COURSE 1

We are surrounded by an increasing number of electric and electronic devices and systems in public spaces, factories, offices or homes [1]. 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 [1].

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 [1].

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 [1].

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 [1].

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 [1].

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 [1].

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 [1].

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 [1].

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. [1].

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 [1].

Power generation

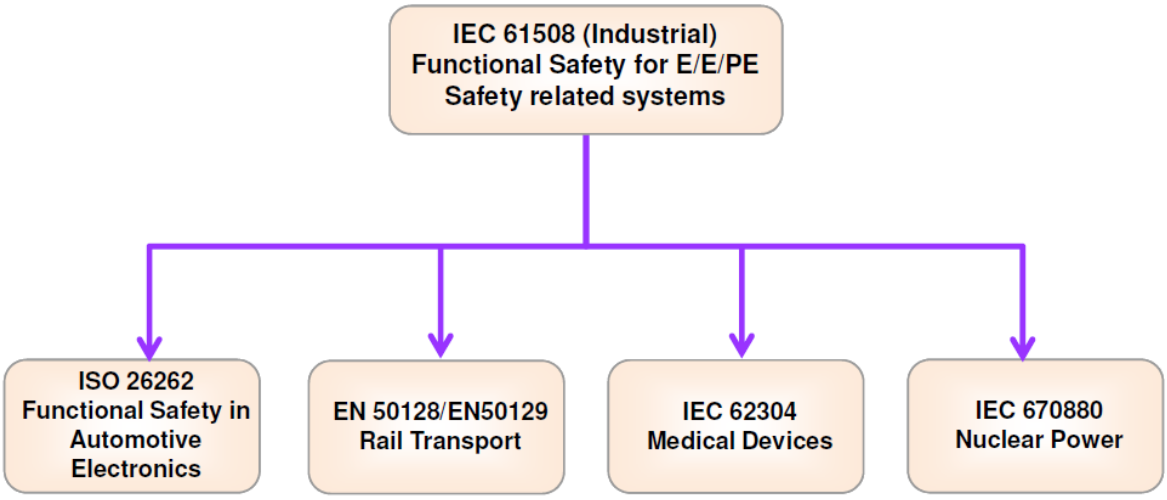
Wherever there is electricity, Functional safety isn't far away. When gale-force winds hit, a wind turbine must be able to turn its blades out of the wind to avoid damage or destruction of the whole installation from overspinning. When vibration levels in a gas turbine exceed a certain maximum, an automatic shut-down mechanism will prevent its disintegration and avoid injuries to surrounding workers [1].

Protect wind turbine investment during storms

Management, systematic techniques, verification and validation

Specific techniques ensure that mistakes and errors are avoided across the entire life-cycle. Errors introduced anywhere from the initial concept, risk analysis, specification, design, installation, maintenance and through to disposal could undermine even the most reliable protection. IEC 61508 specifies techniques that should be used for each phase of the life-cycle.

Industry/application specific variants



1. ***Automotive software***

ISO 26262 is an adaptation of IEC 61508 for Automotive Electric/Electronic Systems. It is being widely adopted by the major car manufacturers [2].

Before the launch of ISO 26262, the development of software for safety related automotive systems was predominantly covered by the Motor Industry Software Reliability Association guidelines. The MISRA project was conceived to develop guidelines for the creation of embedded software in road vehicle electronic systems. A set of guidelines for the development of vehicle based software was published in November 1994.[1] This document provided the first automotive industry interpretation of the principles of the, then emerging, IEC 61508 standard.

Today MISRA is most widely known for its guidelines on how to use the C and C++ languages. MISRA C has gone on to become the de facto standard for embedded C programming in most of safety-related industries and is also used to improve software quality even where safety is not the main consideration. MISRA has also developed guidelines for the use of model-based development.

2. ***Rail software***

IEC 62279 provides a specific interpretation of IEC 61508 for railway applications. It is intended to cover the development of software for railway control and protection including communications, signalling and processing systems [2].

