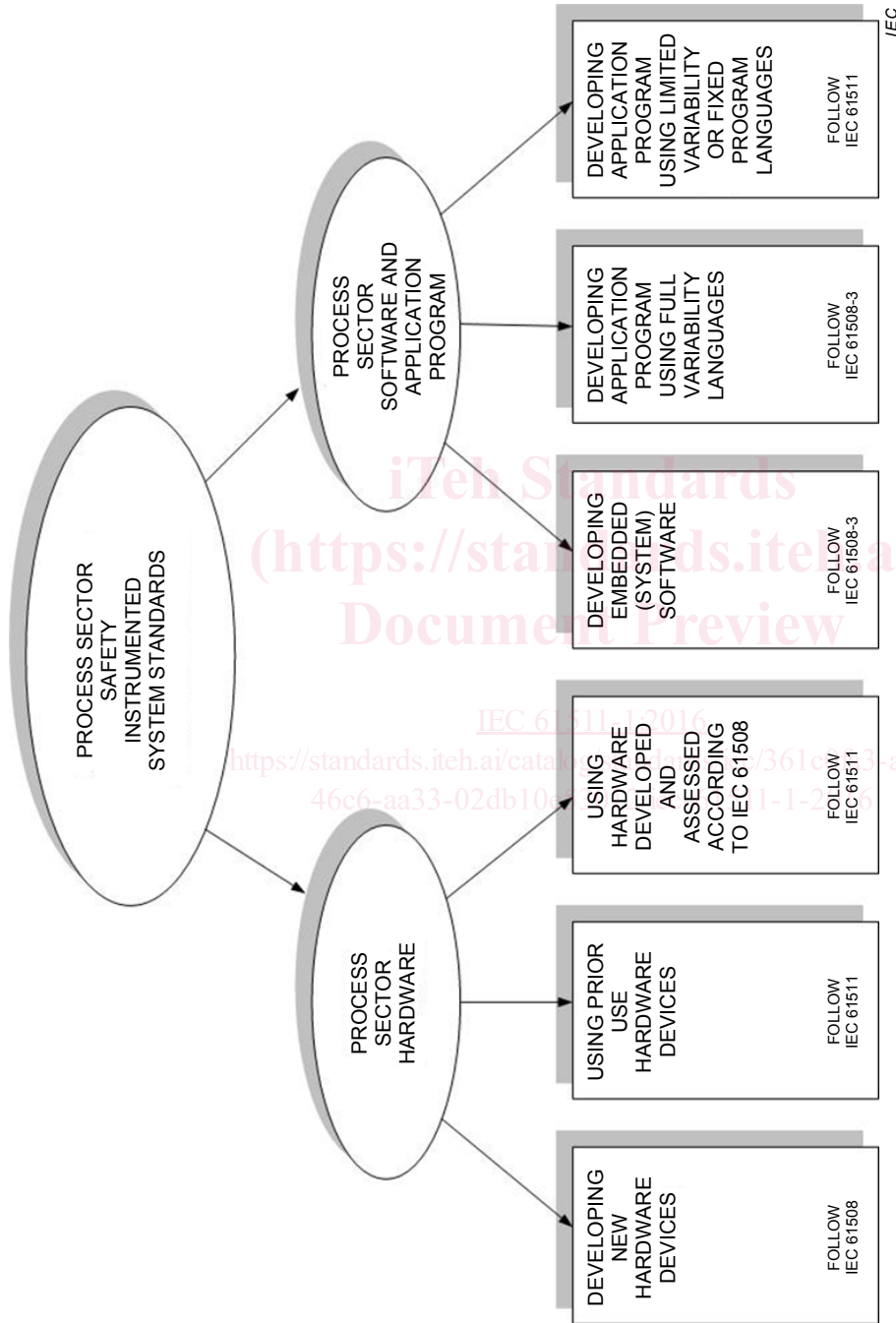


Figure 3 – Detailed relationship between IEC 61511 and IEC 61508 (~~see clause 4~~)

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