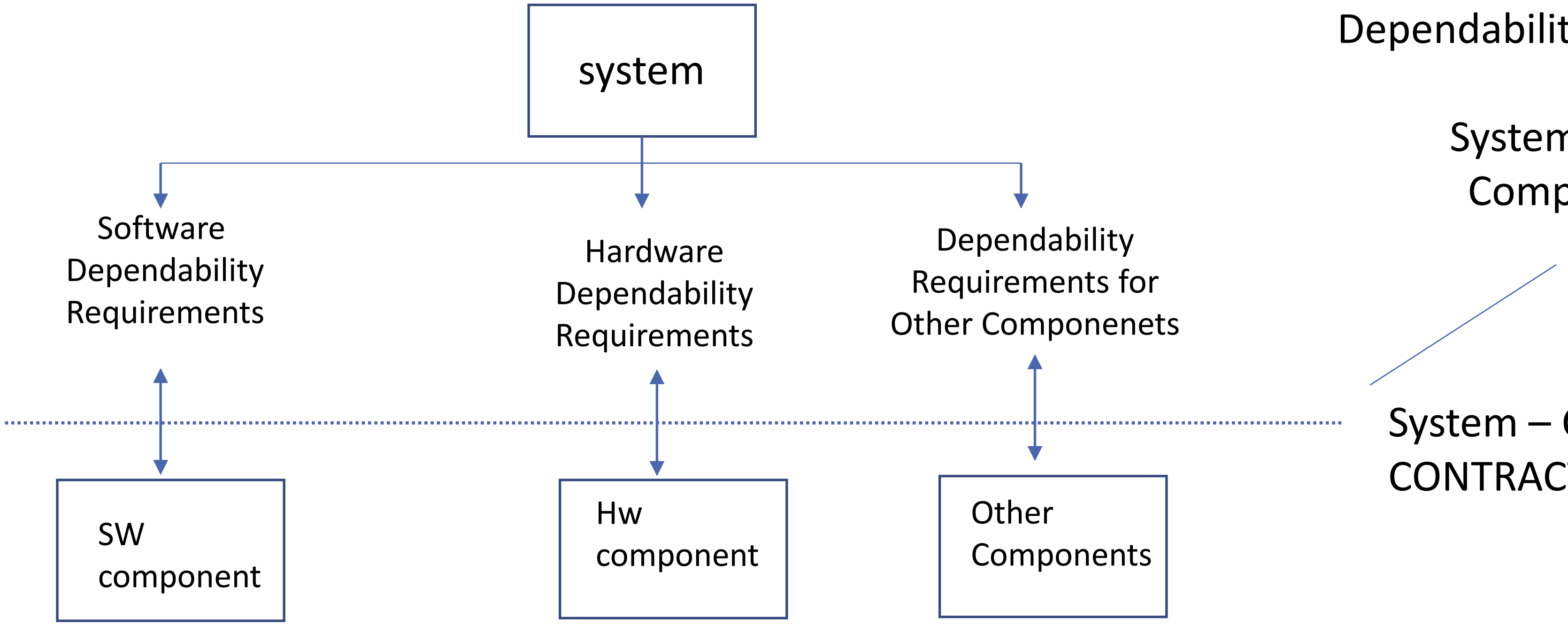
Dependability Assessment

Dependability Assessment

Dependability assessment:

we have to show that the system will meet dependability requirements (often specified in quantitative terms)


system
Software Dependability Requirements
Hardware Dependability Requirements
Dependability Requirements for Other Componenets
SW component
Hw component
Other Components

Dependability CONTRACT concept between System Engineers and Computer Engineers

System – Components CONTRACT Interface

J. Knight. Fundamentals of Dependable Computing. Chapman& Hall, 2012.

Dependability assessment of computer systems

For design faults, quantitative assessment is difficult

Estimates can be achieved for system with low dependability requirements

There is always the concern that

> *“data about rates of failures might not reflect that which is obtained in practice,*
> *because of the operational environment used for testing might not be the*
> *same as the environment where the system is deployed”*

Dependability assessment methods:

- Quantitative assessment: probabilistic assessment with direct measurement or by modelling
- Prescriptive standards: assessment on the process by which an entity is built
- Rigorous argument: an argument is created that an entity is suitable for its intended use

Prescriptive standards

Prescriptive standards regulates sw for use in safety critical systems
Such sw is required to be submitted for approval that it has been produced using a prescriptive standards

There is no basis for the assumption that quantitive dependability requirements will be met following a documented set of development procedures.

