A Look at IEC 61508

The Standard Drives Functional Safety of Machinery in the U.S. and Europe

by Matthias Haynl, TÜV Rheinland

IN THE PAST, industrial machinery safety functions such as e-stop were hardwired, and the failure modes and failure data of these components, such as relays, were very well known. The applicable standards were EN954-1:1996 (Safety of Machinery—Safety Related Parts of Control Systems) for Europe and NFPA 79:1997 (Electrical Safety for Industrial Machinery) for the U.S. Additionally, complex components such as microcontrollers or microprocessors were not considered or allowed to be involved in the performance of the safety functions.

Prior to the changes in the standards, the number of devices used to implement and perform safety functions was not a factor as long as the particular devices had the same safety category. With technology moving forward and complex components—for example, microcontrollers or microprocessors—becoming integrated in safety systems, the fault behavior becomes more sophisticated. When the failure modes and the failure data are not well-defined and the fault conditions cannot be determined completely, the incorrect functioning of these new technologies has to be addressed.

Traditional safety assessments such as for electrical safety are not sufficient to cover all of the safety-relevant aspects of today's technologies. As a result, functional safety, which is an assessment of the components or systems that impact functional hazards, is a critical item to be addressed.

IEC 61508 was introduced in 1999 as the basic standard for functional safety. It is a comprehensive standard composed of seven parts. Parts 1-4 are normative, and parts 5-7 are informative.

WHERE IN THE WORLD?

Functional safety requirements are mandatory for European machinery, but it can be a different story for similar safety requirements in North America. Which regulations do you follow? Join the functional safety discussion at www.ControlDesign.com/functionalsafety.

Application-Independent, Technology-Dependent

IEC 61508 is the basic functional safety standard for designers of functional-safety-related devices and system integrators of safety-related systems. The IEC 61508 standard is application-independent but technology-dependent. Its scope includes electrical, electronic and programmable electronic (E/E/PE) safety-related systems. The standard is written in such a way that it can be used as a framework for other technologies, as well.

IEC 61508 addresses the functional hazards of new technological advances. A major feature of this standard considers the possible occurrence of dangerous failure that might arise from incorrect specifications, omissions, random or systemic hardware failure, software errors, common cause failures, human error and other influences. IEC 61508 contains requirements for preventing failures by avoiding the introduction of faults and for controlling failures by ensuring safety even when faults are present. Additionally, the standard provides new requirements for a product's overall safety lifecycle. This takes into consideration every phase of a product from initial concept to final decommissioning or disposal.

The standard uses a risk-based approach to determine safety integrity requirements of safety-related E/E/PE systems. The probability approach targets random hardware faults that could be dangerous and, if undetected, result in loss of the safety function. It specifies four discrete safety integrity levels (SILs) of safety performance for a safety function. SIL 1 is the lowest level of safety integrity, and SIL 4 is the highest level. Requirements to achieve safety integrity at the higher levels are more meticulous than the lower levels.

One attribute of the SIL classification is the dangerous failure probability. System integrators have to consider all devices and components implemented to perform the safety function and ensure that the dangerous failure probability corresponds to the targeted SIL. Hence, it is important to know how many devices implement and perform the safety function, and the manufacturer of safety-related devices has to determine the specific safety parameters.

Another focus of IEC 61508 is the overall safety lifecycle, the corresponding E/E/PE system safety lifecycle and the software safety lifecycle. The purpose of this is to avoid systematic faults during design and development, installation and commissioning, operation, maintenance and modification of the safety-related equipment and systems. Systematic faults can occur in either hardware or software designs. Measures and techniques to avoid and control them are specified by IEC 61508-2 and IEC 61508-3. To address the functional safety requirements in reference to the overall safety, E/E/PE system safety and software safety lifecycle IEC61508-1 requires an effective management of functional safety (MFS). The MFS covers responsibilities, procedures and activities with respect to the overall safety, E/E/PE system safety and software safety lifecycle.

The standard provides new requirements for a product's overall safety lifecycle. This takes into consideration every phase of a product from initial concept to final decommissioning or disposal.

Functional Safety in Europe

IEC 61508, or EN 61508, is not a harmonized European standard. That means it cannot be used exclusively as proof of CE conformity. To comply with the machinery directive's requirements, the harmonized standards EN 62061:2005 and EN ISO 13849-1:2008 are the most relevant from the functional safety point of view.

The harmonized European standard EN 62061:2005 (Safety of machinery—Functional safety of safety-related electrical, electronic and programmable electronic control systems) is driven by IEC 61508 and makes recommendations for the design, integration and validation of safety-related E/E/PE systems for industrial machines. EN 62061:2005 has the same SILs as IEC 61508, except SIL 4 is as relevant to the risk reduction requirements normally associated with machinery. The main focus of EN 62061:2005 is the safety function—from specification to validation. The standard requires a complete functional safety assessment in reference to IEC 61508 for complex systems or subsystems.

