Introduction to IEC 61508

Ron Bell
Health & Safety Executive
Bootle, UK
ron.bell@hse.gsi.gov.uk

Abstract

Over the past 25 years there have been a number of initiatives worldwide to develop guidelines and standards to enable the safe exploitation of programmable electronic systems used for safety applications. In the context of industrial applications (to distinguish from aerospace and military applications) a major initiative has been focussed on IEC 61508 and this standard is emerging as a key international standard in many industrial sectors.

This paper considers some of the key features of IEC 61508 and indicates some of the issues that are being considered in the current revision.

Keywords: IEC 61508, functional safety, safety integrity level, SIL

1 Background

During the 1980's computer based systems (generically referred to as programmable electronic systems (PESs)) were increasingly being used to carry out safety functions. The driving force was improved functionality and economic benefits (particularly when viewed on a total lifecycle basis). Also, the viability of certain designs could only be realised when computer technology was used. The adoption of PESs for safety purposes had potentially, many safety advantages, but it was recognised that these would only be realised if appropriate design and assessment methodologies were used.

Many of the features of PESs do not enable the safety integrity (that is, the safety performance of the systems carrying out the required safety functions) to be predicted with the same degree of confidence that had traditionally been available for less complex hardware-based ("hardwired") systems. It was recognised that whilst testing was necessary for complex systems it was not sufficient on its own. This meant that even if the PES was implementing relatively simple safety functions the level of complexity of the programmable electronics was significantly greater than the hardwired systems that had traditionally been used. This rise in complexity meant that the design and assessment methodologies had to be given much more consideration than previously was the case and the level of personal competence required to achieve adequate levels of performance of the safety-related systems was subsequently greater.

In order to tackle these problems, several bodies published or began developing guidelines to enable the safe exploitation of PES technology. In the UK, the Health and Safety Executive (1987) developed and published guidelines for programmable electronic systems used for safety-related applications. In Germany, DIN (1990) published a standard and, in the USA, ISA (1996) developed a standard on programmable electronic systems for use in the process industries. Also in the USA, CCPS (1993) produced guidelines for the chemical process sector.

Initially the focus of standards' developments during the early 1980s, in the context of PES applications, was on the software. However, it was becoming increasingly recognised that a holistic, systems based, approach was necessary if an adequate level of safety performance were to be achieved. Such an approach meant addressing:

- The complete system carrying out the required safety function;
- The system architecture;
- Both random hardware failures and systematic failure (including software).

In September 1985, the International Electrotechnical Commission (IEC) set up a Task Group to assess the viability of developing a generic standard for PESs. The outcome of which was the setting up of a working group to develop a systems based approach. A working group had previously been set up to deal with safety-related software. The two working groups collaborated on the development on what was to become IEC 61508. Also, the original scope of PESs was extended to include all types of electro-technical based technologies (electrical, electronic and programmable electronic systems). Parts 1-7 of IEC 61508 were published between 1998-2000. In 2005 IEC TR 61508-0 was published.

2 The 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 follows:

- Part 0: Functional safety and IEC 61508.

  Note: This has the status of a Technical Report and is purely informative.

- Part 1: General Requirements;
- Part 2: Requirements for electrical, electronic and programmable electronic systems;
- Part 3: Software Requirements;
- Part 4: Definitions and abbreviations;
- Part 5: Examples of methods for the determination of safety-integrity levels;
- Part 6: Guidelines on the application of Parts 2 and 6;
- Part 7: Overview of techniques and measures.

Parts 0, 5, 6 and 7 do not contain any normative requirements. Parts 1, 2, 3 contain all the normative requirements and some informative requirements. The formal titles are given in Annex A.

Note: In IEC standards a normative requirement is prefaced by a "shall".

Parts 1, 2, 3 and 4 of IEC 61508 are *IEC basic safety publications*. One of the responsibilities of IEC Technical Committees is, wherever practicable, to make use of these parts of IEC 61508 in the preparation of their own sector or product standards that have E/E/PE safety-related systems within their scope.

