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**.

For the software ……… 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*.

The need for standards

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

- all the processes must be followed

- staff must be trained and motivated

- budget must be sufficient

- managerial support is needed

- ………………….

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

the objective of functional safety is to reduce the probability of failures at a given acceptable rate in presence of malfunctioning behaviors.

The standard provides a reference lifecycle to achieve **functional safety** of E/E/PE systems, based on

-hazards identification/mitigation
- and risk analysis.

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 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

Random hardware *failures that can occur unpredictably during the lifetime of a hardware element, and that follow a probability distribution.*

Systematic failures *“failure related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.”*

The IEC 61508

Central to the standard are the concepts of

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

The standard guides system designers and developers in what they need to do in order to claim that their systems were acceptably safe for their intended uses

Instead of building a system as well as possible, and then assuming that it would be safe, the standard calls for a risk-based approach, in which the safety activities should be based on an understanding of the risks posed by the system

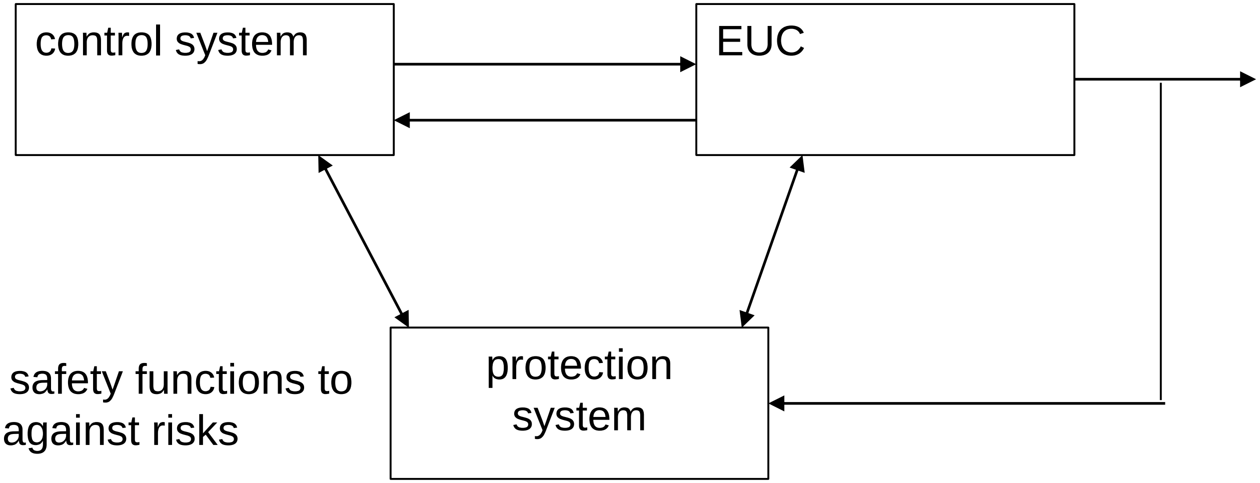
The standard covers the complete safety life cycle, and may need interpretation to develop **sector specific standards**.
It has its origins in the process control industry.

The IEC 61508

IEC 61508 is a common framework on which to design products and systems for safety-related applications

EUC (equipment under control)

identification of hazards + risks arising from the EUC or its interaction with the control system



Identify safety functions to protect against risks

Functional safety:
safety of the EUC that depends on the risk reduction measures

Safety requirements specification: specification of all the requirements of the safety functions for risk reduction

The IEC 61508

Hazard identification consists of an attempt to identify the potential sources of harm

An EUC and its control system may pose many hazards. The risk of unidentified hazards will not be evaluated or reduced.

Identification of hazards (experts in the domain):

- during normal operations
- arising from failures
- foreseeable misuse

Hazard analysis

- chain of the cause and effects of identified hazards and possible accidents
- derive the risk attached to each hazard

Hazardous events:

- Car unintentionally accelerates
- Gear is unintentionally switched to neutral
- Airbags are activated too late

The IEC 61508

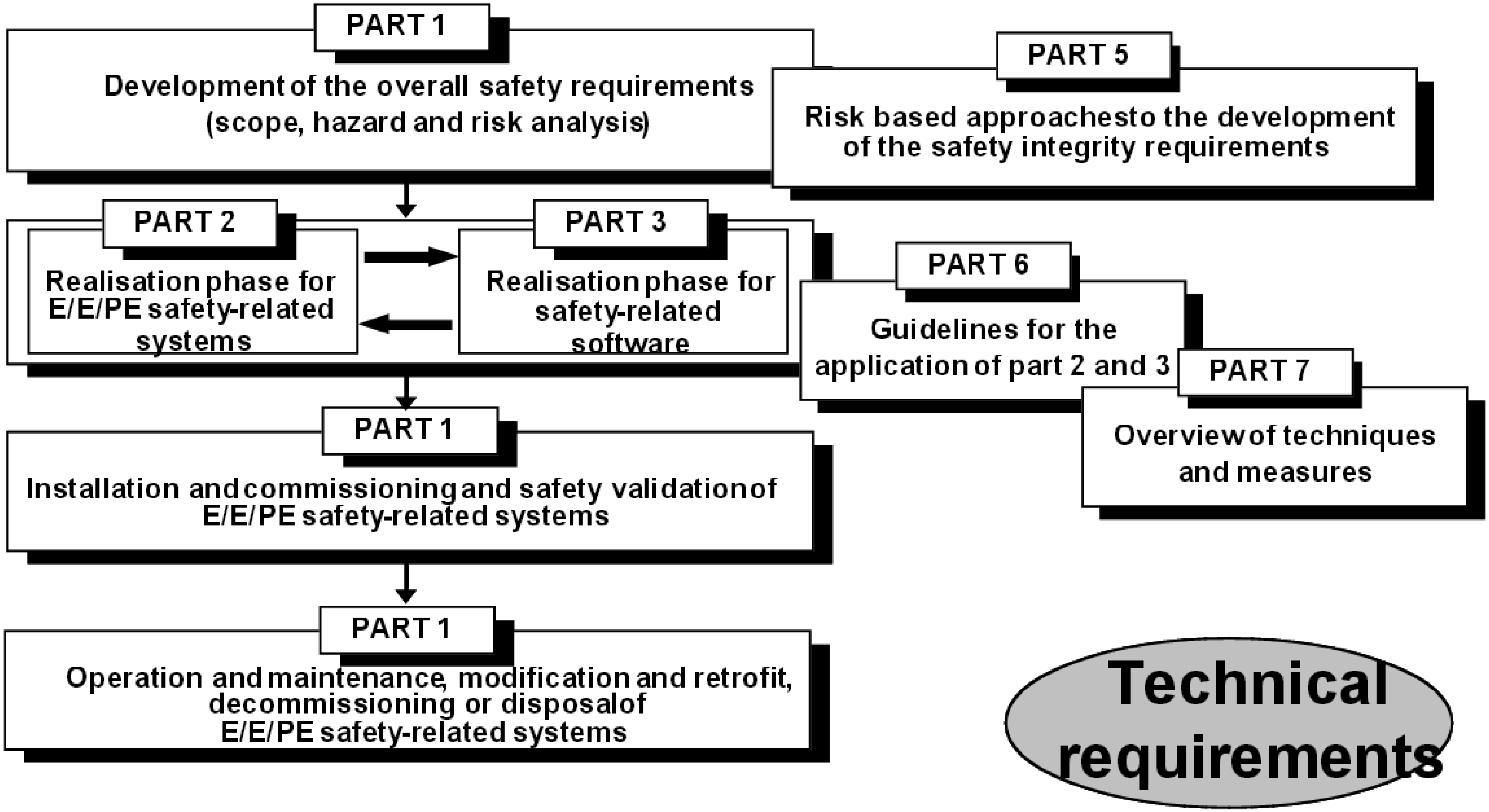
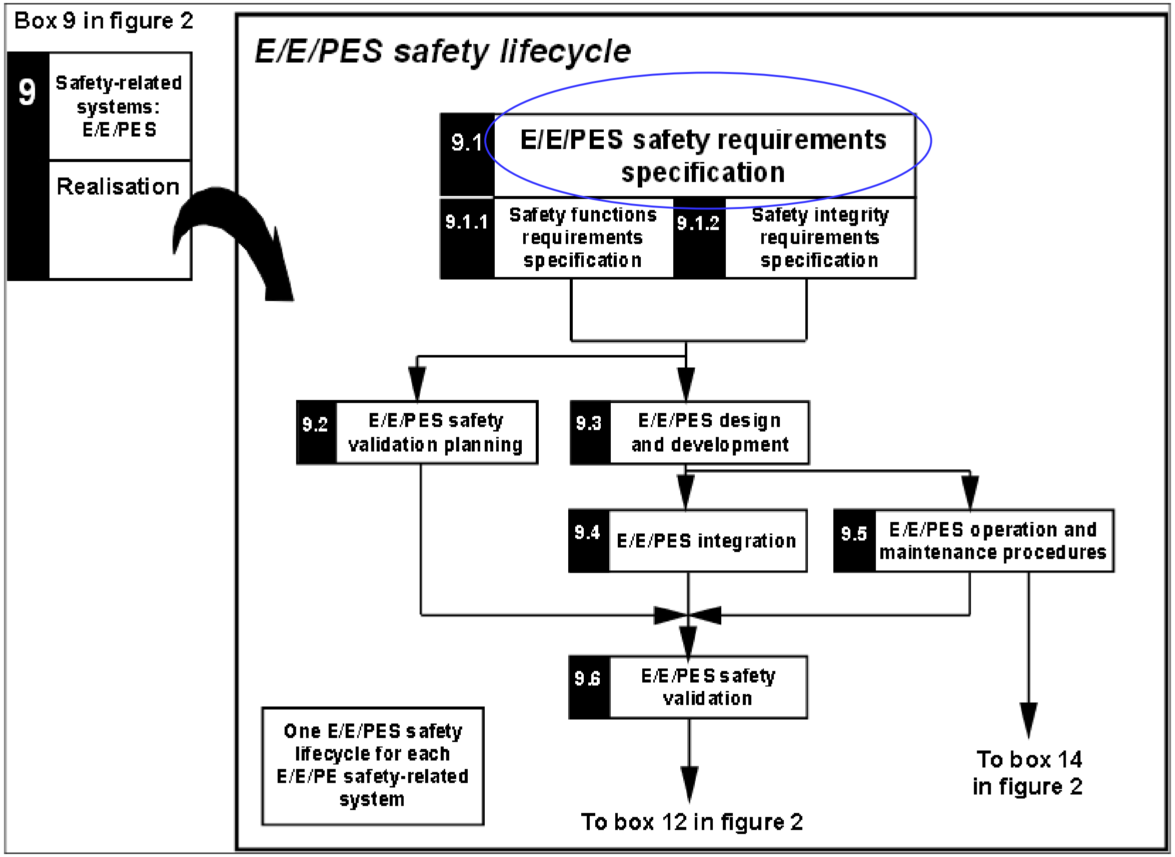

