IEC61508: Assessment, Certification and Other Assurance Measures

Ron Bell

Engineering Safety Consultants Ltd

London, UK

Abstract This paper focuses on the safety assurance measures within international standard IEC 61508, 'Functional safety of electrical, electronic and programmable electronic safety-related systems'. IEC 61508, and other sector and product standards developed from it, have had a major impact on the application of electrical, electronic and programmable electronic safety-related systems. In particular, the paper examines the safety assurance measures that are part of the compliance requirements within IEC 61508. The paper provides an overview of the key features of IEC 61508 which are relevant to effective assurance as well as covering the explicit assurance measures such as functional safety assessment, functional safety audit, verification and validation. The paper also covers various models for certification that have developed in relation to IEC 61508.

1 Background

IEC 61508 applies to safety-related systems when one or more of such systems incorporate electrical, electronic or programmable electronic (E/E/PE) devices. E/E/PE safety-related systems are intended, with the other risk reduction measures and risk parameters, to prevent the specified hazardous event or to mitigate the consequences of the specified hazardous event.

Parts 1 to 7 of IEC 61508 were published during the period 1998-2000. A review process to update and improve the standard was initiated in 2002 and was completed with the publication of IEC 61508 Edition 2 (IEC 2010a) in April 2010.

The application of IEC 61508 and sector and product implementations are increasingly being recognised as 'accepted good practice' and have also influenced sectors which have developed their own standards and have incorporated some of the core concepts that exist within IEC 61508 into their own standards.

2 Structure of IEC 61508

The overall title of IEC 61508 is ‘Functional safety of electrical, electronic and programmable electronic (E/E/PE) safety-related systems’. The Parts are as listed in Table 1.

Table 1. The Parts of IEC 61508

Part	Title
0	Functional safety and IEC 61508
1	General requirements
2	Requirements for electrical/electronic/programmable electronic safety-related systems
3	Software requirements
4	Definitions and abbreviations
5	Examples of methods for the determination of safety integrity levels
6	Guidelines on the application of parts 2 and 3
7	Overview of techniques and measures

In IEC standards, a requirement that has to be satisfied if compliance is to be claimed is referred to as a normative requirement. Such requirements are prefaced by ‘shall’. A requirement prefaced by ‘should’ is informative and can be considered as a recommendation. However, a recommendation may, over time, become normative when that edition of the standard is revised and this should be taken into account.

Parts 1, 2 and 3 contain all the normative requirements and some informative requirements. Parts 0, 5, 6 and 7 do not contain any normative requirements.

IEC 61508 can be used as a standalone standard. Also, as Parts 1, 2, 3 and 4 have been designated as IEC basic safety publications, IEC Technical Committees have, wherever practicable, to make use of IEC 61508 in the preparation of their own sector or product standards that have E/E/PE safety-related systems within their scope. In its role as a basic publication, IEC 61508 has, for example, been used to develop standards for the process (IEC 61511) and nuclear (IEC 61513) sectors and for machinery (IEC 62061) and power drive systems (IEC 61800-5-2).

The application of IEC 61508 as a standalone standard includes the use of the standard:

- as a set of general requirements for E/E/PE safety-related systems where no application sector or product standards exist or where they are not appropriate
- by suppliers of E/E/PE elements for use in all sectors (e.g. hardware and software of sensors, smart actuators, programmable controllers)
- by providing a technical framework for conformity assessment and certification services as a basis for carrying out assessments of safety lifecycle activities.

3 Scope of IEC 61508

IEC 61508 is mainly concerned with E/E/PE safety-related systems whose failure could have an impact on the safety of persons and/or the environment. However, it was recognized that the consequences of failure could have serious economic implications and in such cases the standard could be used to specify any E/E/PE system used for the protection of equipment or product (asset protection).

Some of the key features of IEC 61508 are set out below.

- It enables the development of product and sector international standards, dealing with E/E/PE safety-related systems. This should lead to a high level of consistency (for example, of underlying principles, terminology etc.) both within and across application sectors; this will have both safety and economic benefits.
- It provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems.
- It uses safety integrity levels (SILs) for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems.
- It adopts a risk-based approach for the determination of the safety integrity level requirements.
- It sets numerical target failure measures for E/E/PE safety-related systems that are linked to the safety integrity levels.