3. ***Process industries***

The process industry sector includes many types of manufacturing processes, such as refineries, petrochemical, chemical, pharmaceutical, pulp and paper, and power. IEC 61511 is a technical standard which sets out practices in the engineering of systems that ensure the safety of an industrial process using instrumentation [2].

4. ***Nuclear power plants***

IEC 61513 provides requirements and recommendations for the instrumentation and control for systems important to safety of nuclear power plants. It indicates the general requirements for systems that contain conventional hardwired equipment, computer-based equipment or a combination of both types of equipment [2].

5. ***Machinery***

IEC 62061 is the machinery-specific implementation of IEC 61508. It provides requirements that are applicable to the system level design of all types of machinery safety-related electrical control systems and for the design of non-complex subsystems or devices [2].

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 [2].

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 [1].

Those include for example International Standards for the nuclear sector, for machinery and for power drive systems to mention just a few.

IEC 61508 has the following views on risks [2]:

- ✓ Zero risk can never be reached;
- ✓ Safety must be considered from the beginning;
- ✓ Non-tolerable risks must be reduced (ALARP - "**as low as reasonably practicable**").

Hazard and Risk Analysis

The standard requires that hazard and risk assessment be carried out: 'The EUC (equipment under control) risk shall be evaluated, or estimated, for each determined hazardous event' [2].

The standard advises that 'Either qualitative or quantitative hazard and risk analysis techniques may be used' and offers guidance on a few approaches. One of these, for the qualitative analysis of hazards, is a framework based on 6 categories of likelihood of occurrence and 4 of consequence [2].

Categories of likelihood of occurrence

Category	Definition	Range (failures per year)
Frequent	Many times in system lifetime	$> 10^{-3}$
Probable	Several times in system lifetime	10^{-3} to 10^{-4}
Occasional	Once in system lifetime	10^{-4} to 10^{-5}
Remote	Unlikely in system lifetime	10^{-5} to 10^{-6}
Improbable	Very unlikely to occur	10^{-6} to 10^{-7}
Incredible	Cannot believe that it could occur	$< 10^{-7}$

Consequence categories

Category	Definition
Catastrophic	Multiple loss of life
Critical	Loss of a single life
Marginal	Major injuries to one or more persons
Negligible	Minor injuries at worst

These are typically combined into a risk class matrix

	Consequence			
Likelihood	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

Where:

- Class I: Unacceptable in any circumstance;
- Class II: Undesirable: tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained;
- Class III: Tolerable if the cost of risk reduction would exceed the improvement;
- Class IV: Acceptable as it stands, though it may need to be monitored.

Safety integrity level

The safety integrity level (SIL) provides a target to attain in regard to a system's development. A risk assessment effort yields a target SIL, which thus becomes a requirement for the final system. process (using appropriate quality control, management processes, validation and verification techniques, failure analysis etc.) so that one can reasonably justify that the final system attains the required SIL. Part 2 and 3 of IEC 61508 give guidance on activities to perform in order to attain a SIL [2].

Improved reliability

The meaning of the SIL varies depending on whether the functional component will be exposed to *high* or *low* demand [2]:

- For systems that operate continuously (continuous mode) or systems that operate more than once per year (high demand mode), SIL specifies an allowable frequency of dangerous failure.
- For systems that operate intermittently and at most once a year (low demand mode), SIL specifies an allowable probability that the system will fail to respond on demand.

SIL	Low demand mode: average probability of failure on demand	High demand or continuous mode: probability of dangerous failure per hour
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$ (1 dangerous failure in 1140 years)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$

Failure to safety

Calculation of safe failure fraction (SFF) determines how fail-safe the system is. This compares the likelihood of safe failures with dangerous failures. Reliability by itself is not sufficient to claim a SIL level. There are charts in IEC 61508 that specify the level of SFF required for each SIL.