



Safety standard IEC 61508

Consequences for automation technology and implementation at HIMA

The authors:

Uwe Jüly
Hans-Leo Ross

The origin of safety standards

The development phase is over and implementation is underway. In August 2002, safety standard IEC 61508 was published and came into force throughout Europe as EN 61508. National implementation is currently underway in other parts of the world, for example in Australia (AS 61508), Great Britain (BS IEC 61508) and Germany (DIN EN 61508 (VDE 0803)). This basic specification, which is the first to define comprehensive safety requirements for automation technology, will form the basis of all future safety standards. It is valid for all sectors in which safety-relevant protection functions are set up using electrical, electronic or programmable (electronic) systems.

The standard focuses specifically on all applications in which a malfunction of the safety system would have a devastating effect on the safety of persons and/or the environment. IEC 61508 has also been developed to prevent or limit the financial impact of damage to products or production equipment.

What is the purpose of safety standards? All technical applications carry a risk in terms of safety. The more people, property or environmental areas are affected, the greater the number of measures which must be implemented to minimise risk. Safety standards provide the yardstick for these measures.

Previous safety standards tended to be application-oriented and were often only developed after accidents had occurred. Generally acknowledged principles were only afforded secondary importance. This was illustrated clearly in the 1984 TÜV publication "Microcomputers in safety technology". Existing standards from various areas of application were classified according to five safety categories based on the severity of their requirements. This explains how, for example, railway signalling equipment came to be classified in the same category as press control systems. One of the first application-oriented standards for safety-related electrical/electronic control systems was VDE 0116 (electrical equipment for furnaces). Its 1989 edition also addressed microprocessor systems. VDE 0116 is to be replaced by EN 50156.

It was not long before things moved on. DIN V 19250, "Fundamental safety aspects to be considered for measurement and control equipment", was the first standard based on fundamental risk assessment. It described procedures for classification according to eight safety categories (AK 1 to AK 8) in accordance with DIN 31000 (general guidelines for the safety design of technical products) and entirely independently of areas of application. DIN V VDE 0801 (principles for computers in safety-related systems) is a continuation of this standard. It describes measures that can be employed in safety-related computer systems in order to meet the requirements of the requirement categories defined in DIN V 19251 (Control equipment, requirements and measures for safe guarded functions).

HIMA
Paul Hildebrandt GmbH + Co KG
Industrie-Automatisierung
P.O. Box 1261
68777 Brühl
Germany
Telephone: (+49 62 02) 7 09-0
Telefax: (+49 62 02) 7 09-1 07
E-mail: info@hima.com
Internet: www.hima.com

