

THE ENGINEERING EQUIPMENT AND MATERIALS USERS' ASSOCIATION

Guide to the
Application of IEC 61511
to safety instrumented systems
in the UK process industries

PUBLICATION 222

Edition 1

**Released by IHS
Not for resale**



Copyright © 2009 The Engineering Equipment and Materials Users' Association.
A company limited by guarantee. Registered in England. Company number 477838.

ISBN 0 85931 168 6 Imprint reference 06-2009
Registered and Trading Address
10-12 Lovat Lane London EC3R 8DN
Telephone: +44 (0)20 7621 0011
Fax: +44 (0)20 7621 0022
E-mail: sales@eemua.org
Website: www.eemua.org

ABOUT THE PUBLISHERS

The Engineering Equipment and Materials Users' Association, more commonly known as EEMUA, is a European non-profit membership Association helping companies that own or operate industrial facilities - the *users* of engineering equipment and materials.

EEMUA aims to improve the safety, environmental and operating performance of industrial facilities in the most cost-effective way, thereby demonstrating and pursuing leadership in asset management.

EEMUA Members pursue these aims through collaboration for mutual benefit, sharing engineering experiences and expertise and by promoting their distinct interests as the users of engineering products.

Specifically, the aims of EEMUA Member companies are achieved by:

- providing the organisation within which networking, information sharing and collaboration on non-competitive technical matters can take place;
- influencing the way written regulations are interpreted and applied in practice;
- presenting and promoting Members' views, and encouraging the application of good, sound engineering practices;
- developing user guides, specifications, training and competency schemes;
- facilitating Members' participation in national and international standards making;
- influencing relevant national and European legislation and regulations.

Formed in 1949 as the Engineering Equipment Users Association, and re-named in 1983 (as a result of taking over the materials association, OCMA), EEMUA has for more than fifty years given companies that own and operate process plants, power stations and other significant industrial facilities, a collaborative voice in addressing technical and engineering related issues that impact on good integrity management and asset management practices. The Association is open to companies of all sizes that meet its 'engineering user' criteria. Further details of current Members of EEMUA is available on the Association's website, www.eemua.org.

EEMUA activities often lead to the production of publications. These are prepared for Members' use and are often offered for sale as well.

A list of EEMUA publications for sale is given at the end of this Publication. The full list is also on the Association's website, including details of on-line shopping facilities.

To enquire about corporate Membership, write to enquiries@eemua.org or call +44 (0)20 7621 0011.

ABOUT THIS PUBLICATION

Each authorised copy of this Publication is supplied with an electronic version on CD-rom: attached in a wallet overleaf.

Legal Aspects

All rights, title and interest in this Publication shall belong to EEMUA. All rights are reserved. No part of this Publication, including the CD-rom, may be reproduced, stored in a retrieval system, or transmitted in any form or by any means: electronic, mechanical, photocopying, recording or other, without the express prior written agreement of the EEMUA Executive Director.

Infringement of copyright is illegal and also reduces the Association's income thereby jeopardising its ability to fund the production of future publications.

It has been assumed in the preparation of this Publication that: the user ensures selection of those parts of its contents appropriate to the intended application; and that such selection and application is correctly carried out by appropriately qualified and competent persons for whose guidance this Publication has been prepared. EEMUA and the individual members of the Work Group that prepared this EEMUA Publication do not, and indeed cannot, make any representation or give any warranty or guarantee in connection with material contained herein. EEMUA and the individual members of the Work Group that prepared this EEMUA Publication expressly disclaim any liability or responsibility for damage or loss resulting from the use or reliance on this Publication. Any recommendations contained herein are based on the most authoritative information available at the time of writing and on current good engineering practice, but it is essential for the user to take account of pertinent subsequent developments and/or legislation.

Any person who encounters an inaccuracy or ambiguity when making use of this Publication is asked to notify EEMUA without delay so that the matter may be investigated and appropriate action taken.

Consultation and Feedback

EEMUA encourages constructive comments on this Publication from both Members of the Association and others.

Comments should be sent on the standard feedback form, a copy of which is provided towards the end of this Publication. An electronic version of the feedback form is available from EEMUA - e-mail your request for a copy to enquiries@eemua.org, telephone your request to +44 (0)20 7621 0011, or download the form from the EEMUA website at www.eemua.org. Submit comments by e-mail (preferred) or post.

Comments are considered by the relevant EEMUA Technical Committee and may be incorporated in future editions of this Publication. New editions are published on the EEMUA website.

Contents

Foreword	1
1. Scope	3
2. Terms, Definitions and Acronyms	5
2.1 Terms and Definitions	5
2.2 Acronyms	7
3. Overview of IEC 61511	9
3.1 Background	9
3.2 Scope and Application of IEC 61511	9
3.3 Relationship between IEC 61508 and IEC 61511	9
3.4 Parts of IEC 61511-1	10
3.5 Lifecycle Approach	11
4. Legal Aspects	13
4.1 Health and Safety Legislation	13
4.2 Health and Safety Legislation (Onshore Facilities)	14
4.3 Health and Safety Legislation (Offshore Installations)	14
4.4 Application to Existing Installations	15
4.5 Civil Liabilities	15
5. Common Requirements for all Activities	17
5.1 Responsibilities	17
5.2 Competency	17
5.3 Planning	18
5.4 Verification	18
5.5 Validation	19
5.6 Functional Safety Assessment	19
5.7 Conformity Assessment	22
5.8 Management of Lifecycle Activities	23
5.9 Documentation	23
6. Requirements for Specific Activities	25
6.1 Front End Activities	25
6.2 Application Design and Specification	26
6.3 Integration	34
6.4 Product Supply	39
6.5 Installation	41
6.6 Commissioning	44
6.7 Operation and Maintenance	47
6.8 Modification and Decommissioning	50
Annex A SIL Determination Methods and Calibration	53
Annex B Technology Issues	60
Annex C Example of a Functional Safety Plan Overview	69
Annex D Example Competency Scheme	73
Annex E Example Supplier Safety Validation Plan	82
Annex F Reliability Data and Calculations	94
7. References	99

Tables

Table 1 Application of IEC 61508 and IEC 61511.....	11
Table A.1 Risk graph parameter explanations.....	55
Table A.2 Example consequence equivalence.....	57
Table A.3 Layer of protection analysis (LOPA).....	58
Table D.1 Example generic competence standard.....	75
Table E.1 Quality and functional safety control matrix.....	84
Table F.1 Failure rate data for typical SIS subsystems.....	96
Table F.2 PFD values.....	97

Figures

Figure 1 Safety lifecycle.....	12
Figure 2 Functional safety assessment.....	20
Figure A.1 Risk graph.....	54
Figure F.1 Reliability block diagram.....	96

Foreword

This Guide has been prepared by representatives of EEMUA, the Engineering Equipment and Materials Users' Association; EIC (the Energy Industries Council); Oil & Gas UK (formerly UKOOA) and the Health and Safety Executive (HSE).

