A Survey on the Development and Design Strategies for Safety Related Systems according the Standard IEC/EN 61508

BÖRCSÖK J. SCHWARZ M.H.
Computer Architecture and System Programming
University of Kassel
Wilhelmshöher Allee 73, 34121 Kassel
GERMANY

HIMA Paul Hildebrandt GmbH + Co KG
Albert-Bassermann-Str. 28, 68782 Brühl
GERMANY

*Abstrac*t: - This paper gives a detailed summary on the international safety standard IEC/EN 61508. It describes the requirements for the design of safety related systems and the request to control faults during operations as demanded by the international standard. It describes different aspects for the development of safety hardware systems, which has to be incorporate into the design, to get the system not only certified by an independent organisation, but also to make it safe. The authors discuss different measurements to be taken, to avoid faults and to control faults when the hardware or a component is getting faulty.

Keyword: IEC/EN61508, Safety, Reliability, Safety Integrity Level, Hardware Safety Lifecycle

1 Introduction

Our civilisation is based on a modern industry. Within a modern industrial society, automation technology is a key aspect for success. Industrial processing plants and manufacturing companies relay on automation technology. As a result, the market for industrial automation technology is one of the strongest growing markets [1,2,7].

For a long time a very unadventurous industry, namely safe automation technology, has been changed over the last two decades towards fully electronic control and automation systems [1,2,3].

The processing and manufacturing industries are put under considerable pressure by many, quickly changing requirements. In the last 10 years, the safe automation technology has tremendously improved and changed. Due to the rapid improvements in microelectronics, new opportunities are provided in this area.

Additionally, society requests new requirements for safe products and manufacturing procedures [1,2,4]. Ecological regulations and guiding principles for production security (product liability, machine guideline, safety guideline e.g. IEC61508) are important examples of it.

The globalisation directs industries to an increasingly hard competition. Additionally, economic success of industrial companies is getting more important, which leads into an increase of the plant safety and to produce more efficiently. These circumstances affect significantly the entire automation technology ,81,2].

Furthermore, the global distribution of production plants requires that standardised products are manufactured with equivalent quality and consistent safety standards, independent of the production location.

Following these objectives, then an increased automation level leads automatically to a high modernisation pressure on the technology.

If 100 years ago a mechanical governor was sufficient to perform controlling tasks, nearly all components of a modern production plant have nowadays sophisticated automation equipment; which can be overloaded, coordinated and optimised functions.

Sensors, actors and bus networks should be considered within this scenario as well. Safe automation means to collect information, to process it and, according to the results, to influence the process in such that it performs the intended tasks while ensuring a maximum of safety

The more precise and effective, efficient and accessible, flexible and safer production plants and flows have to be, the more information about the plant state is necessary. As a result, an expanding number of measuring and monitoring points is essential for processing data. This larger amount of information quantity would usually restrict the capacity of I/O units. An I/O unit contains generally hundreds to tens of

thousands I/O ports. The number of required processing I/O ports alone, would go beyond the scope of the geometrical requirements.
Due to these requirements, the manufacturer of safety-related automation systems has to develop innovative approaches which take the requirements demanded by the operators into consideration.
Ancillary conditions to such automation systems are easily operability, simple handling, high reliability and safety for the controlling process.
The requirements for safety-related automation system are as essential as the normative requirements and those given by regulations. These last consider not only the hardware, but the operating system, programming languages for processing applications and diagnostic devices. The overall life cycle of such a system is therefore taken into consideration [1,2,4,6].

2 Application Area

Safety related systems have to be developed, tested, used and maintained according national and internationals standards. The standard IEC/EN 61508 [3,4,6] includes all aspects of :

- Electrical
- Electronical and
- Programmable electronical Systems

for safety related function and usability. This standard provides the basis of all safety related electrical, electronical and programmable electronical systems. The standard enables a systematic and risk based methodology for safety related problems.

3 Failure Rates

For the validation of safety related systems, the failure rate λ has to be determined. The failure rate λ, has the unit ‘ number of failure per hour’ and states the amount failure occurred per hour. Principally, two different types of failure have to be distinguished: safe failures (λ_S) and dangerous failures (λ_D). Safe failures, either undetected (λ_{SU}) or detected (λ_{SD}), both have no influences on the safety function of the system [1, 2].
A dangerous failure results, if it occurs, into a dangerous situation or state of system, and has to be considered when calculating the failure probability. Two different types of dangerous failure exist, dangerous detectable failure and dangerous undetected failure. Figure 1 sketches the four different types of failure which can occur in a system.