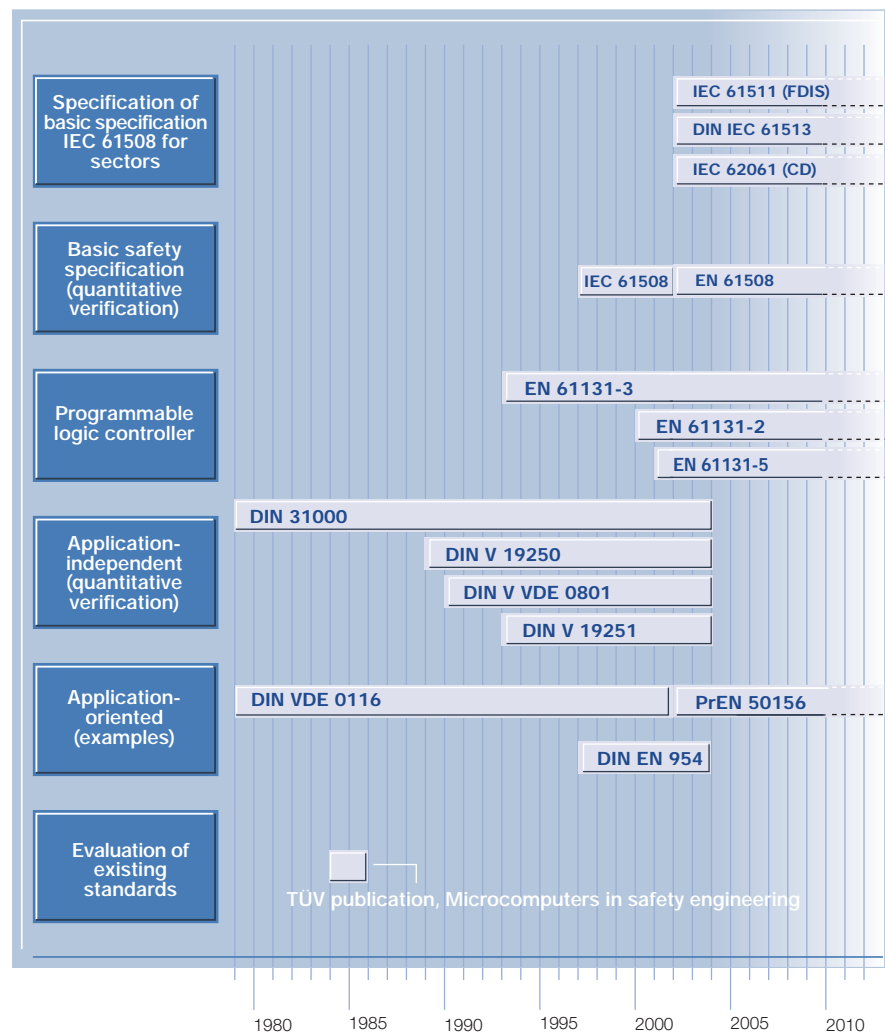


Safety standard IEC 61508

Consequences for automation technology and implementation at HIMA

EN 954 was developed in parallel with DIN V 19250. It addresses (on the basis of DIN V VDE 0801) microprocessor-based systems and a modified version of this specification has been adopted as a safety standard for factory automation. Certification of a system to DIN V 19250 and DIN V 19251 along with DIN V VDE 0801 therefore provided qualitative but not quantitative verification. Clarification was still required for assessing residual risk.

A simplified overview of the history of the development of safety standards is given below.





Safety standard IEC 61508

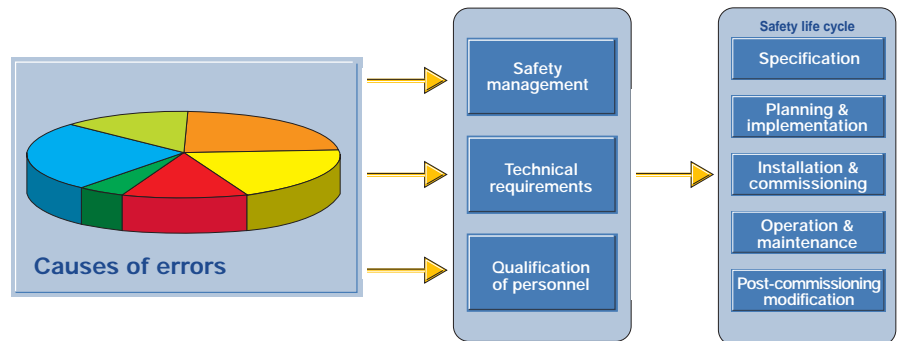
Consequences for automation technology and implementation at HIMA

Standard IEC 61508

IEC 61508 has been described in great detail in various publications. The following descriptions relate to its essential aspects. The introduction of IEC 61508 is the first time that a quantitative analysis of residual risk has been required. The standard sets out the following requirements for minimising this risk:

- Definition and analysis of risk in accordance with detailed failure probability rates - both for the overall protective circuit (loop) from the measuring point via the controller to the actuator and for the overall safety life cycle of the application
- Specification and implementation of measures (management of functional safety) to minimise residual risk
- Use of suitable (certified) devices
- Periodic inspections to ensure that specifications are being adhered to

The graphic below provides an overview of the systematic procedure:



The overall safety life cycle of the application is divided into 16 aspects. IEC 61508 requires that the safety aspects necessary for an application be investigated as early as the ideas phase. Such investigations should take the format of risk analysis and the definition of potential hazards (hazard and risk analysis).

In terms of the "management of functional safety", uppermost priority is given to carrying out all operational sequences and actions safely. This also includes the definition and qualification of responsible personnel. All actions must be recorded in accordance with exact specifications in order to optimise traceability and executed in accordance with the same principle in all 16 phases of the life cycle:

- Definition of safety objectives for each phase, including subordinate phases
- Definition of necessary requirements and specification of these for each relevant area of application
- Drawing up and documentation of a result for each phase to include physical, chemical, process-related, measuring and control and organisational measures as well as measures relating to personnel

