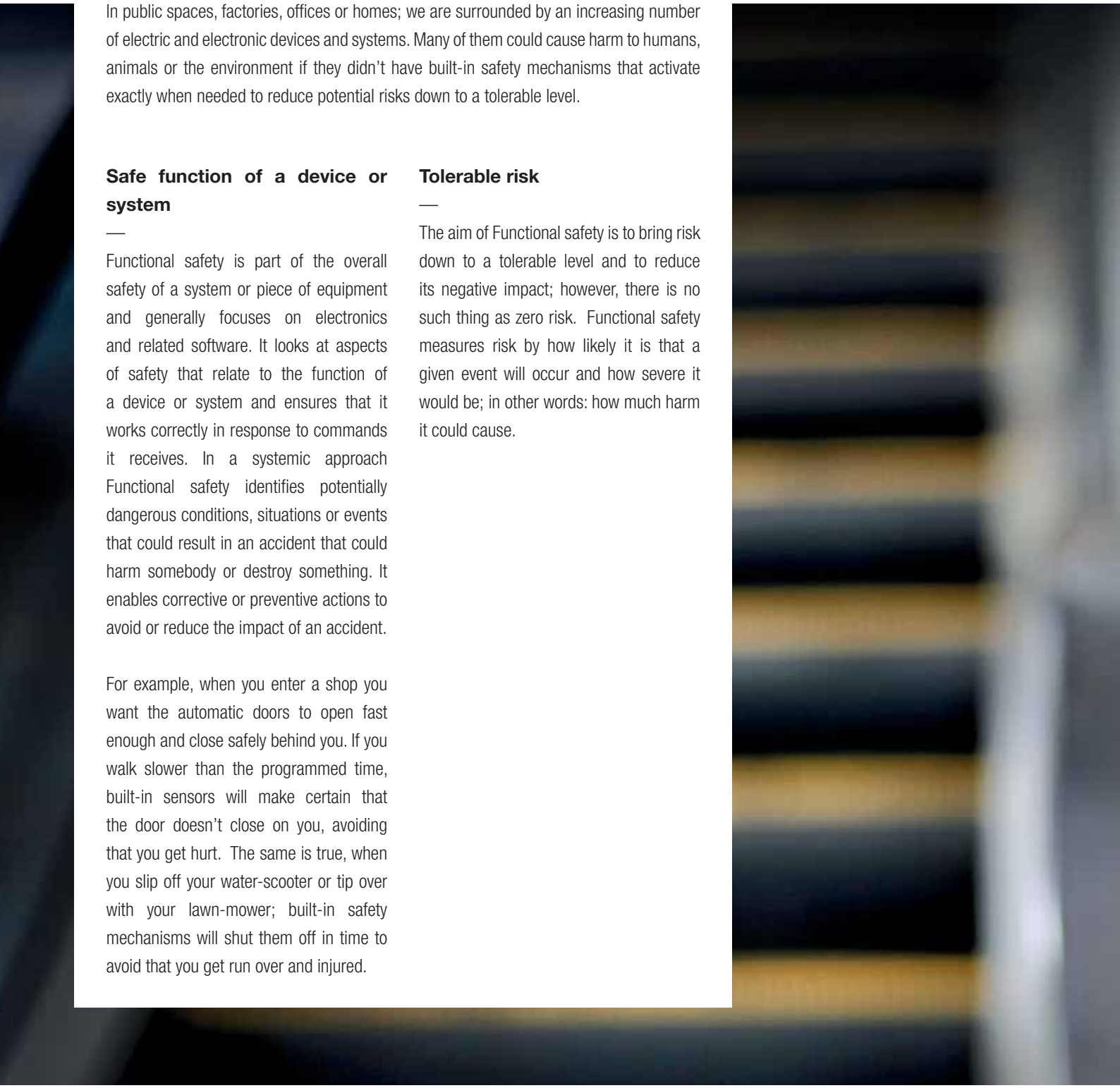
Functional safety

Essential to overall safety

What is Functional safety?

In public spaces, factories, offices or homes; we are surrounded by an increasing number of electric and electronic devices and systems. Many of them could cause harm to humans, animals or the environment if they didn't have built-in safety mechanisms that activate exactly when needed to reduce potential risks down to a tolerable level.



Safe function of a device or system

—

Functional safety is part of the overall safety of a system or piece of equipment and generally focuses on electronics and related software. It looks at aspects of safety that relate to the function of a device or system and ensures that it works correctly in response to commands it receives. In a systemic approach Functional safety identifies potentially dangerous conditions, situations or events that could result in an accident that could harm somebody or destroy something. It enables corrective or preventive actions to avoid or reduce the impact of an accident.

For example, when you enter a shop you want the automatic doors to open fast enough and close safely behind you. If you walk slower than the programmed time, built-in sensors will make certain that the door doesn't close on you, avoiding that you get hurt. The same is true, when you slip off your water-scooter or tip over with your lawn-mower; built-in safety mechanisms will shut them off in time to avoid that you get run over and injured.

Tolerable risk

—

The aim of Functional safety is to bring risk down to a tolerable level and to reduce its negative impact; however, there is no such thing as zero risk. Functional safety measures risk by how likely it is that a given event will occur and how severe it would be; in other words: how much harm it could cause.