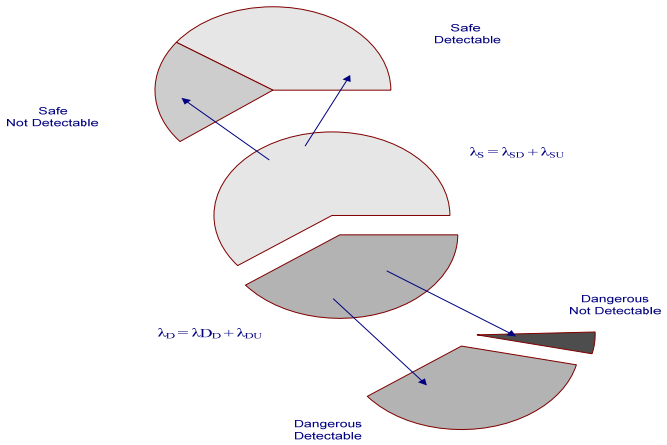

Fig.1 Failure rate distribution

4 Standard IEC/EN 61508

The standard IEC/EN 61508 is detailed in seven chapters, but only the first four present normative requirements for the development. Each chapter and its content are listed in the table below and presented in Figure 2.

Chapter	Content
IEC/EN 61508-1	General requirements
IEC/EN 61508-2	Hardware requirements
IEC/EN 61508-3	Software requirements
IEC/EN 61508-4	Notation and abbreviations
IEC/EN 61508-5	Examples to calculate the different safety integrity levels (SIL)
IEC/EN 61508-6	Application guidelines for IEC/EN 61508-2 and IEC/EN 61508-3
IEC/EN 61508-7	Overview of techniques and actions

Table 1: IEC/EN61508

To eliminate failure efficiently, a structured design, development and maintenance are essential. It should be the aim to either avoid or reduce failures straight from the beginning [4,6].

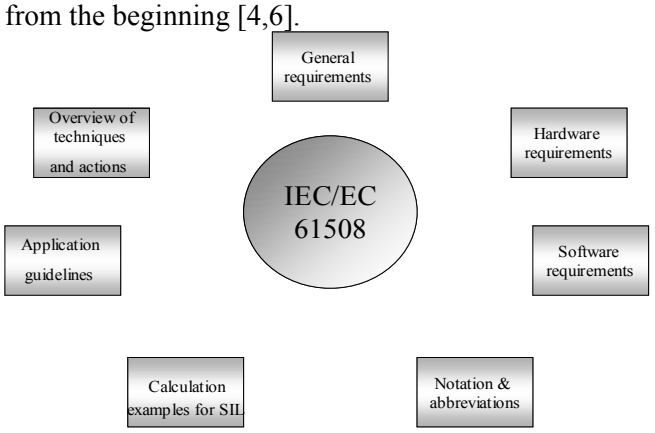

Figure 2: Overview of the different chapters of IEC/EN 61508

Such a strategy is based on the constructive, analytical and testing procedures during the safety lifecycle of product. The standard IEC/EN 61508 describes the required demands of each phase of the lifecycle. Chapter 2 and 3 of the standard details the phases to develop electrical, electronical and programmable electronical systems. Each development phase of a complex safety system is allocated to procedures or methods to minimise or eliminate failures. The procedures and methods are presented in the appendix A and B of parts 2 and 3 of the standard, and are judged according their efficiency and detailed in part 7. The essential idea is that the safety lifecycle is considered in parallel to the development. Organisations, which are certifying products according standards, like the national institute TÜV (Technischer Überwachungs Verein), are using this concept to verify if the safety requirements are fulfilled. A certification usually starts with the accompanying inspection of the requirement specification during the development phase. The quality inspection is carried out during the development, during operation and maintenance and modification of the system.

5 Consistent implementation of the IEC /EN 61508 standard for safety related operations during the whole lifecycle.

The IEC/EN 61508 describes and details the requirements of complex safety systems, using E/EPES systems (electrical, electronic and programmable-electronic Systems).The objective of this standard is to:

- Avoid hazards in systems/equipment of the process industries caused by faulty functioning of the safety system
- Guarantee to be consistent to the international safety standard
- Maintaining the required safety standard for the entire lifecycle.