PART 1
Development of the overall safety requirements (scope, hazard and risk analysis)
PART 5
Risk based approaches to the development of the safety integrity requirements
PART 2
Realisation phase for E/E/PE safety-related systems
PART 3
Realisation phase for safety-related software
PART 6
Guidelines for the application of part 2 and 3
PART 7
Overview of techniques and measures
PART 1
Installation and commissioning and safety validation of E/E/PE safety-related systems
PART 1
Operation and maintenance, modification and retrofit, decommissioning or disposal of E/E/PE safety-related systems
Technical requirements

Figure 1: Technical requirements of IEC 61508.

Safety requirements:

Safety lifecycle

forces safety to be addressed independently of functional issues (safety validated independent of functionality under all operating and failure conditions)


Box 9 in figure 2
9
Safety-related systems: E/E/PES
Realisation
E/E/PES safety lifecycle
9.1
E/E/PES safety requirements specification
9.1.1
Safety functions requirements specification
9.1.2
Safety integrity requirements specification
9.2
E/E/PES safety validation planning
9.3
E/E/PES design and development
9.4
E/E/PES integration
9.5
E/E/PES operation and maintenance procedures
9.6
E/E/PES safety validation
One E/E/PES safety lifecycle for each E/E/PE safety-related system
To box 12 in figure 2
To box 14 in figure 2

Safety requirements: requirements defined for the purpose of risk reduction

Safety requirements: provided by means of safety functions

Safety functions: implemented in safety related systems

A safety requirement can be implemented by a combination of safety functions (different technologies)

Safety integrity requirements: a measure of the rate of unsafe failures

Safety lifecycle

- Consider safety implications of EUC and its control system
- Identify risks and tolerability criteria
- Safety requirements for for risk reduction
- Translation of safety requirements into safety functions
- Implementation of safety functions
- Validation of the safety function

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:

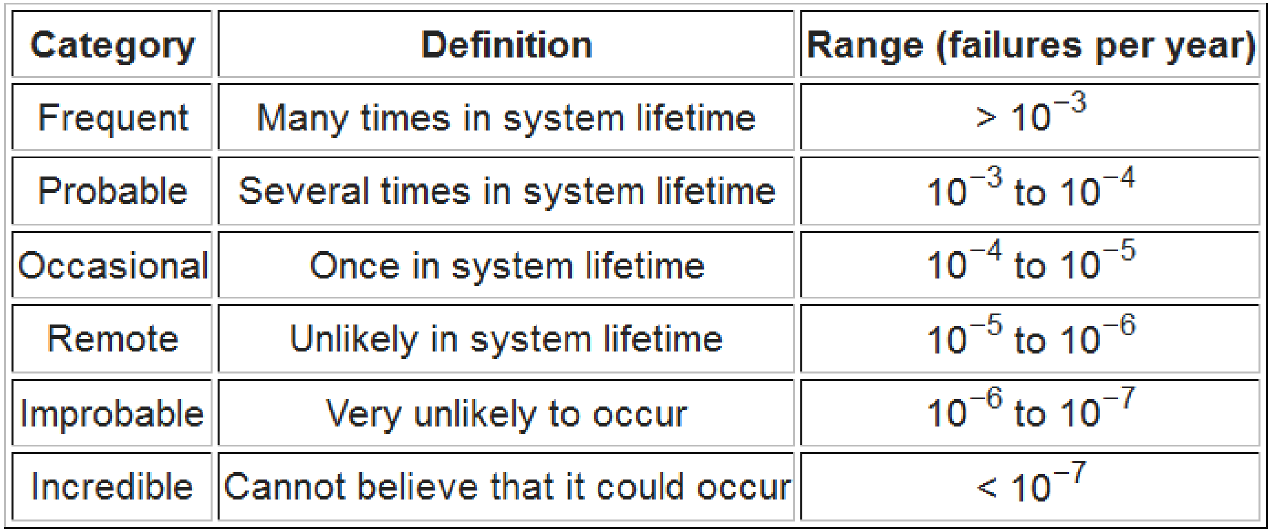
'The EUC (equipment under control) risk shall be evaluated, or estimated, for each determined hazardous event'.