The basic safety publication status of IEC 61508 described above does not apply for low complexity E/E/PE safety-related systems. These are E/E/PE safety-related systems in which the failure modes of each individual component are well defined and the behaviour of the system under fault conditions can be completely determined. An example is a system comprising one or more limit switches, operating one or more contactors to de-energize an electric motor, possibly via interposing electromechanical relays.

IEC 61508 is both a stand-alone standard and can also be used as the basis for sector and product standards. In its latter role, it has been used to develop standards for both the process and machinery sectors and is currently being used to develop a standard for power drive systems. It has influenced, and will continue to influence, the development of E/E/PE safety-related systems and products across all sectors.

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 components and subsystems for use in all sectors (e.g. hardware and software of sensors, smart actuators, programmable controllers, data communication);
- By system builders to meet user specifications for E/E/PE safety-related systems;
- By users to specify requirements in terms of the safety functions to be performed together with the performance requirements of those safety functions;
- To facilitate the maintenance of the "as designed" safety integrity of E/E/PE safety-related systems;
- To provide the technical framework for conformity assessment and certification services;
- As a basis for carrying out assessments of safety lifecycle activities.

This concept is illustrated in Figure 1.

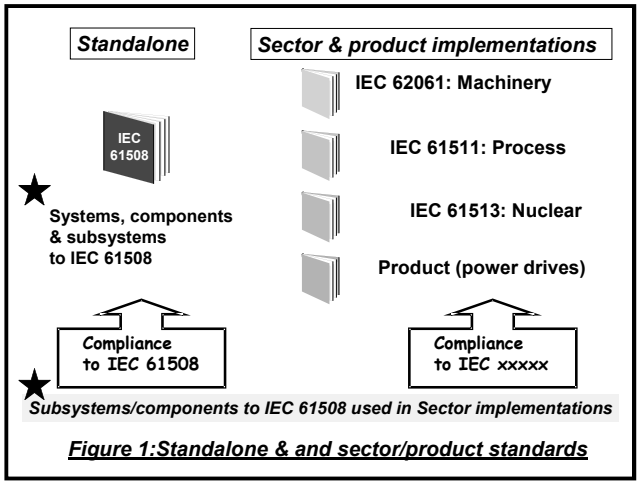

Figure 1:Standalone & and sector/product standards

Sector specific standards based on IEC 61508:

- Are aimed at system designers, system integrators and users;
- Take account of specific sector practice, which can allow less complex requirements;
- Use sector terminology to increase clarity;
- May specify particular constraints appropriate for the sector;
- Usually rely on the requirements of IEC 61508 for detailed design of subsystems;
- May allow end users to achieve functional safety without having to consider IEC 61508 themselves.

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;

Note: This has important implications since it means that IEC 61508, which is identified with functional safety, can be used for the specification and implementation of systems where the functional performance parameter is not safety but, for example, environmental protection or asset protection.

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

1. It enables application sector international standards, dealing with safety-related E/E/PESs, to be developed. This should lead to a high level of consistency (for example, of underlying principles, terminology etc.) both within application sectors and across application sectors; this will have both safety and economic benefits.
2. 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.
3. It uses safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems.
4. It adopts a risk-based approach for the determination of the safety integrity level requirements.
5. It sets numerical target failure measures for E/E/PE safety-related systems that are linked to the safety integrity levels.
6. It sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed for a single E/E/PE safety-related system; for E/E/PE safety-related systems operating in:
   - A low demand mode of operation, the lower limit is set at an average probability of failure of 10^{-5} to perform its design function on demand,
   - A high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of 10^{-9} per hour.

Note: A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

It adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems. The standard does not use the concept of fail-safe, which may be appropriate when the failure modes are well defined and the level of complexity is relatively low, but inappropriate in view of the wide range of complexity of E/E/PE safety-related systems that are within the scope of the standard.