4 Concept of functional safety

Safety is defined as the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly, as a result of damage to property or to the environment.

Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs. In essence, this means the achievement of safety through application of control systems. This requires identifying *what has to be done* and *how well it should be done*.

5 Strategy to achieve functional safety

The strategy for achieving functional safety is made up of the following key elements:

- management of functional safety including competence

- technical requirements for relevant phases of the applicable safety lifecycles
- assurance measures such as verification, validation, functional safety audit and functional safety assessment.

IEC 61508 uses three safety lifecycles in order that all relevant phases are addressed. They are:

- the overall safety lifecycle (see Figure 1)
- the E/E/PE system safety lifecycle (see Figure 2)
- the software safety lifecycle (see Figure 3).

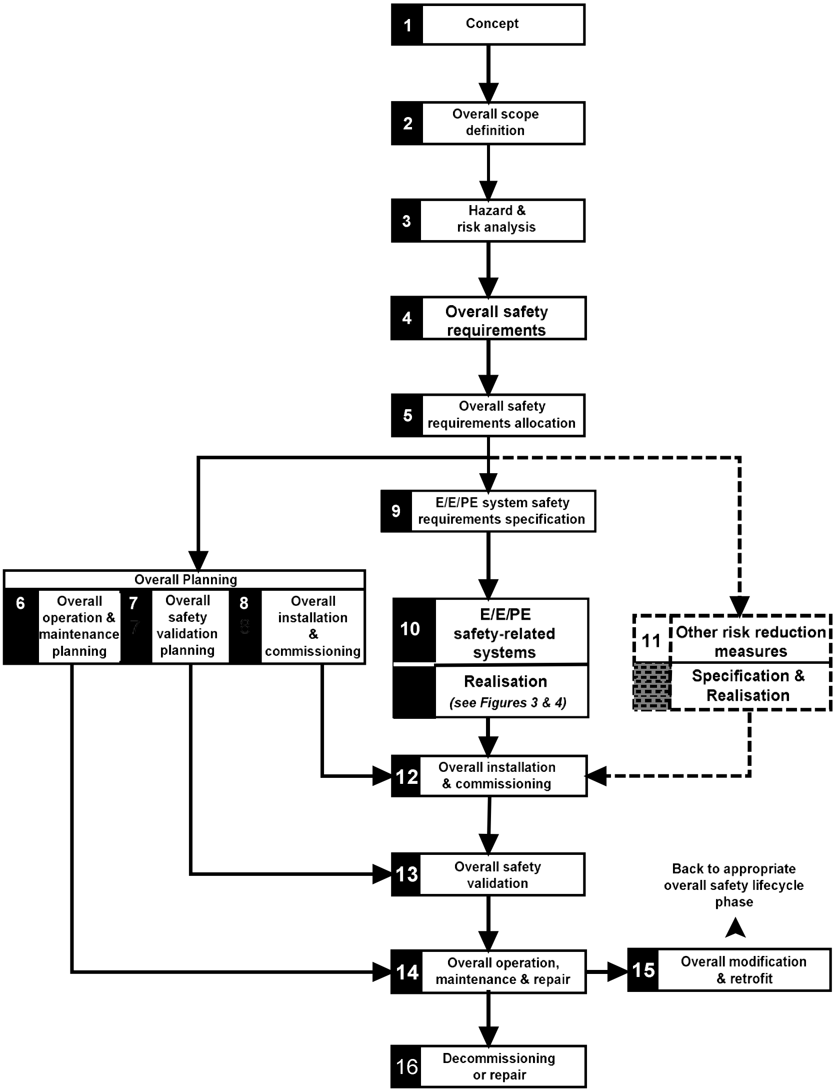
1 Concept
2 Overall scope definition
3 Hazard & risk analysis
4 Overall safety requirements
5 Overall safety requirements allocation
9 E/E/PE system safety requirements specification
Overall Planning
6 Overall operation & maintenance planning
7 Overall safety validation planning
8 Overall installation & commissioning
10 E/E/PE safety-related systems
Realisation (see Figures 3 & 4)
11 Other risk reduction measures
Specification & Realisation
12 Overall installation & commissioning
13 Overall safety validation
Back to appropriate overall safety lifecycle phase
14 Overall operation, maintenance & repair
15 Overall modification & retrofit
16 Decommissioning or repair