Analysis of hazards:

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

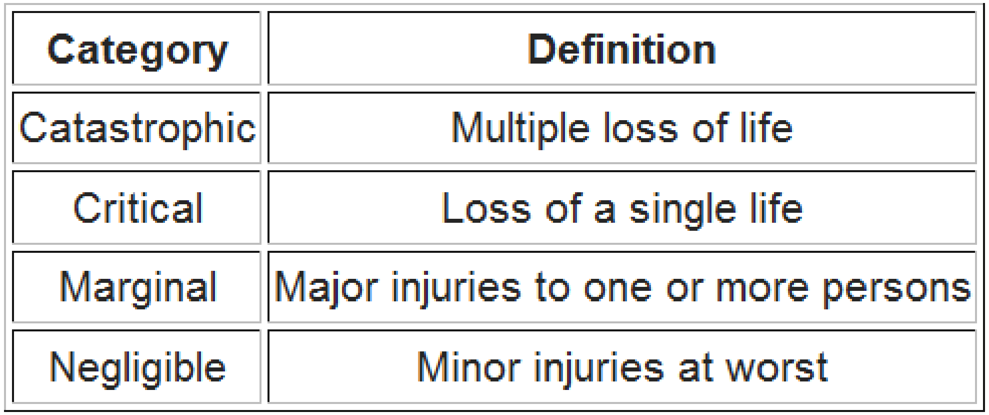
Hazard and Risk Analysis

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	$< 10^{-7}$

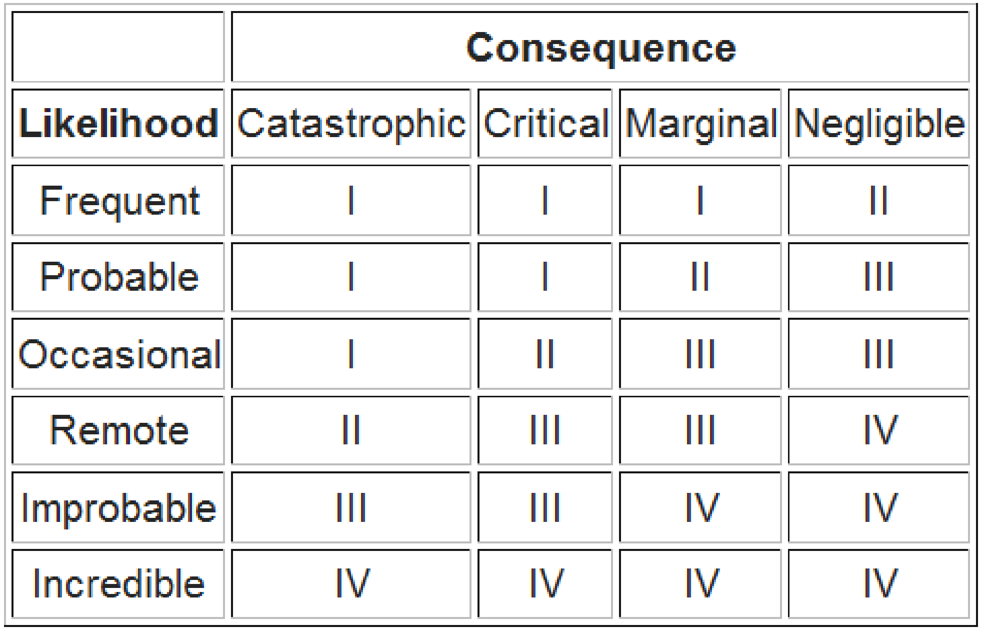
Consequences



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

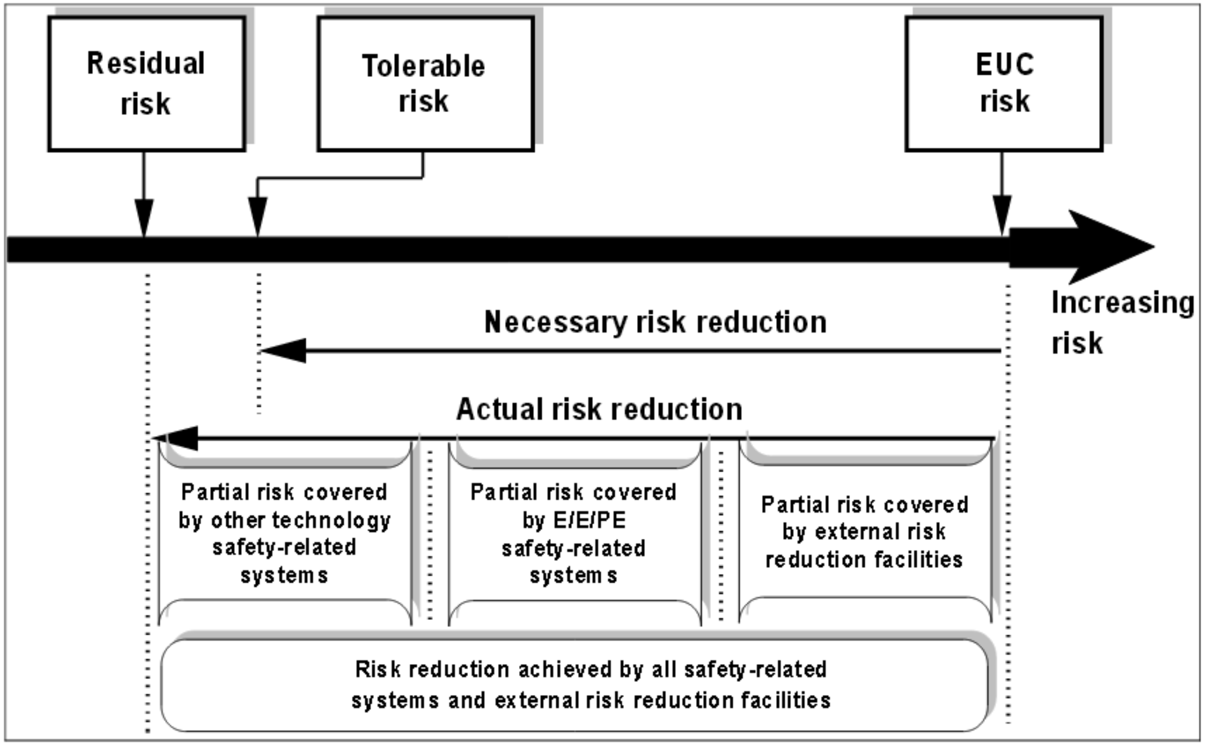
EUC risk = risk araising from Equipment Under Control or from its interaction with the EUC control system

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


Residual risk
Tolerable risk
EUC risk
Increasing risk
Necessary risk reduction
Actual risk reduction
Partial risk covered by other technology safety-related systems
Partial risk covered by E/E/PE safety-related systems
Partial risk covered by external risk reduction facilities
Risk reduction achieved by all safety-related systems and external risk reduction facilities

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.

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.

Safety integrity level - SIL

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

-> a measure of the rate of unsafe failures

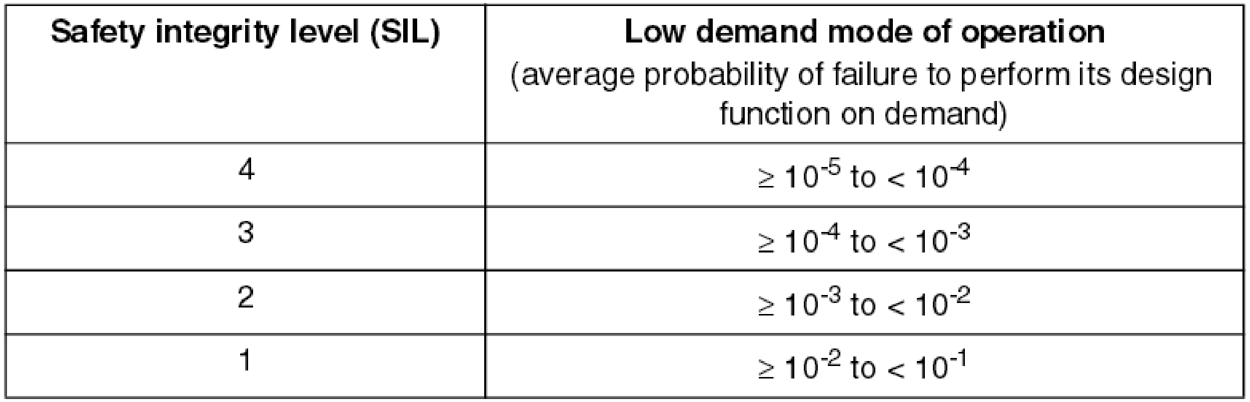
SIL: discrete level for specifying the safety integrity requirements of the safety functions to be allocated to the system