It refers throughout to the international standard IEC 61511, which is published in the UK by BSI as BS EN 61511.

This Guide is intended to explain how to use IEC 61511 effectively. It addresses the responsibility and deliverables of organisations involved in the specification, supply and maintenance of safety instrumented systems (SIS). It should be read in conjunction with IEC 61511-1 and, where appropriate, IEC 61508. In any case of apparent discrepancy between this Guide and IEC 61511 or IEC 61508, the IEC standard should be deemed to take precedence.

Chapter 3 provides an overview of IEC 61511-1, Chapter 4 provides an overview of the legal aspects, Chapter 5 focuses on issues that affect all users, and Chapter 6 addresses activities of specific users covering the whole lifecycle of the SIS. Technical detail and examples are given in the annexes.

This Guide takes the form of guidance and recommendations. It should not be quoted as if it was a specification and particular care should be taken to ensure that claims of compliance are not misleading. It must not be used as a basis for conformity assessment.

Where this guidance identifies specific techniques it does not preclude the use of other suitable approaches which comply with IEC 61511.

Whilst every effort has been made to ensure the accuracy of the information contained in this publication, neither EEMUA, EIC, Oil & Gas UK nor any of their members assume liability for any use made thereof.

For future updates of this Guide please use the feedback form at the back of this Publication.

Acknowledgements

EEMUA, EIC and Oil & Gas UK acknowledge participation of the following in the development of this Guide

Matt Atkinson	Stone and Webster Ltd
Simon Brown	Health and Safety Executive
Parvez Butt	Energy Industries Council (affiliation at time of participation)
Mervyn Currie	BP Exploration Operating Company Ltd
Alan Lewendon	Energy Industries Council (affiliation at time of participation)
Roy Lord	BP Oil UK Ltd (affiliation at time of participation)
Huw Morgan	BP Chemicals Ltd
Don Muir	Hydrocarbon Resources Ltd
Ian Parry	Hima-Sella Ltd
Jeff Pearson	Health and Safety Executive
Ian Ramsay-Connell	Trinity Integrated Systems Ltd
Ken Simpson	Functional Safety Consultancy Ltd
John Todman	AMEC plc
Wayne Vernon	Health and Safety Executive

This page is intentionally blank.

1. Scope

This Guide provides guidance and recommendations on IEC 61511-1 and, as appropriate, IEC 61508 for the specification and implementation of safety instrumented systems (SIS) in the UK process industries.

It provides guidance only where it is considered necessary or useful. The relevant sub-clauses of IEC 61511-1 are referenced in a right-hand column. Clauses marked ** give recommendations beyond the scope of IEC 61511-1 where they are worthy of consideration. Such recommendations are considered to be good practice in the UK. This Guide does not take precedence over, repeat or replace any requirement of IEC 61511-1 or IEC 61508.

This Guide is applicable to process industries such as onshore and offshore oil and gas, non-nuclear power generation, chemicals and petrochemicals. Other process industries may choose to use the guidelines at their own discretion.

It outlines general information for all users, plus guidance on organisational responsibilities for end users, designers, suppliers (of systems and products), integrators, installers and maintainers. It does not provide checklists or detail on how to design, operate and maintain such systems.

This Guide is for use in applications relating to safety of people, but its principles may also be applied to environmental and asset/commercial protection.

Note on Terminology

The words "clause" and "sub-clause" refer to parts of IEC 61511, the words "Chapter" and "Section" refer to parts of this Guide.

This page is intentionally blank.

2. Terms, Definitions and Acronyms

2.1 Terms and Definitions

For the purposes of this Guide, the terms and definitions defined in IEC 61511-1, IEC 61508-4 and the following apply.

Availability	Ability of the SIS (under combined aspects of its reliability, maintainability and maintenance support) to perform its required function at a stated time or over a stated period of time. Proportion of time that an item is capable of operating to specification within a large time interval (Smith ^[1]).
Commissioning	Testing of the full functionality of the installed equipment as applicable, e.g. SIS, in order to demonstrate the system meets agreed requirements.
Competent	For a person to be competent they need qualifications, experience and qualities appropriate to their duties. These include: - such training as would ensure acquisition of the necessary knowledge of the field for the tasks that they are required to perform - adequate knowledge of the hazards and failures of the equipment for which they are responsible - knowledge and understanding of the working practices used in the organisation for which they work - the ability to communicate effectively with their peers, with any staff working under their supervision and with their supervisors - an appreciation of their own limitations and constraints, whether of knowledge, experience, facilities, resources, etc., and a willingness to point these out. (Managing competence for safety-related systems, Part 1^[2])
Diagnostic	Automatic function that detects and reports failures or malfunctions of components in the system.
Down time	Period of time that any system or subsystem is not available to perform its required function.
Duty holder	Organisation that has a specific legal duty under health and safety legislation. <i>Note: Depending on the legislation being considered, the duty holder may be an end user, designer, supplier, integrator, installer or maintainer.</i>
Engineering / design body	Engineering organisation carrying out application design but not equipment design, and potentially also procurement of SIS subsystems on behalf of the end user.
Installation	Setting down and fixing equipment in required locations, interconnection of services and signals, and unpowered testing of the equipment and connectivity.
Legacy system	Existing installed system which may or may not conform to current standards.

Override, Bypass, Inhibit	Facility to change or prevent the normal operation of the SIS. <i>Note: During transient conditions, such as start-up, the override would prevent the SIS performing its normal function with either manual or automatic reinstatement.</i>
Prior use	This concept allows the use of existing devices or subsystems providing that sufficient verifiable operational experience and data from very similar applications is available. This avoids the need to comply with the IEC 61508 techniques and measures for avoidance of systematic faults. <i>Note: Modification might render the prior use argument invalid.</i>
Probability of failure on demand (PFD)	Probability that the item, or system, would be in a failed state at time, t For an item of equipment which has a constant failure rate, λ, the probability of failure on demand is given by: $PFD(t) = (1 - e^{-\lambda t})$ It can be shown that, for $\lambda t \ll 1$, then $PFD(t) \approx \lambda t$ When it is subject to periodic proof tests with a time period, T between proof tests, and any dangerous faults are fixed quickly, then the average probability of failure on demand is given by: $PFD_{avg} \approx \lambda T/2$ In this document the term PFD is used to mean PFD_{avg}.
Process safety time	Period of time between a failure occurring in the process or the process control system and the occurrence of the hazardous event if the safety function is not performed (IEC 61508-2). <i>Note: The safety instrumented system should be able to respond quickly enough under worst case conditions to avert the hazardous event.</i>
Reliability	Probability that an item is able to perform a required function under stated conditions for a stated period of time or for a stated demand (Guidelines for process equipment reliability data ^[3]).
Safety PLC	PLC designed and configured with in-built diagnostics and/or hardware voting/configurations, specifically for safety applications.
SIL claims for equipment	Use of SIL X in the description of a component or subsystem is to indicate in "short form" its capability for use in a SIL X application. <i>Note: Appropriate measures for these items would have been adopted to avoid systematic faults. The manufacturer or supplier will provide the required documentation and figures to support the use of the device, i.e. SFF for specified conditions, PFD for defined test intervals, failure modes, hardware fault tolerance and measures for avoiding systematic faults. These may be supported by third party assessment. However, the complete loop has to be analysed before the SIL of the SIF can be determined.</i>

