

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

Publication 222

Edition 2

Copyright © 2025 The Engineering Equipment and Materials Users Association
A company limited by guarantee. Registered in England. Company number 477838.

ISBN 978-0-85931-244-8

Imprint reference 09-2025
First published 09-2025

Registered Address and Trading Address:
EEMUA, Leytonstone House, 3 Hanbury Drive, London E11 1GA

Telephone: +44 (0)20 7488 0801
Email: sales@eemua.org
Website: www.eemua.org



Engineering Equipment and Materials Users Association

About EEMUA

The Engineering Equipment and Materials Users Association is usually known by its initials, EEMUA. EEMUA is an Association established by the owners and operators of industrial assets. Any organisation that is a substantial user or substantial purchaser of engineering products may apply to become a member of EEMUA. Membership is subject to the approval of Council.

EEMUA Aims

EEMUA aims to improve the safety, environmental and operating performance of industrial facilities in the most cost-effective way, pursuing and promoting leadership in industrial asset management by sharing engineering experiences and expertise, and by the active, enlightened promotion of the distinct interests of users of engineering products. These aims are achieved by various means, including:

- providing the organisation within which networking, information sharing and collaboration among users on non-competitive technical matters can take place;
- influencing the way written regulations are interpreted and applied in practice;
- promoting and presenting 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; and
- influencing relevant national and European legislation and regulation.

The income and resources of EEMUA are applied solely towards the promotion of the aims of the Association. No profit is transferred by way of dividend, bonus or otherwise to members. The work of the Association is mainly carried out by members' representatives on EEMUA Technical Committees, Working Groups, and Forums, supported by EEMUA staff.

Incorporation, Membership and Other Information

For the purposes of conducting its business, EEMUA is incorporated in England and Wales as a company, limited by guarantee, not having share capital. All usual aspects of company management and business administration are dealt with through the EEMUA Chief Executive, including policy implementation and leadership of the Executive team (the staff).

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 ask@eemua.org or call +44 (0)20 7488 0801.

About this Publication

Legal Aspects

All rights, title and interest in this Publication belong to EEMUA. All rights are reserved. No part of this Publication 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 Chief Executive. 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 ask@eemua.org, telephone your request to +44 (0)20 7488 0801, 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 Committees and may be incorporated in future editions of this Publication. New editions are publicised on the EEMUA website.

Contents

Foreword	IX
Acknowledgements.....	X
1. Scope	1
2. Terms, Definitions and Acronyms	2
2.1 Terms and Definitions	2
2.2 Acronyms	4
3. Overview of IEC 61511	6
3.1 Background.....	6
3.2 Scope and Application of IEC 61511	6
3.3 Relationship between IEC 61508 and IEC 61511	7
3.4 IEC 61511	7
3.5 Lifecycle Approach	8
3.6 Potential Issues with IEC 61511-1	10
4. Legal Aspects	14
4.1 Health and Safety Legislation	14
4.2 Other Health and Safety Legislation	15
4.3 Application to Existing Installations	16
4.4 Civil Liabilities.....	17
5. Common Requirements for all Activities	18
5.1 Responsibilities	18
5.2 Competency.....	19
5.3 Planning.....	21
5.4 Verification.....	22
5.5 Validation	22
5.6 Functional Safety Assessment.....	24
5.7 Audit and Revision	27
5.8 Conformity Assessment.....	27
5.9 Management of Lifecycle Activities	28
5.10 Documentation.....	29
5.11 Change Control and Configuration Management	31

6. Requirements for Specific Activities	32
6.1 Front End Activities.....	32
6.2 Hazard and Risk Assessment and Allocation.....	33
6.3 Functional Safety Requirements	40
6.4 Application Design and Engineering	42
6.5 Integration.....	50
6.6 Equipment Procurement	57
6.7 SIS Installation.....	60
6.8 SIS Commissioning and Process Commissioning	62
6.9 Operation and Maintenance	66
6.10 Modification and Decommissioning	70
7. References.....	72
7.1 Standards Referenced.....	72
7.2 Publications Referenced	73
7.3 Further Reading.....	76
Annex A – Technology Issues.....	77
A.1 Introduction	77
A.2 Assessment and Certification.....	77
A.3 AK Certification versus SIL.....	78
A.4 SIS Architecture	78
A.5 Technologies for Logic Solvers.....	78
Annex B – Example Functional Safety Plan Overview	85
Annex C – Example Competency Scheme.....	88
C.1 Generic Competence Standard	88
C.2 Customised Competence Standard	88
C.3 Assessment Process.....	89
C.4 Competence Management System	90
Annex D – Example Supplier Safety Validation Plan	96
D.1 General.....	96
D.2 Competency	96
D.3 Modifications.....	96
D.4 Specification	97
D.5 Random Hardware Failures.....	97
D.6 Systematic Capability	97
D.7 Assessment of Modules	97
D.8 Language and Tools.....	97
D.9 Code Review and Test.....	97
D.10 Validation	97

Annex E – Reliability and Data Considerations	102
E.1 Device Reliability Data	102
E.2 Function Reliability Analysis	102
E.3 Other Factors affecting Function Reliability	104
E.4 Analysis of Failure Data.....	108
Annex F – Reliability Calculation Method	111
F.1 Terminology.....	111
F.2 Basic Reliability Model	112
F.3 Combining Elements in Series.....	113
F.4 Combining Elements in Parallel.....	114
F.5 Complex Redundancy.....	115
F.6 Mean Time Before Failure.....	116
F.7 Availability and Average Probability of Failure.....	117
F.8 Redundant Systems.....	122
F.9 Proof Testing Strategy	124
F.10 Common Cause Failures	125
F.11 General Formulae for Fault Tolerant Systems.....	126
Annex G – ALARP	129
G.1 General.....	130
G.2 Methods	131
G.3 Calibrating Risk Assessment Tools	132
G.4 Hierarchy of Controls	133
G.5 Cost Benefit Analysis.....	134
Annex H – Tolerable Risk Criteria	137
H.1 UK Legislation and Regulation.....	137
H.2 Individual Frequency of Fatality	139
H.3 Societal Risk.....	142
Annex I – Random and Systematic Failures.....	144
I.1 Random Hardware Failures	144
I.2 Systematic Failures.....	145
I.3 Consequences of Systematic Failures	146
Annex J – Complex Functional Safety	148
J.1 Introduction.....	148
J.2 The Combustion Process	151
J.3 Double Block and Vent Philosophy.....	151
J.4 Safety Function Integrity Requirements.....	152
J.5 Valve Proving Philosophy	152
J.6 Control Philosophy	153

J.7 Gas Isolation Function Failure	155
J.8 Fault Tree.....	156
J.9 Failure Assessment	157
J.10 Final Assessment.....	161
Annex K – Selection of Equipment	162
K.1 SIF Design	162
K.2 Systematic Capability Explained	163
K.3 Conformity to IEC 61508 (Route 1 and Route 2)	163
K.4 Alternative Conformity to IEC 61511 (Prior Use).....	164
K.5 Selection of Components by the User	164
K.6 Hardware Fault Tolerance.....	165
K.7 SC as applied to Synthesis of Elements.....	165
EEMUA Publication: Feedback Form	168
EEMUA Publications Catalogue	169
 Tables	
Table 1 – Application of IEC 61508 and IEC 61511	8
Table B. 1 – Example Functional Safety Plan Overview	85
Table C. 1 – Example Generic Competence Standard.....	90
Table D. 1 – Quality and Functional Safety Control Matrix.....	98
 Figures	
Figure 1 – Safety lifecycle	9
Figure 2 – Functional Safety Lifecycle showing FSA	25
Figure H. 1 – R2P2 Tolerability of Risk	138
Figure H. 2 – Company Tolerability of Risk	139
Figure H. 3 – Societal Risk	142
Figure J. 1 – Double Block and Vent	151
Figure J. 2 – Double Block and Vent Fault Tree	156

Foreword

The first edition of this Guide was 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). This second edition has been extensively revised by EEMUA to reflect the greater maturity of the standards and of the understanding of functional safety in general. The opportunity has been taken to add new material to cover some of the points of difficulty which are likely to be encountered and for which the standards as yet provide very little guidance.

It refers throughout to the international standard IEC 61511, which is published in several parts which are available from BSI in the UK as British and European standards.

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 61508.

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 is 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 would like to express its thanks to lead author Ray Martin (EEMUA consultant, formerly with RWE) and the following members of the working group:

Darren Avery	Tata Steel Europe
Diana Davidson	Petroineos
John DeMain	Sabir
Paul Donnelly	EDF-Re
Russell Fraser	SSE
Chris Hastings	SSE
Ross Hemming	AWE
Stephen Merifield	BOC
Jonathan Mills	Syngenta
Pep Monk	ExxonMobil
Nick Moody	Syngenta
Toby Pusey	National Grid
Barry J Smith	Phillips 66
Leon Trunecka	National Gas

Thanks are also due to Colin Easton of Prosalus and Anil Sood of GB HSE for their diligent reading and constructive comments on how the document might be improved.

1 Scope

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

In the detailed sections (chapters 5 and 6), the relevant sub-clauses of IEC 61511-1 are included in a right-hand column for ease of reference to the standard. Where guidance and recommendation are not specifically associated with a clause from the standard, they are marked **.

