20 IEC/EN 61508

Throughout the world, there is a multitude of various committees which have dedicated themselves to the specification of norms and standards, namely in regards to the procedures used in the development, verification, and implementation of systems which are crucial for safety. In the implementation of critically important safety systems, provisions are made in order to maintain a standard for the operation of such installations: to certify a system through a supervising authority, according to the standards and guidelines that are relevant to its implementation.

The application of safety-oriented computer systems in various industrial sectors has lead to a wealth of experience and knowledge in this area. This knowledge is mostly present in compact form, as standards and guidelines, which are designed to assist the designing engineer in achieving a uniformly high standard of quality and safety in prospective systems. Depending on their exact purpose, safety-oriented systems must fulfill certain standards in order to determine developmental methods and system requirements. Certification of the final total process, including the safety system which regulates this process, depends on compliance with these standards, and with the criteria that they define. Nowhere else in industry is strict adherence to standards as strictly regulated as in the implementation of safety-oriented measurement and control[189]- and ESD[190]-technology.

Industry-specific standards and guidelines, such as in the chemical, petrochemical, airline, atomic, and mining industry, each describe the principal dangers inherent in these industries. The remaining risks, which ultimately go hand-in-hand with the demands on reliability and availability, are regulated and defined by the advisement of the supervising authorities and by the industry itself. Resulting from this are the safety requirement standards regarding systems of a specific sector of industry. General standards and guidelines, on the other hand, refer to all industry sectors.[191, 192]

The IEC[193] develops and administers standards in collaboration with national committees. In doing so, work groups are put in place which deal with a special subject at a time; for by example, the Technical Committee 65, which is responsible for „measuring and regulating in industrial processes“. This committee created the document „IEC 61508: Functional Safety: Safety related Systems” which is described in more detail below. The IEC 61508, also labelled basic safety standard, describes the fundamental, complete life cycle of safety-oriented systems. It is subdivided into seven parts, where parts 1, 2, 3, and 4 are

---

[189] MSR-Technik: Messungs-, Steuer- und Regelungstechnik
[190] ESD-Technik: Electronic-Shut-Down-Technik
[191] [HSE-87] HSE, *Programmable Electronic Systems in Safety-Related Applications*; *An Introductory Guide*. Health and Safety Executive. London: Her Majesty’s Stationery Office
[192] [IECa02] IEC 61508, *Functional Safety; Safety-Related Systems.*
[193] International Electrotechnical Commission

also known as basic safety standards and are referred to by technical committees during the creation of standards according to IEC guide 104, and ISO/IEC guide 51.

Aside from the IEC 61508, the next chapter also describes the IEC 61511. The group title of this standard is: „Functional safety: Safety Instrumented Systems for the process industry sector“ [194], in German: „Funktionale Sicherheit: Sicherheitstechnische Systeme für die Prozessindustrie“[195]. This international standard deals with the application of safety-instrumented systems in the process industry. It is the application of the IEC 61508 for process engineering and requires the execution of a hazard and risk analysis. According to this analysis, a specification of the safety-instrumented systems can be designed.

20.1 IEC/EN 61508-1

20.1.1 Outline and Field of Application

It is imperative for the owner of an installation to arrange for adequate safety management. If, in the event of an accident, the safety-oriented system does not conform to the standard, the firm could be held liable for neglecting proper safety guidelines. As such, a proper safety technology, which is in compliance with international standard, is required for all downstream servicing and for outside contractors. The IEC 61508 is an international standard which was issued by the International Electrotechnical Commission (IEC) 1999. It refers to all aspects that are connected to the use of E/E/PES (Electrical / Electronical / Programmable Electronic Systems) for safety-relevant functions and applications. They are fundamentally applicable to all safety-related E/E/PES, in particular during the absence of a special safety standard for an application area. The IEC 61508 standard comprises the following seven parts (61508-1 through 61508-7), see also Figure 20.1:

- Part 1: General requirements
- Part 2: Demands on safety-related electric/electronic/programmable electronic systems
- Part 3: Software requirements
- Part 4: Terms and abbreviations
- Part 5: Examples for determining the level of safety integrity
- Part 6: Application guideline for IEC 61508-2 and IEC 61508-3
- Part 7: Application instructions for procedures and methods

[194] [IEC-02] IEC 65A/324/FDIS 2002, *Functional safety: Safety Instrumented Systems for the process Indus try sector*