2.2 Acronyms

AK	Anforderungsklasse (Requirement Class)
ALARP	As Low As Reasonably Practicable
API	American Petroleum Institute
BPCS	Basic Process Control System (defined in IEC 61511-1)
BS	British Standard
C&E	Cause and Effects (diagram)
CASS	The CASS Scheme Ltd (Conformity Assessment of Safety Systems) (UK not-for-profit organisation)
COMAH	Control of Major Accident Hazards Regulations 1999 (as amended 2005)
CPU	Central Processing Unit
DIN	Deutsches Institut für Normung (German Institute for Standardisation)
DSEAR	Dangerous Substances and Explosive Atmospheres Regulations 2002
E/E/PE	Electrical/Electronic/Programmable Electronic (defined in IEC 61511-1)
EDP	Emergency Depressurisation
EEMUA	Engineering Equipment and Materials Users' Association
EIC	Energy Industries Council
EMC	Electro-Magnetic Compatibility
ESD	Emergency Shutdown
F&G	Fire and Gas
FAT	Factory Acceptance Test
FDS	Function Design Specification
FMEA	Failure Modes and Effects Analysis
FMEDA	Failure Modes, Effects and Diagnostics Analysis
FSA	Functional Safety Assessment (defined in IEC 61511-1)
GA	General Arrangement (drawing)
GB	Great Britain
HAZID	Hazard Identification
HAZOP	Hazard and Operability (study)
HFT	Hardware Fault Tolerance
HIPPS	High Integrity Pressure/Pipeline Protection System
HMI	Human Machine Interface
HSE	Health and Safety Executive (GB regulator)
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer

ISA	International Society of Automation (previously Instrumentation, Systems, and Automation Society)
ISO	International Organization for Standardization
LOPA	Layer Of Protection Analysis
MTTR	Mean Time to Restoration/Repair
PE	Programmable Electronic
PFD	Probability of Failure on Demand
PFEER	The Offshore Installations (Prevention of Fire and Explosion, and Emergency Response) Regulations 1995
PLC	Programmable Logic Controller
PO	Purchase Order
QA	Quality Assurance
QRA	Quantitative Risk Assessment
RFI	Radio Frequency Interference
RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995
SAT	Site Acceptance Test
SCR	The Offshore Installations (Safety Case) Regulations 2005
SFF	Safe Failure Fraction (defined in IEC 61511-1)
SHE	Safety, Health and Environment
SIF	Safety Instrumented Function (defined in IEC 61511-1)
SIL	Safety Integrity Level
SIS	Safety Instrumented System (defined in IEC 61511-1)
SRS	Safety Requirements Specification
UKOOA	UK Offshore Operators Association, now Oil & Gas UK
UPS	Uninterruptible Power Supply
VDU	Visual Display Unit

3. Overview of IEC 61511

3.1 Background

The need for international standards for safety-related systems based on electrical, electronic and programmable electronic (E/E/PE) technology was recognised by the International Electrotechnical Commission (IEC) in the mid 1980s. The development of IEC 61508 was started at that time and the first parts of IEC 61508 were published in 1998.

IEC 61508 is a generic standard, applicable to any industrial application of E/E/PE safety-related systems. It drew from work on the subject in organisations such as ICI and HSE in the UK, DIN in Germany and ISA in the USA. It put together an overall framework addressing the safety integrity of E/E/PE safety-related systems, taking into account hardware, software, human factors and systems aspects in a risk-based approach towards safety.

Whilst IEC 61508 can, in principle, be applied to any industrial application, the IEC recognised that there would be benefits gained by allowing specific industrial sectors to develop their own standards for E/E/PE safety-related systems, providing that the overall principles and approach of IEC 61508 were observed. This would allow the practice and terminology of the sector to be taken into account.

IEC 61511 is the process sector standard based on IEC 61508. Its overall scope is safety instrumented systems in the process industry sector. It was written by a group of international experts and included substantial contributions from chemical/petrochemical process plant operating companies such as BP, Shell, DuPont, BASF and BNFL.

3.2 Scope and Application of IEC 61511

IEC 61511 is intended for application in a wide variety of industries within the process sector, including chemicals, oil refining, oil and gas production, pulp and paper and non-nuclear power generation. The extent to which application of IEC 61511 is required in order to fulfil legal duties for safety is a matter for the relevant regulatory authorities in the specific country concerned. Whilst IEC 61511 is intended to assist companies fulfil their responsibilities for safety, it should not be seen as defining in absolute terms what may be required for safety in any specific country or application. Operating companies should always be aware of the relevant legal requirements relating to particular applications and countries. Refer to Section 4 for GB legislation.

For offshore oil and gas applications, where both API RP 14C ^[4] and IEC 61511 may be specified, consideration should be given to avoiding potential conflict between their prescriptive and risk-based approaches, by specifying ISO 10418 ^[5] instead of API RP 14C. ISO 10418 is very similar to API RP 14C but refers to IEC 61511 for safety instrumented functions.

3.3 Relationship between IEC 61508 and IEC 61511

IEC 61508 is primarily aimed at ensuring that overall systems, from sensor to final elements, are adequate from a safety viewpoint. In order to achieve this, it makes requirements for both the overall system and the items of equipment that

make up the system. This makes it possible to use IEC 61508 as a basis for assessing the suitability of individual items of equipment for application in a safety-related system.

It should be noted that only some parts of IEC 61508 are relevant to individual items of equipment. Many items of equipment are now available on the market that have been assessed and, in some cases, certified, against IEC 61508.

On the other hand, IEC 61511 is aimed at integrators and users of safety instrumented systems. As part of this, it sets criteria for the selection of equipment to be used in the system. It allows equipment to be selected either on the basis of conformity with IEC 61508, or on the basis of "prior use".

In the case "prior use", IEC 61511 sets criteria based on the extent of the equipment's programmability (fixed program or limited variability) and on the required SIL of the safety functions.

3.4 Parts of IEC 61511-1

IEC 61511-1 contains all the "normative" requirements of the standard. These are the requirements that have to be complied with if a claim of conformity with IEC 61511 is to be made. The requirements span all the phases of the risk assessment, specification, design, engineering, installation, commissioning, validation, operation, maintenance, modification and eventual decommissioning of a safety instrumented system. The standard also includes requirements for safety management, including planning and competency.

IEC 61511-2 provides guidance on the application of IEC 61511-1. For each sub-clause in IEC 61511-1, there is a matching sub-clause in IEC 61511-2 that provides any guidance that the IEC working group thought appropriate. In some cases, no guidance is given.

IEC 61511-3:

- provides guidance on the determination of the required safety integrity levels;
- includes general guidance on risk and safety integrity;
- describes the ALARP and tolerable risk concepts; and
- describes five different methods for determining safety integrity level requirements.