The careful examination and inspection allows a systematic approach to the problematic of functional safety.
This approach can be classified into tree parts:

- Determine the safety demands
- Develop and implement the system
- Initiation, safety validation, operation, maintenance

Figure 3 gives an overview of the different phases, which will be now detailed. In the conceptual phase, a deep understanding of the equipment under control is necessary as well as the understanding of the process environment. Additionally, an understanding of potential causes [5,9] of risks and legal regulations are essential. In the subsequent phase the entire application area, including the boundaries and possible external hazards have to be defined. Afterwards, the vulnerability analysis and the risk examination are carried out, which are described in the next phase. All predictable hazards, cases and potential dangerous events have to be considered. Additionally, the probability and potential consequences of these dangerous events and cases have to be estimated.
Afterwards, the safety requirements as well as the allocation of the safety demands have to be stated.
Generally, safety functions and their safety integrity are specified to achieve the necessary functional safety. Additionally, the risk reduction due to external systems has to be indicated. If those phases are completed, then the safety related system could be chosen to achieve the necessary functional safety. Additionally, it has to be identified which safety integrity level (SIL) each safety function has to be possess or achieve. The IEC/EN 61508 standard does not only observe the conceptual and design phase but also defines the considerations and inspection during operation.
Within this section, the phases of the entire operation and the maintenance are described. This phase should, if possible, include the standard procedures for maintenance of the safety function. Additionally, it has to be guaranteed that the safety function is still functional during maintenance. As shown in Figure 3, number 13, a complete validation of the safety has to be carried out.

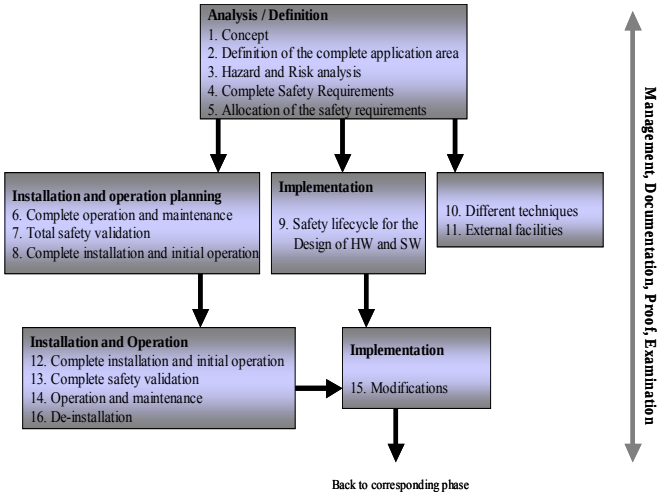

Figure 3: Implementation of the safety relevant techniques for the entire lifecycle according the standard IEC/EN61508.

A plan for the validation procedures for the system is going to be put into operation, where all different operating states have to be considered. Another phase is the entire preparation for the complete installation and initial operation. The organisation and preparation have to consider an observable and controllable installation

and initial operation. Important issues are the time scheduling, the responsibilities and the approach for the installation. Criteria have to be defined when the installation of the equipment or system is completed.
Probably, the most important subject is the implementation of the equipment or system. Within this phase, the actual plan of the safety related system has to be developed and implemented. Within this phase part 2 and part 3 of the standard is of great importance, which are concerned with the development of the hardware and software.
After the conceptual and implementation phase is completed, the installation, initial operation and validation phase of the whole system has to be carried out, according to the defined master-plan. Additionally, the standard defines the approaches for modifications and retrofitting of improved components. It has to be guaranteed that the functional safety is functional during and after modifications. It is important that each step, necessary for the modifications, are precisely planned and all consequences are considered. The de-installation is also considered in the standard. The functional safety of other components and systems has to be evaluated interacting or communicating with the shut down or removed components. Only after the complete analysis, a shutdown and remove can be authorised and carried out.