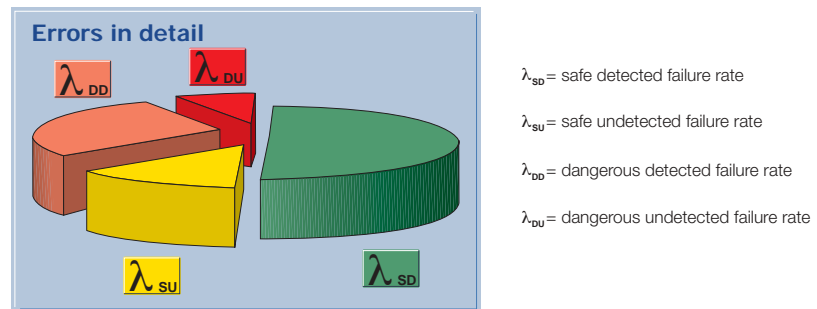


Safety standard IEC 61508

Consequences for automation technology and implementation at HIMA

The previous requirement categories (AK 1 to AK 8) are to be replaced by SILs (Safety Integrity Levels) 1 to 4. A risk graph is used to assess risk in order to define the SIL. A PFH (Probability of Failure per Hour) or PFD (Probability of Failure on Demand) must be defined for each element in the safety loop. The probability rates calculated for each individual element are added together, taking into account safety interconnections, e.g. 1oo2 or 2oo3.

The ability of a system to detect errors and react to them appropriately is an essential factor. This is why distinctions are drawn between dangerous and non-dangerous errors and the possibility of detecting errors or not.



Also relevant to determining the correct SIL are the type of hazard and the technology used, the size of the system and/or object to be protected, the number of working groups involved and the physical expansion of the system. These factors are to be considered as part of an assessment of the "known features/new features of the application".

The standard also permits the use of non-safety-related systems for safety-related applications as long as these have been "proven in use". Such systems must however be defined and documented very much on an application basis. In addition, it must also be possible to expound them completely and transparently at any time in the form of a suitable audit or assessment.

Looking to the future, any CENELEC or CEN standards which do not conform to the new IEC standard must have been modified or withdrawn by August 2004. Sector-specific standards based on IEC 61508 are currently in preparation, e.g. IEC 61511 for the process industry, IEC 61513 for the nuclear industry and IEC 62061 for the manufacturing industry. These sector-specific standards are of importance for the designers and operators of relevant applications.



Implementation of IEC 61508 at HIMA

Safety standard IEC 61508

Consequences for automation technology and implementation at HIMA

As a market-leader in safety engineering, HIMA not only influenced the safety standards of the past but also viewed adherence to them as essential to the company's success. HIMA has been using IEC 61508 as a test standard for all the systems and modules it has launched since 1998.

HIMA was able to verify the standard modules in its Planar4 system for use up to SIL 4, a criterion which is particularly important for HIPPS applications offshore. Numerous other applications for a variety of uses in accordance with many different standards also bear the mark of the market leader. The new HIMatrix series (SIL 3), its programming tool ELOP II Factory and numerous customer projects have been developed, documented and manufactured by HIMA in accordance with IEC 61508.

HIMA's revision of the new V 7.08 operating system in 2002 marked the full introduction of IEC 61508 as the basic standard for the H41q/H51q systems. The company was able to prove that the entire H41q/H51q system family and the ELOP II programming tool meet the requirements of IEC 61508 in full in terms of development, documentation and manufacture. TÜV certificates for application up to SIL 3 were issued in August 2002. This means that the H41q/H51q systems are the first 2oo4D/QMR systems in the world to meet the requirements of the new standard.

By converting to the new standard at such an early stage, HIMA became the first manufacturer of safety-related automation systems in the world to receive the "Functional Safety Management" (IEC 61508) certificate. This management tool benefits all HIMA developments and products in terms of quality and safety, giving the company a decisive competitive edge on the market.

New solutions in the area of safety-related automation are emerging on the basis of the interplay between different standards. Standards such as ATEX 95 require overall consideration of the potential hazards of all safety components. Together with the requirement for IEC 61508, HIMA has applied its many years of expertise in potentially explosive applications and in safety engineering to more new products. A flameproof analogue input module and a flameproof digital output module (essential if you wish to set up complete SIL 3 loops in potentially hazardous areas) have been added to the flameproof components in the H41q/H51q range. This means that safety circuits can be set up with more reliable modules. Detailed diagnostics along with fewer sources of error increase system availability and thus reduce production costs.



Safety standard IEC 61508

Consequences for automation technology and implementation at HIMA

Consideration of entire loops increases the importance of communication between individual components. Networking using safe**ethernet** enables HIMA systems to be integrated into safety networks in accordance with IEC 61508 up to SIL 3. As this type of communication can be set up flexibly and with redundancy, in addition to safety and the typical potential savings made possible by distributed automation concepts (e.g. reduced installation costs) it also leads to a significant increase in system availability.

As has been shown, the introduction of IEC 61508 is presenting us with new ways of approaching cost optimisation. Decisive advantages in terms of cost, right from the start of projects, are why HIMA believes it is right to hold discussions on this subject.