This Guide:

- is applicable to process industries, such as onshore and offshore oil and gas, non-nuclear power generation, chemicals and petrochemicals.
- provides general information on the safety lifecycle covering the responsibilities for end users / duty holders, designers, suppliers (of systems, products and services), integrators, installers and maintainers.
- is primarily aimed at the safety of people, it may also be applied to environmental and asset/commercial protection.
- does not provide checklists or detail on how to design, operate and maintain such systems.
- does not take precedence over, or replace any requirement of IEC 61511-1 or IEC 61508.

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.

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.

Approved Code of Practice	Detailed guidance document with special 'approved by the UK HSE' status, covering a particular set of health and safety regulations.
Availability	Average in time of the likelihood of a defined function being performed successfully.
Commissioning	Final adjustment and testing of a system in the installed environment.
Competence	As applied to a person: the attainment of the necessary knowledge, understanding, training and experience, together with appropriate behavioural qualities, to perform a particular task or role.
Diagnostic	Automatic function that detects and reports malfunctions of elements of a function or 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. Note: The term 'duty holder' is normally used in respect of the owner of process facility as being the organisation that puts employees and contractors at risk. However, depending on the legislation being considered, there are a number of legal duties that cover all aspects (e.g. designer, supplier, integrator, installer or maintainer).
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 predates the existence of IEC 61508 whose equipment parts may not fully conform to that standard. Note: This term is now considered redundant by the UK HSE because such systems would now be expected to be qualified by available routes. The collective term used is 'Installed Systems'.
Mission Time	The time stated by an equipment manufacturer beyond which the stated performance criteria can be expected to deteriorate.
Override, Bypass, Inhibit	Facility to change or prevent the normal operation of a protection function (e.g.: for use during transient conditions or maintenance). Note: at any site, use of terminology normally distinguishes between facilities for automatic, operations and maintenance use.
Prior use	This represents a route for qualification of equipment under IEC 61511 (based on substantive statistical evidence) by a user organisation that has not otherwise been qualified under IEC 61508.

Probability of failure on demand (PFD)	Probability (as a function of time) that a function will not be performed successfully. Note: there is no difference between the term 'probability of failure on demand' and 'probability of failure' (the words 'on demand' are superfluous).
Probability of failure on demand (average) (PFD_{avg})	The average in time of the PFD. Note: In this Guide 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 61508-1). Notes: • The process safety time only applies to a protective SIF. • The specific words in the standard's definitions (see Part 1 3.2.52.1) are misleading because process safety time is intended to be the time taken from the event that the SIF is designed to detect and the expected occurrence of the associated hazardous event.
Reliability	Probability (as a function of time) that an item, or function, will be performed successfully.
Safety Function Description	Term used in this Guide as a description of all safety functions. In respect of a SIF, it is the forerunner to the Safety Requirements Specification.
Safety Integrity Level	Discrete level (expressed as SIL 1 to SIL 4) applying to the degree of reliability of safety instrumented functions and the degree of reliability of equipment for use in safety instrumented functions.
Safety Manual	Documented information that defines the functions and integrity of equipment intended for use in a SIF and how it should be used such that its purported safety functions and integrity are maintained. Note: the standards do not require that the information is provided in a single document or that the document is entitled 'safety manual' provided that the required information is presented in a clear and logical manner.
Safety PLC	High integrity PLC (with in-built diagnostics and/or hardware redundancy) specifically designed for safety applications.
Safety Requirements Specification	Complete specification of all matters having any effect on safety applying to a SIF or SIS (as defined in IEC 61511-1).
Systematic Capability	Discrete level (expressed as SC 1 to SC 4) applying to the degree of confidence that equipment intended for use in safety instrumented systems, and used in accordance with its safety manual, is free from systematic faults.

2.2 Acronyms

ACOP	Approved Code of Practice
AK	Anforderungsklasse (Requirement Class)
ALARP	As Low As Reasonably Practicable
API	American Petroleum Institute
BPCS	Basic Process Control System (as defined in IEC 61511-1)
BS	British Standard
CBA	Cost Benefit Analysis
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) – UK implementation of EU Seveso III Directive.
CPU	Central Processing Unit
DIN	Deutsches Institut für Normung (German Institute for Standardisation)
DSEAR	UK Dangerous Substances and Explosive Atmospheres Regulations 2002
E/E/PE	Electrical/Electronic/Programmable Electronic (defined in IEC 61511-1)
EEMUA	Engineering Equipment and Materials Users' Association
EIC	Energy Industries Council (UK trade association for suppliers to energy industries)
EMC	Electro-Magnetic Compatibility
ESD	Emergency Shutdown
F&G	Fire and Gas
FAT	Factory Acceptance Test
FDS	Function Design Specification
FPL	Fixed Programming Language (as defined in IEC 61511-1), e.g. configuration of a smart sensor or final element
FMEA	Failure Modes and Effects Analysis (refer to IEC 60812)
FMEDA	Failure Modes, Effects and Diagnostics Analysis (refer to IEC 60812)
FSMS	Functional Safety Management System
FSA	Functional Safety Assessment (as defined in IEC 61511-1)
FTA	Fault Tree Analysis (refer to IEC 61025)
FVL	Full Variability Language (as defined in IEC 61511-1) e.g. C, Pascal, SQL
GA	General Arrangement (drawing)
H&RA	Hazard and Risk Assessment
HAZID	Hazard Identification – Hazard Study 2 of IChemE 7 part Hazard Study process
HAZOP	Hazard and Operability (study) – Hazard Study 3 of IChemE 7 part Hazard Study process (refer to IEC 61882 for application guidance)
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
IET	Institution of Engineering and Technology
IPL	Independent Protection Layer
ISA	International Society of Automation
ISO	International Organization for Standardization
LED	Light emitting diode.
LOPA	Layer Of Protection Analysis
LVL	Limited Variability Language (as defined in IEC 61511-1) e.g. Ladder Logic
MTTR	Mean Time to Restoration/Repair
O&M	Operation and Maintenance
PE	Programmable Electronic
PFD	Probability of Failure on Demand (defined in IEC 61511-1)
PFEER	The UK Offshore Installations (Prevention of Fire and Explosion, and Emergency Response) Regulations 1995
PL	Protection Layer
PLC	Programmable Logic Controller
PO	Purchase Order
QA	Quality Assurance
QMS	Quality Management System
QRA	Quantitative Risk Assessment
R2P2	Reducing Risks, Protecting People, HSE ^[1]
RFI	Radio Frequency Interference
RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (UK) 1995
SAT	Site Acceptance Test
SC	Systematic Capability
SCR	The Offshore Installations (Safety Case) Regulations (UK) 2005
SFD	Safety Function Description
SFF	Safe Failure Fraction (defined in IEC 61508-2)
SHE	Safety, Health and Environment
SIF	Safety Instrumented Function (defined in IEC 61511-1)
SIL	Safety Integrity Level
SINTEF	Norwegian research and technology association
SIS	Safety Instrumented System (defined in IEC 61511-1)
SRS	Safety Requirements Specification
TRC	Tolerable Risk Criteria
UK	United Kingdom
T6A	The 61508 Association
UKOOA	UK Offshore Operators Association, now Oil & Gas UK
UPS	Uninterruptible Power Supply

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 is a risk based standard whose fundamental principle is that risk is something that is tolerated by society in order to achieve some perceived gain. For more information, refer to Annex H – Tolerable Risk Criteria.

The standard 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 (including systematic failures) and systems aspects in a risk-based approach towards safety.

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

IEC 61511 is the process industries daughter standard of 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 across all types of process industries 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 legal responsibilities for safety, it should not be seen as defining in absolute terms the legal requirements of any specific country. In the UK, the regulatory authority recognises IEC 61511 as a 'benchmark standard', i.e. whilst it is not an ACOP, it is considered to be relevant good practice in the process industries and that safety related systems will be managed in accordance with it or equivalent. Operating companies should always be aware of the relevant legal requirements relating to particular applications and countries. Refer to Section 4 for Legal Aspects.

Note: For offshore oil and gas applications, where both API RP 14C^[2] and IEC 61511 may be seen as relevant good practice, consideration should be given to avoiding potential conflict between prescriptive and risk-based approaches. This could be accomplished by specifying ISO 10418 instead of API RP 14C. Both are similar but the former defers to IEC 61511 for safety instrumented functions.

3.3 Relationship between IEC 61508 and IEC 61511

IEC 61508 is aimed at risk assessment and ensuring that overall systems, from sensor to final elements, perform adequately where safety is concerned for all E/E/PE applications. It covers design and implementation at all levels.

IEC 61511 is aimed at operating companies and integrators, i.e. the users of equipment. Being aimed specifically at process industries, it is an easier starting point for those industries than IEC 61508.

IEC 61511 covers the selection of safety related equipment but it does not cover the manufacture. There are other aspects it doesn't cover, such as application software based on full variability languages and systematic capability (refer to Annex K – Selection of Equipment) for combining of elements. For areas it doesn't cover, it refers to its mother standard.

Although the requirements are onerous, IEC 61511 also allows for qualification of equipment that has not been qualified to IEC 61508 by the route of 'Prior Use' (refer to Annex A – Technology Issues) where equipment has been in use which has demonstrably suitable reliability.

Manufacturers have to qualify their equipment to IEC 61508. There is no requirement for independent assessment but many items of equipment are now available that have been assessed (and in some cases, certified) for conformance to IEC 61508, by external assessors. However, the manufacturer of an item declares its conformity to the standard and therefore takes overall responsibility.