6 System Evaluation according the standard IEC/EN 61508

Safety related systems, developed according the standard IEC/EN 61508, have to fulfil the requirements of the maximum value of tolerable probability of failure of the safety function, to be suitable for the specified application. That is the reason why a specified development process and methodology are necessary, where each step of the development is documented, calculations are reproducible, system features are testable and observable.
A suitable method or model for development is the V-model, which was developed in the late 1980's from the federal department of defence in Germany. Figure 4 shows the concept of the V-model. Characteristic for this method is that the development is accompanied by documentation procedures and management, which is appropriate for functional safety requirements.
Verification and validation are important issues, occupy a major part during the development of safety critical systems, and are based on test procedures. One part is the preparation of the module and system integration tests. The actual validation of the complete system is normally done in the final phase of the development of the system.

The validation planning should start within a very early development phase. The classic V-model owns a secondary information path from the early development phase to a later one. In Figure 4 it is shown that for every phase on the left hand side an equivalent on the right hand side exist, which is a test plan that states how the tests have to be implemented and verified. Every level of the test plan identifies characteristics, which have to be examined in order to obtain useful, meaningful and sufficient tests. The latter one, depends on the safety integrity level of the application area of test object. Generally, before a system or equipment is going to be implemented, the validation including all safety factors, which may influence the safety of the system, have to be evaluated.

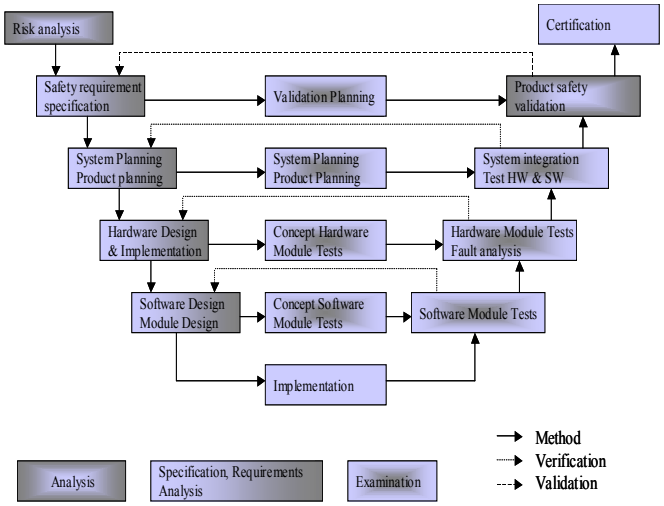

Figure 4: V-Model

7 Safety Integrity Level Requirements

In the standard IEC/EN 61508, the requirements of the safety related systems and equipment are divided into four safety integrity levels (SIL 1 to 4). Equipment, sensors, units or systems, which are part of a safety function, have to have a safety classification. Additionally, a new quality and recognition is required and added to the perception of safety. For example, in Germany, only a qualitative consideration is necessary, while the international standard demands a numerical measure for process industries. Additionally, the numerical minimum requirements of the probability of failure are based on the PLT/PLC safety units depending of the safety system.
To evaluate the safety functions of a system, three different values are of great importance:

- Hardware Fault Tolerance (HFT)
- Probability of Failure on Demand (PFD)
- Safe Failure Fraction (SFF)

The safety integrity level is one of the four discrete cascaded levels. Each safety level corresponds to a probability of failure. SIL-4 (Safety Integrity Level 4) complies with the highest safety level and SIL-1 is the lowest.

SIL	Low demand mode of operation (Average probability of failure to perform its design function on demand)	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Table 2: Definition of Safety Integrity Level According to IEC 61508

Table 2 shows the different requirements of the altered safety integrity levels (SIL) in dependence to the probability of failure. The probability values are defined as a PFD-value (probability of failure on demand), if the system is in a low demand mode and has to execute a safety function. However, if a system is operating in a high demand mode or continuous mode and a safety function has to be executed, then the probability of failure is specified with the PFH value (probability of failure per hour). Its dimension or unit is (1/h).

7.1 Operation in low demand mode

The requested rate of the safety related system is not more than one execution per year and is not larger as twice the frequency of the poof test interval T_1.
For a safety related electrical, electronic and programmable electronic system, operating in low demand mode, the lower bound of the averaged probability, that the requested safety function fails to be executed is 10^{-5}

Example:

$$T_1 = 10\ years \tag{1}$$

The requested rate amounts:

$$\frac{2}{10\,years} = \frac{1}{5\,years} \tag{2}$$

Consequently, the safety function will be requested once every 5 years.

