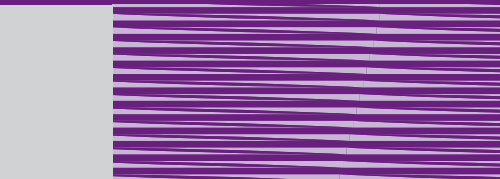
A decorative graphic on the left side of the page, featuring a solid purple vertical bar followed by a series of horizontal lines that transition from purple to a lighter shade.

**Functional safety of
electrical/electronic/
programmable electronic
safety-related systems**

IEC 61508

International Electrotechnical Commission

Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs



IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems

The challenge

Electrical, electronic or programmable electronic systems increasingly carry out safety functions. These systems are usually complex, making it impossible in practice to fully determine every failure mode or to test all possible behaviour. It is difficult to predict the safety performance, although testing is still essential.

The challenge is to design the system in such a way as to prevent dangerous failures or to control them when they arise.

Dangerous failures may arise from:

- incorrect specifications of the system, hardware or software;
- omissions in the safety requirements specification (e.g. failure to develop all relevant safety functions during different modes of operation);
- random failures of hardware;
- systematic failures of hardware and software;
- common cause failures;
- human error;
- environmental influences (e.g. electromagnetic, temperature, mechanical phenomena);

- supply system voltage disturbances (e.g. loss of supply, reduced voltages, re-connection of supply).

IEC 61508 contains requirements to minimize these failures in E/E/PE safety-related systems.

E/E/PE safety-related systems

IEC 61508 covers functional safety of safety-related systems that use electrical and/or electronic and/or programmable electronic (E/E/PE) technologies. The standard applies to these systems irrespective of their application.

An example E/E/PE safety-related system using electrical (or electro-mechanical) technology is the guard interlocking and emergency stopping system for machinery.

Many safety-related systems that would have used electro-mechanical technology or solid-state electronics now use programmable electronics instead. Devices such as programmable controllers, programmable logic controllers (PLCs) and digital communication systems (e.g. bus systems) are part of this trend. Furthermore, enabling technologies, such as application specific integrated circuits (ASICs), micro-processors, and intelligent sensors, transmitters and actuators, are increasingly being integrated into products and systems.

Example applications include crane safe load indicators, variable speed motor drives used to restrict speed for protection, systems for interlocking and controlling the exposure dose of medical radiotherapy machines, or the indicator lights, anti-lock braking, and engine-management systems on automobiles.

Other examples are emergency shutdown systems in hazardous chemical plants, railway signalling systems and fly-by-wire operation of aircraft flight control surfaces.



Recent developments include network based safety-related systems, often facilitated by internet technology. An example is the remote monitoring, operation or programming of a network-enabled water treatment plant.

An E/E/PE safety-related system covers all parts of the system that are necessary to carry out the safety function (i.e. from sensor, through control logic and communication systems, to final actuator, including any critical actions of a human operator).

An E/E/PE system may be safety-related even if it does not have any direct control over potentially hazardous equipment. For example an information-based decision support tool might be safety-related if erroneous results affect safety.

Objectives

The standard aims to:

- release the potential of E/E/PE technology to improve both safety and economic performance;
- enable technological developments to take place within an overall safety framework;



- provide a technically sound, system-based approach, with sufficient flexibility for the future;
- provide a risk-based process for determining the required performance of safety-related systems;
- provide a generically-based standard that can be used directly by industry but can also help with developing sector standards (e.g. machinery, process chemical plants, medical or rail) or product standards (e.g. power drive systems);
- provide a means for users and regulators to gain confidence when using computer-based technology;
- provide requirements based on common underlying principles to facilitate:
 - improved efficiencies in the supply chain for suppliers of subsystems and components to various sectors,
 - improvements in communication and requirements (i.e. to increase clarity of what needs to be specified),
 - the development of techniques and measures that could be used across all sectors, increasing available resources,

- the development of conformity assessment services if required.