For example, no guarantee that developers follow the standard precisely as intended

However, the use of standards in industry has proven successfully: large number of systems has been proved to have an acceptable failure rate.

Prescriptive standards

Approach chosen by many government agencies:

requiring prescriptive standards

A prescriptive standard addresses major aspects of dependability

- dictates development practice
- requires the use of techniques generally accepted to be usefull to improve dependability

  (a prescriptive standard for sw will require to adopt certain testing techniques)
- developed to be used at the level of application system or computer system

Documents: Standard + Interpretation of the standard + What is required for compliance

Prescriptive standards

Examples:

Overally system level

- **DoD Mil std 882B**: System Safety Program Requirements
- **IEC 61508**: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related

Application level

- **RTCA DO-178B** Software Considerations in Airbone Systems and Equipment Certification
- **NASA-STD 8739.8** Software Assurance Standard
- **ISO 26262**: Road vehicles – Functional safety (adaptation of IEC 61508 specific to the application sector of electrical and electronic systems in automotive industry)
- **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

Rigorous Argument

Approach to dependability assessment based upon the use of **rigorous argument**

Develop a system + Develop an argument to justify a claim about dependability of the system

- The method makes the developers’ rationale EXPLICIT:
  developers must have a rationale for the choice of their technologies

Argument of the developers: we believe that the system we have built meets the dependability requirements because ……

Decision about the use of the system is based on:

Argument + Associated Evidence

Rigorous arguments: Safety Case

A **Safety Case** should communicate a clear, comprehensive and defensible argument that a system is acceptably to operate in a particular context

A Safety Case consists of a structured argument, supported by a body of evidence, that provides a compelling, comprehensive and valid case that a system is safe for a given application in a given environment.

Goal Structuring Notation: used for documenting arguments

Many regulations are based on Safety Cases

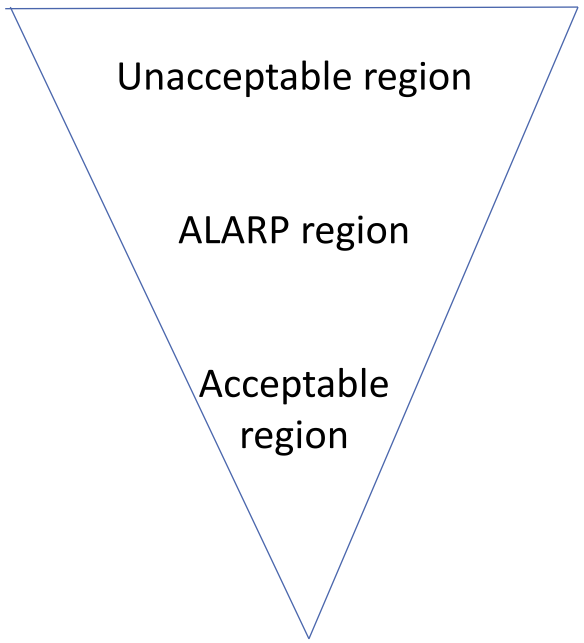
Acceptably safe uses the ALARP principle

Risk analysis

As Low As Reasonably Practicable - ALARP

the risk of a system with high consequences of failure is reduced to a point where further reductions would not be commensurate with the cost of acheiving such reductions

(gross disproportion between the costs and the benefits)