4 What is 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. For example, an over temperature protection device, using a thermal sensor in the windings of an electric motor to de-energise the motor before they can overheat, is an instance of functional safety.

Neither safety nor functional safety can be determined without considering the systems as a whole and the environment with which they interact.

5 Strategy to Achieve Functional Safety?

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

- Management of functional safety;
- Technical requirements for each phase of the Overall. E/E/PES and Software Safety Lifecycles;
- Competence of persons (currently no normative requirements);
- 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 B1 in Annex B);
- The E/E/PES Safety Lifecycle (see Figure B2 in Annex B);
- The Software Safety Lifecycle (see Figure B3 in Annex B).

In order to deal in a systematic manner with all the activities necessary to achieve the required safety integrity level for the E/E/PE safety-related systems, IEC 61508 adopts the overall safety lifecycle as the technical framework and this should be used as a basis for claiming conformance to IEC 61508. A different overall safety lifecycle can be used to that given in Figure B1, providing the objectives and requirements of each clause of this standard are met.

The overall safety lifecycle encompasses the following risk reduction measures:

- E/E/PE safety-related systems;
- Other technology safety-related systems;
- External risk reduction facilities.

The portion of the overall safety lifecycle dealing with E/E/PE safety-related systems is expanded and shown in Figure B2. This is termed the E/E/PES safety lifecycle and forms the technical framework for IEC 61508-2. The software safety lifecycle is shown in Figure B3 and forms the technical framework for IEC 61508-3.

The overall, E/E/PES 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/PES 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/PES or software safety lifecycles. This has been done in order to reduce the complexity of the overall, E/E/PES and software safety lifecycle figures. These activities, where required, will need to be applied at the relevant phases of the overall, E/E/PES and software 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 Health and Safety Executive

(1995). The study analysed a number of accidents an incidents involving the safety-related control systems. Figure 2 shows the primary cause of failure by each lifecycle phase.

Note: It is acknowledged that because of the small sample size the results of the analysis have low statistical significance, and therefore care needs to be taken in using these results to generalise for all control system failures. Even so, there are many useful lessons to be learned from summaries of incidents such as these.

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.

The control system needs to be continually reviewed throughout all lifecycle phases, both from the perspective of the equipment-under-control and the detailed design and implementation of the control system itself. Otherwise the end result is a machine, or plant, with inadequate protection against the hazardous events.

Other studies provide support for these conclusions. In the area of software development a number of studies have shown that errors made during specification account for most software faults and failures.

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.

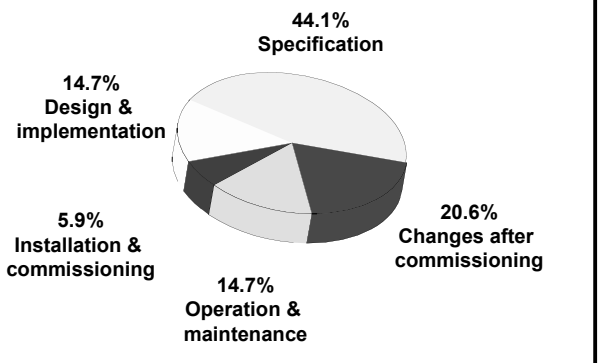

Figure 2: Primary cause, by phase, of control system failures

6 The 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 …… which is intended to achieve or maintain a safe state for the equipment under control in respect of a specific hazardous event".

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 and it is the safety function that is the basis of the functional specification of the safety-related system.

It is necessary to determine the safety performance of each safety function and IEC 61508 adopts a risk-based approach to achieve this. The safety performance is referred to as the safety integrity and is determined from the risk assessment. This is illustrated in Figure 3.