Fact

—

Identify dangerous conditions to prevent accidents

Functional safety is everywhere

The concept applies to everyday life and every industry you can think of. It is fundamental for most safety-related systems. The oil and gas industry, nuclear plants, the manufacturing sector, your car, medical devices, transportation all rely heavily on Functional safety to achieve safety in areas where the operation of equipment can give rise to hazards.

Automotive

In your car, Functional safety ensures that airbags instantly deploy during impact to protect you and your loved ones, but absolutely not when you are simply driving. It controls the fuel injector to ensure that your car doesn't accelerate when you didn't give the command; it makes certain that your ABS brakes activate when needed. When your child has her hands on the electric rear-window you are closing, Functional safety protocols ensure that this resistance stops the window from cutting her fingers off. Functional safety ensures the correct operation of all automotive electronics and its control software.

Transportation

When you board a train, the subway or a cable car, Functional safety ensures that the doors close before the vehicle departs and that they don't open while it is in movement. They also ensure that the railway signalling system helps avoid that an oncoming train crosses your train's path.

Aviation is among the safest industries in the world and it applies Functional safety in many areas, including for example the automated flight control system. The two-axis autopilot system controls the pitch and roll of the aircraft and controls heading and altitude, all of which are programmed to respect certain Functional safety parameters, activating alarms and other measures when they are breached.

Medical

In healthcare the presence or absence of Functional safety protocols can mean the difference between life and death of a patient. In addition to electric or mechanical aspects that impact safety, Functional safety ensures that a given apparatus functions correctly in response to inputs. For example, if an infusion pump malfunctions, Functional safety protocols will ensure that alarms are activated to signal the malfunction and if relevant that the pump is deactivated to protect the patient from harm through over-dosing. A different set of safety protocols ensures that a patient who undergoes cancer radiation therapy only receives exactly the programmed dose of gamma radiation, no more.

Manufacturing

—

Functional safety is the best way of reducing inherent risks in hazardous industrial processes both within a factory or chemical plant and out in the field. An automatic valve closure mechanism will ensure that dangerous chemicals are mixed in exactly the required quantities. A crane safe load indicator will avoid that overloading will collapse the crane and kill workers or innocent bystanders. Sensors or laser barriers will automatically shut-down a robot, when a human or object enters its activity range, preventing injuries or avoiding potentially costly damage to machinery. A pressure valve will open or close precisely when it is electronically given the instruction to do so. When such security-devices fail to operate as they should, for example during deep-sea oil drilling or during the filling of a chemical tank, major disasters can ensue.

↙

Fact

—

Reduce inherent risks
in hazardous industrial processes

The challenge

Electrical, electronic or programmable electronic systems (E/E/PE) carry out a multitude of safety functions. The challenge is to design safety-systems in such a way as to prevent dangerous failures or to control them when they arise. These systems are usually complex, making it impossible in practice to fully determine every potential failure, but testing is nevertheless essential to rule out as many as possible.

Power generation

—

Wherever there is electricity, Functional safety isn't far away. When gale-force winds hit, a wind turbine must be able to turn its blades out of the wind to avoid damage or destruction of the whole installation from overspinning. When vibration levels in a gas turbine exceed a certain maximum, an automatic shut-down mechanism will prevent its disintegration and avoid injuries to surrounding workers.

Fact

—

Protect wind turbine investment during storms

A systems approach

Many systems today are designed to automatically prevent dangerous failures or to control them when they arise.

Such failures can arise for example from:

- → random or systematic failures of hardware or software
- → human error
- → environmental circumstances such as for example temperature, weather, electro-magnetic interference or mechanical phenomena
- → loss of electricity supply or other disturbances
- → incorrect specifications of the system; both hardware or software;
- → omissions in the specifications of safety requirements (e.g. failure to put in place all relevant safety functions in line with different modes of operation).

So called electrical, electronic or programmable safety-related systems (E/E/PE) cover all the parts of a device or system that carry out automated safety functions. This includes everything from sensors, through control logic and communication systems, to final actuators, including any critical actions of a human operator as well as environmental conditions.

Many technologies

—

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.'

Fact

—

Protect man and machine

IEC work in Functional safety

The IEC 61508 series are the International Standards for electrical, electronic and programmable electronic safety related systems. It supports the assessment of risks to minimize these failures in all E/E/PE safety-related systems, irrespective of where and how they are used.

IEC 61508 sets out the requirements for ensuring that systems are designed, implemented, operated and maintained to provide the required safety integrity level (SIL). Four SILs are defined according to the risks involved in the system application, with SIL4 being used to protect against the highest risks.

Parts framework of IEC 61508

—

The International Standards consist of seven 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 techniques and measures.

The International Standard is used by a wide range of manufacturers, system builders, designers and suppliers of components and subsystems and serves as the basis for conformity assessment and certification services. Safety system managers use it as a basis for carrying out assessments of safety lifecycle activities. The Standard is also used by many IEC TCs (Technical Committees) while preparing their own sector or product specific International Standards that have E/E/PE safety-related systems within their scope. Those include for example International Standards for the nuclear sector, for machinery and for power drive systems to mention just a few.

Further information

—

You can find further information on IEC 61508 and Functional safety, including details on how to obtain the International Standard, in the Functional safety zone of the IEC web site:

www.iec.ch/functionalsafety

↙

Fact

—

Control the opening and closing protocols of doors


6.1

International
Electrotechnical
Commission

3 rue de Varembe
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 02 11
info@iec.ch
www.iec.ch

IEC Functional safety:2015-03(en)