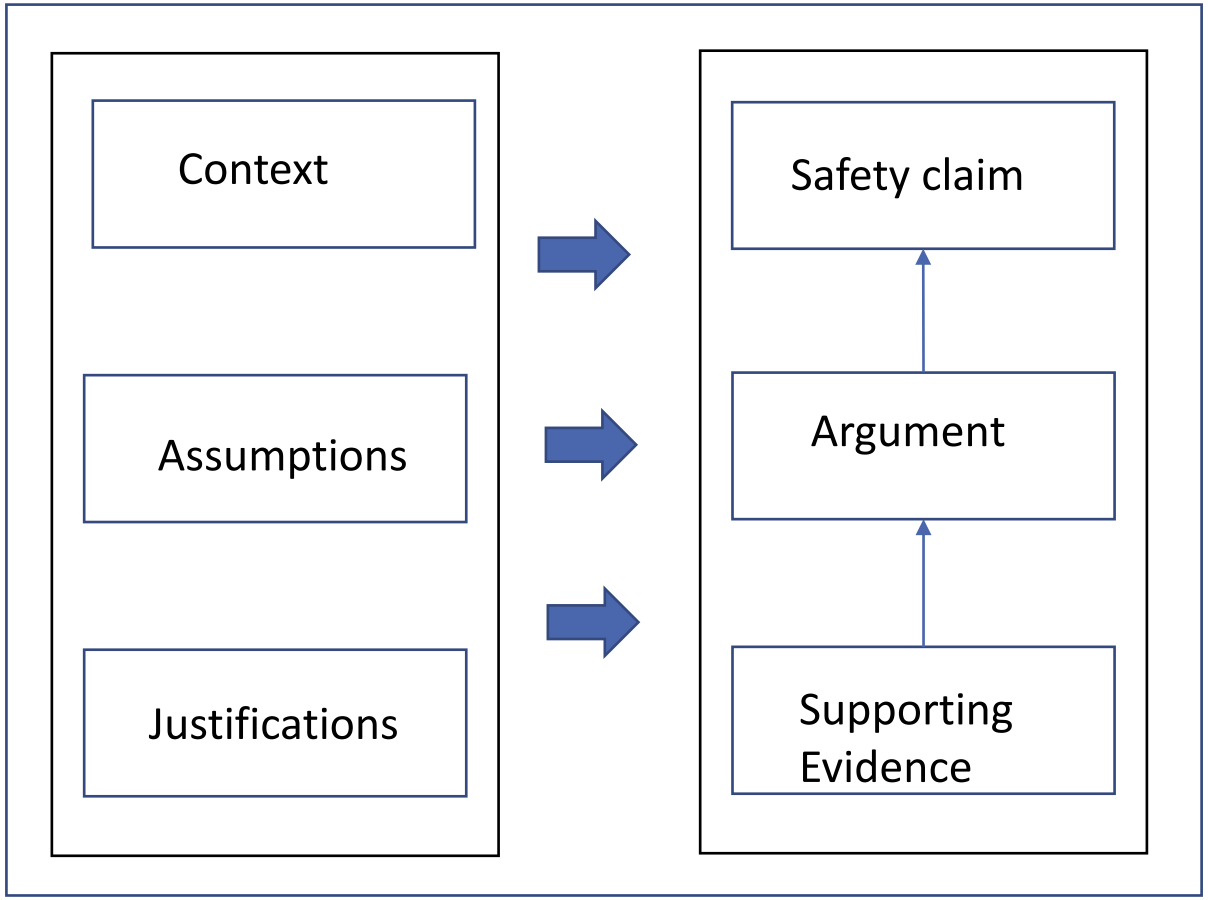
For failures with different consequences,

ALARP is applied for each the possible failures

Primarily used in U.K. (The Heath and safety at work etc, Act 1974)

Rigorous arguments: Safety Case

Overall structure of a Safety Case



For other dependability attributes, the term Assurance Case is used.

Example of prescriptive standard: IEC 61508

IEC 61508:
Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
an international standard of rules for programmable systems applied in industry

Functional safety is part of the overall safety that depends on a system operating correctly in response to its inputs also in presence of ponetially dangerous situations.

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

Functional safety specifically covers possible hazards (dangerous conditions) created when failures of the safety functions performed by E/E/PE occur; reduces the impact of risk (by corrective actions).

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

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.

- Functional safety provides the assurance that the safety-related systems will offer the necessary risk reduction required to achieve required safety level.

- Safety critical application fields, all rely heavily on functional safety to achieve safety for the equipment giving rise to the hazards.

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.