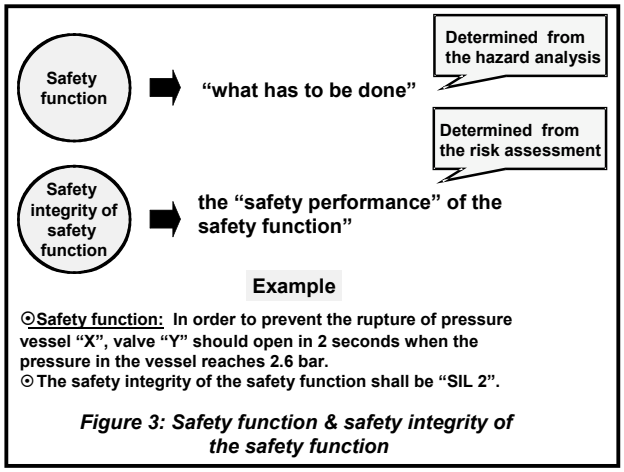

Figure 3: Safety function & safety integrity of the safety function

7 Safety-Related System

A safety-related system is a system that is capable of carrying the requirements specified in each safety function 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)

8 Safety Integrity Levels

The failure categories in IEC 61508 relate to failures arising from (1) random hardware failures and (2) systematic failures (see Figure 4). The challenge to anyone designing a complex system such as a programmable electronic system is to determine how much rigour/assurance/confidence is necessary for the specified safety performance level. IEC 61508 tackles this on the following basis:

- That it is possible to quantify the random hardware failures and therefore estimate whether the target failure measure has been achieved.
- That is not usually possible to quantify those elements giving rise to systematic failure behaviour.

IEC 61508 sets four Safety Integrity Levels (SILs). SIL 1 is the lowest and SIL 4 is the highest level of safety integrity. Each SIL has a target failure measure. It is the SIL of the safety function(s) to be carried out by a safety-related system that determines the measures that need to be taken in the design of the safety-related system. Therefore, for:

- *Systematic Safety Integrity*: "Packages" of measures are used for different systematic failure mechanisms and these are in general qualitative measures with increasing rigour/assurance/confidence the higher the SIL.
- *Hardware Safety Integrity*: Quantitative modelling of the random hardware failure together with specified fault tolerance requirements graded against the SIL but with reduced fault tolerance requirements if certain diagnostic coverage levels have been achieved.

This concept is illustrated in Figure 4.

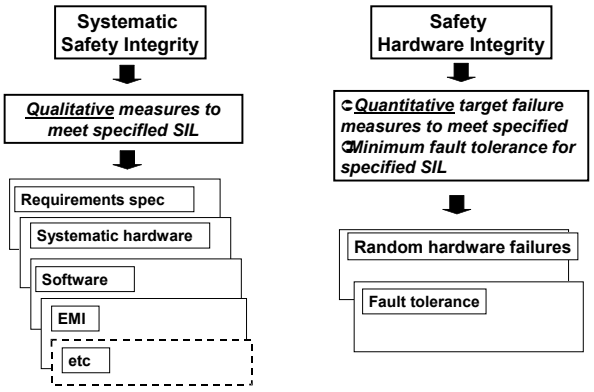

Figure 4: Achievement of safety integrity to meet specified SIL

The target failure measures for E/E/PE safety-related systems carrying safety functions of specified SILs are set out in Tables 1 and 2. It can be seen from Tables 2 and 3 that the SILs are linked to the target failure measures depending upon the mode of operation.

The mode of operation is an important concept and is the way in which a safety-related system is intended to be used, with respect to the frequency of demands made upon it, which may be either:

- **Low demand mode:** where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof-test frequency;
- **High demand or continuous mode:** where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof-check frequency

Safety functions operating in a:

- Low demand mode of operation would typically be implemented by a *protection system architecture (see Figure 5);*
- *High demand mode of operation* would typically be implemented by a *protection system architecture* or a *safety-related control system architecture (see Figure 5);*
- Continuous mode of operation would typically be implemented by a *safety-related control system architecture (see Figure 5).*

