Standards

The need for standards

Computer-based systems (generically referred to as programmable electronic systems) are being used in all application sectors to perform non-safety functions and, increasingly, to perform safety functions.

Safety critical systems:

we need a **safety culture**, but safety culture is not enough

Standards enforce rules of conduct; documentation must be open to external inspection and audit

We need standards, but good standard can still lead to a bad system; were all the processes followed? Were the staff trained and motivated? Was there a sufficient budget and managerial support? ……

Safety cannot rely on testing

(www.adeptis.ru/vinci/m_part7.html)

Program testing can be used to show the *presence* of bugs, but never to show their absence.

E. Dijkstra, quoted in Dahl et al., *Structured Programming*.

Functional safety

Functional safety is a concept applicable across all industry sectors. It is fundamental to the enabling of complex technology used for safety-related systems.

It provides the assurance that the safety-related systems will offer the necessary risk reduction required to achieve safety for the equipment.

International Standard Organization (ISO) has formed joint committees with the International Electrotechnical Commission (IEC) to develop standards and terminology in the areas of electrical, electronic and related technologies

The IEC 61508

IEC 61508:
Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems **(E/E/PE, or E/E/PES)**
an international standard of rules for programmable systems applied in industry

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

The standard covers safety related systems when one or more of such systems incorporate E/E/PE devices

The standard specifically covers possible hazards created when failures of the safety functions performed by E/E/PE safety related systems occur

All IEC International Standards in the IEC 61508 series were developed by IEC SC (Subcommittee) 65 A: Industrial-process measurement, control and automation - Systems aspects.

The IEC 61508

The standard covers the complete safety life cycle, and may need interpretation to develop **sector specific standards**. It has its origins in the process control industry.

The safety life cycle has 16 phases which roughly can be divided into three groups as follows:

- Phases 1-5 address analysis
- Phases 6-13 address realisation
- Phases 14-16 address operation.

All phases are concerned with the safety function of the system.

The IEC 61508

The standard has seven parts:

Parts 1-3 contain the requirements of the standard (normative)

- IEC 61508-1: General requirements
- IEC 61508-2: Requirements for E/E/EP safety related systems (hardware)
- IEC 61508-3: Software requirements

Parts 4-7 are guidelines and examples for development and thus informative.

- IEC 61508-4: Definitions and abbreviatios
- IEC 61508-5: Methods for determining safety integrity levels
- IEC 61508-6: Guidelines for the application of 1 and 2
- IEC 61508-7: Techniques and measures