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

Specify the SIL of the safety requirements for each risk reduction

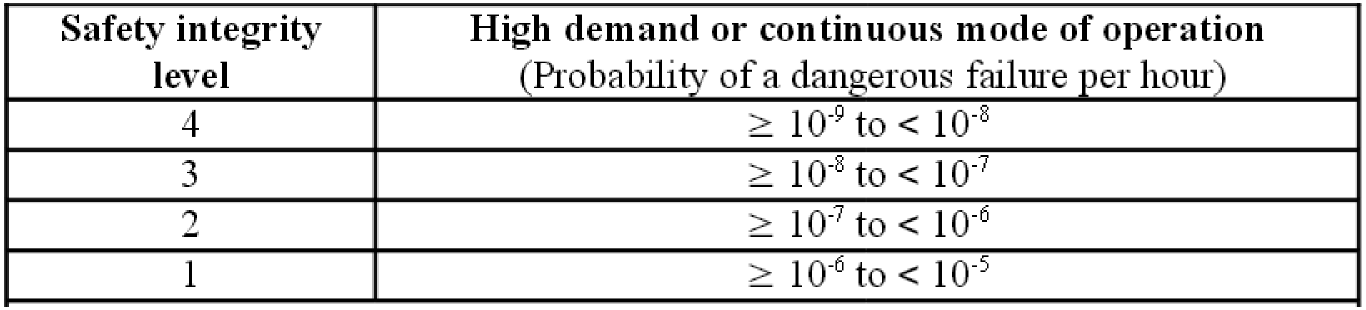
Safety integrity level - SIL

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



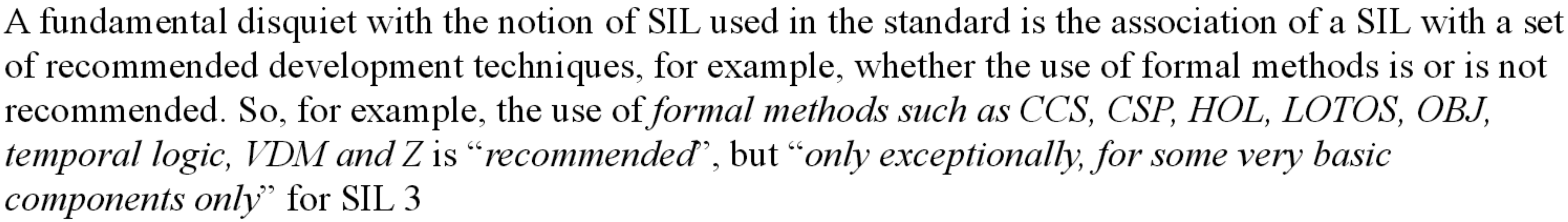
Safety integrity level	**High demand or continuous mode of operation** (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

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 (for complex system and sw), or by establishing that the device has sufficient operating history to argue that it has been proven in use (for electromechanical hw).

When evidence of the rate of dangerous failures cannot be determined, the SIL is use to define the rigour to be used in the development process



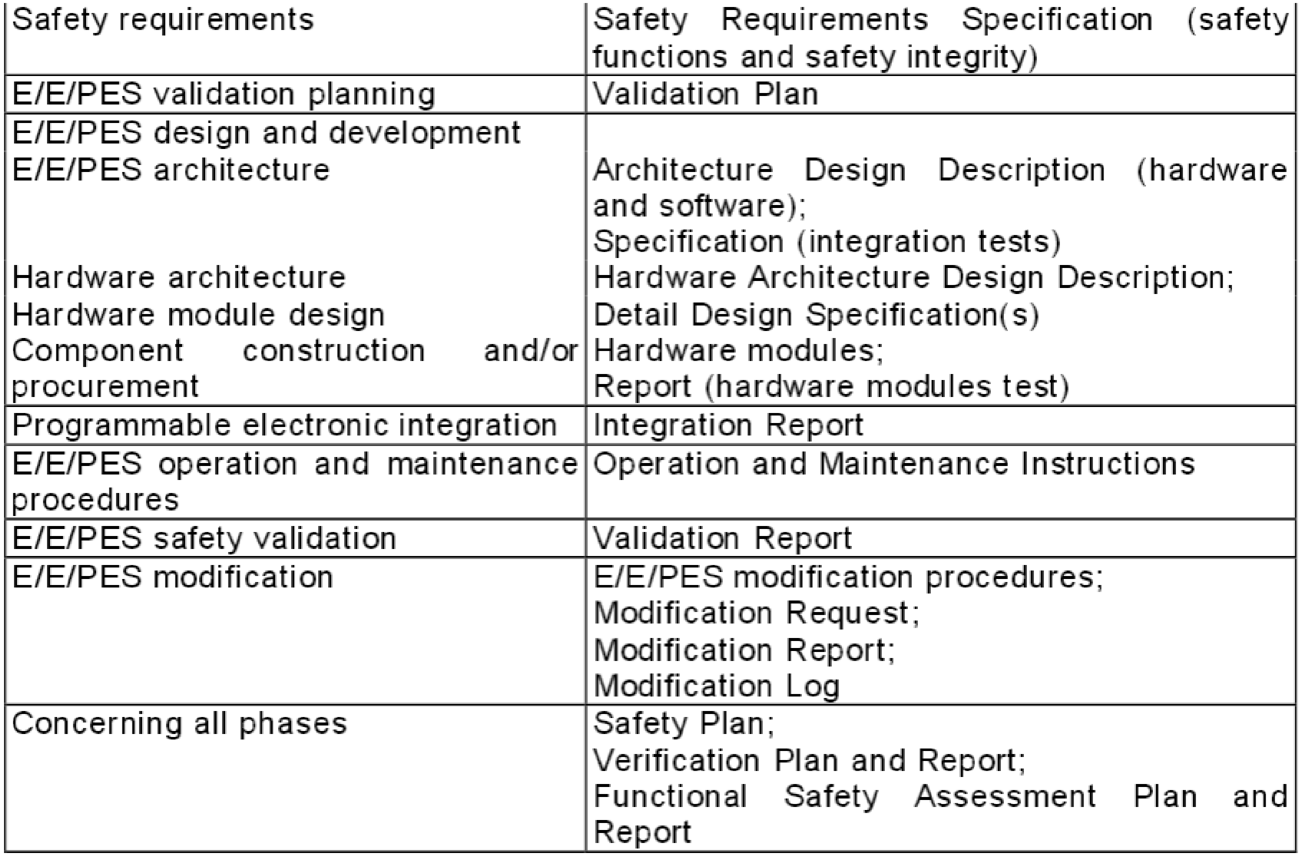
A fundamental disquiet with the notion of SIL used in the standard is the association of a SIL with a set of recommended development techniques, for example, whether the use of formal methods is or is not recommended. So, for example, the use of *formal methods such as CCS, CSP, HOL, LOTOS, OBJ, temporal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

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	Architecture Design Description (hardware and software); Specification (integration tests)
Hardware architecture	Hardware Architecture Design Description;
Hardware module design	Detail Design Specification(s)
Component construction and/or procurement	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)