Fig. 1. Overall safety lifecycle from IEC 61508 Edition 2

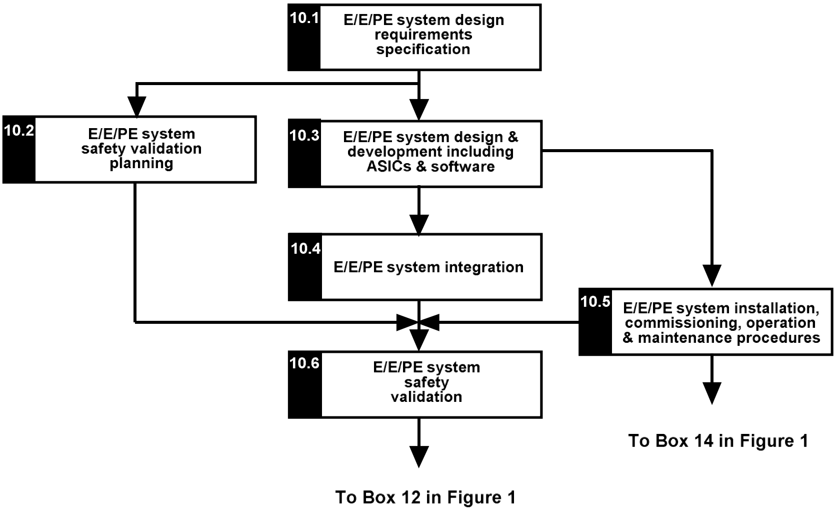
10.1
E/E/PE system design requirements specification
10.2
E/E/PE system safety validation planning
10.3
E/E/PE system design & development including ASICs & software
10.4
E/E/PE system integration
10.5
E/E/PE system installation, commissioning, operation & maintenance procedures
10.6
E/E/PE system safety validation
To Box 12 in Figure 1
To Box 14 in Figure 1

Fig. 2. E/E/PE system safety lifecycle (in realisation phase) from IEC 61508 Edition 2

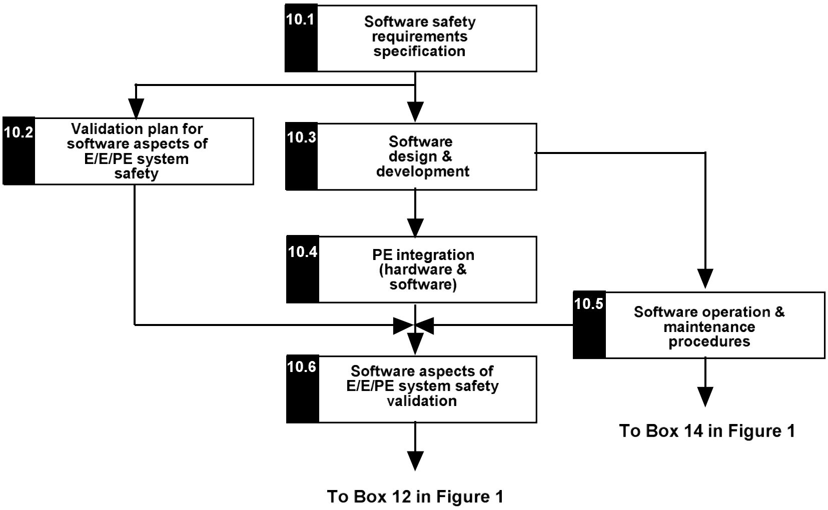
10.1
Software safety requirements specification
10.2
Validation plan for software aspects of E/E/PE system safety
10.3
Software design & development
10.4
PE integration (hardware & software)
10.5
Software operation & maintenance procedures
10.6
Software aspects of E/E/PE system safety validation
To Box 12 in Figure 1
To Box 14 in Figure 1

Fig. 3. Software safety lifecycle (in realisation phase) from IEC 61508 Edition 2

In order to deal in a systematic manner with all the activities necessary to achieve the required safety integrity for the E/E/PE safety-related systems, IEC 61508 adopts the overall safety lifecycle indicated in Figure 3 as the technical framework. The overall safety lifecycle specified in IEC 61508 should be used as a basis for claiming conformance to the standard, but a different overall safety lifecycle can be used to that given in Figure 3, providing the objectives and requirements of each clause of the standard are met.