The IEC 61508

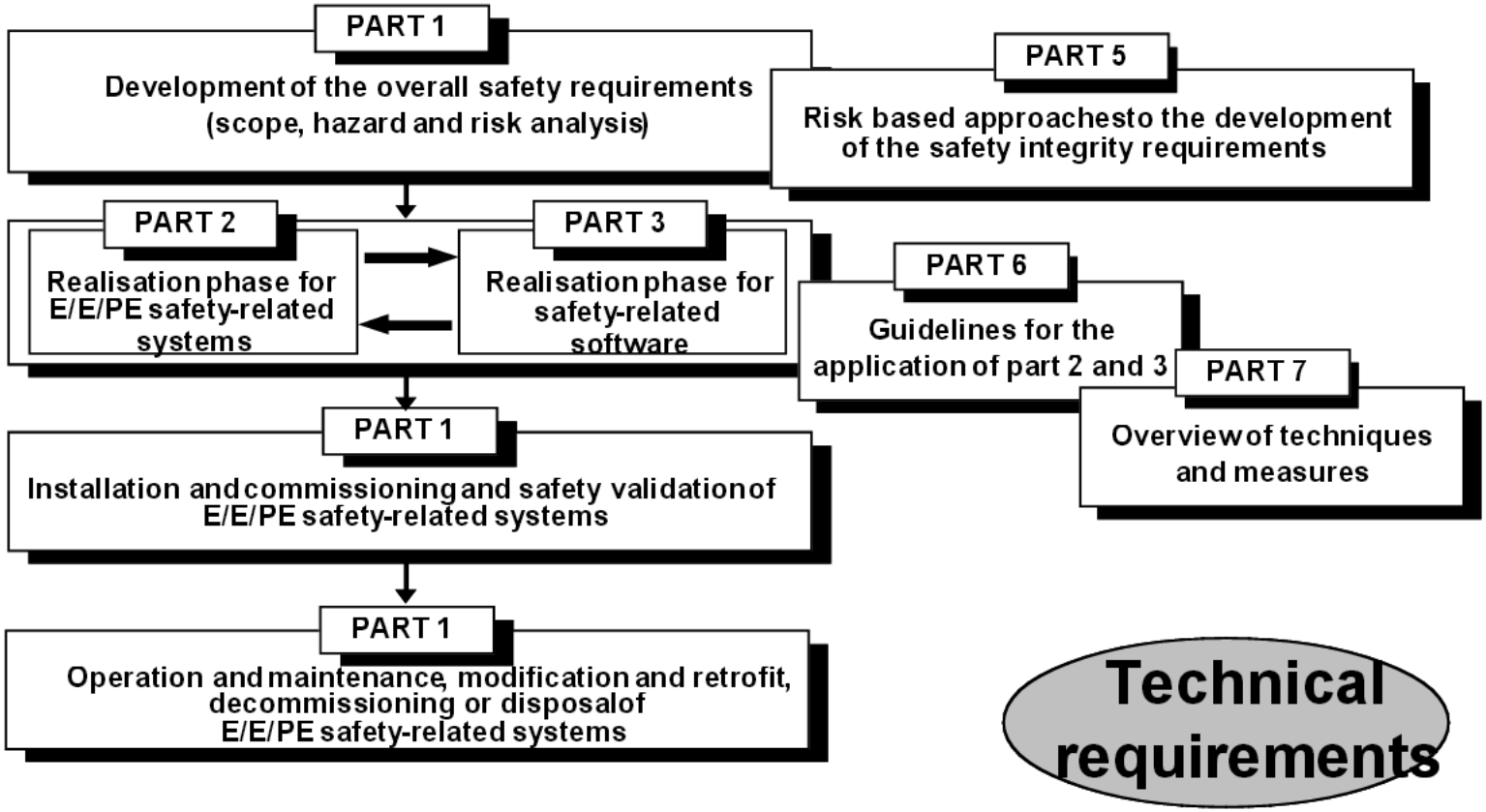


Figure 1: Technical requirements of IEC 61508.