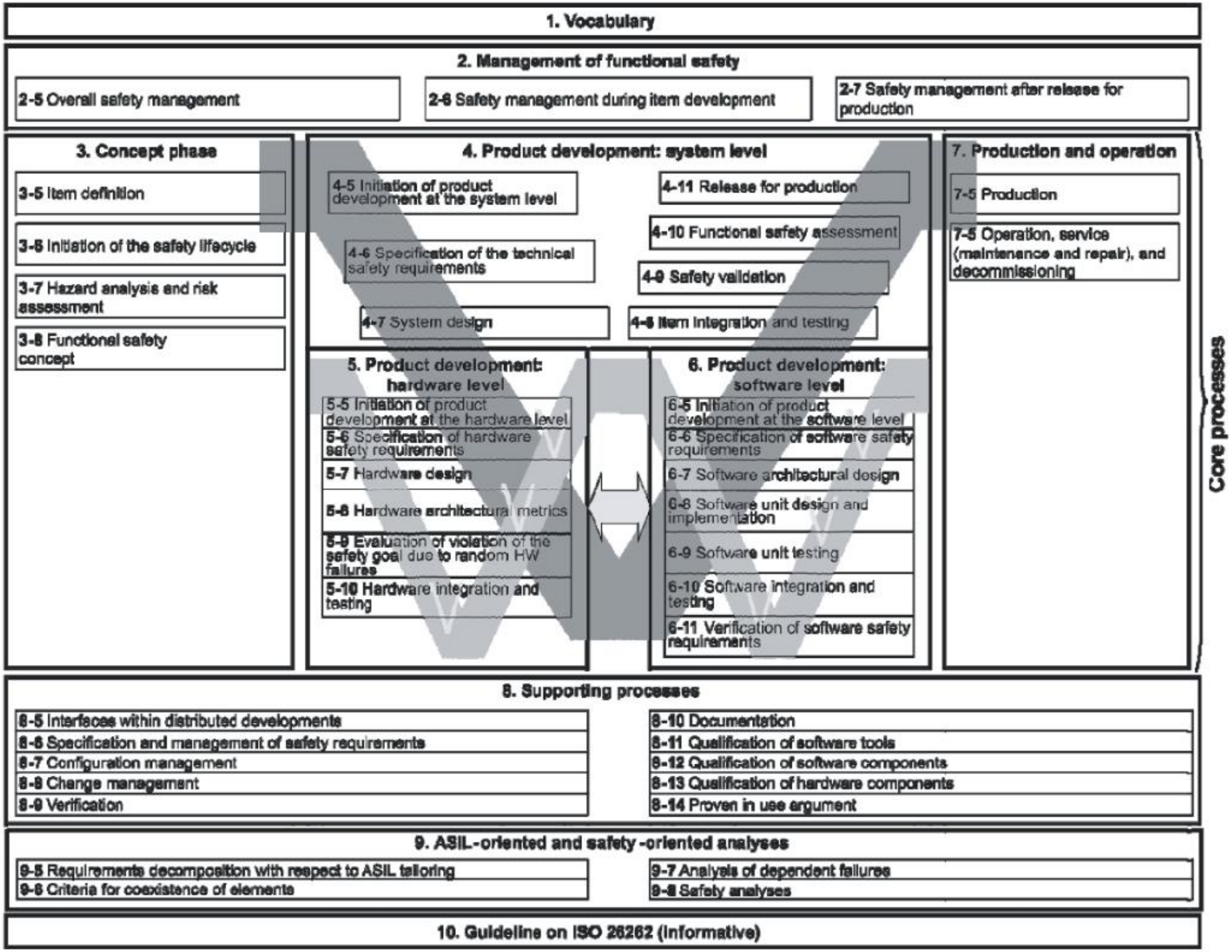
The Nuclear Power Plant Application Field
IAEA safety standards series (INTERNATIONAL ATOMIC ENERGY AGENCY)
NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants: Safety Guide

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.

…………………………

ISO/DIS 26262: Road vehicles – Functional safety



1. Vocabulary

2. Management of functional safety

2-5 Overall safety management

2-6 Safety management during item development

2-7 Safety management after release for production

3. Concept phase

3-5 Item definition

3-6 Initiation of the safety lifecycle

3-7 Hazard analysis and risk assessment

3-8 Functional safety concept

4. Product development: system level

4-5 Initiation of product development at the system level

4-6 Specification of the technical safety requirements

4-7 System design

4-8 Item integration and testing

4-9 Safety validation

4-10 Functional safety assessment

4-11 Release for production

5. Product development: hardware level

5-5 Initiation of product development at the hardware level

5-6 Specification of hardware safety requirements

5-7 Hardware design

5-8 Hardware architectural metrics

5-9 Evaluation of violation of the safety goal due to random HW failures

5-10 Hardware integration and testing

6. Product development: software level

6-5 Initiation of product development at the software level

6-6 Specification of software safety requirements

6-7 Software architectural design

6-8 Software unit design and implementation

6-9 Software unit testing

6-10 Software integration and testing

6-11 Verification of software safety requirements

7. Production and operation

7-5 Production

7-6 Operation, service (maintenance and repair), and decommissioning

Core processes

8. Supporting processes

8-5 Interfaces within distributed developments

8-6 Specification and management of safety requirements

8-7 Configuration management

8-8 Change management

8-9 Verification

8-10 Documentation

8-11 Qualification of software tools

8-12 Qualification of software components

8-13 Qualification of hardware components

8-14 Proven in use argument

9. ASIL-oriented and safety-oriented analyses

9-5 Requirements decomposition with respect to ASIL tailoring

9-6 Criteria for coexistence of elements

9-7 Analysis of dependent failures

9-8 Safety analyses

10. Guideline on ISO 26262 (informative)

2. Management of Functional Safety

The following clauses are identified:

Overall Safety Management

the outcomes of this clause are a set of organization-specific rules and processes for functional safety, evidence for the competence and qualification of the persons in charge of carrying out the activities and evidence of a proper quality management system.

Safety Management during Item Development

this clause aims at the definition of safety management roles and responsibilities, and the definition of the requirements on the safety management, regarding the development phases.

Safety management after release for production

this clause defines the responsibility of the organizations and persons responsible for functional safety after release for production. This concerns activities for maintaining the functional safety of the item in the lifecycle phases after release.

3. Concept Phase

The following clauses are identified:

Item definition, Initiation of the safety lifecycle

The goals of these clauses is to define and describe the item and support an adequate under-standing so that each activity of the safety lifecycle can be performed

Hazard Analysis and Risk Assessment

The hazards of the item shall be systematically determined, with techniques such as checklists and FMEA, in terms of the conditions or events that can be observed at the vehicle level. The effects of hazards shall be identified for relevant operational situations. All identified hazards shall be classified with respect to severity, probability of exposure or controllability. ASIL shall be determined for each hazardous event using the proper combination of the previous parameters. A safety goal shall be determined for each hazard, and expressed in terms of functional objectives.

Functional Safety Concept

The goals of this clause is to derive the functional safety requirements, from the safety goals, and to allocate them to the preliminary architectural elements so to ensure required safety

4. Product Development: System Level

Basically, the objectives of this part are:

- determine and plan the functional safety activities during the subphases of the system development, included in the safety plan.

- develop the technical safety requirements, which refine the functional safety concept considering the preliminary architectural design.

- verify through analysis that technical safety requirements comply to the functional safety requirements. The response of the system or any of its elements to stimuli, including failures shall be specified for each technical requirement, in combination for each possible operating state.

5. Product Development: Hardware Level

This part consists of the following clauses:

Initiation of Product Development at the Hardware Level

to determine and plan the functional safety activities during the individual sub-phases of hardware development, which is included in the safety plan. This activity includes the Hardware implementation of the technical safety concept; the Analysis of potential faults and their effects; and the Coordination with software development.