3.4 IEC 61511

IEC 61511-1 contains all the “normative” requirements of the standard. These are the requirements that have to be complied with in order to claim conformity.

The requirements span all the phases of the safety lifecycle, including hazard and risk assessment, allocation of safety functionality, specification, design, engineering, installation, commissioning, validation, operation, maintenance, modification and eventual decommissioning of a safety instrumented system.

It is important to understand that safety functionality is more general than just the safety functions. For example, if there are many safety functions that result in a unit trip, the tripping mechanism is normally a common path to all safety functions. In IEC 61511, the safety functions are defined as end-to-end (or so-called pipe-to-pipe): the result is some functionality that is common to several safety functions. Another example is in batch control safety systems, where a process can't be started unless a sequence of events has occurred in the appropriate order. There is no end-to-end function but it is certainly safety functionality. Other examples are where data capture is part of the high integrity requirements.

The standard also contains requirements for safety management, including planning, competency and assessment.

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, much of which provides guidance. In some cases, no guidance is given.

IEC 61511-3 provides more general guidance, including:

- guidance on the determination of the required safety integrity levels;
- guidance on risk and safety integrity;
- guidance on ALARP and tolerability of risk concepts; and
- five different methods for determining safety integrity requirements.

It is important to recognise that these methods are examples which were aimed at specific needs. They should only be adopted by a duty holder if they are suitable for the specific needs and are (where relevant) calibrated to the specific tolerable risk criteria.

It is the responsibility of the duty holder to ensure that allocating safety functionality and integrity is carried out using a method that is suitable for the specific application and that meets applicable regulatory requirements.

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 IEC 61511-2 and IEC 61511-3
Selection of equipment for use in a safety-instrumented system on the basis of "Prior Use"	IEC 61511-1 and IEC 61511-2
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 Variable Language (FVL) 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 Variable Language (LVL) and Application Program (AP) for a specific process sector application	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

The lifecycle approach recognises that having effective functional safety requires much more than specifying, supplying and installing sensors, logic solvers and final elements. To achieve process safety, a holistic picture must be used. The roles of all non-SIS elements (including human

elements) need to be taken into account in functional safety, and plant integrity issues must also be managed.

The use of the term 'lifecycle' underlines that all aspects of process safety must be maintained throughout the life of the plant, from initial conception through to decommissioning. Any changes and any new information must first be assessed for its impact on the safety lifecycle: the lifecycle activities and documentation must then be revisited and revised accordingly.

The safety lifecycle phases are identified by the numbers in Figure 1 below (this follows the safety lifecycle from IEC 61511-1) and references the phases of the lifecycle.

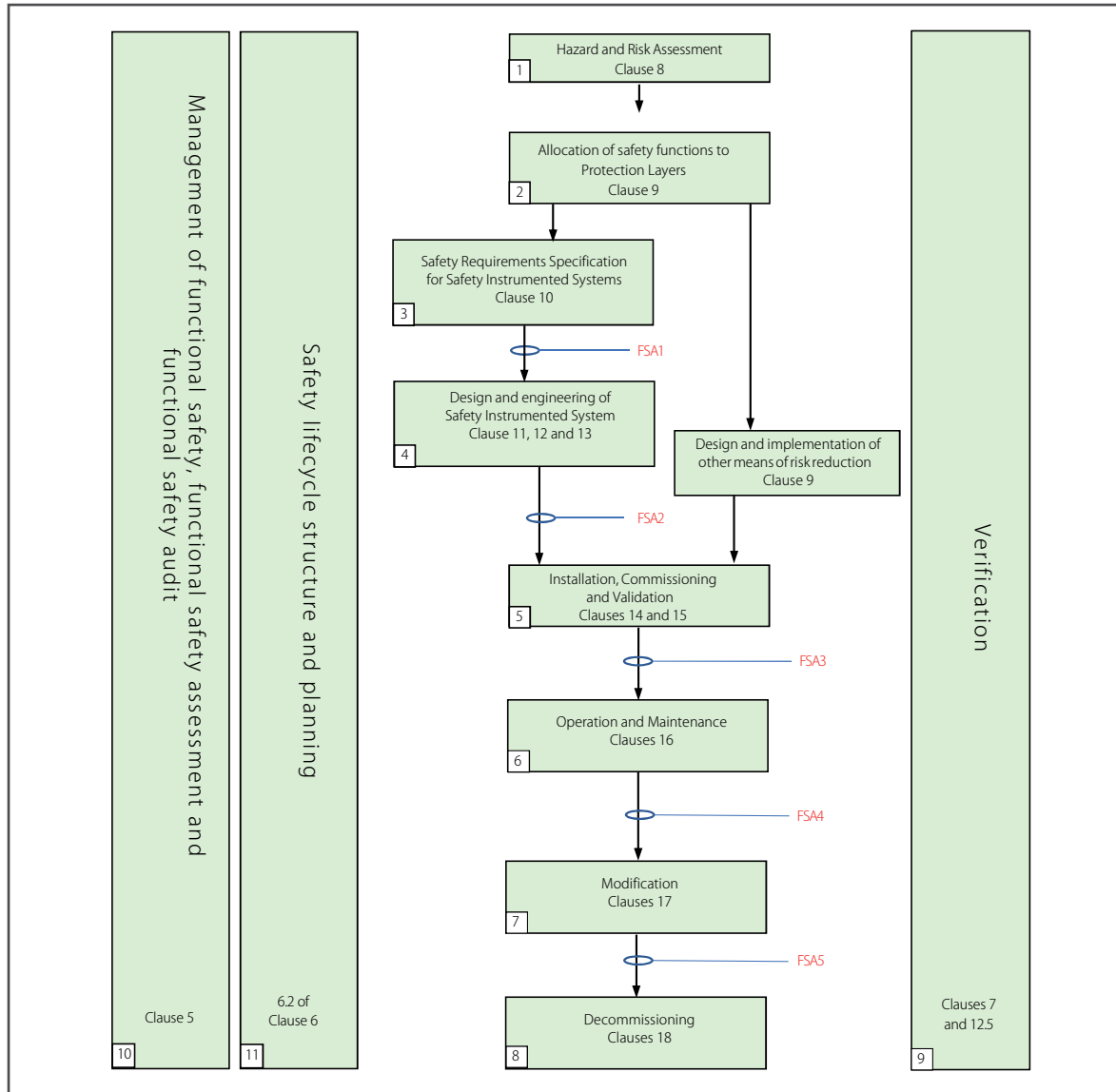


Figure 1 – Safety lifecycle

Note: The above, as a lifecycle diagram is not intended to be seen as a 'once-through' process. In getting to 'Organisational Completion' the phases 1 to 5 may have been repeated in whole or in part, or may have been applied on a staggered basis to different areas of design. It should be understood that there are iterative loops around phases 6 and 7: FSA4 is expected periodically during O&M and FSA5 is expected after any modification (where FSA5 would revisit any affected parts of FSA1, 2 and 3).

3.6 Potential Issues with IEC 61511-1

It is very clear, both from the introduction to IEC 61511-1 and from Clause 8 that the preference is an inherently safe design. IEC 61511 should be viewed as a valiant attempt to cover a variety of cases where that may be difficult or impossible to achieve with confidence. As such the limitations of the standard and the difficulty of writing for the general case need to be appreciated. It gives no guidance on analysing mechanical parts of devices nor their reliability, even if they have instrumented parts. ISO 13849 is referred to but itself has severe limitations.

3.6.1 Process Safety

IEC 61511 addresses functional safety in the process industries and, in particular, the functional safety that depends on electrical, electronic and programmable electronic (E/E/PE) technology. It should be appreciated that IEC 61511 only gives specific guidance on the development of E/E/PE systems and doesn't therefore cover all of process safety in detail.

Process safety falls into two main complementary strands:

- Plant integrity – which considers the ongoing physical robustness and general condition of the plant (including machinery) against its defined safety duties.
- Functional safety – which considers the functions of systems, equipment and people which keep the process from overstressing the plant.

The two strands work together to maintain process safety. For example, it is of no use having a safety function that will trip the plant if the pressure exceeds 120 barg if the pressure parts fails at 110 barg.

Note: The first strand is sometimes referred to as 'asset integrity' but this term is usually reserved for as a more general term which refers to the integrity of all aspects of a plant in performing all its expected duties in its asset owner's interest.

IEC 61511 is relevant only to the second strand (functional safety).

Although IEC 61511 addresses E/E/PE functional safety, it calls for a Functional Safety Management System which is required to address all aspects of functional safety. As it is aimed at safety in the process industries, it should perhaps also call for a Process Safety Management System which addresses all aspects of process safety.

3.6.2 The purpose of Hazard and Risk Assessment

IEC 61511 can lead to the impression that:

- the purpose of a 'Hazard and Risk Assessment' is to determine functional requirements for E/E/PE systems. In reality, H&RA would need to address process safety as a whole.
- Risk assessment is a one-off activity which is separate from design. In particular, it examines a partially completed design which leads to a specification for added instrumented functional safety which, once complete, would result in a safe process. In reality, design is a top-downward process and risk assessment is a partner of design. If they are defined separately, they must still be seen as bound together (risk assessment informs design and vice versa).

In this Guide the lifecycle Hazard and Risk Assessment is treated as the 'formal' risk assessment which results in the description of all hazards and risk control measures and assigns formal duties including functional safety, plant integrity and any other necessary organisational duties.