The IEC 61508

Central to the standard are the concepts of

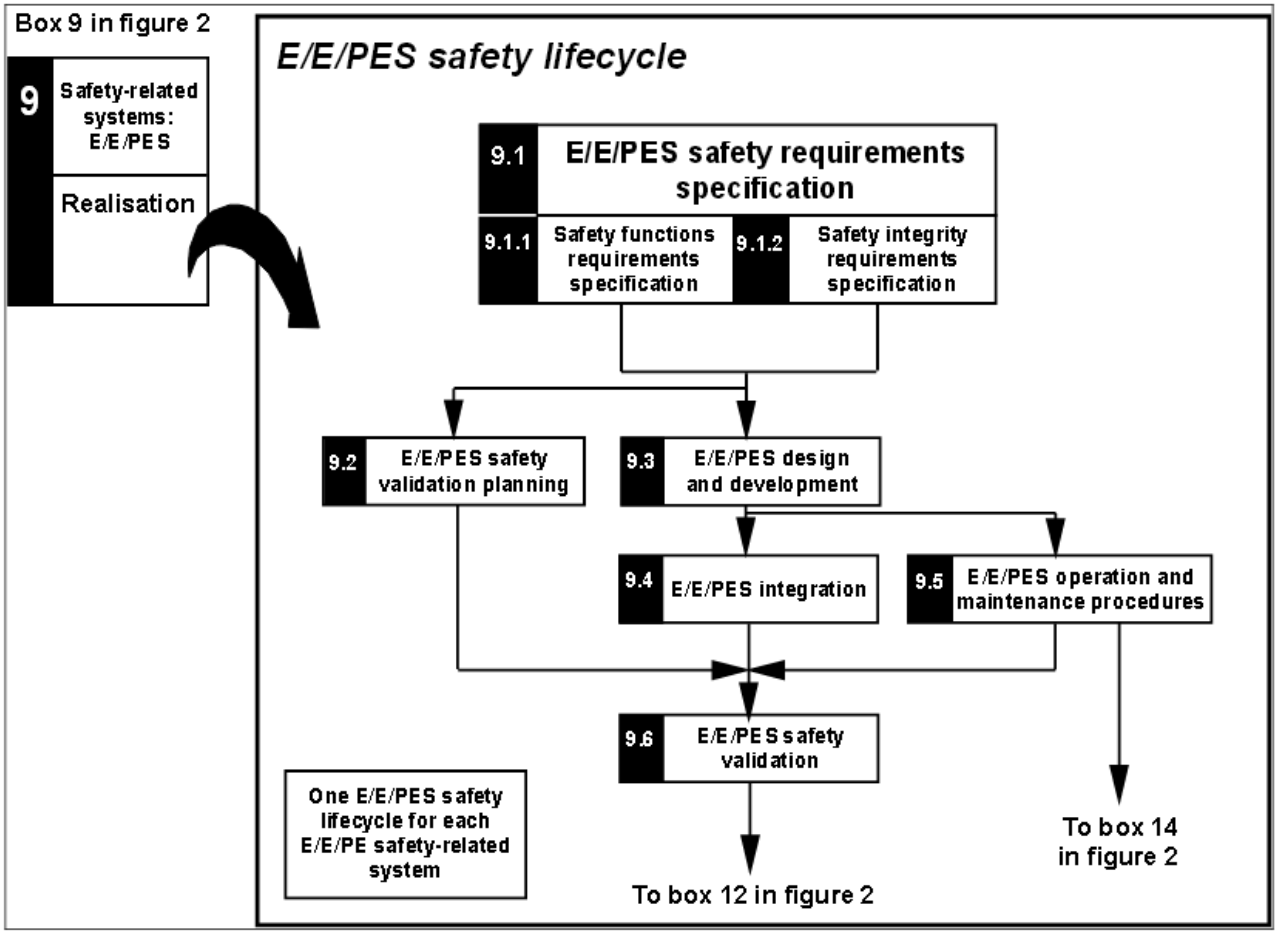
safety life cycle, risk and safety functions, safety integrity levels

The safety life cycle is defined as an engineering process that includes all the steps necessary to achieve required functional safety

The risk is a function of frequency (or likelihood) of the hazardous event and the event consequence severity.

Safety integrity levels are introduced for specifying the target level of safety functions to be implemented by E/E/PE safety-related systems

Safety lifecycle



The figure shows only those phases that are within the realisation phase

Risks and Risk reduction

IEC 61508 has the following views on risks:

- Zero risk can never be reached
- Safety must be considered from the beginning
- Non-tolerable risks must be reduced

We must understand the risks; reduce unacceptable risks; and demonstarte this reduction.

High level of documentation.

Hazard and Risk Analysis

The standard requires that hazard and risk assessment should be carried out:

'The EUC (equipment under control) risk shall be evaluated, or estimated, for each determined hazardous event'.

Analysis of hazards:

framework based on 6 categories of occurrence and 4 of consequence, combined into a risk class matrix.

Hazard and Risk Analysis

Frequency

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	$< 10^{-7}$

Consequences

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

Hazard and Risk Analysis

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

Class I: Intolerable in any circumstance;
Class II: Undesirable and 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: Negligible (acceptable as it stands, though it may need to be monitored).