The overall safety lifecycle encompasses the following risk reduction model:

- E/E/PE safety-related systems
- other risk reduction measures.

Whilst IEC 61508 provides design requirements for the achievement of functional safety for E/E/PE safety-related systems, it does not provide design requirements for ‘other risk reduction measures’ but does take into account the risk reduction achieved by such measures.

The portion of the overall safety lifecycle dealing with E/E/PE safety-related systems is expanded and shown in Figure 2. This is termed the E/E/PE system safety lifecycle and forms the technical framework for IEC 61508-2. The software safety lifecycle is shown in Figure 3 and forms the technical framework for IEC 61508-3.

It is very important to recognize that the overall, E/E/PE system safety and software safety lifecycle figures are simplified views of reality and as such do not show all the iterations relating to specific phases or between phases. Iteration, however, is an essential and vital part of development through the overall E/E/PE system safety and software safety lifecycles.

Activities relating to the management of functional safety, verification and functional safety assessment are not shown on the overall E/E/PE system safety and software safety lifecycles. This has been done in order to reduce the complexity of the safety lifecycle activities. These activities will need to be applied at the relevant phases of the safety lifecycles.

Evidence of the need to adopt an approach that covers all phases of the overall safety lifecycle is illustrated in a study undertaken by the UK Health and Safety Executive (HSE 2003). The study analyzed a number of accidents and incidents involving safety-related control systems. Figure 4 shows the primary cause of failure for each lifecycle phase.

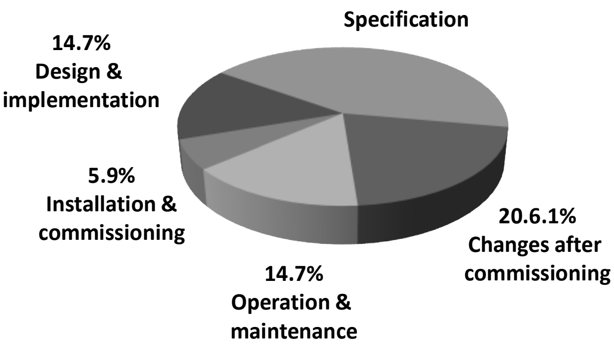

Fig. 4. Primary cause, by phase, of control system failures

The analysis suggests that most control system failures may have their root cause in an inadequate specification. In some cases this was because insufficient hazard analysis of the equipment under control had been carried out; in others it was because the impact on the specification of a critical failure mode of the control system had not been assessed.

Based on the HSE study, more than 60% of failures were 'built in' to the safety-related system before being taken into service. Whilst the primary causes by phase will vary depending upon the sector and complexity of the application, what is self-evident is that it is important that all phases of the lifecycle be addressed if functional safety is to be achieved.

6 Essence of functional safety

A cornerstone of functional safety is the safety function. The safety function is defined as follows:

> 'Function to be implemented by an E/E/PE safety-related system, or other risk reduction measures, that is intended to achieve or maintain a safe state for the equipment under control in respect of a specific hazardous event.'

There is a need to specify the functional safety performance requirements for each safety function and this is the objective of the E/E/PE system safety requirements specification which contains the requirements for all the safety functions being carried out by the E/E/PE safety-related system.

If the safety function is performed the hazardous event will not take place. The safety function is determined from the hazard analysis. It is the safety function that determines *what has to be done* to achieve or maintain a safe state for the equipment under control.

IEC 61508 adopts a risk-based approach to the development of the specification of the required safety performance of each safety function. The safety performance is referred to as the safety integrity and is determined from the risk assessment. This is illustrated in Figure 5.

7 Safety-related systems

A safety-related system is a system that is capable of carrying out the various specified safety functions and also capable of carrying them out with the required safety integrity. It is the safety integrity requirement of the safety function that sets the safety integrity requirements for the safety-related system. A safety-related system will carry out many safety functions and must be of sufficient safety integrity to carry out the safety function with the highest safety integrity requirement (unless special measures are taken).