Hazard and Risk Assessment should not terminate with an assignment for functional safety. The expected (and later actual) performance of that risk reduction should be taken into account such that the risk assessment is aimed at modelling the residual risk.

3.6.3 Hierarchy

If a site cooling water system is considered properly in a risk assessment, it would probably become clear that it would have an effect that would lead towards danger in many scenarios. Thus, it would be likely to have a significant effect overall on the site expected fatality rate. In this case, the top-level safety function is 'the continuous supply of cooling water'. Assuming that this had been considered in risk assessment and that an integrity requirement for cooling water had been set, the cooling water system would be likely to involve some mechanical redundancy (e.g. redundant pumps). In such an instance, E/E/PE functions are likely to be required for: monitoring the delivery of cooling water and the pumps; in the case of failure, cutting in standby pumps and possibly closing off recirculation routes on failed pumps.

This serves to illustrate some interesting issues:

- Safety functionality is often hierarchical in nature and thus safety functionality and integrity requirements can be inherited from above.
- Design is hierarchical and risk assessment should be too. If design and risk assessment are partners, risk assessment should also be hierarchical in structure.
- Safety functionality is always process orientated.
- In process safety, machines can be energised in the safe state.
- A protective function is not always a trip.

3.6.4 Hardware Fault Tolerance

Hardware Fault Tolerance (HFT) is where the hardware design of a safety function can tolerate some faults which result in loss of integrity but without loss of function.

For instance, it is common to use 2oo3 voted input channels. This subsystem can tolerate one channel giving a faulty dangerous signal and thus it is said to have $HFT=1$.

It is important to recognise though, that HFT is not always about redundant channels. For instance, if a fan needs to run as part of a safety function and a flow switch is installed such that it gives a positive signal when it detects flow, this has the potential to have $HFT=1$.

The system would need to constantly check that the flow switch state matches that expected, and that change of state occurs only in the expected time window. No single fault can then avoid detection.

In the case of 2oo3 voted input, there is no immediate danger although the situation has become more dangerous due to reduced integrity.

In the case of the fan, a discrepancy could signal fan failure which could mean immediate danger. In such circumstance, the fault reaction of the system would probably be to attempt to cut-in a standby fan or place the process into a safe state via some other means.

This is also a case where the hardware structure of a SIF doesn't necessarily follow the 'input > logic solver > output' form that is implied by the standard.

3.6.5 Overall Risk Reduction Limitation

In edition 2, the standard introduced a clause (IEC 61511-1 9.2.8) that limits the overall risk reduction that can be claimed from a SIS to the rating of the SIS.

Whilst aiming for as much diversity as possible is good advice, this clause can be impracticable (and 'less safe') in circumstances where being functionally safe relates to sequential action (for example, in combustion processes).

In contrast IEC 62061 (the machinery daughter standard of IEC 61508) does not impose the same limitation. This leads to complications and conflicts in good practice resulting in some industrial situations where equipment is qualified to a machinery standard even in the absence of a machine.

It would be far preferable if a future edition of the standard properly addressed this issue.

3.6.6 Validation

In the IEC 61511, validation is not well defined. It seems that when the standard was written its meaning developed some variations from clause to clause.

In the lifecycle, 'validation' is a term associated with formal testing at site which follows on at the end of commissioning.

In clause 3, it states that, in respect of the standard, it means demonstrating that the SIFs/SIS after installation meet the safety requirements specification in all respects.

However:

- There is a note in part 1 (clause 13) to say that FAT can be part of validation and, in clause 14, it refers to commissioning the SIS so it is ready for 'final system validation', so it appears that validation is testing but wider than SAT.
- In clause 6, it states that validation covers integrity aspects as well as functionality but, clearly, integrity is not something that is established by testing.
- In clause 15, it states that validation planning of the SIS shall be carried out throughout the SIS safety lifecycle and shall define all the activities and equipment required for validation. This implies it is much more than testing.

It should be understood that:

- design is structured and formal testing must follow that structure in order to be successful. If the SIS is complex in structure, it follows that so must be the formal testing;
- testing should follow the well accepted V-model (see Wikipedia for definition);
- the integrity of the SIF / SIS cannot be tested, it must be assessed by calculation and conformance to standard and must include potential systematic causes of failure.

Validation is therefore better thought of as the structuring and aggregation of all the formal testing together with the collation of all relevant records, including those of integrity assessments, verification records and any other means to avoid systematic failure, in establishing that the SIF / SIS meets the safety requirements specification in all respects.

Note: On this final point, validation as described in the standard only refers to SIS/SIFs and only from the establishment of the safety requirements specification onwards.

3.6.7 Random and Systematic Failures

IEC 61511 defines a systematic failure as one which relates to a 'pre-existing' fault which consistently occurs under particular conditions. In contrast, the more general definition of systematic failures is human or organisational errors.

Pre-existing implies that the fault is one that occurred in the design and implementation phases whereas systematic failures can also include failures in operation and maintenance.

When so-called random hardware failures are investigated in detail, it is very rare to find a failure which is truly random. Detailed examination usually reveals a built-in weakness (which is by definition, systematic).

For a clearer understanding of where random and systematic overlap and how they should be dealt with, refer to Annex I – Random and Systematic Failures.

4 Legal Aspects

4.1 Health and Safety Legislation

4.1.1 General Aspects

Legislation, and the role of IEC 61511 differs from country to country and, whether a company is located in one country or is international, it is important for the company to recognise the relevant legal and regulatory aspects for each location.

In the UK, the Health & Safety at Work etc. Act 1974^[3] is the primary legislation for workplace health and safety in the UK. It places a general duty on both employers and employees to ensure safety, so far as is reasonably practicable. It also places a duty 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 remains safe;
- take sufficient 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 are made by the Health and Safety Executive (HSE) and provide more specific requirements for particular applications (see also Sections 4.2 and 4.3 below).

The HSE interpretation of ensuring safety 'so far as is reasonably practicable' is that risks should be assessed, relevant good practice should be applied and risks should be reduced to a level that is 'as low as reasonably practicable' (ALARP).

When assessing whether relevant good practice has been applied, the HSE relies on authoritative documented sources, such as:

- its own Approved Codes of Practices (ACOPs) which have a special legal status;
- HSE guidance provided on their website <https://www.hse.gov.uk/> ;
- British and European Standards (e.g. BS EN 61508 and BS EN 61511);
- International Standards (e.g. ISO 9001);
- Other National Standards (e.g. NFPA 85); and
- other guidance issued by authoritative bodies (e.g. ISA, EEMUA).

Where risk control measures in use are either the subject of an ACOP or if there is widespread evidence of the effectiveness of control measures (e.g. risks arising in a car park or general measures to prevent slips, trips and falls), the HSE will generally consider the adoption of good practice to be sufficient to claim an ALARP position.

For process hazards that are not covered by ACOP, ALARP is established by demonstrating, adoption of good practice, suitable and sufficient risk assessment, risks are tolerable, and the costs of implementing additional or alternative risk reduction is grossly disproportionate to the benefit.

In cost benefit analysis, the HSE advocates the use of a 'factor of gross disproportion' and 'value of averted fatality' are used in establishing the human cost of a hazardous event. For further information refer to Annex G – ALARP.

4.1.2 IEC 61511 and ALARP

IEC 61511 is now generally accepted internationally as providing the framework for functional safety.

In the UK, the HSE refers to BS EN 61511 as a 'benchmark standard' for managing functional safety aspects in the process and related industries – i.e. the adoption of the standard (or equivalent process) is an expectation. Adoption of the standard is therefore seen as relevant good practice and is a step towards claiming an ALARP position. For further detail, refer to Annex G – ALARP.

It is important to be aware that, in the UK, ALARP is the regulator's interpretation of the law. IEC 61511 is applied in a similar way to the Highway Code: it is not law but failure to follow it can be used by the regulator in prosecutions.

Note: Strictly, the standard it is not applicable where functional safety consists entirely of non-E/E/PE equipment. However:

- that case no longer exists in practice because relevant good practice would dictate its use.
- where a safety function consists of entirely of non-E/E/PE equipment (e.g. a non-instrumented pressure relief valve), it forms part of functional safety and therefore comes under the functional safety management system (FSMS) required by the standard – i.e.: it forms a layer of protection in hazard scenarios that must be risk assessed in combination with other safety measures; it must be allocated a duty; its safety function must be specified in terms of function and integrity; and its performance must be monitored and maintained.

4.2 Other Health and Safety Legislation

IEC 61511 does not address major accident hazards or explosive atmospheres specifically but it does address the control of all process hazards. As such, its adoption by duty holders helps demonstrate that critical hazardous occurrences are under control.

4.2.1 Major Accident Hazards

Legislation exists in most countries to control the likelihood and consequences of major hazard occurrences for onshore industries.

The Seveso Directives are the main part of EU legislation concerned with the control of on-shore major accident hazards involving dangerous substances.

Implementation of these directives in the UK is via the Control of Major Accident Hazards (COMAH) Regulations 1999^[4] as amended in 2005.

The latest directive, the Seveso III Directive, came into force in 2015 and is implemented in the UK by Control of Major Accident Hazards (COMAH) Regulations 2015^[5].

4.2.2 Explosive Atmospheres

Legislation exists in most countries to control the likelihood and consequences of industrial explosions.