Hazard and Risk Analysis

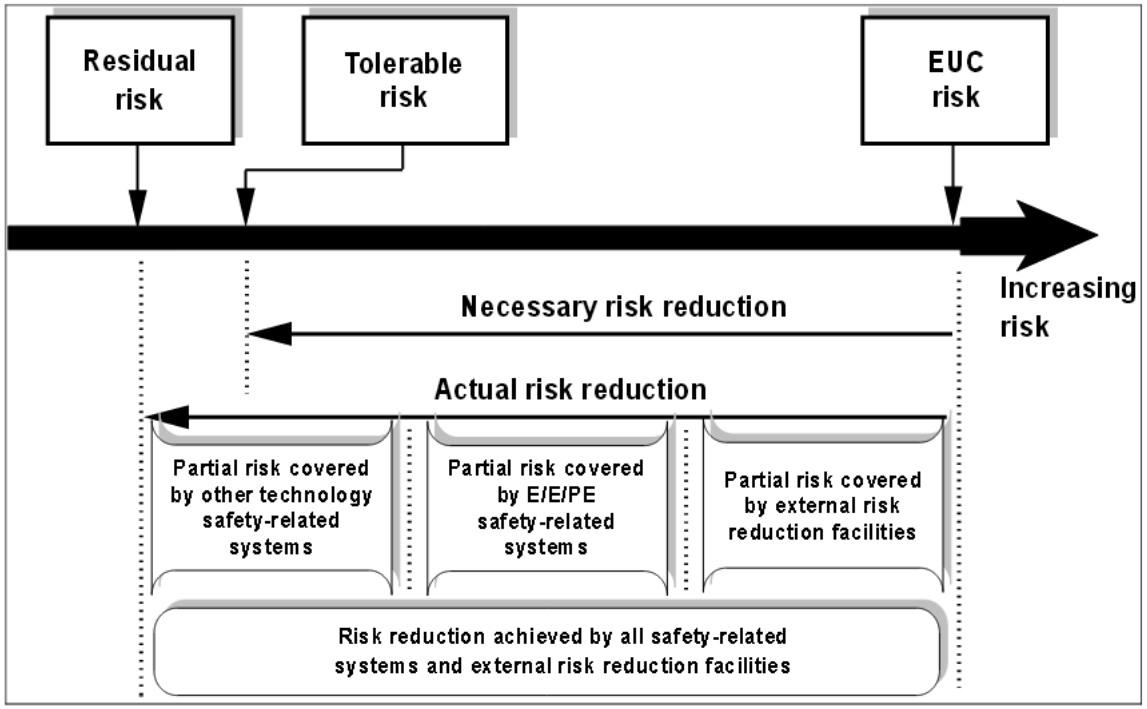
EUC risk = risk araising from Equipment Under Control or from its interaction with the EUC control system

Risk = hazard Frequency x Consequences

Risk reduction: in the hazard and risk analysis, hazardous events are identified and the necessary risk reduction for these events determined.

Tolerable risk: risk which is accepted in context based on the current values of society

Determining Risk Reduction



Let us consider a specific hazardous event, E, and suppose one has determined the EUC risk of E and the tolerable risk of E (in other words, what risk "society accepts" of E). Suppose further than the EUC risk of E is higher than the tolerable risk of E. Then one must take steps to ensure that the risk of E in the overall system S is reduced to at most the tolerable risk of E. The means envisaged by IEC 61508 for the risk reduction in the E/E/PE part is the introduction of functions which specifically reduce the risk of E, so that the risk of E in the operation of the system S′, where

- S′ = EUC enhanced with the introduced functions

is at or below the tolerable risk of E. The risk of E in the operation of S′ is called

- **Residual risk**: risk remaining after protective measures have been taken

Tools to evalaute risks

As particular tools are used FMEDA and Markov models. Failure modes and effects analysis (FMEA) is a way to document the system being considered using a systematic approach to identify and evaluate the effects of component failures and to determine what could reduce or eliminate the chance of failure. An FMEDA extends the FMEA techniques to include on-line diagnostic techniques and identify failure modes relevant to safety instrumented system design.

Safety integrity level - SIL

Safety Integrity: probability of safety related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

SIL: discrete level for specifying the safety integrity requirements

IEC 61508 standard: four SILs are defined, with SIL 4 being the most dependable and SIL 1 being the least.

The requirements for a given SIL are not consistent among all of the functional safety standards.

A SIL is determined based on a number of quantitative factors in combination with qualitative factors such as development process and safety life cycle management.

Safety integrity level - SIL

For on demand operation

Safety integrity level (SIL)	Low demand mode of operation (average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

For continuous operation

Safety integrity level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Safety integrity level - SIL

Certification schemes are used to establish whether a device meets a particular SIL.