IEC 61508

The standard consists of 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

IEC 61508

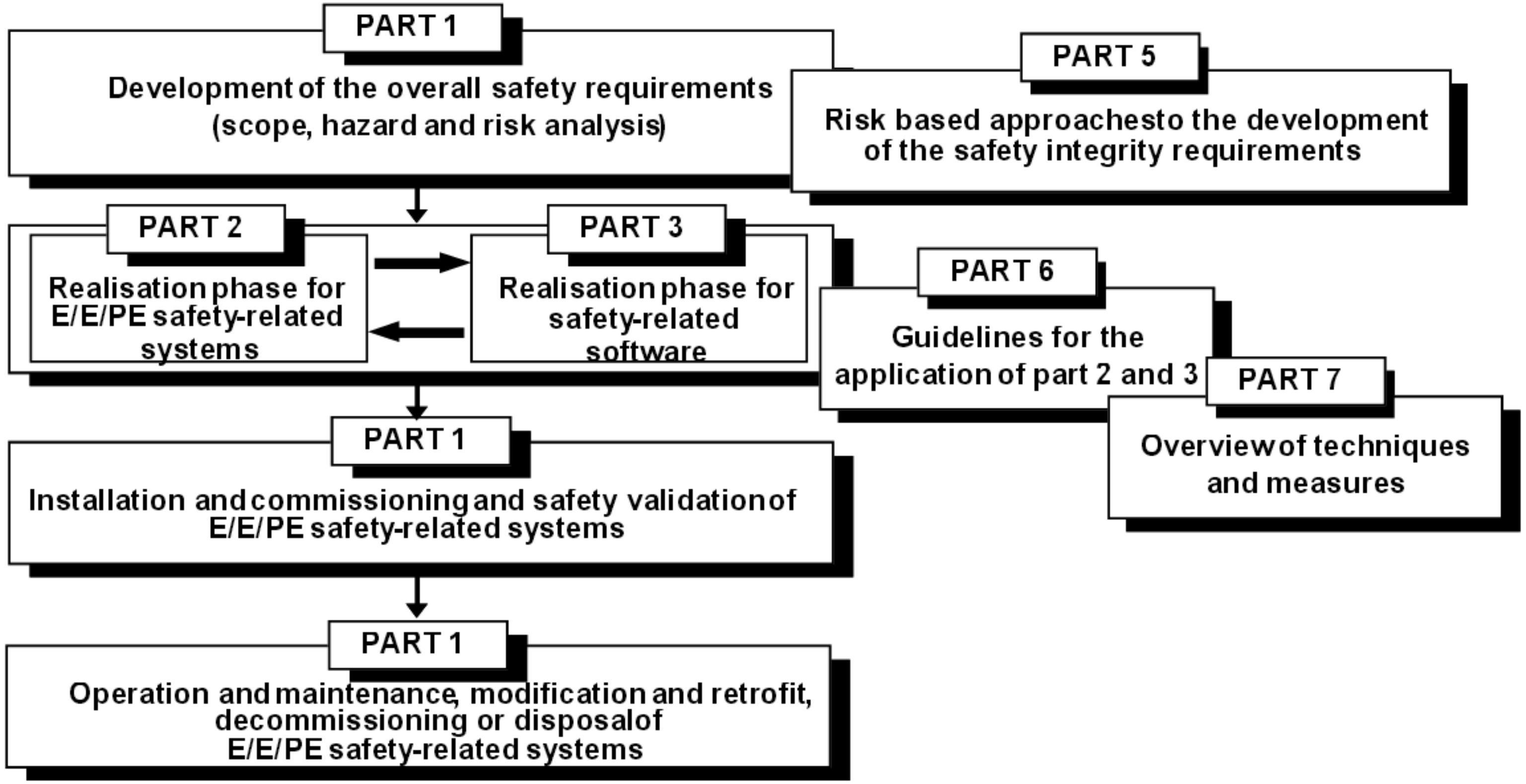

PART 1
Development of the overall safety requirements (scope, hazard and risk analysis)
PART 5
Risk based approachesto the development of the safety integrity requirements
PART 2
Realisation phase for E/E/PE safety-related systems
PART 3
Realisation phase for safety-related software
PART 6
Guidelines 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

Figure 1: Technical requirements of IEC 61508.

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*
- ***Hazards** must be identified.*
- *The **risk** is a function of frequency (or likelihood) of the hazardous event and the event consequence severity.*
- ***Safety integrity levels (SIL)** are introduced for specifying the target level of safety functions to be implemented by E/E/PE safety-related systems*

Risk 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.