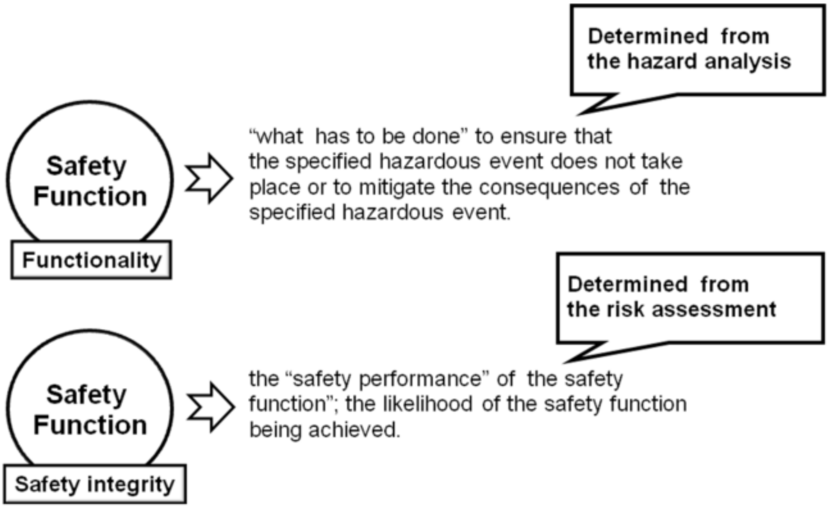
Determined from the hazard analysis
Safety Function
Functionality
"what has to be done" to ensure that the specified hazardous event does not take place or to mitigate the consequences of the specified hazardous event.
Determined from the risk assessment
Safety Function
Safety integrity
the "safety performance" of the safety function"; the likelihood of the safety function being achieved.

Fig. 5. The functionality and safety integrity of a safety function

Safety integrity is made up of hardware safety integrity (in relation to random failures) and systematic safety integrity (in relation to systematic failures).

8 Safety Integrity Levels (SILs)

Each safety function to be carried out by an E/E/PE safety-rated system is specified in terms of the Safety Integrity Level (SIL). Tables 2 and 3 relate the target failure measures to the SIL.

Table 2. Safety integrity levels: target failure measures for a safety function operating in a low demand mode of operation

SIL	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	10^{-5} to < 10^{-4}
3	10^{-4} to < 10^{-3}
2	10^{-3} to < 10^{-2}
1	10^{-2} to < 10^{-1}

The target failure measure is specified as either:

- the average probability of dangerous failure on demand of the safety function, (PFD_{avg}), for a low demand mode of operation (see Table 2)
- the average frequency of a dangerous failure of the safety function [h_{-1}], (PFH), for a high demand mode of operation (see Table 3)

- the average frequency of a dangerous failure of the safety function [h_{-1}], (PFH), for a continuous mode of operation (see Table 3).

Table 3. Safety integrity levels: target failure measures for a safety function operating in a high demand or continuous mode of operation

SIL	Probability of dangerous failure per hour (PFH)
4	10^{-9} to < 10^{-8}
3	10^{-8} to < 10^{-7}
2	10^{-7} to < 10^{-6}
1	10^{-6} to < 10^{-5}

It can be seen from Tables 2 and 3 that the SILs are related to the target failure measures depending upon the ‘mode of operation’. The mode of operation has important implications when determining the SIL of a safety function to meet a target risk frequency.

9 Compliance to IEC 61508

The compliance model for IEC61508 is indicated in Figure 6.