The requirements of these schemes can be met either by establishing a rigorous development process, or by establishing that the device has sufficient operating history to argue that it has been proven in use.

A fundamental disquiet with the notion of SIL used in the standard is the association of a SIL with a set of recommended development techniques, for example, whether the use of formal methods is or is not recommended. So, for example, the use of *formal methods such as CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z* is "*recommended*", but "*only exceptionally, for some very basic components only*" for SIL 3

There is a wide range of methods applied to the analysis of hazards and risk around the world and an overview is provided in both IEC/EN 61511 and IEC/EN 61508. These methods include techniques such as

HAZOP	**HAZ**ard and **OP**erability study
FME(C)A	**F**ailure **M**ode **E**ffect (and **C**riticality) **A**nalysis
FMEDA	**F**ailure **M**ode **E**ffect and **D**iagnostics **A**nalysis
ETA	**E**vent **T**ree **A**nalysis
FTA	**F**ault **T**ree **A**nalysis

and other study, checklist, graph and model methods.

COMPLIANCE

The IEC 61508 standard states: “To conform to this standard it shall be demonstrated that the requirements have been satisfied to the required criteria specified (for example safety integrity level) and therefore, for each clause or sub-clause, all the objectives have been met.”

Sample Documentation Structure (Annex A)

The documentation has to contain enough information to effectively perform each phase of the safety life cycle (Clause 7), manage functional safety (Clause 6), and allow functional safety assessments (Clause 8). However, IEC 61508 does not specify a particular documentation structure. Users have flexibility in choosing their own documentation structure as long as it meets the criteria described earlier. . An example set of documents for a safety life cycle project is shown in Table 3.

Safety requirements	Safety Requirements Specification (safety functions and safety integrity)
E/E/PES validation planning	Validation Plan
E/E/PES design and development E/E/PES architecture Hardware architecture Hardware module design Component construction and/or procurement	 Architecture Design Description (hardware and software); Specification (integration tests) Hardware Architecture Design Description; Detail Design Specification(s) Hardware modules; Report (hardware modules test)
Programmable electronic integration	Integration Report
E/E/PES operation and maintenance procedures	Operation and Maintenance Instructions
E/E/PES safety validation	Validation Report
E/E/PES modification	E/E/PES modification procedures; Modification Request; Modification Report; Modification Log
Concerning all phases	Safety Plan; Verification Plan and Report; Functional Safety Assessment Plan and Report

Table 3

Personnel Competency (Annex B)

IEC 61508 specifically states, “All persons involved in any overall, E/E/PES or software safety life cycle activity, including management activities, should have the appropriate training, technical knowledge, experience and qualifications relevant to the specific duties they have to perform.” It is suggested that a number of things be considered in the evaluation of personnel. These are:

1. engineering knowledge in the application;
2. engineering knowledge appropriate to the technology;
3. safety engineering knowledge appropriate to the technology;
4. knowledge of the legal and safety regulatory framework;
5. the consequences of safety-related system failure;
6. the assigned safety integrity levels of safety functions in a project;
7. experience and its relevance to the job.

The training, experience, and qualifications of all persons should be documented. The Certified Functional Safety Expert (CFSE) program was designed to help companies show personnel competency in several different safety specialties.

Sector specific standards

Automotive application field

ISO/DIS 26262: Road vehicles – Functional safety

adaptation of IEC 61508 specific to the application sector of electrical and electronic systems in the road vehicle industry

Railways application field

CENELEC EN 50128: Railway applications — Software for railway control and protection systems

developed by the European Committee for Electrotechnical Standardization (CENELEC), is part of a series of standards that represent the railway application-specific interpretation of the IEC 61508 standard series

Airborne Application Field

RTCA/DO-254

formally recognized by the Federal Aviation Agency (FDA) in 2005 as a means of compliance for the design of complex electronic hardware in airborne systems. Published by RTCA (Radio Technical Commission for Aeronautics)

The Nuclear Power Plant Application Field

IAEA safety standards series (INTERNATIONAL ATOMIC ENERGY AGENCY)
NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants: Safety Guide

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 through the use of instrumentation.

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 also for the design of non-complex subsystems or devices.

…….