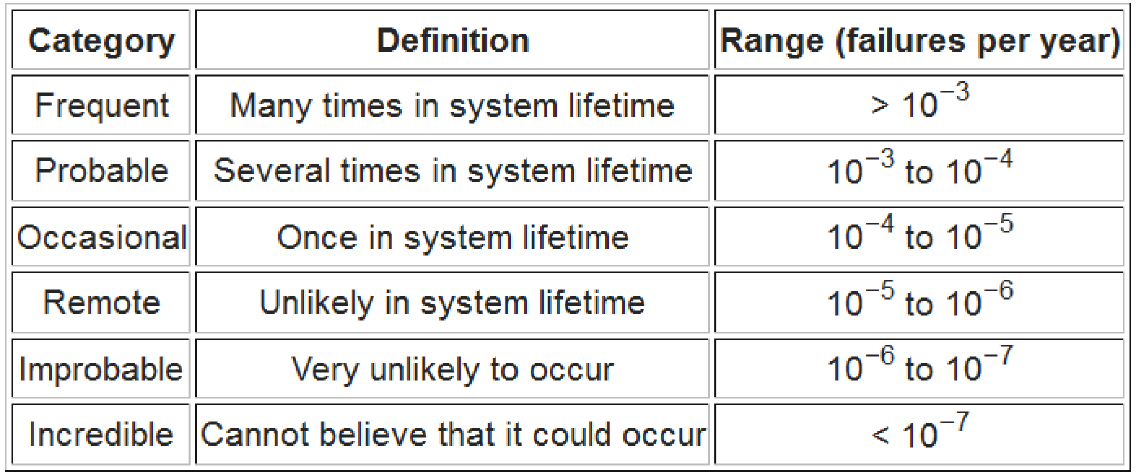
High level of documentation.

Hazard and risk class matrix

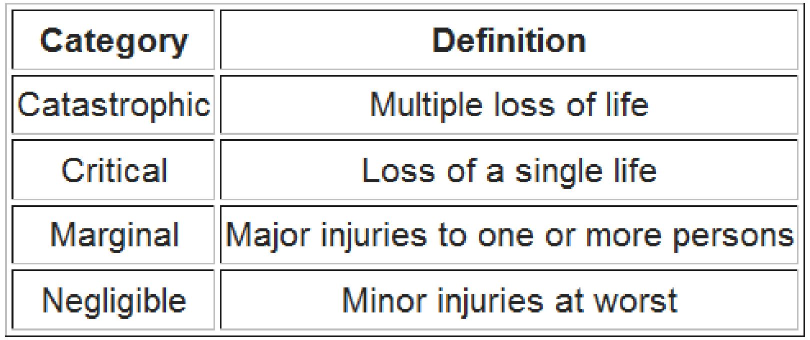
The standard requires that hazards and risk assessment should be carried out
'The EUC (equipment under control) risk shall be evaluated, or estimated, for each determined hazard’.

Analysis of hazards: framework based on a risk class matrix, that is the combination of

- 6 categories of occurrence and
- 4 categories of consequence



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	$< 10^{-7}$

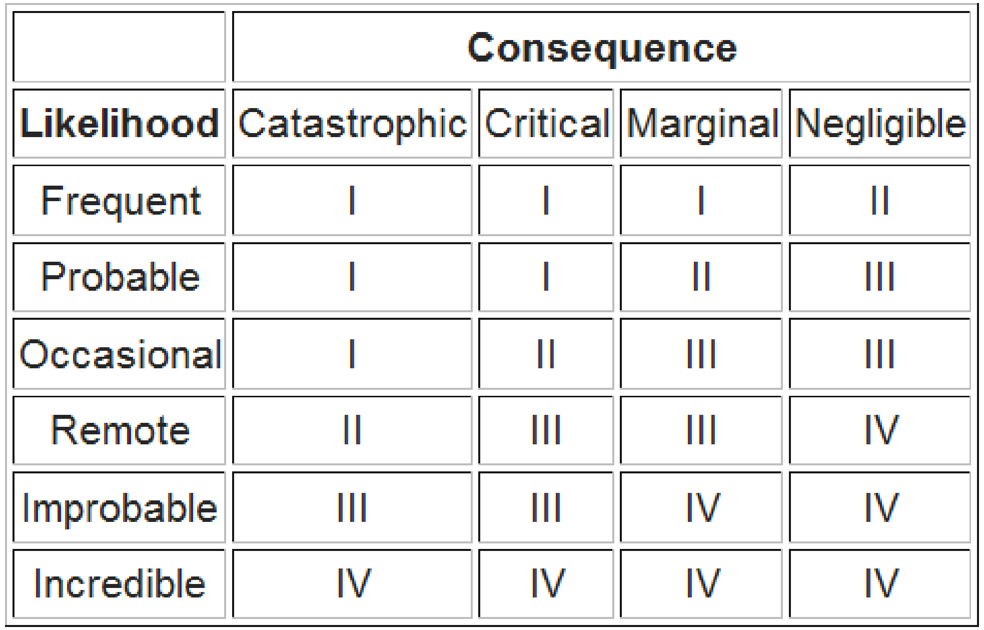


Category	Definition
Catastrophic	Multiple loss of life
Critical	Loss of a single life
Marginal	Major injuries to one or more persons
Negligible	Minor injuries at worst