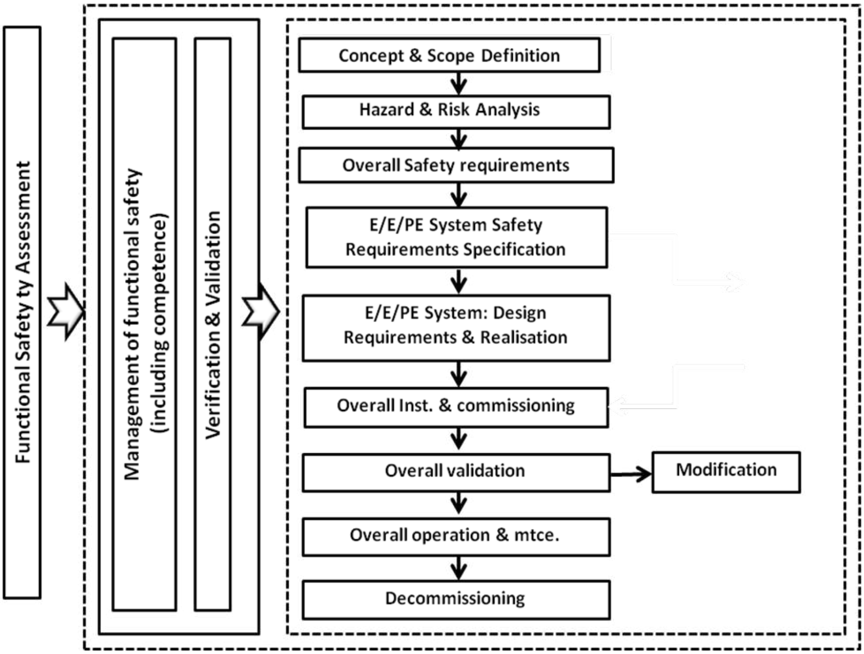
Functional Safety ty Assessment
Management of functional safety (including competence)
Verification & Validation
Concept & Scope Definition
Hazard & Risk Analysis
Overall Safety requirements
E/E/PE System Safety Requirements Specification
E/E/PE System: Design Requirements & Realisation
Overall Inst. & commissioning
Overall validation
Modification
Overall operation & mtce.
Decommissioning

Fig.6. Compliance to IEC 61508, showing a simplified overall safety lifecycle (compare with Figure 1)

It can be seen that compliance to IEC 61508 in respect of any safety life-cycle clauses for which compliance is to be claimed requires the following.

Technical requirements. All relevant clauses in relation to any safety lifecycle phase (i.e. overall safety lifecycle, E/E/PE system safety lifecycle and software safety lifecycle) have to be met.

Functional safety management. The requirements relating to management have to be met in the context of the relevant safety life cycle phases.

Verification is required to be undertaken for each relevant safety lifecycle phase.

Validation is required to be undertaken with respect to the E/E/PE safety-rated system in respect of the specified safety functions.

Functional safety assessment is required to be carried out for all relevant safety life cycle phases.

Competence. All persons with responsibilities (i.e. including all persons involved in any overall, E/E/PE system or software lifecycle activity, including activities for verification, validation, management of functional safety, functional safety audit and functional safety assessment), have to have the appropriate competence. This would include training, technical knowledge, experience and qualifications relevant to the specific duties that they have to perform.

10 Key safety assurance measures

The key assurance measures in the achievement of functional safety, in compliance with IEC 61508, are:

- functional safety assessment;
- functional safety audit;
- verification;
- validation;

These are considered in Sections 10.1 to 10.4.

10.1 Functional safety assessment

The objective is to arrive at a judgement on the adequacy of the functional safety achieved by the E/E/PE safety-related system(s) or compliant items (e.g. elements, subsystems) based on compliance with the relevant clauses of this standard.

All relevant safety life cycle phases are within scope of the functional safety assessment including functional safety management, verification, validation and documentation.

Those undertaking a functional safety assessment have to meet specific independence requirements. There are three levels of independence which are:

- independent person
- independent department
- independent organization.

The criteria for the above three levels of independence are specified in IEC 61508-1.

The degree of independence depends upon:

- the consequence in the event of a hazardous event arising, with the consequence parameter being used as a factor in the degree of independence (see Table 4)
- the SIL or the systematic capability of the safety function (see Table 5).

With respect to Tables 4 and 5:

- 'X' is the level of independence specified is the minimum for the specified consequence (Table 4) or safety integrity level or systematic capability (Table 5). If a lower level of independence is adopted, then the rationale has to be specified.
- 'Y' is the level of independence specified that is considered insufficient for the specified consequence (Table 4) or safety integrity level or systematic capability (Table 5).