It is important to recognise that these methods need to be calibrated and might need to be adapted for specific process applications. It is the responsibility of the end user to ensure that SIL determination is carried out using a method that is suitable for the specific application.

SIL determination methods and calibration are given in Annex A.

An introduction to the range of technologies available for the implementation of safety functions is given in Annex B.

Table 1 summarises the applicable standards for various activities.

Table 1 Application of IEC 61508 and IEC 61511

Activity	Applicable standard(s)
Specification and design of a safety instrumented system for a specific process sector application	IEC 61511-1 and IEC 61511-3
Selection of equipment for use in a safety-instrumented system on the basis of "prior use"	IEC 61511-1
Conformity assessment of equipment that may be used in a variety of safety-related applications	IEC 61508-2 and IEC 61508-3
Design/development of embedded (system) or full variability software for equipment used in safety-related applications	IEC 61508-3
Design/development of equipment that may be used in a variety of safety-related applications	IEC 61508-2 and IEC 61508-3
Development of limited variability application software for a specific process sector application (e.g. PLC ladder logic)	IEC 61511-1
Installation, commissioning, operation and maintenance of a safety instrumented system in a specific process sector application	IEC 61511-1

3.5 Lifecycle Approach		IEC 61511-1 sub-clauses
3.5.1	The lifecycle approach recognises that having effective safety instrumented systems requires much more than specifying, supplying and installing sensors, logic and final elements. The overall context of the processing facility needs to be understood, as does the role of other non-SIS means of protection. This is to enable a holistic picture of risks and how they are managed, from early design activities through operations and maintenance until final decommissioning, to be understood.	
3.5.2	The safety lifecycle phases are identified by numbers in Figure 1. IEC 61511-1 Figure 8 also identifies the clauses that detail the respective requirements for each lifecycle activity.	Figure 8
3.5.3	Annex C provides an example of an overview of a functional safety plan detailing, for each lifecycle phase, the objectives, inputs, outputs, person or organisation responsible, tools and processes and target dates.	Table 2

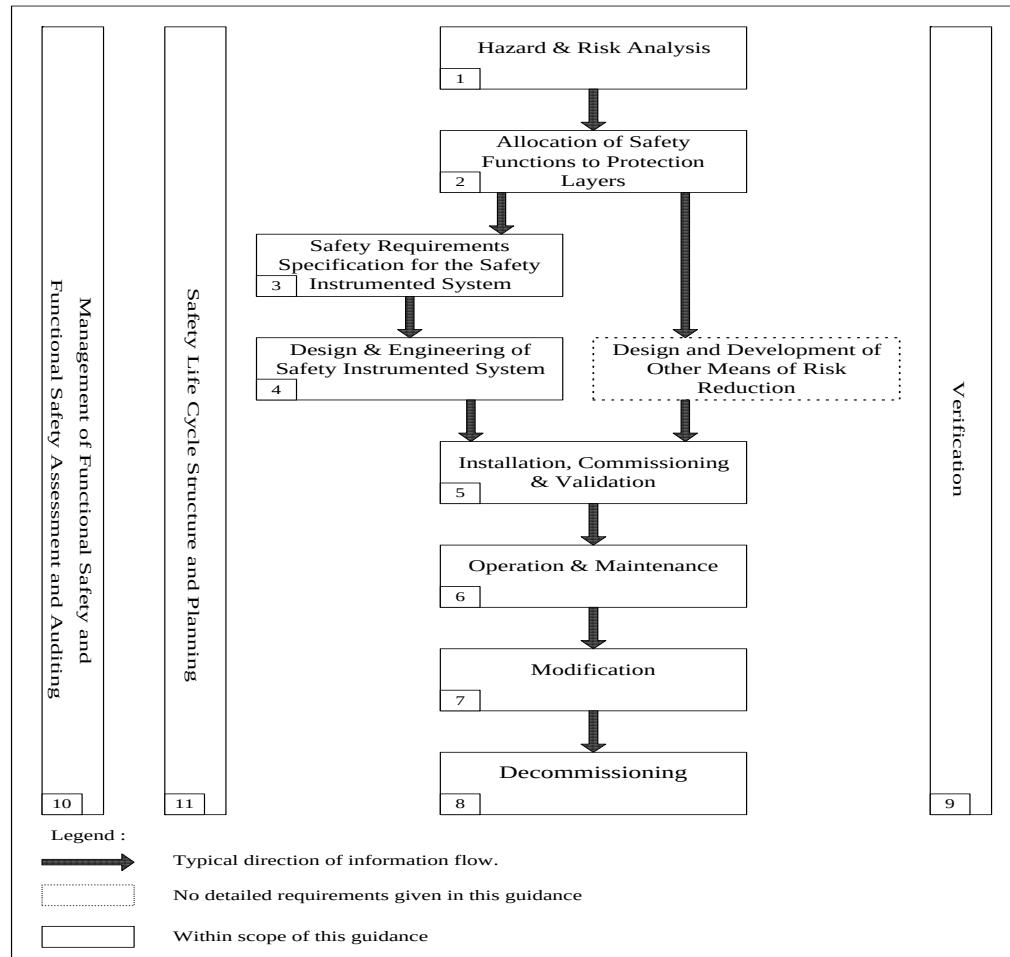


Figure 1 Safety lifecycle

4. Legal Aspects

4.1 Health and Safety Legislation

4.1.1 General Aspects

The Health & Safety at Work etc. Act 1974 ^[6] is the 'top level' legislation for workplace health and safety in Great Britain. It places a general duty on both employers and employees to ensure safety, so far as is reasonably practicable. It also places duties on any person who designs, manufactures, imports or supplies any article for use at work to:

- ensure, so far as is reasonably practicable, that the article is so designed and constructed that it shall be safe at all times;
- carry out testing and examination as may be necessary to ensure the article is safe;
- provide adequate information about the use for which the article is designed and tested to ensure it shall be safe;
- take steps to ensure, so far as is reasonably practicable, that persons who have been supplied with the article are provided with any revisions of information that may be necessary to ensure safety.

Regulations made under the Health & Safety at Work etc. Act provide more specific requirements for particular applications (for example, see Sections 4.2 and 4.3 below).

The Health and Safety Executive (HSE) interpretation of ensuring safety 'so far as is reasonably practicable' is that risks should be reduced to a level that is 'as low as reasonably practicable' (ALARP). Broadly this means reducing risks to a level beyond which the cost of any further risk reduction is 'grossly disproportionate' compared with the benefit gained (Ref ^[7]).

In general terms, HSE relies on authoritative documented sources of good practice, such as the Health and Safety Executive's Approved Codes of Practice (these have a special legal status), HSE guidance and British or international standards such as IEC 61508 and IEC 61511 when assessing whether risks have been reduced to a level which is ALARP.

4.1.2 IEC 61511 and ALARP

IEC 61511 is now generally accepted in the control systems community internationally as setting the benchmark of good practice in the process and related industries.