Hazard and risk class matrix

Risk = Hazard Frequency x Consequence

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;

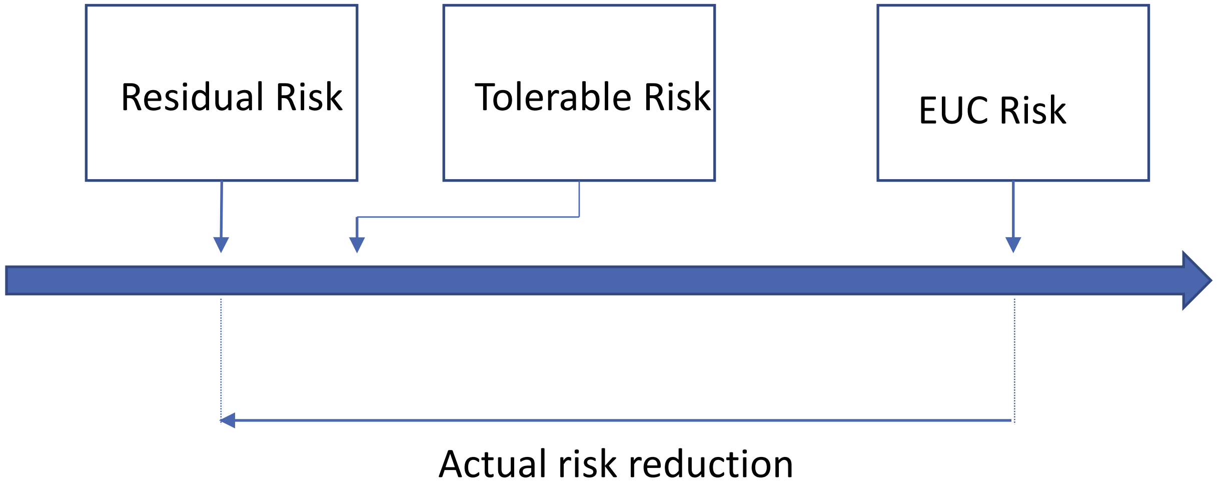
Class II: Undesirable and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained;

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).

Risk reduction

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



If EUC risk of a hazard E is higher than the tolerable risk, the risk must be reduced.

The standard suggests the following: introduction of functions which reduce the risk of E building a system S' such that is at or below the tolerable risk of E
S' = EUC + introduced functions,

The risk of E in the operation of S' is called
Residual risk: risk remaining after protective measures have been taken.

Tools to evaluate the risk:
Failure Mode and Effects Analysis (FMEA), FMEDA (include on-line diagnostic techniques), Markov models.

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.

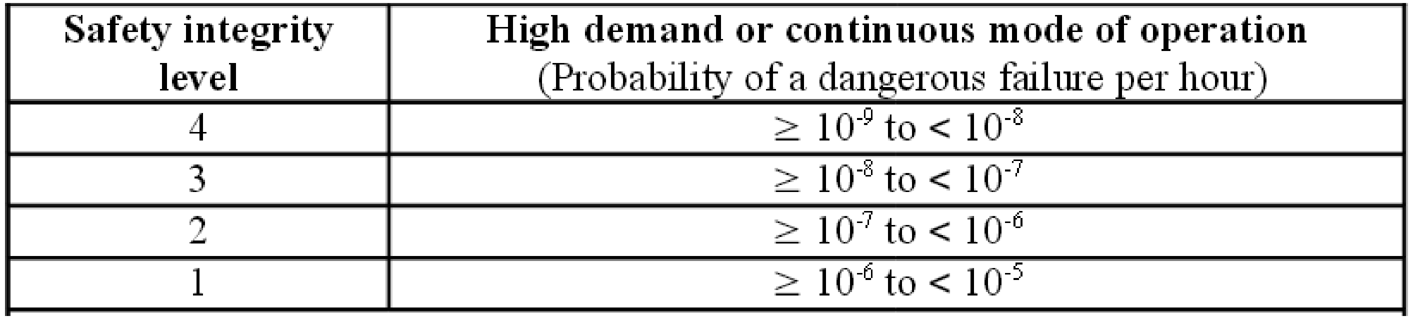
- SIL: discrete level for specifying the safety integrity requirements