The ATEX Directives are the main part of EU legislation concerned with explosive atmospheres. The original directive, in 1999, dealt with the requirements for health and safety of workers exposed to explosive atmospheres. The later directive, 2014, is concerned with equipment and protective systems associated with explosive atmospheres.

Implementation of these directive in the UK is via the Dangerous Substances and Explosive Atmospheres (DSEAR) Regulations, 2002. The HSE publishes these regulations and guidance in L138^[6] which has ACOP status.

Note: DSEAR covers the risk assessment and implementation of necessary measures in order to avoid harm as a result of substances which are dangerous to health. DSEAR is an ACOP which is enforced by the HSE which covers defined good practice for avoidance of risk in this subject area.

Under DSEAR, where atmospheres are potentially explosive, instrumentation, electrical and mechanical equipment are required to conform to a particular standard of equipment (e.g. by conformance to IEC 60079 series standards) designed to reduce risk of an explosive mixture coming into contact with an ignition source.

It should be noted that this is an area of process safety risk assessment mitigation measures that aligns with that of previous definitions of 'plant integrity' rather than that of 'functional safety' because it represents a passive attribute of the plant – its function is static.

Instrumentation is often required to be both ATEX and SIL compliant. Only the SIL requirements are considered further in this Guide.

4.3 Application to Existing Installations

In the early years after the first publication of IEC 61508, SIS/SIFs that existed prior to that, were commonly referred to as 'legacy'. The term 'legacy', in reality, applies to the plant as a whole.

In some cases, it was successfully argued with regulators that, because of its age, the plant would soon be closed and, thereby, that it was not reasonably practicable to retrospectively apply the standard given that the expected cost would be grossly disproportional to the expected benefit.

Now, more than two decades later, the argument no longer exists. Regulators (such as the UK HSE) are aware that there is suitable provision within IEC 61508 for manufacturers of equipment to produce a 'Proven in Use' case or within IEC 61511 for duty holders to produce a 'Prior Use' case for equipment and that suitable time has passed to make use of these provisions. The HSE now consistently refers only to the 'management of installed systems' which applies to all SIS/SIFs where the expectation is that IEC 61511 is applied.

4.4 Civil Liabilities

In addition to criminal legislation, in many countries there is additional civil protection. For example, in the UK, the Consumer Protection Act 1987^[7] applies to goods used at a place of work as well as all consumer goods. Other countries have similar legal provision.

The Consumer Protection Act gives a person, injured by defective products, the right to sue for damages. The injured person can take action against a “producer” (usually the manufacturer but can be supplier). What classifies as a “producer” of a safety instrumented system may vary according to circumstances but, for example, a systems integrator may be regarded legally as a “producer”.

In civil cases, the standard of proof required is a lot less than criminal cases and thus, this form of law can and has been used. If it can be demonstrated that, on ‘the balance of probabilities’, a defect in equipment contributed to death, personal injury or damage to private property, the injured party has a right to sue the producer for damages. There is no need to prove that the producer was in any way negligent, 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 can be held liable (refer to Guide to the Consumer Protection Act 1987^[8]

5 Common Requirements for all Activities

Notes:

- This Chapter lists recommendations applicable to all lifecycle activities. Further requirements for specific activities are stated in the respective parts of Chapter 6.
- The symbol ** in the right-hand column indicates recommendations beyond that of IEC 61511-1.

5.1 Responsibilities

Commentary		IEC 61511-1 sub-clauses
5.1.1	If conformance of safety instrumented systems to IEC 61511 is intended, it is a management responsibility to ensure that the necessary policy and strategy for achieving functional safety is identified together with methods for evaluating the achievement, and communicated within the organisation.	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

Commentary	IEC 61511-1 sub-clauses
5.2.1 The standard requires that personnel, departments or organisations involved in safety lifecycle activities are competent to carry out the tasks or activities assigned to them and that such competencies remain under assessment. Competency covers the knowledge, understanding and application (the 'know what, why and how') and is gained through education, training and experience. At all levels and for all tasks, it includes behavioural skills and for some tasks, it includes thinking and shaping (analytical) skills. Notes: • Competency applies to all organisations, their departments and their processes as well as to individuals. • Competency must be formally assessed. • Competency assessment also covers that of all external suppliers (of goods and services); • Competency is not static: a lack of use of a skill can cause degradation over time. • Competency must be kept up to date: changes happen in technology and relevant good practice that requires skills to be updated. • To assess a person's competence requires a higher degree of competence. • an individual's competence is generally regarded as representing transferrable skills: however, it is important that an organisation has competent systems and that management of competence includes the training of newcomers in their use.	5.2.2.2
5.2.2 Many countries have competency standards covering activities related to SIS/SIFs. In the UK, in 2007, the HSE produced high level guidance aimed at the competency management system - refer to HSE Managing Competence for Safety Related Systems (Parts 1 and 2)^[9]. In support of that, in 2016, the IET produced more detailed guidance including detailed examples – refer to IET Code of Practice: Competence Criteria for Safety Related Systems Practitioners^[10].	**
5.2.3 Roles should be defined for such personnel, departments and organisations units working with SIS/SIFs. For each role, required competencies (in terms of engineering knowledge, training, experience, and personal qualities) must be defined that address all relevant aspects, including: - the process application; - the technologies used; - the sensors, logic solvers and final elements chosen; - the integrity levels involved; - the complexity of the analysis; - the complexity of the required systems.	5.2.2.2 notes

Commentary		IEC 61511-1 sub-clauses
5.2.4	The competency of persons, departments or organisations carrying out safety lifecycle activities should be continually assessed. The assessments should be tailored to the specific roles and should include, where appropriate, familiarity with parts of IEC 61508 and IEC 61511. Assessments should be evidence based and documented. An example personnel competency scheme is provided in Annex C – Example Competency Scheme.	5.2.2.2 **
5.2.5	Any gaps in competence should be identified and compensating measures and action plans put in place. These may include restricting a person's responsibilities while the gap exists and/or using additional person(s) in checking or supervisory roles.	5.2.2.2 **
5.2.6	Ongoing training should be provided to ensure that personnel remain competent to perform their roles. This is particularly important where personnel are rarely required to use related skills, e.g. the maintenance of highly reliable SIS, or an operator action in a process upset situation when an automatic protection function has failed.	5.2.2.2 ** 16.2.6 **
5.2.7	Organisations and departments should be able to demonstrate implementation of suitable functional safety management covering the lifecycle activities within their scope.	5.2.2.2 **
5.2.8	If a supplier makes any claim for a product or service pertaining to IEC 61508/61511, the supplier must have a suitable QMS and FSMS. The FSMS must comply with IEC 61508 or relevant daughter standard. The duty holder must be satisfied that the supplier has the necessary competence including the necessary systems and procedures.	5.2.5.2
5.2.9	Use of organisations with accredited competency schemes in the development and use of safety instrumented systems and use of competent third parties to assess and audit potential suppliers is encouraged. However, responsibility for safe operations remains with the ultimate duty holder.	5.2.5.2 **
5.2.10	CASS (Conformity Assessment of Safety related Systems) is a free to use, transparent template-based methodology, hosted on T6A website, which provides methods for a documented assessment of an organisation's capability in respect of the requirements of IEC 61508 or related standard.	**

5.3 Planning

Commentary		IEC 61511-1 sub-clauses
5.3.1	The functional safety plan should identify the activities to be carried out and the persons, department or organisation that would carry out these activities. It is not necessarily (and is unlikely to be) a single document.	5.2.4 6.2 **
5.3.2	It should be clearly understood that the lifecycle phases depicted in IEC 61511-1 (6.1) do not themselves form an activity plan. Safety planning can (and should) be integrated into the wider project / activity plan, which should be updated whenever necessary throughout the safety lifecycle. In practical projects: • design of different facilities is often staggered in time. • emerging design decisions can necessitate revisiting and updating the outputs of safety lifecycle activities. The developing project / activity plan must accurately reflect and allow appropriate time and resources for these activities. To be avoided is any inference that the project team in general follow one plan and only specific disciplines follow the safety plan. It should be noted that implementation of IEC 61511 may require more resources in early stages of the project in comparison with approaches that predated the standard. However, experience has shown that this reduces the burden of demonstrating to the regulator that an adequate level of safety has been achieved	5.2.4 ** 6
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. Verification should also form part of the functional safety planning.	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 to the tools and processes to be used. Target dates, document numbers and descriptors can be added, as shown in the overview example in Annex B – Example Functional Safety Plan Overview.	6.2.2 Table 2 **

5.4 Verification

Commentary		IEC 61511-1 sub-clauses
5.4.1	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. Verification should be planned, carried out and documented for each lifecycle activity. A lifecycle phase may be broken down into several parts which can be verified separately. It is part of planning to address these aspects.	7 12.7 **
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 of something requiring verification. Note: FAT is normally considered as part of the Validation process but is also subject to Verification.	7.2 **
5.4.3	Verification can normally be carried out by another person in the organisational team responsible for the activity. The requirement in the standard, regarding independence is that the level of independence required forms part of the verification planning which implies that it must be justified. Where there is significant complexity or novelty or high SILs are involved, it is recommended that independent departments or companies are used.	7.2.1 **