The overriding legal requirement in GB is that risks are reduced 'so far as is reasonably practicable' (SFAIRP). HSE uses the term 'as low as is reasonably practicable' (ALARP) to mean essentially the same. The use of IEC 61511 assists in demonstrating that risks have been reduced to a level that is SFAIRP/ALARP.

Duty holders are free to take other action to ensure that risks relating to the use of safety related control and protection systems are ALARP.

4.2 Health and Safety Legislation (Onshore Facilities)

4.2.1 Control of Major Accident Hazards

Conformity with IEC 61511 assists duty holders in demonstrating compliance with the Control of Major Accident Hazards Regulations 1999 (COMAH) ^[8] (as amended by the Control of Major Accident Hazards (Amendment) Regulations 2005 ^[9]), in particular:

- Regulation 4: Every operator shall take all measures necessary ...
- Schedule 4, Part 1, 3: demonstrating that adequate safety and reliability have been incorporated ...
- Schedule 4, Part 2, 4c: description of technical parameters and equipment ...

4.2.2 Dangerous Substances and Explosive Atmospheres Regulations

Conformity with IEC 61511 assists duty holders in demonstrating compliance with the Dangerous Substances and Explosive Atmospheres Regulations 2002 (DSEAR) ^[10], in particular:

- Regulation 5: ... the employer shall make a suitable and sufficient assessment of the risks to his employees ...
- Regulation 6 (3): ...the employer shall, so far as is reasonably practicable, apply measures, consistent with the risk assessment and appropriate to the nature of the activity or operation - (a) to control risks ...
- Regulation 6 (8): ... the employer shall, so far as is reasonably practicable, take the general safety measures specified in Schedule 1 ...
- Schedule 1, 3: Designing, constructing, assembling, installing, providing and using suitable work processes so as to reduce risk.
- Schedule 1, 4: Maintaining work processes in an efficient state, in efficient working order and in good repair.

4.3 Health and Safety Legislation (Offshore Installations)

There are a number of offshore-specific legal requirements relevant to safety instrumented control, prevention, protection and mitigation systems.

4.3.1 Safety Case Regulations

Conformity with IEC 61511 assists duty holders in demonstrating compliance with the Offshore Installations (Safety Case) Regulations 2005 (SCR) ^[11], in particular:

- Regulation 12 (1) (d): all major accident risks have been evaluated and measures have been, or will be, taken to control those risks to ensure that the relevant statutory provisions will be complied with.
- Regulation 19: ... shall ensure that a record of the safety-critical elements and the specified plant is made ... a verification scheme ... is drawn up ...
- Schedule 7: Matters to be provided for in a verification scheme ... 3. The nature and frequency of examination and testing.

4.3.2 Prevention of Fire and Explosion, and Emergency Response Regulations

Conformity with IEC 61511 assists duty holders in demonstrating compliance with the Offshore Installations (Prevention of Fire and Explosion, and Emergency Response) Regulations 1995 (PFEER) ^[12], in particular:

- Regulation 4: ... appropriate measures ... protecting persons ... from fire and explosion ...
- Regulation 5: ... assessment of ... events which could give rise to ... a major accident involving fire or explosion ... and the establishment of appropriate standards of performance ... and the selection of appropriate measures ... (The guidance refers to the establishment of performance standards of functionality and availability which may be qualitative or quantitative.)
- Regulation 9: ... appropriate measures to ... prevent uncontrolled release of flammable or explosive substances ...
- Regulation 10: ... appropriate measures ... to detect fire and ... accumulations of flammable or toxic gases ... and conveyed to places from which control action can be instigated ... (alarms).
- Regulation 11: ... audible and, where necessary, visual alarms ...
- Regulation 12: ... appropriate measures to ... limiting the extent of an emergency ... including combat fire and explosion ... to provide, where appropriate, remote operation of plant ... (*Note: e.g. ESD, Blowdown, EDP*). (The HSE guidance to this regulation requires automatic operation where reasonably practicable.)
- Regulation 13: ... protecting persons ... from the effects of fire and explosion ... and any arrangements are capable of remaining effective in an emergency ...

4.4 Application to Existing Installations

The overall duties under the Health and Safety at Work etc. Act are to ensure, so far as is reasonably practicable, the safety of employees, and to ensure, so far as is reasonably practicable, that other persons are not exposed to risks to their health or safety.

These duties apply in relation to all installations whether they existed at the time of the publication of IEC 61511 or have been designed and constructed since the publication of the standard. In that sense, publication of IEC 61511 has not changed the absolute legal requirements. (See Section 4.1.2.)

Those who are responsible for existing (legacy) plant should be familiar with the standard and should be aiming to demonstrate conformity with the requirements of the standard over a period of time. This means balancing the associated risks against the cost and trouble of further risk reduction in line with the ALARP principle. For plant that has operated safely over a period of time, it may well be that no physical changes are required in order to achieve this.

4.5 Civil Liabilities

The Consumer Protection Act 1987 ^[13] applies to goods used at a place of work as well as all consumer goods. It gives people injured by defective products the right to sue for damages. An injured person can take action against a "producer"

(usually the manufacturer), an importer or an "own-brander" (a supplier who puts their name on a product and gives the impression that they are the producer). What classifies as a "producer" of a safety instrumented system may vary according to circumstances but, for example, a system integrator may be regarded as a "producer".

If it can be proved that, on the balance of probabilities, a defect in a safety instrumented system contributed to death, personal injury or damage to private property, then a person who has suffered harm has a right to sue the producer for damages. There is no need to prove that the producer was in any way negligent, but only that the system was defective and that the defect contributed to the harm.

Liability under this Act extends to suppliers of components and subsystems. If it can be shown that a defect in a component or subsystem contributed to the harm, both the system producer and the supplier of a component or subsystem may be liable.

The Act does not extend to pure information. For example, a design consultant would not be liable under the Act for a mistake in a design that causes a system to be defective. Similarly, liability does not extend to a supplier of software, only to the producer of the overall system. However, note that a supplier of software may have criminal liability under health and safety legislation. It should be noted that the Act places no financial limit on a producer's total liability (Guide to the Consumer Protection Act 1987, ^[14]).