[195] [DIN-03] DIN IEC 61511, Teil 1 bis 3, (VDE 0810 Teil 1), *Funktionale Sicherheit: Sicherheitstechnische Systeme für die Prozessindustrie*

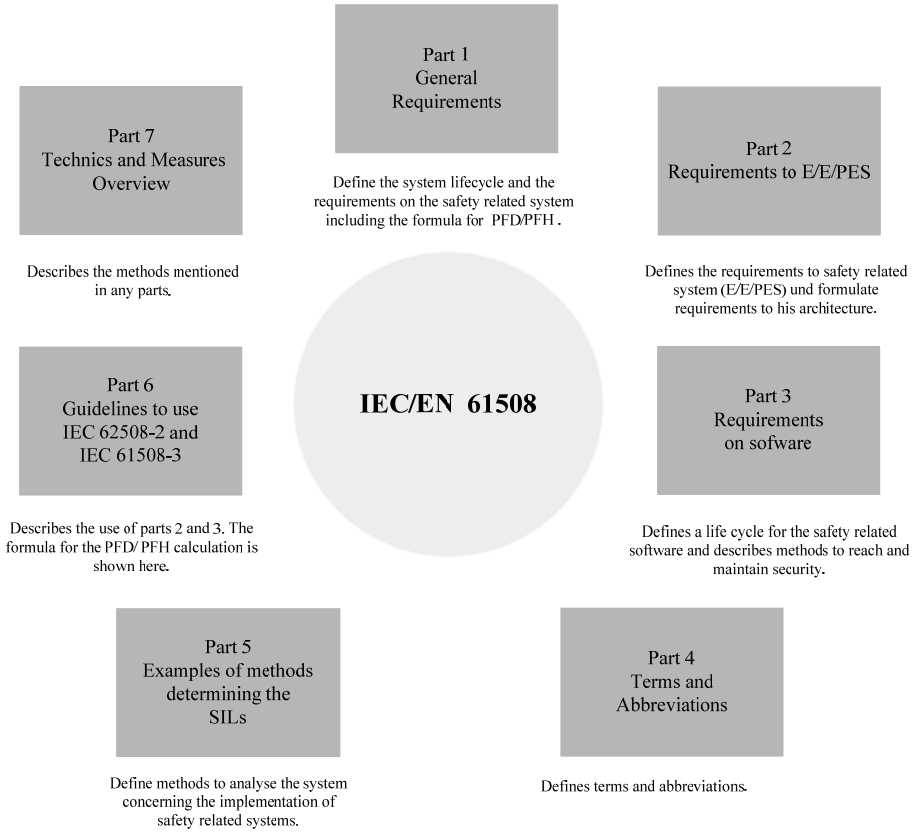

Figure 20.1: Outline of the parts of the IEC/EN 61508

This standard facilitates a systematic, risk-based approach to safety-relevant problems. Part 1 of this standard specifies the general requirements which are applicable to all other parts. Parts 2 and 3 define additional requirements of system hardware and software. Part 4 explains the definitions and abbreviations used in this standard. Part 5 provides guidelines for the application of part 1, and part 6 provides guidelines for the application of parts 2 and 3. Finally, part 7 contains an overview of procedures and methods.

This International Standard regards all relevant safety-related phases of the total concept of E/E/PES and of the software safety lifecycle, from the concept, through development, execution, implementation and maintenance until deactivation. It allows for the compilation of application-specific international standards, which are concerned with safety-related E/E/PES. Furthermore, it provides a method for developing the specifications of safety requirements, which is necessary in the achievement of stipulated functional safety for the safety-related E/E/PE system. It utilizes the safety integrity level for specifying the goal of the safety integrity of related functions. In order to determine the demands placed upon the safety integrity level, it applies a risk-based approach to the problem in which criteria for numeric failures are set.

The standard is universally valid and applicable to all safety-related systems.

Figure 20.2 shows the assignment of parts of the standard to the requirements with regards to the safety lifecycle. The requirements differentiate between technical and other requirements (for example, documentation and management of functional safety).

20.1.2 Compliance with this Standard

In order to achieve compliance with this standard, it must be proven that the requirements are fulfilled and of accord with the specified criteria. Excempt are systems of low complexity, for which reliable field experience is at hand. Their requirements were, and are, integrated into the safety standards of various application fields.