5.5 Validation

Commentary		IEC 61511-1 sub-clauses
5.5.1	The standard defines the activity of validation as confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled. The objective of validation is to ensure that the installed and commissioned SIS and all associated SIFs achieve all the requirements stated in the associated SRS(s).	15
5.5.2	Validation is often seen as a word meaning ‘formal testing’ but it can be seen from the definition above that (although it includes formal testing) validation has a wider meaning (see also 3.6.6). For example, if the SIS SRS stated a requirement that the SIS should be supplied via the site emergency power supply, the supporting evidence may involve more than testing. Validation (see IEC 61511-1 Table 2) also includes integrity (which cannot be established by testing).	** Table 2

AVA Documents
Document Sharing Hub

5.6 Functional Safety Assessment

Commentary	IEC 61511-1 sub-clauses
5.6.1 Functional Safety Assessment (FSA) is a proceduralised process culminating in a judgement as to the functional safety of a process and safety integrity achieved of related SIFs/SISs which covers all stages of the safety lifecycle. It is a team-based judgement where, collectively, the team possesses a high degree of competence in all the aspects relevant to the particular assessment. The team must include at least one senior competent person not involved in the relevant stage(s). IEC 61511 does not specify the level of independence in further detail, but expects the level of independence to be justified depending on risk, complexity, novelty etc. IEC 61508, the mother standard, states that, at SIL 3, organisational independence is highly recommended. Although there may be some overlap, FSA should not be confused with the process of Audit. It is possible to have an FSA which makes a judgment that functional safety has been achieved even if audit has revealed some failings. Figure 1 illustrates the process according to IEC 61511 (Refer to section 3.5). However, in the following, this guidance suggests some practical differences: • Stage 2 – At the time of Allocation, the full Safety Requirement Specification is unlikely to exist. This stage is, instead referred to as a Safety Function Description. • Stage 3 – the detailed Safety Requirement Specification is completed as part of the design and build of the SIS hardware and software. • FSA applies to all functional safety and not just that of the SIS but the standard gives no guidance on the approach. Figure 2, below better illustrates these subtle differences.	5.2.6.1 **

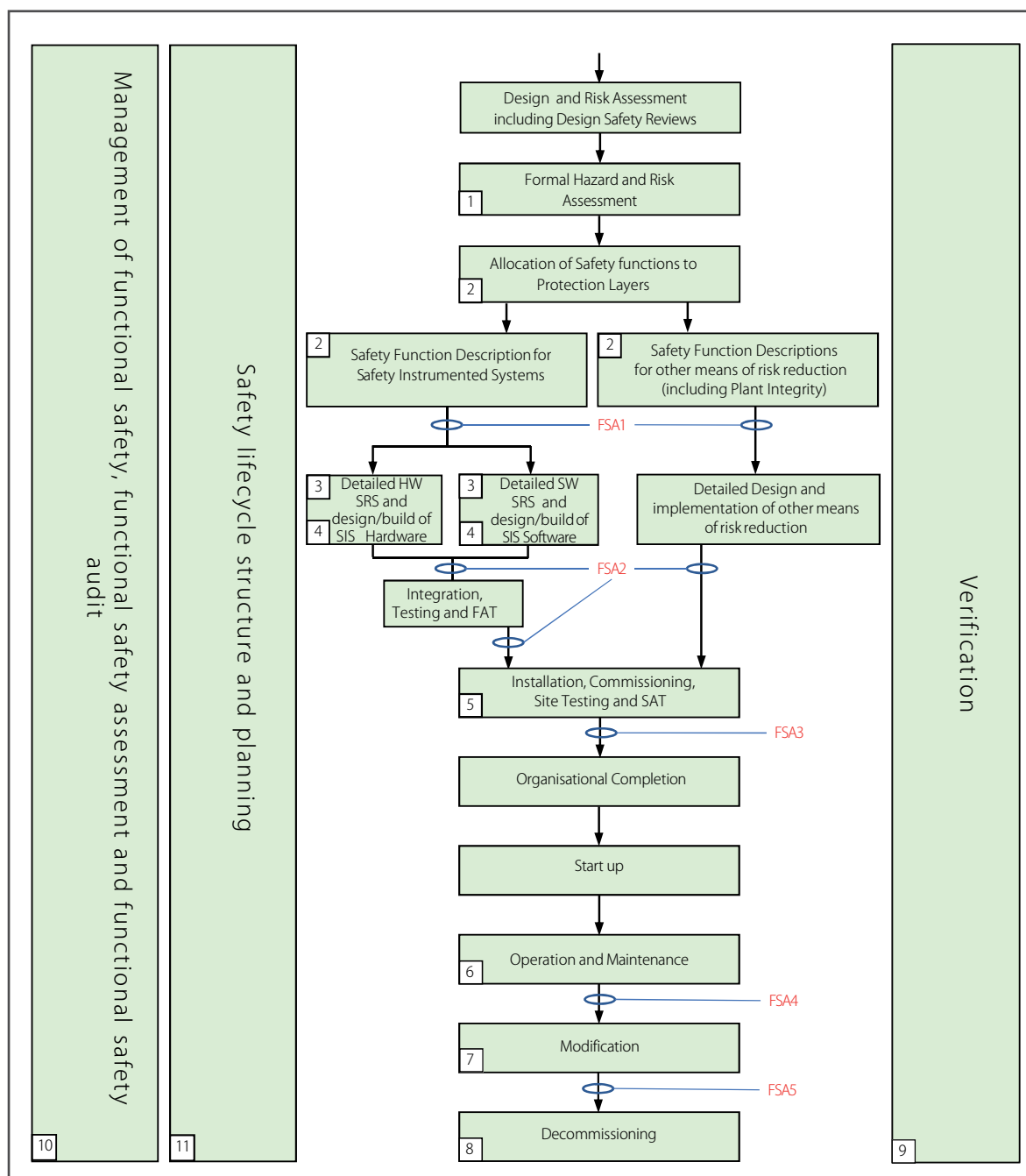


Figure 2 – Functional Safety Lifecycle showing FSA

Note: The above, as a lifecycle diagram is not intended to be seen as a 'once-through' process. In getting to 'Organisational Completion' the phases 1 to 5 may have been repeated in whole or in part, or may have been applied on a staggered basis to different areas of design. It should be understood that there are iterative loops around phases 6 and 7: FSA4 is expected periodically during O&M and FSA5 is expected after any modification (where FSA5 would revisit any affected parts of FSA1, 2 and 3).

Commentary		IEC 61511-1 sub-clauses
5.6.2	FSA should occur only when any relevant validation activities are complete. FSA should consider any recommendation arising from FSAs addressing stages earlier in the lifecycle. FSA stages 1,2 and 3 must be complete and any associated actions and recommendations addressed prior to process hazards being present.	5.2.6.1
5.6.3	There is no specific stipulation that FSA1 and FSA2 be carried out at the earliest opportunity in the safety lifecycle but it is recommended in order that if any issues need to be addressed in design, awareness of such is gained as early as possible and thus that FSA1 and FSA2 are carried out at the places shown in the Functional Safety Lifecycle.	**
5.6.4	The number and scope of assessment activities should be identified in safety planning. Stages 1,2 and 3 depend on the size and complexity of the project, novelty of the technology used and the highest integrity level involved.	5.2.6.1
5.6.5	The FSA should include consideration of: • hazard and risk assessment and allocation; • functional safety management; • safety requirements specification; • 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 processes and results; • validation processes and results. It is essential that FSA of the SIS should consider the complete system (i.e. all SIFs from start to end together with any system added diagnostics). It is also essential that it addresses any wider SIS requirements).	5.2.6.1.5 **
5.6.6	The scope of FSA includes software tools used where their use could have an impact on safety in any lifecycle phase. Such tools may include those used for risk assessment, programming and configuration, reliability calculation, and the maintenance management system used.	5.2.6.1.6

Commentary		IEC 61511-1 sub-clauses
5.6.7	Audits may also be carried out to check that the procedures are suitable and that they are being followed. Audit findings, where available, should be taken into consideration during FSA.	**

5.7 Audit and Revision

Commentary		IEC 61511-1 sub-clauses
5.7.1	IEC 61511 requires that auditing is carried out in order to ensure that the functional safety management system (FSMS) is in place, up-to-date, and being followed. Although there may be some overlap, it should not be confused with the process of FSA.	5.2.6.2.1
5.7.2	The scope of safety auditing is all procedures necessary applying to all safety lifecycle activities. Note: the procedures should be identified in the planning activities but this gives the auditor the scope to recognise relevant procedures whether or not identified in planning.	5.2.6.2.2 **
5.7.3	The basic level of independence for audit activities is 'an independent person not undertaking work on the SIS to be audited'. Note: procedures are to be in place that define the degree of independence for a particular organisation	5.2.6.2.3
5.7.4	Management of change procedures are required to be in place to cover initiation, documentation, review, approval and implementation of any changes to the SIS (other than like-for-like replacement).	5.2.6.2.4

5.8 Conformity Assessment

Commentary		IEC 61511-1 sub-clauses
5.8.1	Third party assessment of conformity of people's competency, organisational competency and of systems and subsystems capability is not a requirement of the standard.	11.5.2 11.5.3
5.8.2	Third party assessment of conformity of systems and subsystems is not a requirement of the standard. However, the duty holder has responsibility to assess the suitability of the functional safety management of suppliers of equipment in connection with the SIS (see 5.2.7). Note: Third party assessments of conformity by reputable independent organisations can play a useful role in fulfilling this obligation and are recommended wherever practicable.	11.5.2 11.5.3 **