5. Common Requirements for all Activities

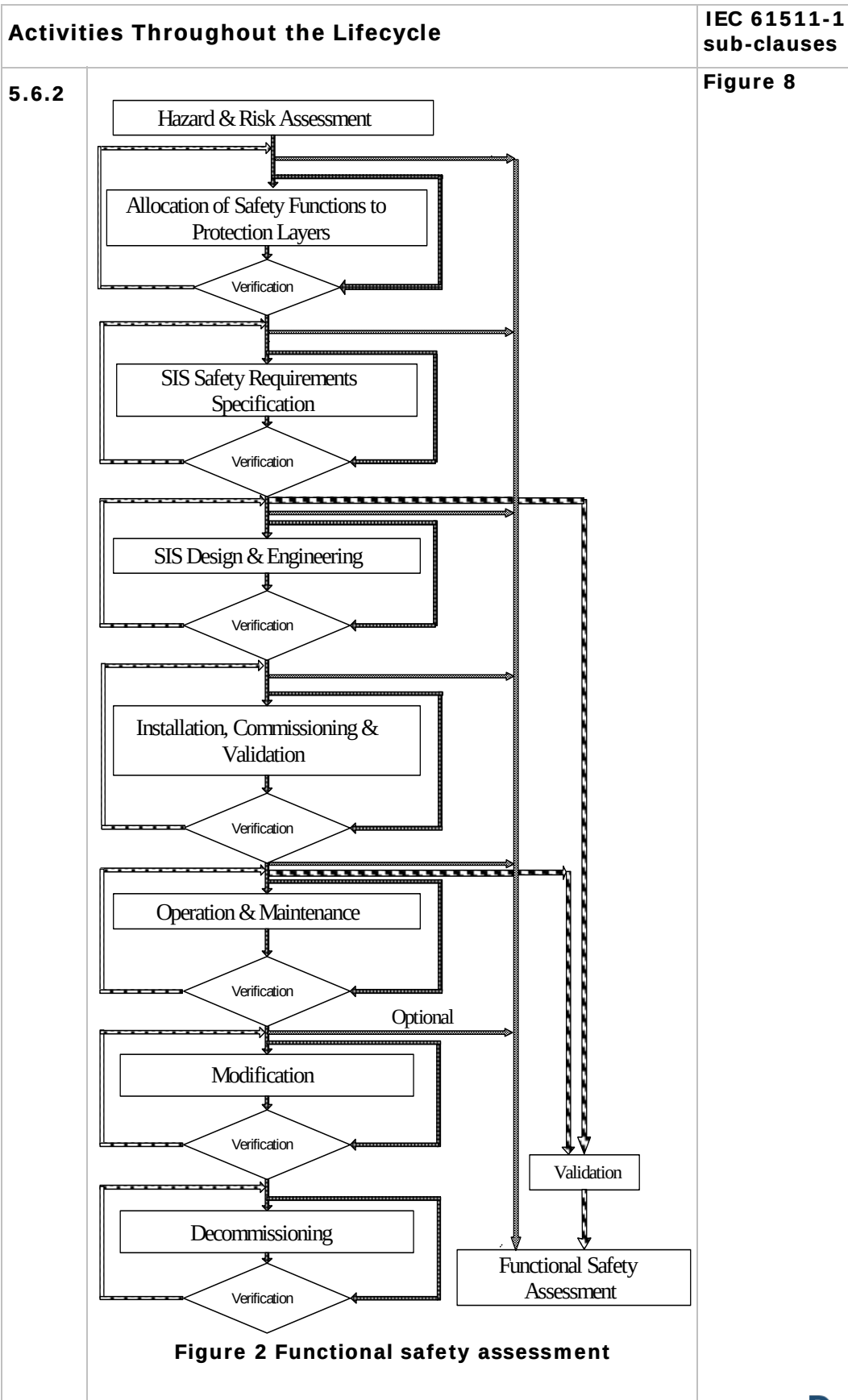
Note: This Chapter lists recommendations applicable to all lifecycle activities. Further requirements for specific activities are stated in the respective parts of Chapter 6.

*** Recommendations beyond the scope of IEC 61511-1*

Activities Throughout the Lifecycle		IEC 61511-1 sub-clauses
5.1 Responsibilities		
5.1.1	If conformance of safety instrumented systems to IEC 61511 is intended, it is the responsibility of management to ensure that the necessary organisational structure and procedures are in place to implement the requirements of the standard.	5.2.1
5.1.2	IEC 61511 requires that persons, departments or organisations responsible for carrying out or reviewing any of the lifecycle phase activities should be identified and should be informed of the responsibilities assigned to them.	5.2.2.1
5.2 Competency		
5.2.1	The standard requires that personnel, departments or organisations involved in safety lifecycle activities at SIL 1 or higher are competent to carry out the activities for which they are accountable. Ref ^[2] is the HSE's guidance on competence management systems.	5.2.2.2
5.2.2	Roles should be defined for such personnel, departments and organisations that state required competencies in terms of engineering knowledge, training and experience, and personal qualities appropriate to the: • process application; • technologies used; • sensors and final elements; • complexity; • integrity levels involved; and • management and other activities as applicable.	5.2.2.2 notes
5.2.3	The competence of persons, departments or organisations carrying out safety lifecycle activities should be assessed against the requirements of the respective roles, including evidence of familiarity with IEC 61508 and IEC 61511. These assessments should be documented. An example personnel competency scheme is provided in Annex D. Ref ^[15] has competence criteria for safety-related system practitioners supporting the competence management system in ^[2] .	5.2.2.2 **
5.2.4	Any shortfalls in competence should be identified and compensating measures put in place. These may include restricting a person's responsibilities until he/she is deemed competent in a particular area and using an additional person who is competent in the particular area to check or supervise the work of the person concerned.	**

Activities Throughout the Lifecycle		IEC 61511-1 sub-clauses
5.2.5	Ongoing training should be provided to ensure that personnel remain competent to perform their responsibilities. This is particularly important where personnel are rarely required to use related skills, e.g. maintenance of highly reliable SIS and operator action in a process upset situation when an automatic protection function has failed.	5.2.2.2 16.2.4
5.2.6	Organisations and departments should be able to demonstrate implementation of a functional safety management scheme covering the lifecycle activities within their scope.	**
5.2.7	Use of organisations with accredited competency schemes in the development and use of safety instrumented systems is encouraged. However, accountability for safe operations remains with the duty holder. CASS provides a methodology to allow an organisation to obtain accreditation of their functional safety capability.	**
5.3 Planning		
5.3.1	The safety planning required by the standard may be incorporated into a wider project or activity plan and should be updated with the lifecycle development. <i>It should be noted that implementation of IEC 61511 may require more resources in early stages of the project compared with previous approaches. However experience has shown that this reduces the burden of demonstrating that an adequate level of safety has been achieved.</i>	5.2.4 Note
5.3.2	The functional safety plan should identify the activities to be carried out and the persons, department or organisation that would carry out these activities.	5.2.4 6.2
5.3.3	The functional safety plan should also identify, for each lifecycle activity, the criteria, techniques, measures and procedures to ensure the activity is correctly carried out and the verification required.	6.2.3 7
5.3.4	Example summary tables listing lifecycle activities with their objectives, inputs and outputs are given in IEC 61511-1, Table 2. These need to be related to the responsible persons, department or organisation, and also tools and processes to be used. Target dates, document numbers and descriptors can be added, as shown in the overview example in Annex C.	Table 2
5.4 Verification		
5.4.1	Verification should be planned, carried out and documented for each lifecycle activity. Examples of verification activities are design reviews and audit of installation and commissioning procedures. The aim of verification is to ensure that the outputs from each phase of the lifecycle meet the objectives and requirements set for the lifecycle phase.	7 12.7