Parts framework of IEC 61508

The standard consists of 7 parts:

- IEC 61508-1, General requirements;
- IEC 61508-2, Requirements for electrical/electronic/programmable electronic safety-related systems;
- IEC 61508-3, Software requirements;
- IEC 61508-4, Definitions and abbreviations;
- IEC 61508-5, Examples of methods for the determination of safety integrity levels;
- IEC 61508-6, Guidelines on the application of IEC 61508- 2 and IEC 61508-3;
- IEC 61508-7, Overview of measures and techniques.

IEC 61508 as a stand-alone standard

IEC 61508 can be used directly by industry as a stand-alone standard, including use:

- as a set of general requirements for E/E/PE safety-related systems where no application sector or product standards exist or where they are not appropriate;
- by suppliers of E/E/PE components and subsystems for use in all sectors (e.g. hardware and software of sensors, smart actuators, programmable controllers);
- by system builders to meet user specifications for E/E/PE safety-related systems;
- by users to specify requirements in terms of the safety functions to be performed together with the performance requirements of those safety functions;
- to help with maintaining the "as designed" safety integrity of E/E/PE safety-related systems;
- to provide the technical framework for conformity assessment and certification services;
- as a basis for carrying out assessments of safety lifecycle activities.

IEC 61508 as a basis for other standards

Parts 1, 2, 3 and 4 of IEC 61508 are IEC basic safety publications. One of the responsibilities of IEC technical committees is, wherever practicable, to make use of these parts of IEC 61508 while preparing their own sector or product standards that have E/E/PE safety-related systems within their scope. For more details see IEC Guide 104, The preparation of safety publications and the use of basic safety publications and group safety publications and ISO/IEC Guide 51, Safety aspects – Guidelines for their inclusion in standards.

IEC 61508 is the basis for a published nuclear sector standard. It is also currently being used as a basis for developing other sector standards (e.g. machinery, process) and product standards (e.g. power drive systems). It is therefore influencing the development of E/E/PE safety-related systems and products across all sectors.

Many requirements of IEC 61508, particularly in parts 2 and 3, are not repeated in the application sector or product standards but are referenced instead. The result is that most users will need IEC 61508 also.

The market for any product, component or subsystem that complies with IEC 61508 is potentially very large since in principle they are capable of meeting the requirements of any sector standard based on IEC 61508.

Further information

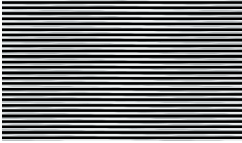
You can find further information on IEC 61508 and functional safety, including details on how to obtain the standard, in the Functional Safety Zone of the IEC web site (<http://www.iec.ch/functionalsafety>).

The IEC

The IEC has served the world's electrical industry since 1906, developing international standards to promote quality, safety, performance, reproducibility and environmental compatibility of materials, products and systems.

The worldwide use of IEC standards supports the transfer of electrotechnology, assists conformity assessment (for example, certification) and promotes international trade of uniform high-quality products and services. International standards establish objective specifications that both buyer and seller can rely on. For buyers, they widen the range of choices and lower costs, primarily because they often increase the number of competitors. For sellers, global standards broaden the number of potential

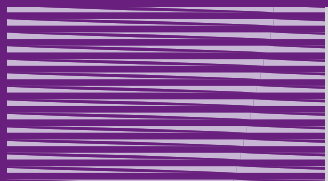




customers and reduce the cost of meeting their needs. In short, for everyone in society, international standards raise the overall efficiency and productivity of the economy.

The IEC membership, which now comprises more than 60 countries, includes all the world's major trading nations. This membership collectively represents about 85 percent of the world's population and 95 percent of the world's electrical generating capacity.

The worldwide use of IEC standards supports the transfer of electrotechnology, assists certification and promotes international trade of uniform high-quality products and services.



For further information

Up-to-date information about the work on renewable and alternative energy standards carried out in IEC TC 4, 82, 88 or 105, as well as information about the Commission's conformity assessment activities and about ACEA, can be obtained from the IEC's website, at www.iec.ch. Equally, any of the IEC's National Committees, whose addresses are available on the IEC website or from IEC Central Office, can also provide information.



International Electrotechnical Commission

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland
Telephone: +41 22 919 0211
Telefax: +41 22 919 0300
E-mail: info@iec.ch
Web: www.iec.ch