Specification of Hardware safety requirements

Hardware design

Hardware Architectural Metrics

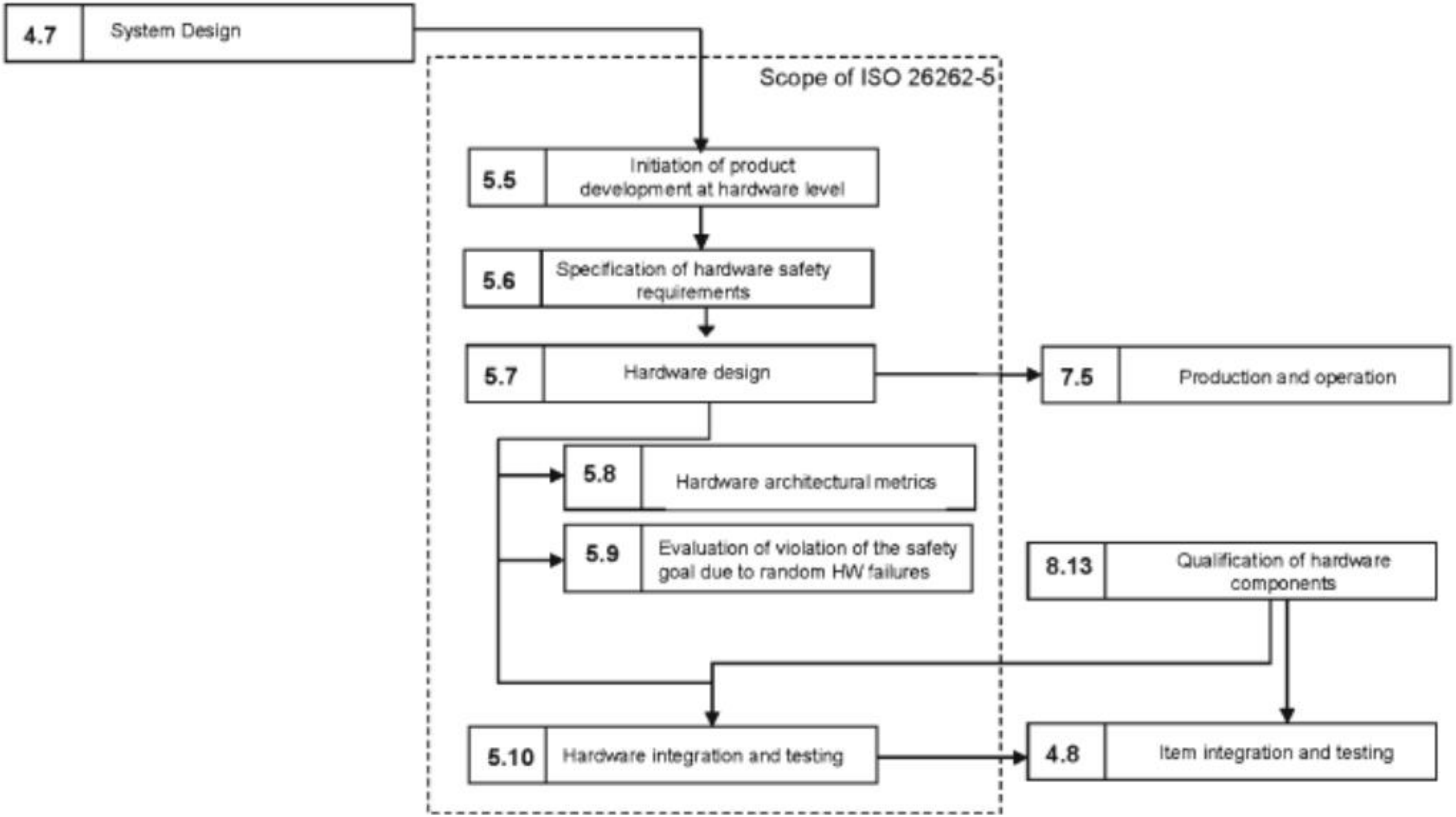
to infer if the residual risk of safety goal violation, due to random hardware failures of the item, is sufficient low

Evaluation of Violation of the Safety Goal due to Random HW Failures

to infer if the residual risk of safety goal violation, due to random hardware failures of the item, is sufficient low

Hardware integration and testing.

ISO 26262-5: Product development: hardware



4.7 System Design

Scope of ISO 26262-5

5.5 Initiation of product development at hardware level

5.6 Specification of hardware safety requirements

5.7 Hardware design

7.5 Production and operation

5.8 Hardware architectural metrics

5.9 Evaluation of violation of the safety goal due to random HW failures

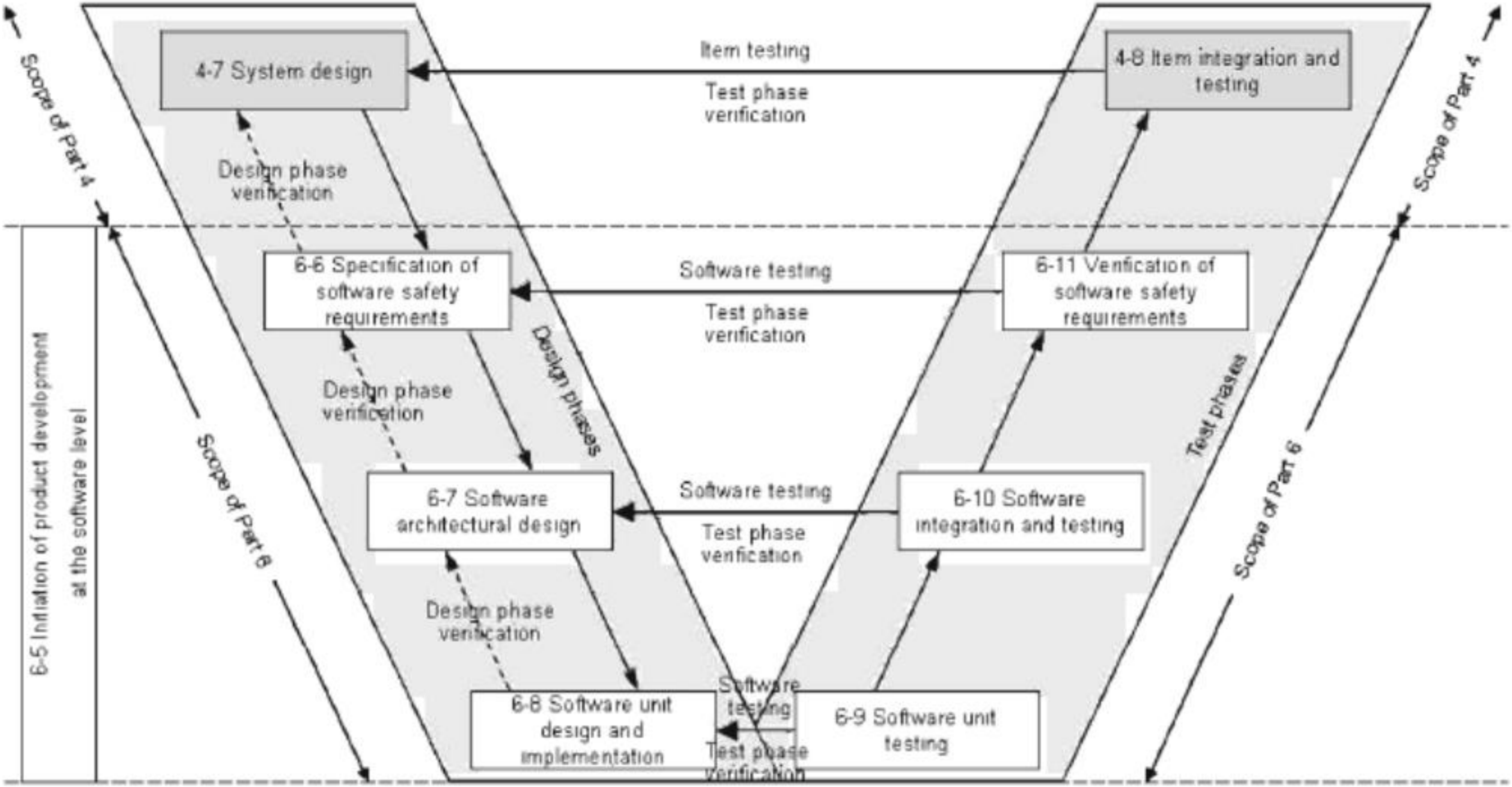
8.13 Qualification of hardware components