Activities Throughout the Lifecycle		IEC 61511-1 sub-clauses
5.4.2	Verification procedures should identify the criteria, techniques and tools to be used and the personnel to be involved. Procedures for Factory Acceptance Testing (FAT) of systems or subsystems are an example. However, for a system integrator, the FAT could be considered as part of their validation process.	7.1.1 **
5.4.3	Verification can normally be carried out by the person or team that carried out the activity unless there is significant complexity or novelty or high SILs are involved. <i>Note: There is no requirement in the standard for independent verification. However this should not be confused with requirements for verification in the Offshore Installations (Safety Case) Regulations.</i>	7.1.1.2 Note
5.5 Validation		
5.5.1	Validation should be planned, carried out after installation and documented. Site Acceptance Testing (SAT) and commissioning may be considered as part of validation. Factory Acceptance Testing (FAT) would be validation for a system integrator.	15
5.5.2	Validation procedures should provide assurance that the SIS safety requirements specification has been met and that any recommendations from earlier verification activities and reviews have been satisfactorily addressed. All operating modes should be addressed.	15.2
5.5.3	Design tools should also be validated and certified where appropriate. Design tools should be valid for the application.	**
5.5.4	The extent and rigour of validation should be commensurate with the complexity of the SIS, the safety integrity level involved and the confidence gained from verification activities at each earlier phase. It should cover, for example, normal, emergency and erroneous operation, extreme environmental conditions, including EMC, and variations in, and loss of, utilities such as electrical supply (voltage and frequency) and instrument air.	** 15.2.4
5.6 Functional Safety Assessment		
5.6.1	Functional Safety Assessment (FSA), the process culminating in a judgement as to the functional safety and safety integrity achieved, should be planned. A minimum of one assessment should be carried out prior to the introduction of process fluids into the plant. Projects may perform additional assessments if so defined, such as after design and after several years' operation. Figure 2 illustrates the process.	5.2.6.1



Activities Throughout the Lifecycle		IEC 61511-1 sub-clauses
5.6.3	The number and scope of assessment activities should be identified in the safety plan. They depend on the size and complexity of the project, novelty of the technology used and the highest integrity level involved. Assessments would include review of verification reports for each lifecycle phase, together with validation reports. As a minimum, an assessment should be undertaken before commissioning of the plant. Assessments are required when operating conditions, operating competencies or operating staffing levels change materially, or when there are plant changes affecting SIS conditions.	5.2.6.1
5.6.4	The assessment team skills should include technical safety, process engineering and operations. IEC 61511 does not specify the level of independent assessment required except that the team should include at least one senior competent person not involved in the project design team. However IEC 61508 states that, at SIL 3, an independent organisation is highly recommended. This may be achievable from within a large company.	5.2.6.1.2 **
5.6.5	The scope of FSA should include software tools used where their use could have a significant impact on safety in any lifecycle phase. Such tools may include those used for SIL determination, programming and configuration, reliability calculation, and the maintenance management system used to schedule proof testing.	5.2.6.1.5

Activities Throughout the Lifecycle		IEC 61511-1 sub-clauses
5.6.6	The functional safety assessment should include consideration of: • hazard and risk assessment; • functional safety management; • safety plan; • hardware details; • minimum hardware fault tolerance; • random failure rates; • expected demand rate; • specification for proof testing and maintenance programme for the equipment; • design processes/systematic failures; • equipment quality; • software design process techniques/measures adopted; • maintenance; • operational and security arrangements; • organisational interfaces; • recommendations to address shortcomings; • verification results; • validation results. It is essential that all analysis should consider the complete system, from input transducer to the actuation of the final control element. The majority of the system hardware dangerous failures are usually due to the field devices and the analysis would be found to be particularly sensitive to variations in these areas. The majority of the systematic failures are due to human error in specifying, implementing, or maintaining the system.	5.2.6.1.4 **
5.6.7	Audits may also be carried out to assure quality and conformance to standards and procedures.	5.2.6.2
5.7 Conformity Assessment		
5.7.1	Third party certification or conformity assessment of people's competency, organisational competency and of systems and subsystems capability is not a requirement of the standard. However, independent review and accreditation increases confidence and can reduce the activities required to assure suitability for the given application.	11.5.2 11.5.3 **

Activities Throughout the Lifecycle		IEC 61511-1 sub-clauses
5.7.2	Use of systems and subsystems that are conformity assessed to specific integrity levels in accordance with IEC 61508 by reputable independent organisations is recommended where practicable. Assessment reports should be read for the conditions they assume and reports should contain full backup of the sources of data and evaluation of techniques and procedures. This does not supersede the requirement to assess complete safety instrumented functions including sensors, logic solver and final elements. <i>Note: Selection may alternatively be based on "prior use", but this demands greater effort to meet the requirements for evidence of suitability.</i>	11.5.2 11.5.3 **
5.7.3	Systems and subsystems implementing safety integrity functions SIL 1 and above should be manufactured under a recognised quality management system such as the ISO 9000 series standards.	5.2.5.2 **
5.8 Management of Lifecycle Activities		
5.8.1	SIS lifecycle activities may be carried out by different organisations and departments within the same organisation. The end user should ensure that systems are in place to provide: • clear accountabilities across the various departments and organisations, including sub-suppliers; • appropriate communication between different parties; • handover of information and delivery of equipment between parties in accordance with the lifecycle plan and activity programme.	**
5.9 Documentation		
5.9.1	All information necessary for specification, implementation, verification and validation (including initial and ongoing proof testing) and the results of assurance activities, operations, maintenance and modification should be documented.	19
5.9.2	Documentation should be: • accurate, readily understandable, relevant to the application and easily accessible; • traceable to the requirements of clauses of IEC 61511; and • version controlled and managed under a formal document control scheme. SIS-specific information should be collected and maintained in a single document file with less specific information referenced from it. Alternatively, if it better fits a company's document management system that SIS-specific documents are held in different locations, a directory of SIS-specific and related documents and their locations should be maintained in an SIS file.	19.2.2 19.2.5 19.2.6 19.2.8

Activities Throughout the Lifecycle	IEC 61511-1 sub-clauses
5.9.3 Documents should be kept up to date throughout the life of the SIS to demonstrate conformity throughout the lifecycle and provide a basis for modifications. These would typically include: • functional safety management plan. This includes documentation of all the management aspects in Chapter 5 of this Guide; • hazard and risk assessment (including integrity level requirements) and associated assumptions; • safety requirement specification; • details of the equipment used for safety instrumented functions; • reliability assessment of equipment used for safety instrumented functions using actual test results where possible; • organisation responsible for maintaining functional safety at each phase of the lifecycle; • procedures required to achieve and maintain functional safety; • details of modifications; • details of design, construction and testing at factory and at site; • functional safety assessment (FSA); • action tracking and follow-up of recommendations from reviews, audits and functional safety assessments; • actual operation experience including the demand rates, systematic failures and failure rates. Further guidance on the documentation requirements for each user category is given in Chapter 6 of this Guide.	19.2.9
5.9.4 An example supplier safety validation plan is included in Annex E.	**