Commentary		IEC 61511-1 sub-clauses
5.8.3	Certificates and assessment reports for items of equipment, issued by third parties can vary considerably in scope and quality. Duty holders must therefore satisfy themselves of the validity of any certificates and/or declarations of conformity for equipment forming part of a SIF/SIS apply in the context of the application. Establishing validity involves reading any relevant safety manuals, certificates, assessment reports and any relevant schedules. These duties can be devolved to reputable third parties. Note: Equipment can be qualified by the duty holder on the basis of 'Prior Use', but this demands a good deal of effort to establish suitable statistical evidence.	** 11.5.3
5.8.4	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 **

5.9 Management of Lifecycle Activities

Commentary		IEC 61511-1 sub-clauses
5.9.1	SIS lifecycle activities may be carried out by different organisations or different departments within the same organisation. The duty holder 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

Commentary	IEC 61511-1 sub-clauses
5.10.1 IEC 61511 requires suitable information to be provided which must be accurate, easy to understand, available, maintainable and editable and under revision control. Such is applicable throughout the Safety Lifecycle. Capturing of all relevant safety documentation for a SIF or SIS is therefore a basic requirement. The term Safety File is commonly used to describe this capturing of documentation and may be understood as a single file of documentation pertaining to one SIF or SIS. The standard does not stipulate the production of a Safety File (and for many reasons, it is not usually practicable). A single Safety File for a SIF covering the whole Lifecycle would only be suitable for a Hazard that is protected by unique PLs of which one is the SIF under consideration. As this situation is the exception rather than the rule, a single file which captures all relevant information might be possible but could not be the master document. In this Guide, it is referred to as Safety Filing and it should be understood that this term represents relevant documentation covering the whole safety lifecycle of a number of SIFs and SISs. Safety Filing should be generated covering all relevant information, including hazard and risk assessments; allocation; safety requirements specifications; design and engineering of SIFs and SISs; selection of equipment; reliability calculations; validation; proof testing procedures; monitoring (expected demand rate versus actual demand rate, details of proof test findings, ongoing review and reliability assessments, and data capture requirements). Safety filing should be constructed in way so as to minimise repetition (where master documentation is repeated elsewhere) but, importantly, to aid useability. Lifecycle tasks should be considered and facilitated by the safety filing.	19 **

Commentary	IEC 61511-1 sub-clauses
5.10.2 Documentation must 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/SIF-specific information should be collected and maintained in a single 'Safety File' with less specific information referenced from it. Alternatively, if it better fits a company's document management system, SIS/SIF-specific information can be held in different secure locations and referenced from a Safety File. In keeping with other aspects of functional safety, the SIS/SIF documentation location should be managed in its entirety in a manner commensurate with the highest relevant SIL.	19.2.2 19.2.5 19.2.6 / 19.2.8 **
5.10.3 Documents must be kept up to date throughout the lifecycle of the SIS/SIF. 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 specifications; • details of the equipment used for safety instrumented functions; • reliability assessment of equipment used for safety instrumented functions augmented with 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 assessments (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.	19.2.9 **

5.11 Change Control and Configuration Management

Commentary		IEC 61511-1 sub-clauses
5.11.1	Change control and configuration control relate to objects (e.g. a document, a module of application software, a hardware device, a system of hardware, a system of software). There is a point in time for any object when it is not under change or configuration control (e.g. initial draft, initial assemble) – this is usually in the early stages of design prior to any formalised process.	**
5.11.2	Change control (otherwise known as management of change) is applied to all objects. It provides traceability and relates to any change (whether it reflects a change to specification or to an inconsistency with other objects, an error or an omission).	**
5.11.3	Configuration control relates specifically to any defined object of hardware, system software and application software for complete system down to smallest device and its related documents. It is a process for controlling build history and traceability and relates to any functional or physical characteristic of a product or system (where the term product includes any procured devices).	5.2.7 **
5.11.4	Every identified object (hardware or software) or document must be placed under formal change control and (where relevant) configuration control. Once under change control and/or configuration control, an object must remain so.	**
5.11.5	The point in time at which change (and where relevant) configuration control is implemented in an object's life is a matter of optimum choice and good practice but must occur prior to it being involved in and formalised process, including: • formal review; • formal checking; • formal test; • any verification or validation activity; • any use as input to a safety lifecycle activity.	**

6 Requirements for Specific Activities

6.1 Front End Activities

6.1.1 Introduction

Commentary		IEC 61511-1 sub-clauses
6.1.1.1	This section addresses activities that generally precede Phase 1 activities shown in the safety lifecycle in Figure 1 – Safety lifecycle	
6.1.1.2	If responsibilities for information provision, risk assessment, allocation, specification, design, implementation, verification, validation, planning, audit and assessment are divided between different organisations, the scope, boundaries, boundary conditions and cross boundary effects, together with the responsibilities of each organisation must be clearly defined.	**
6.1.1.3	Phase 1 (Hazard and Risk Assessment) and Phase 2 (Allocation of Safety Functions to Protection Layers) may be seen as the ‘formal’ activities. Prior to that, earlier risk assessments / studies take place which are an inherent part of the ALARP approach. ALARP is often thought to be something which is applied at the end of a project whereas it should be seen as something that runs throughout the safety lifecycle. Refer to ALARP at a Glance ^[11] and Annex G – ALARP.	**

6.1.2 Supervision

Commentary		IEC 61511-1 sub-clauses
6.1.2.1	The duty holder, with legal responsibility for safe operation of the process plant, should put in place a management system to manage all safety activities (including functional safety). IEC 61511 refers to this as a Functional Safety Management System (FSMS). The duty holder must also ensure that all intended suppliers of equipment and services have a suitable FSMS in place.	5.2.1.2

6.1.3 Pre-Phase 1 Activities

Commentary		IEC 61511-1 sub-clauses
6.1.3.1	In the UK as with many other countries, the regulator requires risks to be managed ALARP. This approach includes: • giving due regard to the 'hierarchy of controls' which set a priority order for a way risk controls in a project should be approached, and; • relevant good practice. Refer to Annex G – ALARP.	**
6.1.3.2	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 to Phase 6 (operation and maintenance) including FSA defined and supported by management; • initial contracts in place, where required, for managing all process safety related activities; • personnel responsible for carrying out early functional safety activities identified and confirmed as competent to perform these activities; • internal company and external standards and procedures (applicable to all functional safety activities) defined and communicated to all affected organisations and personnel (this includes the methods of risk assessment to be used together with any relevant calibration, in keeping with the duty holder's risk tolerability criteria).	**

6.2 Hazard and Risk Assessment and Allocation

6.2.1 Introduction

Commentary		IEC 61511-1 sub-clauses
6.2.1.1	IEC 61511-1 does not detail the process for Hazard and Risk Assessment, nor for Allocation of Safety Functions, but it clearly identifies the requirement for it. Some examples of methods used are given in IEC 61511-3 but it should be understood that these are only examples of processes that have previously been used as part of addressing the needs of a particular plant / process lifecycle. Care should be taken in choosing a process that is relevant to a specific project.	**

Commentary	IEC 61511-1 sub-clauses
6.2.1.2 Some techniques have a tendency to overlook the full requirements of H&RA (which are restated here to emphasise the point). H&RA shall be carried out on the materials, process and equipment. It shall result in: • a description of each identified hazardous event and the factors that contribute to it; • a description of the likelihood and consequence of each hazardous event; • consideration of process operating modes such as normal operation, start-up, shutdown, maintenance, process upset, and emergency shutdown; • a determination of additional risk reduction necessary to achieve the required functional safety; • a description of, or reference to information on, the measures taken to reduce or remove hazard and risk; • a detailed description of the assumptions made during the analysis of the risks, including demand rates on the protection layers and the average frequency of dangerous failures of the initiating sources, and of any credit taken for operational constraints or human intervention; • identification of those safety functions applied as SIFs. The H&RA shall be recorded in such a way that the relationships between the above items are clear and traceable.	8.2.1/3
6.2.1.3 H&RA also includes a requirement that a 'security' risk assessment of all SIS/SIFs must also be carried out and measures put in place to minimise the likelihood of compromise (unintended or otherwise). A security risk assessment must include a description of the identified threats, the likelihood of occurrence and the potential consequences, together with the measures taken to remove or reduce the risks. Note: Much of the available guidance concentrates on cyber security but it should be understood that the requirement covers all security risk including: • normal HMI access controls; • physical ports on electronic equipment; • access to configuration parameters / devices for inputs and outputs; • access control to cabinets and enclosures, UPSs etc.	8.2.4