CD: IEC 62061	Machine safety
CDV: IEC 61511	Safety-instrumented systems for the process industry
EN 50126	Rail industry applications: Specification and proof of safety
EN 50128	Software for rail guidance and supervision systems
EN 50129	Safety-relevant electronic systems for signal technology
pr EN 50156	Electrical equipment of furnace devices

The IEC/EN 61508 is applicable both as a stand-alone standard, as well as a basic standard.

20.1.3 Documentation

The entire documentation must contain sufficient information to make it possible for all phases of the safety lifecycle- as well as all occurring design and verification tasks. safety management, and safety inspection- to be executed efficiently. Documentation should be accurate and concise, making it easy to understand. Furthermore, it must be accessible and serviceable at all times. The individual segments of this standard specify exactly which information has to be documented.

20.1.4 Safety Management

Persons or organizations responsible for individual phases, or for the entire lifecycle, must specify all technical and management activities. These ensure that the E/E/PES will achieve and maintain the required functional safety. Among these activities are, most notably, the organization of the internal information flow, the strategy for achieving functional safety, and the qualifications of the personnel involved. It is mandatory to create a plan that includes all of the aforementioned activities in order to achieve safety.

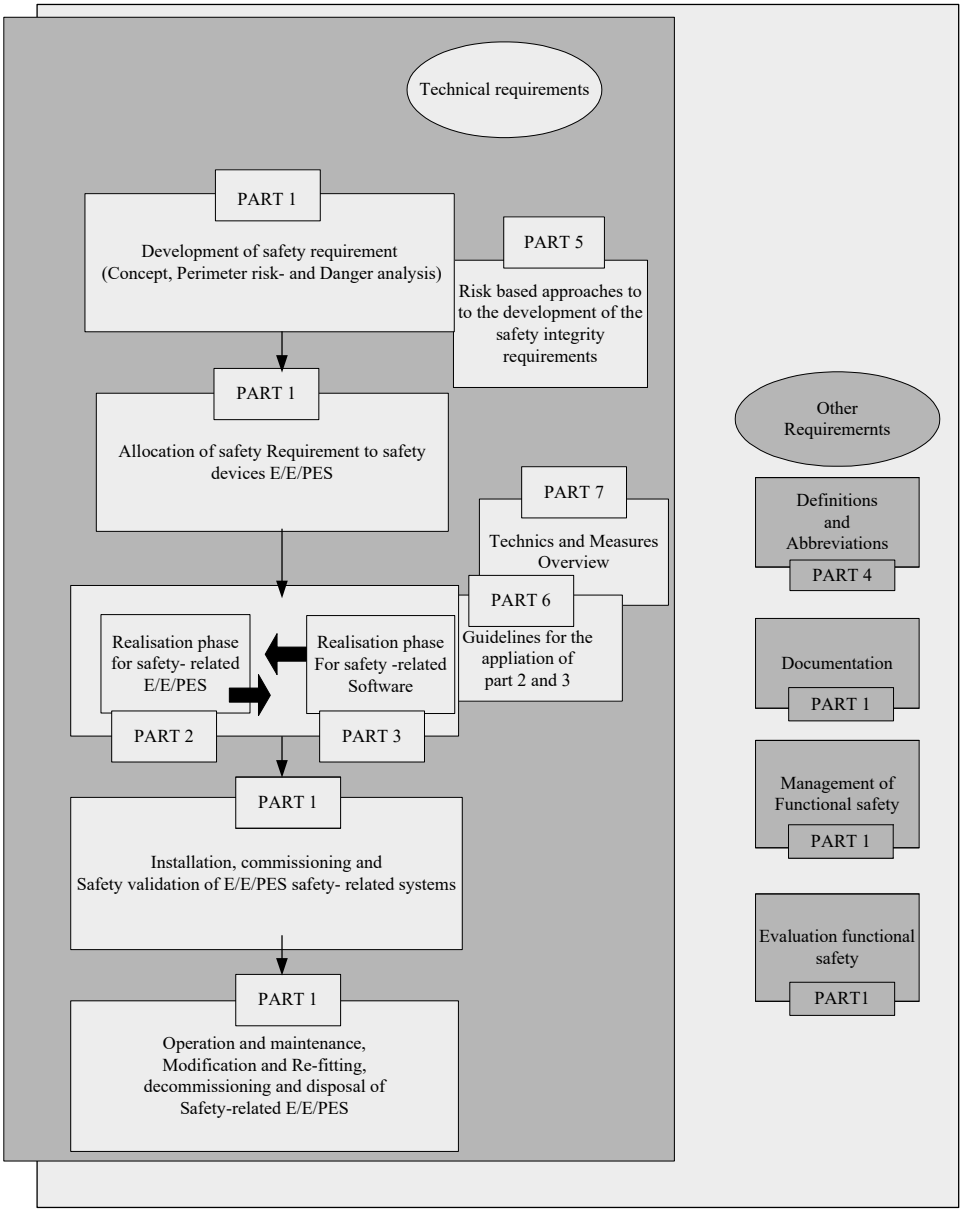

Figure 20.2: Complete structure of the IEC/EN 61508

20.1.5 The Complete Safety Lifecycle

The following safety lifecycle (see Figure 20.3) is defined in order to achieve a systematic approach to the problems of functional safety. Upon application of the safety lifecycle, the safety integrity level (SIL) is achieved.

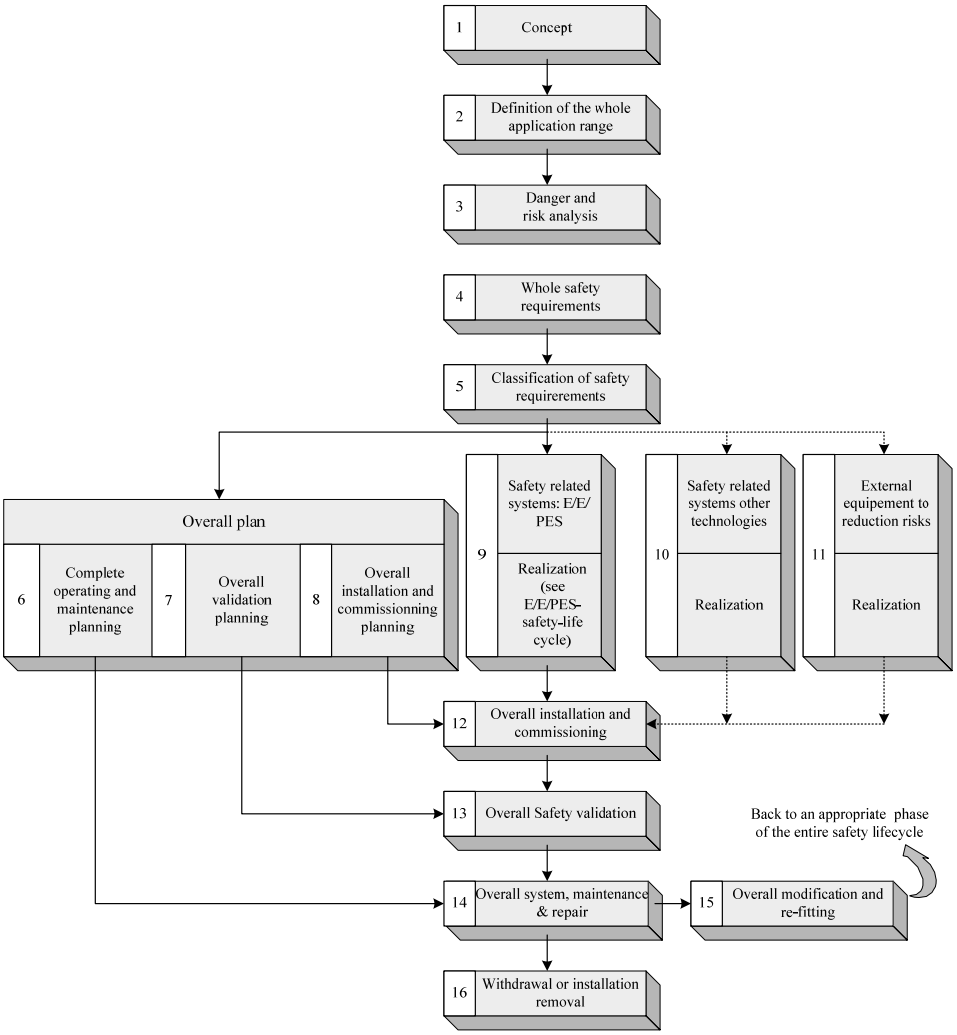

Figure 20.3: Entire safety lifecycle

The safety lifecycle contains 3 methods to minimize risk: phases 9, 10, and 11. In the following segment, the individual phases from Figure 20.3 are illustrated in more detail.

In the *concept* phase, a sufficient understanding of the EUC installation (plant, machine, etc.) and its environment must be achieved. This phase also includes observations regarding probable safety hazards and legal provisions. In the following phase, the *entire appli-*