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

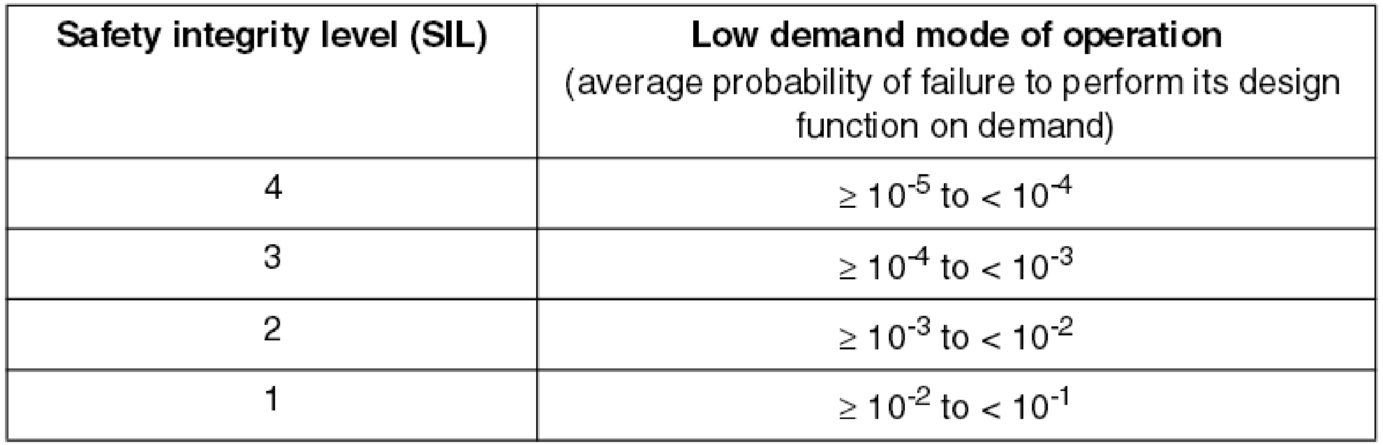
- The requirements for a given SIL are not consistent among all of the functional safety standards. A SIL is determined based on a number of quantitative factors in combination with qualitative factors such as development process and safety life cycle management.

Safety Integrity Level – SIL

- Hazards of a control system must be identified then analysed through risk analysis.
- Mitigation of these risks continues until their overall contribution to the hazard are considered acceptable.
- The tolerable level of these risks is specified as a safety requirement in the form of a target 'probability of a dangerous failure' in a given period of time, stated as a discrete SIL.



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)	**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 $< 10^{-1}$