Commentary	IEC 61511-1 sub-clauses
6.2.1.4 Cyber security is a specialist area. Attackers are able to gain access through passive means (such as URL spoofing, phishing, social engineering) or by active means (such as exploiting unpatched security holes; trojans or other malware; domain hijacking and ransomware). Attacks come from individuals, organised gangs and even state sponsorship (where the cost of paying numerous full-time hackers is of little concern). With respect to a SIS, the key concern is that of safety compromise. This is a developing area where there is now a considerable amount of good practice guidance in existence but which is being continually expanded. The general good practice recommendation is that the risk assessment should follow a team approach involving functional safety and cyber security specialists. The difficulty is always in judging what the potential consequences are when considering what measures would be required and there appears to be no clear answer. Cyber threats should probably therefore be treated in a similar way to that of Systematic Capability: i.e. the aiming point should be that the probability of a successful cyber attack should be vanishingly small with respect to the probability of random hardware failure for any given safety function, and the protection level afforded to a SIS should be based on the highest integrity function within. In most countries, there are special regulations relating to what is regarded as national infrastructure / essential services where considerations affect health and safety of the public in a much wider context than that of an individual plant's SIS/SIFs. In the UK, the HSE produced operational guidance (OG86^[12]), first published in 2017 which is updated to reflect current developments. OG86 is free to download and gives a good overview of what is currently available. The reader is directed to publications such as: • IET, COP cyber security and safety (note: this is not an ACOP); • ISA, TR84-00-09-Part-1 Cyber Security for Safety-Related Systems; • ISA99/IEC 62443 series of standards; • T6A, An introduction to Cyber Security for Safety-Related Systems. • EEMUA Industry Information Sheet 2 – Cyber security assessment process for industrial control systems	

Commentary	IEC 61511-1 sub-clauses
6.2.1.5 In general, H&RA and Allocation refers to the formal process of risk assessment and allocation of all safety duties relating to plant integrity and to functional safety. In order to formally allocate all such duties, the design must at that point be mature. It should be understood that there are other risk assessment activities which must take place before and alongside design in order to arrive at a point suitable for formal H&RA and Allocation. For further information, refer to Annex G – ALARP.	**

6.2.2 Formal H&RA and Allocation

Commentary	IEC 61511-1 sub-clauses
6.2.2.1 The purpose of a formal hazard and risk assessment is not to just to determine the SIL of the SIFs but to formally document the detailed risk and risk control mechanisms (see 6.2.1.2) and thus demonstrate that (including allowance for risk reduction afforded by any SIFs) residual risks are tolerable (and, in countries such as the UK, ALARP). Note: Relevant good practice (which must be included in the design) often includes the provision of high integrity E/E/PE functions (e.g. an E-Stop on a standard motor starter). Thus, the function and integrity requirements of SIFs should be well understood before formal H&RA. If a formal risk assessment identifies a risk (or ALARP) gap, it should trigger a design iteration.	
6.2.2.2 The objective of a formal hazard and risk assessment and allocation of risk reduction targets to PLs is to: • review the process and identify and describe in detail any sequence of events arising from failures of protection measures (equipment, systems and people) that lead to a hazardous event that has the potential to cause harm to people, environment or commerce; • identify non-SIS barriers or devices which would reduce the probability of this event occurring (e.g. mechanical devices, alarms, operational procedures, etc); • identify human exposure (where, when and to what extent humans are vulnerable to hazardous events); • identify and describe safety functionality (including SIFs) covering both the function and the reliability performance; • overall, to ensure that risks associated with the hazardous event are both tolerable (and, in some countries such as the UK, ALARP) Notes: • The above applies to all operating modes and sequence steps of the process. • Consideration should be given to the effect of operation of a protective function on any other hazardous events.	8.2.1 / 9.2

Commentary	IEC 61511-1 sub-clauses
6.2.2.3 If there is need for a SIL 4 function (risk reduction $>10\,000$ or a frequency of dangerous failures $< 10^{-8}$ per hour) whether in a single SIS, multiple SIS or SIS in conjunction with a BPCS protection layer, IEC 61511 requires a reconsideration in order to justify this level of instrumented risk reduction. Where such a risk reduction is justified, where possible, the required risk reduction should be split across several independent layers of protection that collectively achieve the same end. The standard states that implementation of SIL 4 SIFs 'need to be avoided'. This falls short of stating that they must be avoided. In general, SIL 4 functions should be avoided. They are extremely difficult to implement, validate and maintain.	9.2.5 / 9.2.6 / 9.2.7 12.2.3 9.2.5 Note **
6.2.2.4 If there is a perceived need for a SIL 3 function (risk reduction $>1\,000$ or a frequency of dangerous failures $< 10^{-7}$ per hour), consideration should be given to keeping these as simple as possible and separate from other SIS / SIFs. Notes: • There is considerable overhead in implementing SIL 3 functionality due to the increased hardware reliability and requirement to avoid systematic errors. Therefore, SIL 3 functions are generally uncommon and, when they do occur, they are usually associated with specialist equipment with specific functionality in dedicated logic solvers. • Because of the requirement to engineer a whole SIS to the highest SIL, the additional burden for lower SIL functions is normally prohibitive. • In the UK, it is not uncommon for the HSE to challenge the perceived need for a SIL 3 risk reduction.	**
6.2.2.5 Because of the requirement that a SIS in its entirety must be subjected to lifecycle activities commensurate with the highest contained SIL, this Guide recommends that: • All SIFs with $SIL > 2$ should be standalone and designed and implemented by suitably competent organisations. • All SIFs with $SIL > 3$ should be implemented in multiple independent layers.	**

Commentary	IEC 61511-1 sub-clauses
6.2.2.6 IEC 61511 stipulates that if the risk reduction associated with a hazard is allocated to several SIFs within one SIS, then the SIS shall meet the overall risk reduction requirement. Whilst this is certainly good engineering practice, there are certain hazards (e.g. associated with combustion) where control and protection is necessarily carried out by a single SIS and where attempting to meet this requirement conflicts with other good practice and would increase risk overall. As such, vendors of equipment intended for the use in such circumstances appear to use the daughter standard of IEC 61508 aimed at safety of machinery (IEC 62061) which does not have the same stipulation. This practice works reasonably effectively enough on packaged units / machines (e.g. a stand-alone boiler). It should however be understood that the applicable standards then require that a risk assessment is carried out on the resultant equipment under control and protection to establish the level of residual risk and ensure its tolerability. The 'packaged unit / machine' concept is difficult to establish if combustion equipment is procured in more general thermo-processing situations. This Guide therefore recommends that it is permitted to deviate from this clause in the standard provided that a robust justification is documented and a quantitative risk assessment methodology is utilised with suitable competence.	9.2.8 **
6.2.2.7 Risk assessments should involve a multi-disciplinary team which collectively has the necessary competence (e.g. process, chemical, mechanical, electrical, control and operational aspects) including detailed understanding of: • the hazards; • relevant good practice; • the safety measures adopted or to be adopted; Notes: • As well as the main process, any package equipment, utility systems must be assessed; • Risk assessments should clearly identify how events in one part of the plant may lead towards danger in other parts; • Risk assessments should clearly identify how events in the plant may lead towards danger to neighbouring sites and / or public spaces.	8.1 Note 1

Commentary		IEC 61511-1 sub-clauses
6.2.2.8	The design process should provide traceability from the identification of the hazardous event, the risk assessment, the allocation of requirements, through to implementation. All safety functions should have unique identifiers which should be referenced in relevant risk assessments, allocations and safety requirements specifications.	8.2.3 **
6.2.2.9	Accurate and adequate documentation is required in order to carry out the risk assessment. Documentation should generally include process flow diagrams, piping and instrument diagrams, process description, SIF/SIS logic, vessel and pipework specifications, HAZOP reports, relief valve specifications, control descriptions, operation and maintenance instructions, hazardous events (together with harm zones and associated vulnerabilities) and operational and maintenance occupancy schedules.	**
6.2.2.10	Risk assessments must be documented. The documented information must include assumptions made and credit taken for control and protection measures. Particular attention should be given to where common causes affect the independence of protection measures and/or affect the independence between initiating cause and protection measures. In such cases, either credit should not be taken for a protection measure or the complex combined effect should be analysed using suitable quantitative techniques.	8.2.1 / 8.2.3
6.2.2.11	Where an assumption is made on the integrity of a protection measure, it should be forwarded to the allocation process such that it becomes a target against which performance is monitored. Where an assumption is about an external event, the occurrence of the external event should be monitored against the assumption or, where the expected frequency of the external event is so low that monitoring makes little difference, alike events across a wider population should be monitored.	**

6.3 Functional Safety Requirements

6.3.1 Introduction

Commentary		IEC 61511-1 sub-clauses
6.3.1.1	This section addresses Phases 3 of the SIS lifecycle as defined in IEC 61511-1. See Figure 1 – Safety lifecycle	
6.3.1.2	There is an inference in IEC 61511 that the production of a Safety Requirements Specification (SRS) is a single point in the safety lifecycle. The contents of an SRS should address a list of '29 bullet points' given in sub-clause 10.3.2. but many of those bullet points would not be addressed until SIS application specialists are involved and, thus, would fall within Phase 4. To distinguish the SRS as developed in Phase 4 from the point of exit of H&RA and Allocation, this Guide refers to the document as the Safety Function Description. It is recommended (for reasons of ownership) that it remains a separate document from the SRS. As with IEC 61511, this Guide doesn't concern itself further with the development of equipment designs or procedures to support non-instrumented functional safety but Safety Function Descriptions are required for all functional safety. Where this Guide refers to Safety Requirements Specifications (SRSs) they relate only to those relevant to SIS/SIFs.	10.3.2 **

6.3.2 Safety Function Description

Commentary		IEC 61511-1 sub-clauses
6.3.2.1	The formal allocation of safety functionality to protection layers is made by means of a Safety Function Description (SFD). An SFD should be generated for each protection layer involved in the control or mitigation of a hazardous event, describing the functions allocated to people, systems and equipment. This is an important step because all safety functionality should be owned and managed throughout the safety lifecycle.	