Информационна сигурност

SAFETY-RELATED SYSTEMS ACCORDING TO IEC 61508

MARK DIETZ[1]
[1] UNIVERSITY OF LIBRARY STUDIES AND INFORMATION TECHNOLOGIES
CORRESPONDING AUTHOR: MARK-DIETZ@GMX.NET

Abstract: *This paper presents the structure of a safety instrumented system, the Safety integrity level (SIL) considerations and the reference to IEC 61058.*

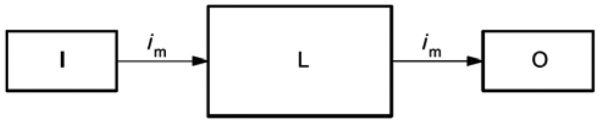
Key words: *Safety-related system, SIL, IEC 61508, Safe Failure Fraction, Probability of a Dangerous Failure per Hour.*

INTRODUCTION

The influence of functional safety is steadily increasing in many areas. What was implemented mechanically some time ago is now being mapped electrically/electronically with programmable electronic systems (PES). Proven knowledge about this is now available in compact form in the form of standards and guidelines. This helps developers to achieve a uniformly high level of quality and safety for new systems being developed. However, not only the development, but also the operation of a safety-related system, requires certification in accordance with the relevant standards and guidelines.

GENERAL REQUIREMENTS

Safety-related systems differ from "normal" programmable systems by their defined shutdown behavior in the event of a fault and are described by a processing chain with "sensors-logic-actuators".



Key
im = interconnecting means
I = input device (sensor)
L = logic
O = output device (main contactor)

Fig. 1 **one-channel architecture [1]**

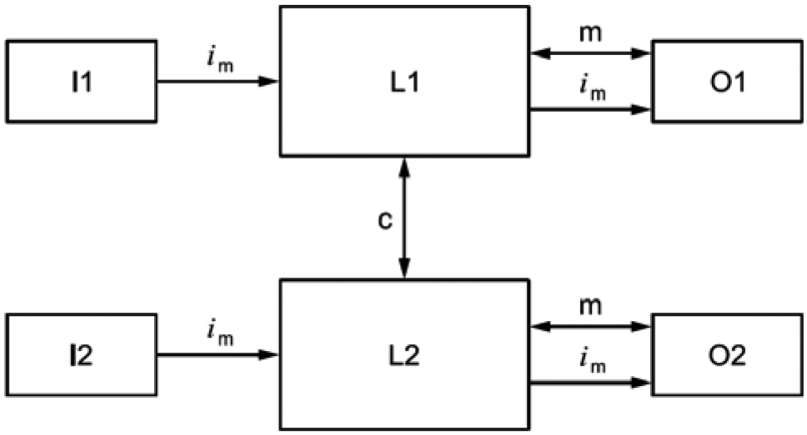
Availability can be increased through a modular design and the use of redundant modules. Together with the application software, well-structured and easy-to-understand control systems can be implemented for plants or plant sections with potential hazards.

Safety standards such as IEC 61508 place requirements on a systematic approach to the development of safety-related E/E/PE systems in order to minimize outgoing hazards and risks to a tolerable residual risk. Consequently, dangerous system malfunctions must be avoided or at least controlled. These failures can be caused, for example, by systematic errors (human error such as specification errors, design errors, implementation errors and installation/operating errors) or by random hardware errors (limited reliability of hardware components). The goal of functional safety is thus the development of measures and their technical implementation to avert or prevent hazards [2, 5].

Failures and errors must be detected safely. Safe means that the system (assembly) must assume a safe state in the event of a fault without endangering the environment in any way. Sensor components and safety-oriented control systems (safety PLC systems) are required to meet this requirement. Thus, a "simple" sensor must become a sensor with more information content or even more intrinsic intelligence [3, 34].

However, if an error or even an accident occurs, compliance with the standards is used in the development of the system. If the standards were violated or not observed, there is a risk of severe civil and criminal penalties. Certification to functional safety standards does not exempt a product from liability, but it does mitigate the claims that arise in the event of a system failure [2, 6].

Safety systems can be single-channel, dual-channel, or multi-channel. While single-channel systems react to errors with a failure, two-channel or multi-channel systems can check each other and detect errors.



Key
Im = interconnecting means
c = cross monitoring
I1, I2 = input device (sensor)
L1, L2 = logic
m = monitoring
O1, O2 = output device (main contactor)

***Fig. 2* two-channel architecture [1]**

The measurand for the architecture is the HFT value (hardware fault tolerance) and means how many dangerous faults are possible due to the architecture without endangering the safety function. If the HFT value is 0, there is no hardware fault tolerance, and any fault can lead to failure of the component. If, on the other hand, a two-channel architecture exists, this architecture has an HFT value of 1, since a subsystem can fail in the event of a fault without the safety function being endangered. In addition, there are systems with an HFT value of 2. With this structure, two subsystems can fail in each case and the safety function continues to be executed safely [4, 236].