7.2 Operation in high demand mode or continuous mode

The requested rate for a safety related system is larger than once per year or is larger as twice the frequency of the poof test interval T_1
For a safety related electrical, electronic and programmable electronic systems, operating in high demand or continuous mode, the lower bound of the averaged probability, that the requested safety function fails to be execute is 10^{-9}
Example:

$$T_1 = 6\ months \tag{3}$$

The requested rate amounts to:

$$\frac{2}{6\,months} = \frac{1}{3\,months} = \frac{4}{1\,year} \tag{4}$$

Consequently, the safety function will be requested on average once every three months or once every quarter of a year.

8 Hardware Safety Lifecycle

Figure 5 shows how to apply the hardware safety lifecycle according the standard IEC/EN61508. It consists of six different implementation phases, where different operations have to de completed. During phase 1, the specification of the safety requirements for electrical, electronic and programmable electronic systems have to be established. The necessary safety functions and the required safety integrity level have to be determined to provide the requested functional safety. The second phase consists of the planning phase for the validation of the E/E/PE- systems regarding safety. The concept and layout of safety related E/E/PE- systems are accomplished in phase 3, in consideration with requirements of the safety function and safety integrity level. Within phase 4, the integration of the designed safety related E/E/PE-components into the overall safety system is completed. It has to be proven with tests that safety related E/E/PE-system corresponds totally with the concept and layout of safety related E/E/PE- system. Phase 5 ensures that methods and techniques are developed to keep the functional safety functioning during operation and maintenance. Phase 6 is the validation stage for the safety related E/E/PE- system according the requested safety function and safety integrity. Those phases without phase 1, which is the specification of the safety requirements, are accomplished within the development departments.

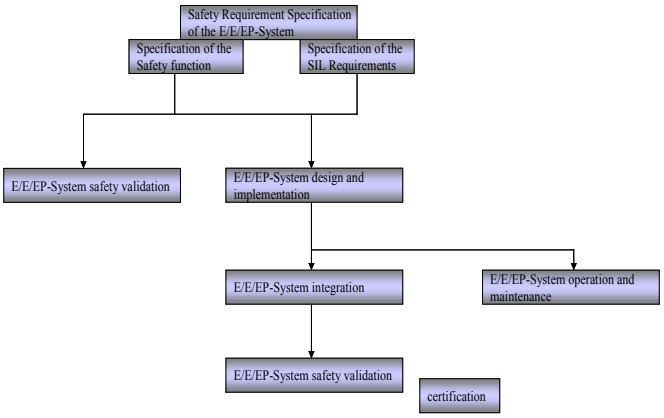

Fig 5: Hardware Safety Lifecycle

9 Conclusion and Summary

The paper gave an overview of the requirements for the development and design of safety hardware systems according to international standards and finally to get the system verified by an independent test organisation such as TÜV.

It presented fundamental considerations of functional safety and described concepts for the development and design of safety systems operating in process or automation industries with a low or high demand on safety.

The paper detailed how to avoid faults from the beginning but also how to deal with faults if a hardware component if getting faulty according to standard IEC/EN61508.

References:

[1] Börcsök, J. (2004)a *Elektronische Sicherheits-systeme*, Hüthig publishing company

[2] Börcsök, J. (2004)b *Elektronic Safety Systems*, Hüthig publishing company

[3] Börcsök, J. (2002) *International and EU Standard 61508,* Presentation within the VD Conference of HIMA GmbH + CO KG

[4] Börcsök, J. (2000/2001) *Functional Safety Computer Architecture Part 1 and Part 2*, Internal report

[5] Goble, W. M. *Safety of programmable electronic systems – Critical Issues, Diagnostic and Common Cause Strength* Proceedings of the IchemE Symposium, Rugby, U.K. Institution of Chemical Engineers, 1995

[6] IEC/EN *61508: International Standard 61508 Functional safety: Safety-related System*. Geneva, International Electrotechnical Commission

[7] Lewis E. E. *Introduction to reliability engineering*, 2nd ed.New York, John Wiley, 1996

[8] Storey N. *Safety critical computer systems*, Addison Wesley, 1996

[9] Velten-Philipp W., Houtermans M. J. M. *The effect of diagnostic and periodic testing on the reliability of safety systems* TÜV, Köln, 2006