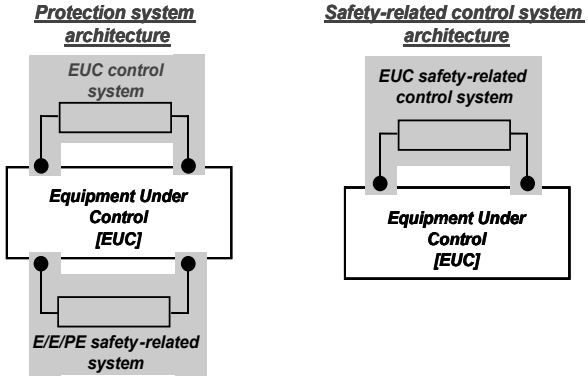

Figure 5: Safety-related system architectures

It should be noted that when determining the SIL, from a basis of knowing the target failure measure (which is established from the tolerable risk), the *demand rate* is relevant when the safety function is operating in a low demand mode of operation but not when the safety function is operating in a high demand or continuous mode of operation.

Table 1: Safety integrity levels: target failure measures for a safety function operating in a low demand mode of operation.

Safety integrity level	Low demand mode of operation (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

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

Safety integrity level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$

1	≥ 10^{-6} to < 10^{-5}

9 Risk Based Approach

The required safety integrity of the E/E/PE safety-related system, with respect to a specific safety function, must be of such a level as to ensure that:

- The failure frequency of the safety-related systems is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk, and/or
- The safety-related systems modify the consequences of failure to the extent required to meet the tolerable risk.

The failure frequency, with respect to a specific safety function, of the safety-related systems necessary to meet the tolerable risk (see (1) above) is determined taking into account any other risk reduction measures such as other safety-related systems and any legitimate managed risk reduction measures.

The determination of this failure frequency, with respect to a specified safety function, allows the target failure measure to be established and then the SIL to be established (from the linkage of SILs to target failure measures in Table 1 or Table 2).

The determination of the SIL for a specified safety function then allows the design process for the E/E/PE safety-related system to proceed (see Figure 4).

10 Revision of IEC 61508

IEC 61508 is currently being revised and it can be seen from the revision schedule in Table 3, that the first opportunity that National Committees will have to comment on Parts 1-4 will be in November 2005. The two IEC Maintenance Teams involved in the revision will then address the comments. Parts 1-4 will then be re-issued, together with Parts 5-7, for comment and voting in December 2006. The Final Draft for comment and voting will be issued to National Committees in January 2007 with a target date for publication of the revised standard of May 2008.

Prior to the revision process beginning in earnest, National Committees submitted their comments on the current standard. The National Committee comments are the key input to the revision process.

A key consideration during the revision process has been the need to ensure that any changes proposed added real value to standard and to balance any perceived benefits made to the standard against the economic costs to users' of the standard of implementing the changes. Increased costs of additional requirements in the standard would impact on all users but would have a significant impact on those organisations that have invested in the current standard.

The Maintenance Teams considered a very large number of issues including:

- ***Clarity of requirements:*** The need to make clearer the compliance requirements related to elements. The concept of "SIL capability" will be proposed to address the systematic aspects. It is hoped this will be of benefit to manufacturers of subsystems.
- ***Programmable devices such as ASICS*:** Proposals covering ASICS will be included in the Draft.
- ***Component Criticality*:** This concept, which relates to systematic issues, would allow the synthesis of two elements of, say, "SIL 1 capability" to be considered as an element of "SIL 2 capability" providing specific requirements for independence are met. A proposal on this concept will be in the Draft.
- ***Security*:** Currently the standard does not explicitly cover security considerations. The standard requires; "IEC 61508-1; 7.4.2.3: The hazards and hazardous events of the EUC and EUC* control system shall be determined under all reasonably foreseeable circumstances (including fault conditions and reasonably foreseeable misuse)". Whilst it could be argued that the words "…. under all reasonably foreseeable circumstances" are sufficient to cover security considerations, it is proposed to address this issue at the systems level and if necessary refer out to standards that have a specific remit to deal with security issues.
- ***Proven-in-use*:** The standard covers this concept but is being revised and further development is being considered.
- ***Digital communications:*** The current requirements in the standard will be clarified and further elaborated.