Table 4. Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 1 to 8 and 12 to 16 inclusive (see Figure 1))

Minimum level of independence	Consequence			
	A	B	C	D
Independent person	X	X1	Y	Y
Independent department		X2	X1	Y
Independent organization			X2	X

Table 5. Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 9 and 10, including all phases of E/E/PE system and software safety lifecycles (see Figures 1, 2 and 3))

Minimum level of independence	SIL/systematic capability			
	1	2	3	4
Independent person	X	X1	Y	Y
Independent department		X2	X1	Y
Independent organization			X2	X

The functional safety assessment may be carried out after each safety lifecycle phase or after a number of safety lifecycle phases subject to the overriding requirement that a functional safety assessment be undertaken prior to the determined hazards being present.

10.2 Functional safety audit

In IEC 61508, a functional safety audit is defined as:

> 'Systematic and independent examination to determine whether the procedures specific to the functional safety requirements to comply with the planned arrangements are implemented effectively and are suitable to achieve the specified objectives'

The evidence obtained from the functional safety audit will form part of the evidence assessed as part of the functional safety assessment.

It will be necessary that periodic functional safety audits be specified for:

- the frequency of the audits
- the level of independence of those carrying out the audits
- the necessary documentation and follow-up activities after an audit has been completed.

10.3 Verification

In IEC 61508, verification is the activity of demonstrating for each phase of the relevant safety lifecycle (overall, E/E/PE system and software), by analysis, mathematical reasoning and/or tests, that, for the specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase.

An example of verification activities will include:

- reviews on outputs (documents from all phases of the safety lifecycle) to ensure compliance with the objectives and requirements of the phase, taking into account the specific inputs to that phase
- design reviews
- tests performed on the designed products to ensure that they perform according to their specification
- integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner.

The documentation related to verification would be assessed as part of the functional safety audit and the functional safety assessment.

10.4 Validation

In IEC 61508, validation is the activity of demonstrating that the safety-related system under consideration, before or after installation, meets in all respects the safety requirements specification for that safety-related system.

Therefore, for example, validation of the E/E/PE safety-rated system means confirming by examination and provision of objective evidence that the E/E/PE safety-rated system satisfies the E/E/PE system design requirements specification.

In IEC61508 there are three validation phases:

- overall safety validation (see Figure 1)
- E/E/PE system validation (see Figure 2)
- software validation (see Figure 3).

The documentation related to validation would be assessed as part of the functional safety audit and the functional safety assessment.

10.5 Conformity assessment and certification

10.5.1 The fundamentals

The terms ‘conformity assessment’ and ‘certification’ are often misunderstood. In this paper the term conformity assessment is defined as[1]:

> ‘... activity that provides demonstration that specified requirements relating to a product, process, system, person or body are fulfilled’

Conformity assessment may be undertaken by:

- a first party: this could be manufacturer of a specified product
- a second party: this could be user of a specified product
- a third party: this is a body that is independent of the first and second parties.

A body that carries out third-party conformity assessment within the framework of ISO/IEC 17065:2012 is referred to as a certification body. The scope of ISO/IEC 17065:2012 is specified as follows:

> ‘This International Standard contains requirements for the competence, consistent operation and impartiality of product, process and service certification bodies. Certification bodies operating to this International Standard need not offer all types of products, processes and services certification. Certification of products, processes and services is a third-party conformity assessment activity (see ISO/IEC 17000:2004, definition 5.5).

[1] ISO/IEC 17000:2004 Conformity assessment – vocabulary and general principles

> 'In this International Standard, the term "product" can be read as "process" or "service", except in those instances where separate provisions are stated for "processes" or "services" (see ...).'

Therefore, certification bodies carrying out conformance assessment in compliance with ISO/IEC 17065: 2012 are undertaking third-party conformity assessment[2].

There is no requirement in IEC 61508 for compliance to be attested by a certification body as defined previously. It is a compliance requirement in IEC 61508 that an independent functional safety assessment be undertaken with respect to all relevant clauses applicable to the entity in question. The degree of independence, as part of that assessment process, will depend upon the criteria set out in IEC 61508 (see Section 10.1).

However, although there is no requirement within IEC 61508 that conformity assessment be undertaken by a certification body, companies often seek conformity assessment to IEC 61508 from a certification body operating within the framework of ISO/IEC 17065:2012.