6. Requirements for Specific Activities

Activities at Specific Stages of the Lifecycle		IEC 61511-1 sub-clauses
6.1 Front End Activities		
6.1.1 Introduction		
6.1.1.1	This sub-clause addresses activities that precede Phase 1 activities shown in the safety lifecycle in Figure 1.	-
6.1.1.2	If responsibilities for information provision, design, implementation, verification and assessment are divided between different organisations, the scope, boundaries, boundary conditions and responsibilities of each organisation need to be defined	**
6.1.2 Pre-phase 1 Activities		
6.1.2.1	Before commencing Phase 1 of the safety lifecycle, hazard and risk assessment, the following activities should be completed: • process design well developed but not finalised; • proposed deployment of operations and maintenance people across the process plant defined; • strategy for managing SIS activities from Phase 1 (hazard and risk assessment) to Phase 6 (operation and maintenance) including FSA defined and supported by management; • initial contracts in place, where required, for managing SIS activities; • personnel responsible for carrying out early SIS activities identified and confirmed as competent to perform these activities; • internal company and external standards and procedures applicable to all SIS activities defined and communicated to all affected organisations and personnel. This includes the methods of SIL determination to be used are defined and calibrated in accordance with end user risk tolerability criteria. Annex A provides guidance on SIL determination methods and calibration.	6.2 Table 2 **
6.1.3 Supervision		
6.1.3.1	The end user, who, in most cases, would also be the duty holder with legal responsibility for safe operation of the process plant, should put in place sufficient management of SIS activities to be assured of their correct implementation. This includes initiating audits and/or functional safety assessments.	5.2.1.2

Activities at Specific Stages of the Lifecycle		IEC 61511-1 sub-clauses
6.2 Application Design and Specification		
6.2.1 Introduction		
6.2.1.1	This sub-clause addresses Phases 1 to 3 of the SIS lifecycle as defined in IEC 61511-1. See Figure 1.	-
6.2.1.2	Those responsible for application design and engineering should, in addition to the common recommendations in Chapter 5: • develop a safety plan - Appendix C provides an example overview; • produce a hazard and risk assessment; • develop safety requirements specifications; • develop hardware architectures; • develop agreed proof test intervals; • perform reliability calculations; • carry out procurement with associated certification and assessment reports. They may also support installation, Site Acceptance Test (SAT) and commissioning.	**
6.2.2 Hazard and Risk Assessment and Allocation to SIS Protection Layers		
6.2.2.1	Inherently safe design should be developed as far as reasonably practicable before reliance on SIS to reduce risk. This means, for example, giving priority to full pressure rating of pipework and vessels where practicable.	8.1 Note 2
6.2.2.2	The objective of a hazard and risk assessment and allocation of risk reduction is to: • review the process and identify hazardous events arising from failures of the process, operations or control system that have the potential to either cause a harmful event, environmental event or business threatening event; • identify non-SIS systems or devices in place which would reduce the probability of this event occurring (i.e. mechanical devices, alarms, operational procedures, etc); • identify where SIFs are required and their necessary risk reduction contribution to ensure that risk of the hazardous event is below an acceptable target level. This results in reliability performance requirements for each SIF in the form of a PFD or SIL value. Consideration should be given to any new hazards introduced by operation of each SIF.	8.2.1 9.2

Activities at Specific Stages of the Lifecycle		IEC 61511-1 sub-clauses
6.2.2.3	The methods for carrying out a hazard and risk assessment depend on size and complexity of the project or modification. These can include HAZID, HAZOP, "What If" and desktop studies. For HAZOP, reference should be made to IEC 61882 ^[16]. <i>Some organisations carry out HAZOP studies tailored to control and safety systems, which are known as CHAZOP.</i>	**
6.2.2.4	SIL determination may use risk graphs, LOPA or quantitative assessment methods. Where consequences are particularly severe, fully quantified risk analysis techniques may be required. The team should not be overly conservative in their assessment because increasing a SIL by 1 adds to complexity, capital costs and maintenance requirements, and can increase the spurious trip rate. Requirements for SIL 4 safety functions should be avoided where practicable by changes in the process design or adding diverse layers of protection. SIL 4 safety functions are unlikely to be accepted by the HSE. <i>Note: Risk graphs, LOPA or quantitative methods for PFD or SIL determination can be found in the standards. The designer needs to select, develop and calibrate the method to the end user and project requirements. Examples of calibrated risk graphs and layer of protection analysis (LOPA) are included in Annex A.</i>	9.2.2 9.2.3 **
6.2.2.5	SIL determination should be carried out after HAZOP, or similar hazard and risk assessment techniques, using the same assumptions, where relevant, from the HAZOP study. It is possible to carry out SIL determination integrated with the HAZOP study.	**
6.2.2.6	These studies should each involve a multi-disciplinary team who have knowledge of the process, project, instrument, safety and operation engineering and be carried out for main process and utility systems and also for equipment packages.	8.1 Note 1
6.2.2.7	The design process should provide traceability from the hazard through the SIF requirement to its implementation, e.g. a safety function number could be included in the hazard and risk assessment to uniquely identify the function and link it to a cause and effect diagram or other means of representation.	8.2.3
6.2.2.8	Any software tools used for selecting SILs or PFD requirements should be verified against known manual test cases. Those who use these tools should understand the techniques to be used and how the tools implement the techniques. They should also be able to judge the adequacy of the results.	**

Activities at Specific Stages of the Lifecycle		IEC 61511-1 sub-clauses
6.2.2.9	Accurate and adequate documentation and drawings are required for the SIL determination study. This may include process flow diagrams, or piping and instrument diagrams, cause and effects diagrams, vessel and pipework specifications, HAZOP reports, relief valve specifications and operational staffing plan.	8.2.1 **
6.2.2.10	SIL determination should be documented. This should include assumptions made and credit taken for each protection layer. Particular attention should be given where there are common causes between protection layers and between initiating cause and protection layers, such that either no credit is claimed or appropriate allowance is made for the common cause failures.	8.2.3
6.2.2.11	Where fire and gas detection systems are installed or proposed, their reliability performance should be specified using either risk graphs or LOPA as for process plant protection SIFs, or alternatively, specified at a level that can reasonably be achieved, such as 90% probability of detecting the defined size gas release or fire size and taking any specified action. This performance is checked to ensure that it reduces escalation potential and is adequate when considering ALARP. By exception, detection for particular hazards may require to be more reliable than the assumed 90%. <i>It should be noted that the incremental consequences of a detection system not operating in a given area can vary depending on potential escalation and a range of outcomes may need to be addressed.</i>	**
6.2.2.12	On brownfield sites where an existing safety system is to be included in the plant protection, the new facilities should meet the requirements of IEC 61511. The changes should not jeopardise protection of the existing plant.	**
6.2.3 Safety Requirements Specification		
6.2.3.1	The functional and integrity requirements of all SIFs should be included in the safety requirements specification.	10.3.1