**Note: EUC =Equipment Under Control*

Table 3: Revision Schedule for IEC 61508

Milestone	Target date
Parts 1-4: Draft issued to National Committees for comment.	11/2005
Parts 1-7: Committee Draft issued to National Committees for comment and voting.	12/2006
Parts 1-7: Final Draft issued National Committees for comment and voting.	1/2008
Publication of the revised IEC61508	**5/2008**

11 References

Health and Safety Executive (1987). "Programmable electronic systems in safety-related applications": "1. An introductory guide", ISBN 011 8839062 "2. General technical guidelines", ISBN 011 8839063.

DIN (1990): DIN VDE 0801 “Principles for computers in safety-related systems” (“Grundsatze fur Rechner in System mit Sicherheitsaufgaben.

ISA (1996) “Application of safety instrumented systems for the process industries”. Published by ISA NC 27709, USA.

CCPS (1993) “Guidelines for Safe Automation of Chemical Processes”. Published by the Center for Chemical Process Safety of the American Institution of Chemical Engineers, New York NY 10017, USA.

Health and Safety Executive (1995): “Out of Control (why control systems go wrong and how to prevent failure)”. HSE Books 2003. ISBN 0 7176 2192 8. <www.hsebooks.co.uk>

12 Further information

- IEE Functional Safety Professional Network www.iee.org/pn/functionalsafety
- IEC Functional Safety Zone www.iec.ch/functionalsafety
- Functional and IEC 61508
- IEC 61508 Brochure
- FAQ’s on IEC 61508

Annex A
The Parts of IEC 61508

- IEC TR 61508-0: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508

- IEC 61508–1: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements

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

- IEC 61508-3:1998: Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 3: Software requirements.

- IEC 61508-4:1998: Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 4: Definitions and abbreviations

- IEC 61508-5:1998: Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels

- IEC 61508-6: Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 6: Guidelines on the application of parts 2 and 3

- IEC 61508-7: Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 7: Overview of techniques and measures