In order to be able to determine the characteristics of the probability of failure, IEC 61508 also requires an assessment of whether the components used are "Type A" or "Type B". Type A components exist if the failure behavior of all components used is sufficiently known (for example through field experience) and can be determined under fault conditions. This would be, for example, simple systems such as pressure switches. "Type B" components exist when the failure behavior of at least one of the components used is not fully known or determinable. A complex component would be, for example, processors [5, 54].

Safety integrity level SIL	Minimum hardware fault tolerance
1	0
2	1
3	2
4	no specific requirements apply

Table 1. Minimum hardware fault tolerance of sensors, actuators and logic systems

Another parameter is the safe failure fraction (SFF). The SFF is defined as the ratio of the addition of the safe and the dangerous but detectable failure rates and the total failure rate of a unit. The IEC 61508-2 refer to the architectural limitations of the HFT and the SFF depending on the components used (type A and type B) in relation to the achievable SIL [5, 54].

Safety failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Table 2. Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem

Safety failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	Not Allowed	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Table 3. Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

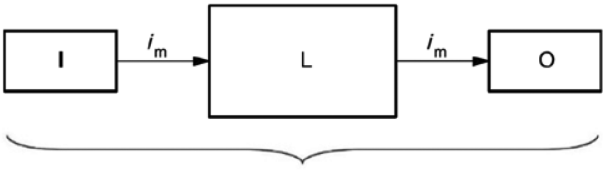
The failure limits for random hazardous failures of the hardware are determined for each safety function using the specified safety integrity levels in ICE 61508-1, Tables 3 [7, 58]. The failure rates thus determined concern the hardware components used by the safety function.

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Table 4. Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

The PFH value indicates the average probability of a dangerous failure per hour and is a specification for the realization of the electronics. Hardware architecture and measures for fault prevention or diagnostics must ensure compliance with the failure limits [8, 63].

The failure limit value (PFH value) of the safety function must be divided among the hardware components involved in the safety function. If a component is involved in several safety functions, then the lowest assigned failure limit value applies to this component.



Hardware:
PFH (total) = PFH (I) + PFH (L) + PFH (O)

Fig. 3 Assignment of the failure limit value [7]

As shown, the safety PLC (Programmable Logic Controller) forms the digital brain of the system, so to speak, and takes over the detection via the sensors and the triggering via the actuators. The most important difference between a fail-safe PLC and a standard PLC is that this safety PLC is internally redundant and diversified. This is achieved, among other things, by means of two different processor types that monitor each other and assume a safe state for the system in the event of a detected fault.

In addition, the software portion for the execution and monitoring function must also be directly assigned to the required Safety Integrity Level (SIL). This means that the software must also be developed in accordance with the requirements of the assigned SIL. In general, IEC 61508-3 requires [9, 23] that an application program must also be tested, verified, and validated, as must the associated hardware [8, 64].

CONCLUSION

In summary, it can be derived that a central role for a safety consideration is the so-called Safety Integrity Level (SIL) according to IEC 61508. This safety integrity level is a measure of the quality of the safety functions. The higher the risk posed by a machine, the higher the requirements for the reliability of its safety functions. SIL represents a classification scheme for complete safety systems consisting of sensor, controller and actuator. IEC 61508 specifies four different safety levels (SIL 1 to SIL 4), with SIL 4 placing the highest demands on safety. The requirements of SIL 4 are so high that this level is not even relevant for the safety of machines or vehicles; only SIL 1, 2 and 3 occur here. Which SIL level is re-

quired in each case must be determined on the basis of risk assessments.

REFERENCES

1. ISO 13849-1. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design, International electrotechnical commission, 2015.
2. Ulrike Weinrich. Methods for determining the failure rates of electrical and electronic systems using the example of steering electronics, Wiesbaden, Springer, 2019.
3. Roland Werthschützky. Sensor Technologies 2022, Berlin, AMA Association for Sensor and Measuring Technology e.V., 2018.
4. Alfred Neudörfer. Designing safety-compliant products. Methods and systematic collections of solutions for the EC Machinery Directive., Berlin, Heidelberg, Springer, 2016.
5. Josef Börcsök. Functional safety, basic features of safety-related systems, Vol 4, Berlin, VDE VERLAG, 2015.
6. IEC 61508-2. Functional safety of electrical/ electronic/ programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety related systems, International electrotechnical commission, 2010.
7. IEC 61508-1. Functional safety of electrical/ electronic/ programmable electronic safety-related systems – Part 1: General requirements, International electrotechnical commission, 2010.
8. Peter Löw, Roland Pabst, Erwin Petry. Functional safety in practice, application of DIN EN 61508 and ISO/DIS 26262 in the development of series products, Heidelberg, dpunkt, 2010.
9. IEC 61508-3. Functional safety of electrical/ electronic/ programmable electronic safety-related systems – Part 3: Software requirements, International electrotechnical commission, 2010.