When a third-party undertaking conformity assessment has been accredited as being in compliance with ISO/IEC 17065:2012 they are referred to as accredited certification bodies. Accreditation is carried out by a nationally appointed body such as the United Kingdom Accreditation Service (UKAS).

In the context of a specified product (e.g. sensor containing hardware and software) that is deemed to be in compliance with IEC 61508, the product manufacturer may request that an accredited certification body undertake the functional safety assessment. This approach is often adopted on the basis that conformity assessment by an accredited certification body provides a high level of confidence of compliance, which is valuable in terms of their own legal position and also valuable commercially by providing strong and supportable evidence of compliance to IEC 61508.

Companies procuring elements to IEC 61508 will, as a first priority, usually seek to procure elements that have been certified as complying with IEC 61508 by an accredited certification body.

10.5.2 What can be certified?

Certification can be undertaken on:

1. A specified product (e.g. sensor comprising complex electronics (hardware and software)). This will be referred to as a 'certified sensor'.

[2] ISO/IEC 17065: 2012 'Conformity assessment – Requirements for bodies certifying products, processes and services' is the international standard for certification bodies operating third-party conformity assessment schemes. This standard will be used by accreditation bodies as the basis of their accreditation of certification bodies and supersedes ISO/IEC Guide 65:1996 'General requirements for bodies operating product certification systems'. Within Europe, EN ISO/IEC 17065:2012 will replace EN 45011:1998.

2. The functional safety management system in respect of the specified scope of the activities of:

   - a systems integrator
   - an end user with respect to the operation and maintenance phase requirements.

The certification model in item 2 above is essentially a capability assessment of the organisation involved and provides confidence that, in the context of a systems integrator, they have the capability within the defined scope on the certificate of being able to comply with relevant clauses in IEC 61508.

11 Documentation and traceability

The documentation clause in IEC 61508 states:

> '**5.1.1** The first objective of the requirements of this clause is to specify the necessary information to be documented in order that all phases of the overall, E/E/PE system and software safety lifecycles can be effectively performed.
>
> '**5.1.2** The second objective of the requirements of this clause is to specify the necessary information to be documented in order that the management of functional safety (see Clause 6), verification (see 7.18) and the functional safety assessment (see Clause 8) activities can be effectively performed.'

The focus of the documentation clause is on information rather than physical documents. The clause, as written, provides explicit forward traceability but by indicating the necessary information is documented 'in order that all phases of the overall, E/E/PE system and software safety lifecycles can be effectively performed' it is clear that both forward and backward traceability is a necessary requirement of IEC 61508.

The information, and the traceability of the information relating to the relevant phases of the various safety lifecycles, is a prerequisite to effective safety assurance. This cannot be underestimated since it will be necessary to manage the equipment for possibly 25 years and probably within that time a number of modifications will necessitate impact analyses to be undertaken. Without robust traceability it would not be possible to assure that the target risk is being maintained.

Although documentation and traceability are not usually seen as an explicit safety assurance measure it is a cornerstone on which an effective safety assurance policy has to be based.

12 Concluding comments

IEC 61508 has a number of key compliance requirements which can be regarded as explicit safety assurance measures (i.e. functional safety assessment, functional safety audit, verification and validation) and these are all necessary as part of robust safety assurance strategy. However, a vital part of the safety assurance is the ability to understand the processes that have been undertaken in the relevant phases of the safety lifecycles. That is, robust information and traceability of the information is a cornerstone of an effective safety assurance strategy.

The holistic approach adopted in IEC 61508 to the achievement of functional safety provides a sound basis for ensuring that the initial design, the ongoing maintenance of the design and subsequent modifications to the design are managed in a systematic manner. The documentation clause which focuses on information rather than physical documents provides requirements that facilitate forwards and backward traceability.

Acknowledgments The author thanks the International Electrotechnical Commission (IEC) for permission to reproduce information from its international publication IEC 61508 ed.2.0 parts 1 to 7 (2010). All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy therein.

References

HSE (2003) Out of control: why control systems go wrong and how to prevent failure, 2nd edn. HSE Books. http://www.hse.gov.uk/pubns/books/hsg238.htm**.** Accessed 10 October 2012

IEC (2010a) IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1 to 7, Edition 2.0. International Electrotechnical Commission