5.10 Hardware integration and testing

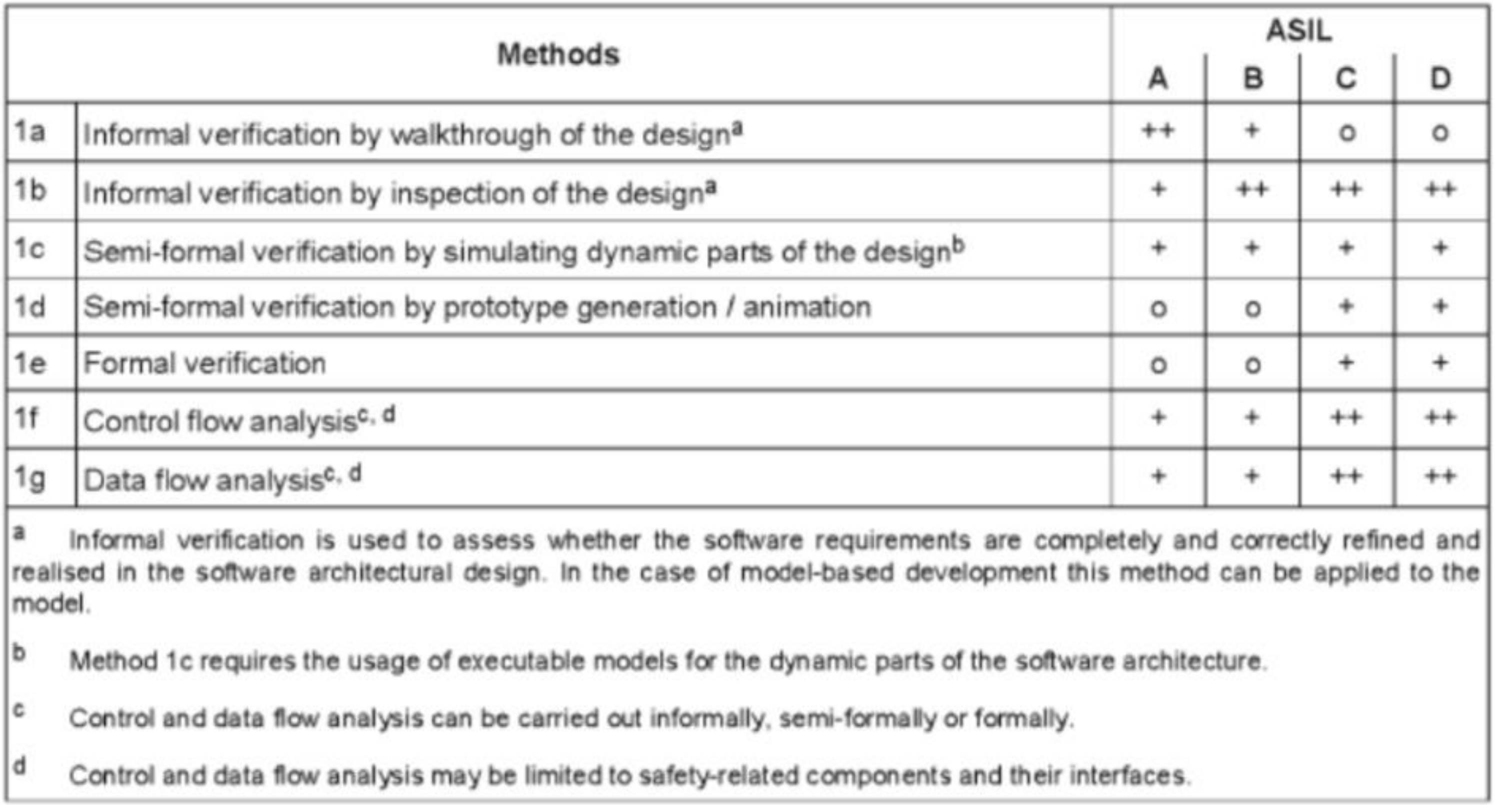
4.8 Item integration and testing

6. Product Development: Software Level

Reference phase model for the software development process for an item



Scope of Part 4
4-7 System design
Item testing
Test phase verification
4-8 Item integration and testing
Scope of Part 4
Design phase verification
6-5 Initiation of product development at the software level
6-6 Specification of software safety requirements
Software testing
Test phase verification
6-11 Verification of software safety requirements
Design phases
Test phases
Design phase verification
Scope of Part 6
Scope of Part 6
6-7 Software architectural design
Software testing
Test phase verification
6-10 Software integration and testing
Design phase verification
6-8 Software unit design and implementation
Software testing
Test phase verification
6-9 Software unit testing



Methods		ASIL			
		A	B	C	D
1a	Informal verification by walkthrough of the design[a]	++	+	o	o
1b	Informal verification by inspection of the design[a]	+	++	++	++
1c	Semi-formal verification by simulating dynamic parts of the design[b]	+	+	+	+
1d	Semi-formal verification by prototype generation / animation	o	o	+	+
1e	Formal verification	o	o	+	+
1f	Control flow analysis[c, d]	+	+	++	++
1g	Data flow analysis[c, d]	+	+	++	++

[a] Informal verification is used to assess whether the software requirements are completely and correctly refined and realised in the software architectural design. In the case of model-based development this method can be applied to the model.

[b] Method 1c requires the usage of executable models for the dynamic parts of the software architecture.

[c] Control and data flow analysis can be carried out informally, semi-formally or formally.

[d] Control and data flow analysis may be limited to safety-related components and their interfaces.

"++" The method is highly recommended for this ASIL.

"+" The method is recommended for this ASIL.

"o" The method has no recommendation for or against its usage for this ASIL.

Methods for the verification of the software architectural design

7. Production and Operation

This part specifies requirements on production, operation, service, and decommissioning.

In particular
the Production aims at developing a production plan for safety-related products and to ensure that the required functional safety is achieved during the production process.

8. Supporting Processes

This part consists of the following clauses:

- Interfaces within distributed developments
- Specification and management of safety requirements
- Configuration management
- Change management
- Verification
- Documentation
- Qualification of software tools
- Qualification of software components
- Qualification of hardware components
- Proven in use argument.

The objective of Verification is to ensure that all work products are correct, complete, and consistent; and that all work products meet the requirements of ISO 26262.

The objective of Documentation is to develop a documentation management strategy so that every phase of the entire safety lifecycle can be executed effectively and can be reproduced.

9. ASIL-oriented and Safety-oriented Analyses

This part includes the activities on:

Requirements decomposition with respect to ASIL tailoring,

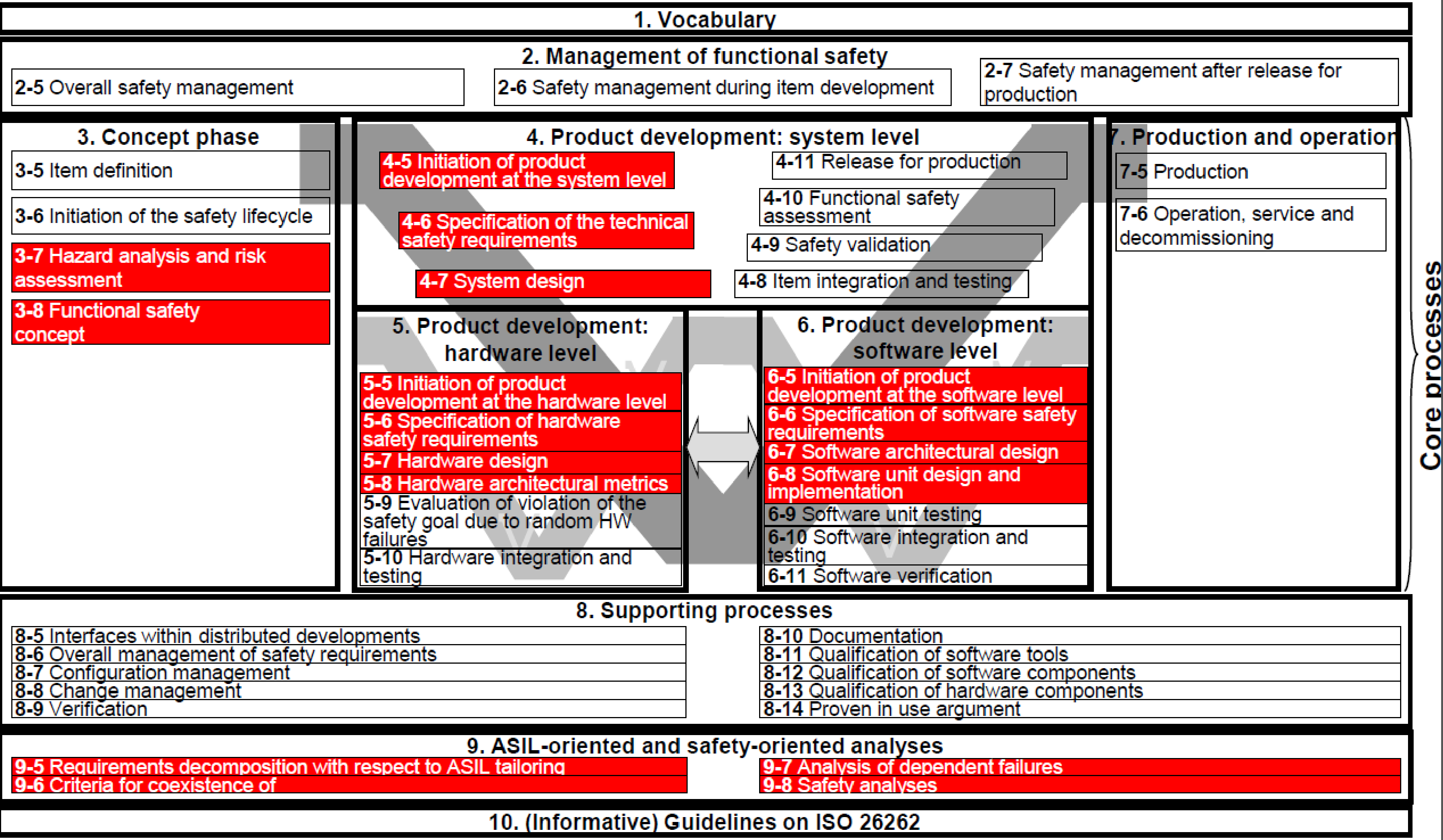
Criteria for coexistence of elements

Analysis of Dependent Failures and Safety Analyses

> the evaluation for dependent failures is fundamental in order to identify any single cause that could bypass or invalidate the independence or freedom from interference between elements of an item required to comply with its safety goals.

SAFE project

SAFE – Motivation
Scope with respect to ISO26262



1. Vocabulary

2. Management of functional safety
- 2-5 Overall safety management
- 2-6 Safety management during item development
- 2-7 Safety management after release for production

3. Concept phase
- 3-5 Item definition
- 3-6 Initiation of the safety lifecycle
- 3-7 Hazard analysis and risk assessment
- 3-8 Functional safety concept

4. Product development: system level
- 4-5 Initiation of product development at the system level
- 4-6 Specification of the technical safety requirements
- 4-7 System design
- 4-8 Item integration and testing
- 4-9 Safety validation
- 4-10 Functional safety assessment
- 4-11 Release for production

5. Product development: hardware level
- 5-5 Initiation of product development at the hardware level
- 5-6 Specification of hardware safety requirements
- 5-7 Hardware design
- 5-8 Hardware architectural metrics
- 5-9 Evaluation of violation of the safety goal due to random HW failures
- 5-10 Hardware integration and testing

6. Product development: software level
- 6-5 Initiation of product development at the software level
- 6-6 Specification of software safety requirements
- 6-7 Software architectural design
- 6-8 Software unit design and implementation
- 6-9 Software unit testing
- 6-10 Software integration and testing
- 6-11 Software verification

7. Production and operation
- 7-5 Production
- 7-6 Operation, service and decommissioning

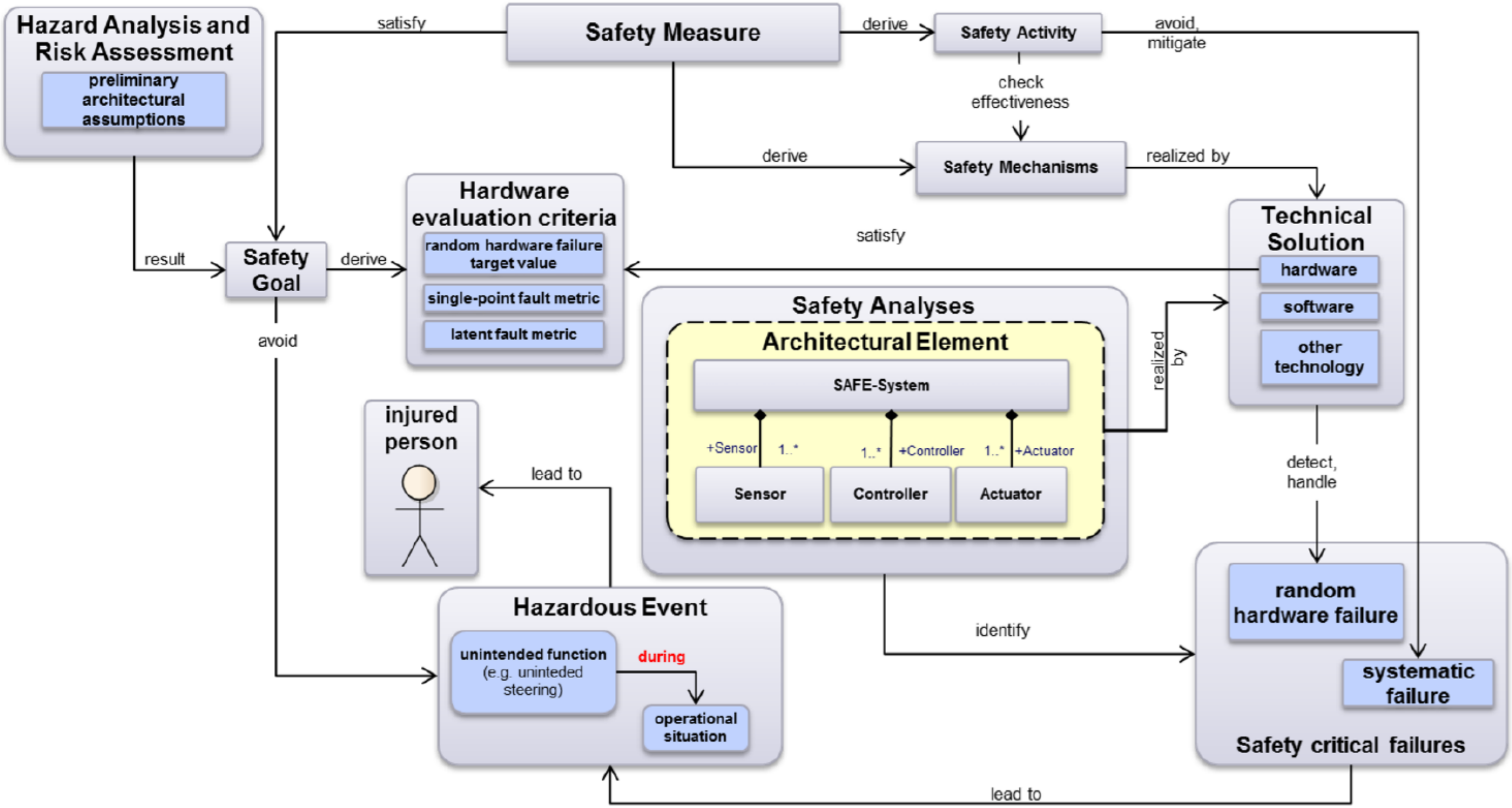
Core processes

8. Supporting processes
- 8-5 Interfaces within distributed developments
- 8-6 Overall management of safety requirements
- 8-7 Configuration management
- 8-8 Change management
- 8-9 Verification
- 8-10 Documentation
- 8-11 Qualification of software tools
- 8-12 Qualification of software components
- 8-13 Qualification of hardware components
- 8-14 Proven in use argument

9. ASIL-oriented and safety-oriented analyses
- 9-5 Requirements decomposition with respect to ASIL tailoring
- 9-6 Criteria for coexistence of
- 9-7 Analysis of dependent failures
- 9-8 Safety analyses

10. (Informative) Guidelines on ISO 26262

SAFE project



System development and Safety analysis in automotive