Annex B

IEC 61508 Safety Lifecycles

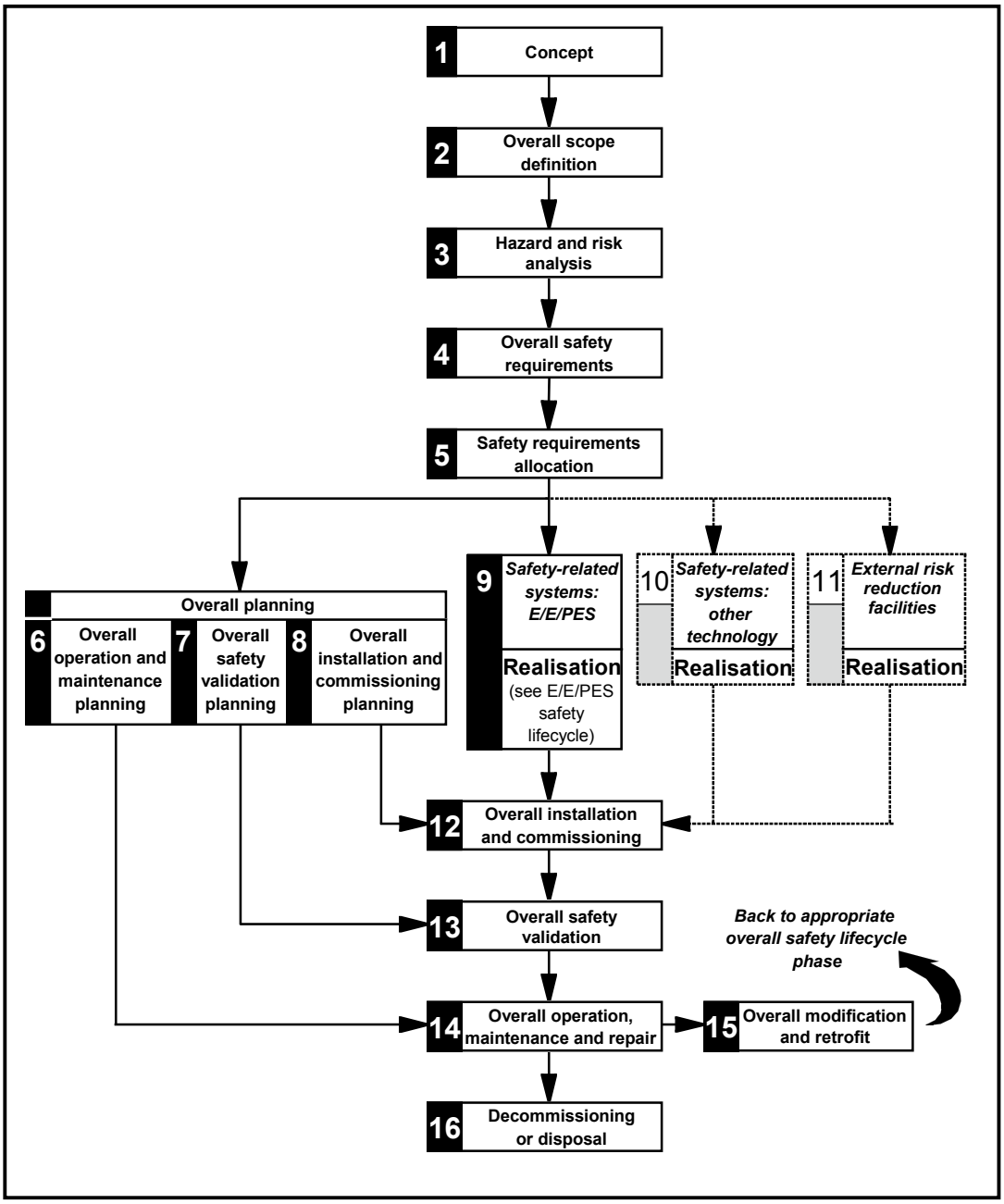

Figure B1: Overall Safety Lifecycle