It is also important to note that the application-dependent standard EN 62061:2005 also specifies increased severity levels for EMC testing. The standard makes references to general electrical safety requirements for machinery, for example, to EN 60204-1 for protection against electric shock.

The harmonized European standard EN ISO 13849-1:2008 (Safety of machinery—Safety-related parts of control systems) combines the complex probability method from IEC 61508 and the deterministic category approach from EN 954-1 on the basis of the risk assessment. The safety classifications of EN ISO 13849-1:2008 are performance levels (PLs), where PL a is the lowest level and PL e the highest. The simplified procedure under EN ISO 13849-1:2008 considers the relevant parameters and architectures to provide a practical assessment solution for machinery safety. The simplified procedures could be used only for the designated architectures described in the standard.

The requirements of EN ISO 13849-1:2008 and EN 62061:2005 are to some extent identical and complementary. The scope or introduction to the standards determines which of the two is most applicable.

Functional Safety Requirements in the U.S.

In the U.S., the mandatory requirements for certification and validation of safety systems designed for machinery safety are specified under the Code of Federal Regulations (CFR), available from OSHA. The 29 CFR 1910, Subpart O, specifies the minimum requirements for machinery and machine guarding—for example, 29 CFR 1910.217 for presence-sensing devices, or 29 CFR 1910.212 for machine guarding.

Requirements can be found in 29 CFR 1910.217 for safe conditions in the event of any single failure. In

IEC 61508: THE BASIC STANDARD FOR FUNCTIONAL SAFETY

Functional safety assessments of the components or systems address the correct performance of the assigned safety functions as required for the necessary level of risk reduction. In 1999, the new standard IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems) was issued. IEC 61508 consists of the following parts:

Part 1: General requirements
Part 2: Requirements for E/E/PE safety-related 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 IEC 61508-2 and IEC 61508-3
Part 7: Overview of techniques and measures

STANDARDS IN RELATIONSHIP

Overall, there are similarities to the EU and U.S. approaches with regard to the safety loop and the risk-based approach. The following table shows the advantages and weaknesses of the standards.

Standard	Pros	Cons
IEC 61508	Assessment of the complete safety lifecycle	Non-harmonized European standard
	Covers hardware and software for simple and complex systems	Complex and sophisticated for safety of machinery, especially for the machine builder
IEC 62061 EN 62061	Partly simplified approach as under IEC 61508 (e.g., QM requirements)	References to IEC 61508 can lead to a difficult understanding
	Covers configuration, parameterization and embedded software aspects	
	Complex systems and components are covered up to SIL3	
	Harmonized European standard	
ISO 13849 EN ISO 13849	Simpler approach as under IEC 61508 (e.g., QM requirements, calculation of safety-related parameters)	Restrictions apply for complex electronics regarding the PL
	Covers configuration and parameterization and embedded software aspects	Not applicable for complex programmable systems
	Continues with the EN 954-1 requirements	Results of the safety parameters are very conservative
	Covers non-electrical, electromechanical and complex electronics	
	Harmonized European standard	
29 CFR 1910, Subpart O	Simpler approach as under IEC 61508 (e.g., QM requirements)	Probability approach is not covered
	Regulates the requirements for all kinds of machinery and the related equipment	Not suitable for complex electronics (e.g., safety-related PLC)
	OSHA-recognized third-party validation required	Does not specify specific standards

addition, the term "control reliability" is specified and drives requirements regarding the design, validation and certification of safety-related systems. Of note is a requirement that an OSHA-recognized third-party validation organization shall be used to validate whether:

- The design of components, subsystems, software and assemblies meets OSHA performance requirements and are ready for the intended use
- The performance of combined subsystems meets OSHA's operational requirements.

Typical analysis methods like failure mode and effect analysis (FMEA), as well as the general approach to perform a risk evaluation and a hazard analysis, are referenced. The probability approach—for example, under EN ISO 13849-1:2008 or EN 62061:2005—is not considered or required under the OSHA requirements at this point in time; however the deterministic approach regarding the system architecture and behavior are similar to the EN 954-1:1996 requirements. Application-dependent standards for the U.S. would be ANSI B11.19:2003 (Performance criteria for Safeguarding) or NFPA 79:2007 (Electrical Standard for Industrial Machinery).

Future Developments and Directions

Machine components and safety functions will become more complex and sophisticated. Intelligent and distributed control will manage functions such as an intelligent safety area around hazardous areas or objects. New communication media such as wireless technology will be in the safety loop to reduce wiring and provide more mobility and flexibility. The use of safety communication buses is *de facto* a standard today.

Functional safety requirements are mandatory for machinery safety in Europe. Yet it also is wise to consider these requirements for machinery in North America. It is likely that updates to related standards are going to cover new approaches and technological advancements to address overall functional safety hazards.

MATTHIAS HAYNL has been manager of functional safety with TÜV Rheinland's Functional Safety Division since 2003. He has experience in the testing and assessment of safety-related systems of power plants, nuclear power plants, processing machinery and industrial machinery. He can be reached at info@us.tuv.com.