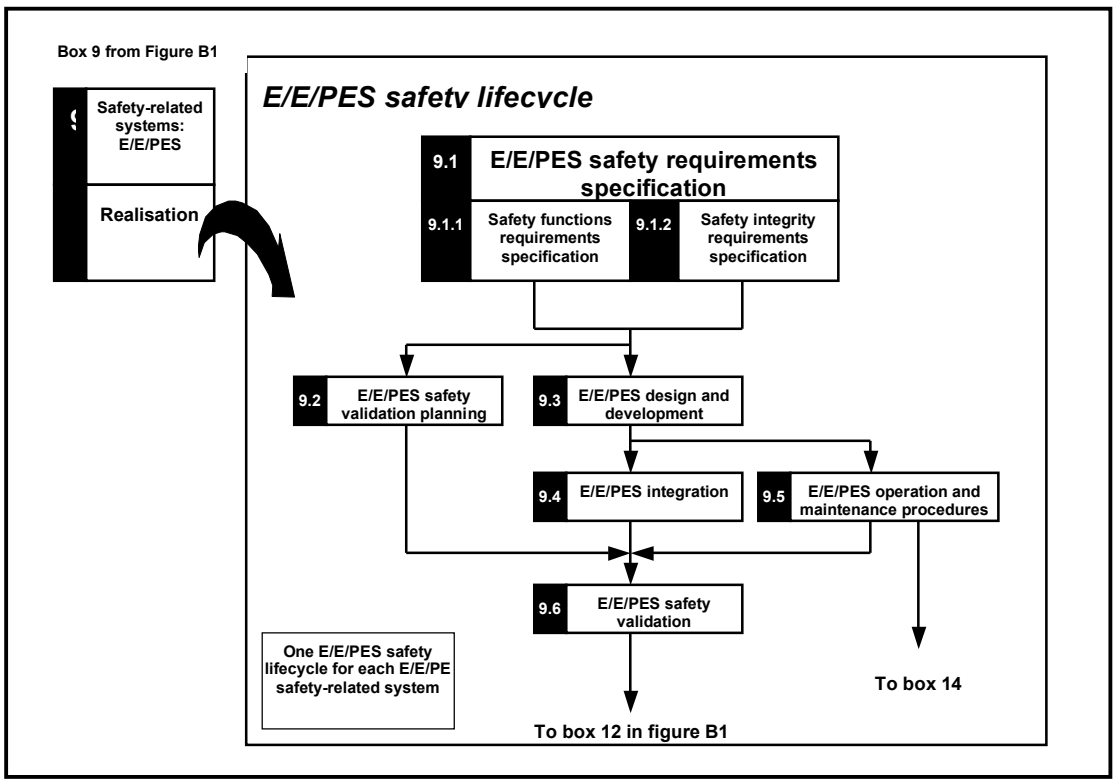

Figure B2: E/EPES Safety Lifecycle

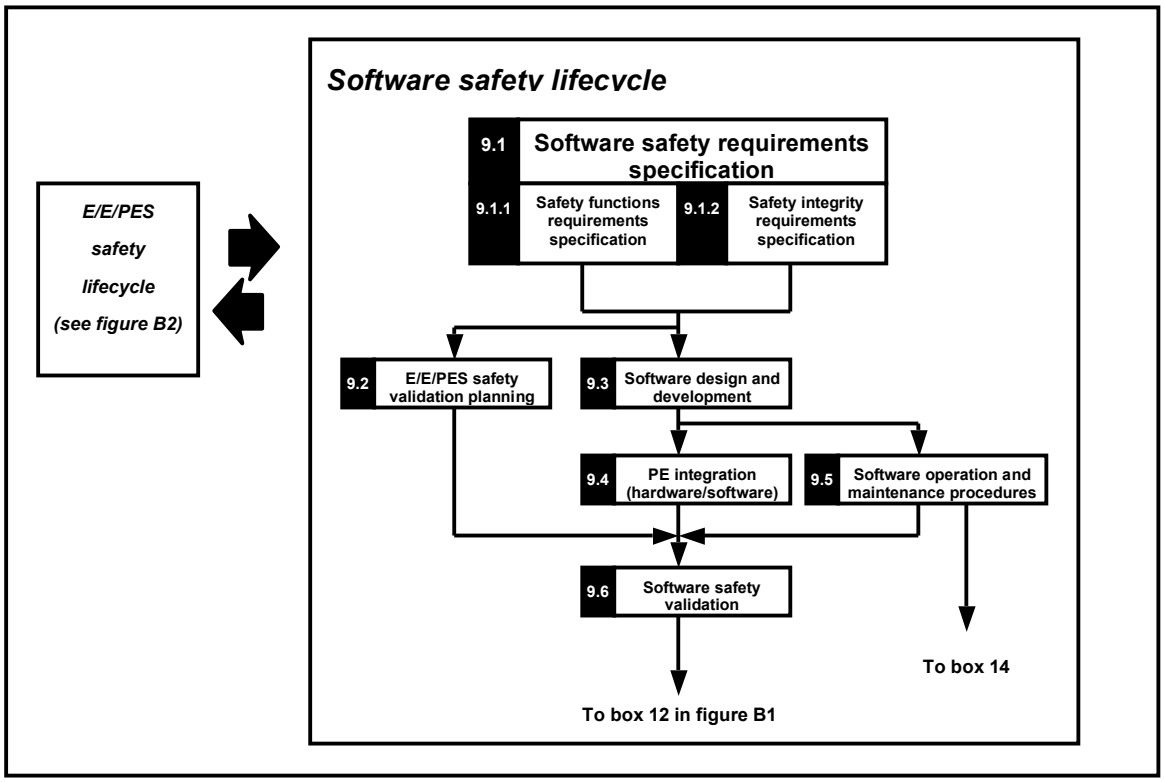

Figure B3: Software Safety Lifecycle