Safety Integrity Level – SIL

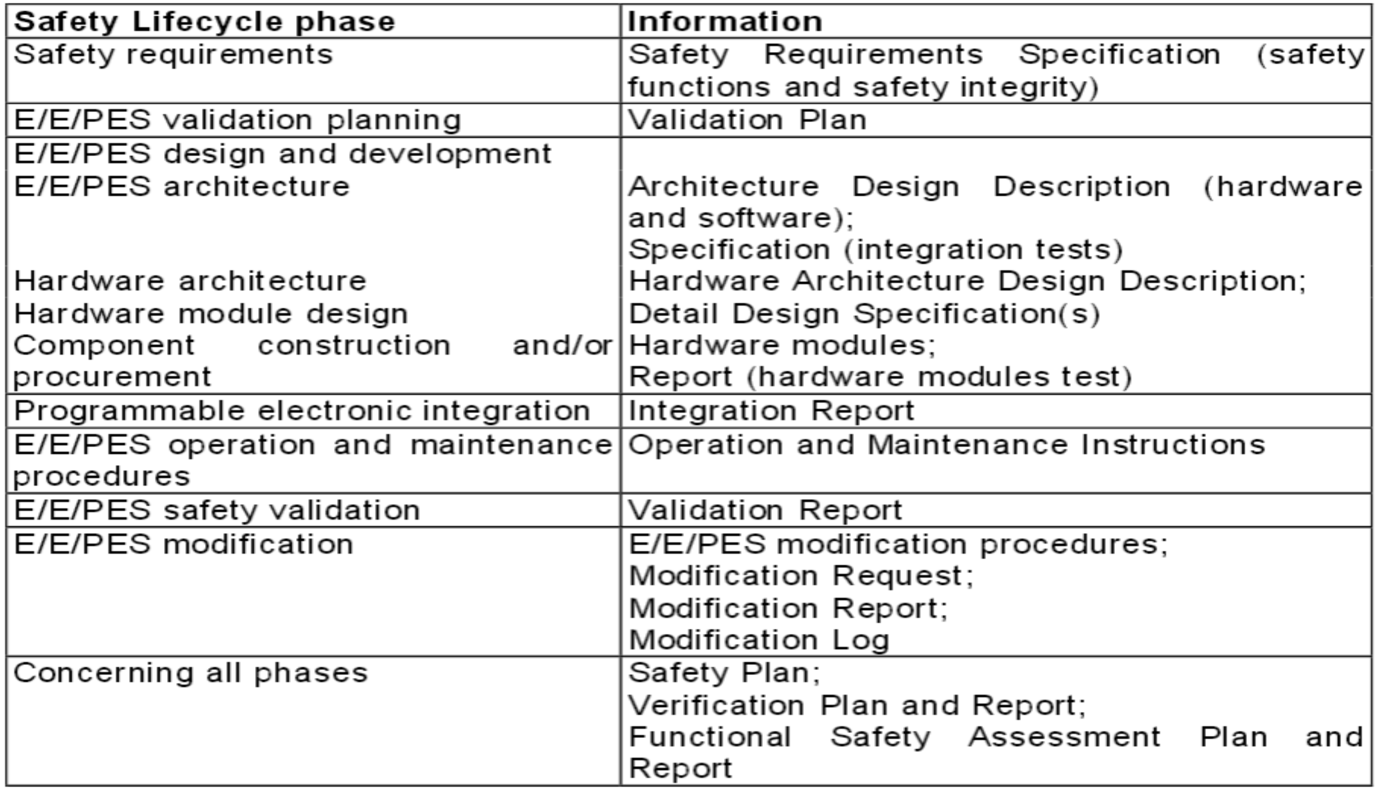
- Certification schemes are used to establish whether a device meets a particular SIL.
- The requirements of these schemes can also be met by establishing a rigorous development process, or by establishing that the device has sufficient operating history to argue that it has been proven in use.
- Association of SIL with a set of recommended development techniques.
- The use of formal methods such as CCS, HOL, LOTOS, OBJ, Temporal logic, VDM and Z is *recommended*, but , *only exceptionally for some very basic components only, for SIL3*

Documentation

Sample documentation structure (Annex A)

Users can choose any documentation structure that meets the following criteria.

The documentation has to contain enough information to perform (i) safety lifecycle, (ii) Manage functinal safety (iii) allows Functional safety assessment.



Safety Lifecycle phase	**Information**
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

An example of documents for safety life cycle project

Personnel Competency / Compliance

PERSONNEL COMPETENCY   The standard states:

''All persons involved in any overall, E/E/PES or software safety lifecycle activity, including Management activities, should have the appropriate training, technical knowledge, experienceand qualifications revelavt to the specific duties they had to perform.''

It is suggested that a number of things be considered in the evaluation of personnel:

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 regulator framework
5. The consequences of safety-related failures
6. The assignemnt of safety integrity levels of the safety functions ina project
7. Experience and its relevance to the job. The training experience, and qualification of persons should be documented.

COMPLIANCE   The standard states:

''To conform to this standard it shall be demonstarted that the requirements have been satisfied to the required criteria specified (for example safety integrity level) and therefore, for each clause and sub-clause, all the objective have been met.''

Security

Risk analysis

ISO 26262: Road vehicles – Functional safety (adaptation of IEC 61508 specific to the application sector of electrical and electronic systems in automotive industry)

Problems caused by malicious attacks are not addressed by the hazard analysis and risk assessment within the ISO 26262 standard

Cyber-security as a risk factor to be considered in the hazard and risk analysis

ISO/SAE CD 21434 -Road Vehicles –Cybersecurity engineering
https://www.iso.org/standard/70918.html (draft 2020)

Schmittner et al., Towards a Framework for Alignment between Automotive Safety and Security Standards Conference Paper · September 2015

Risk assessment tools

risk assessment tools implement several risk assessment methodologies

- DREAD risk assessment method
- Common Vulnerability Scoring System (CVSS)
- OWASP Risk Rating Methodology
- SAHARA

DREAD risk assessment method

Categories of risk analysis

– **D**amage potential
Ranks the extent of damage that occurs if a vulnerability is exploited

– **R**eproducibility
Ranks how often an attempt at exploiting a vulnerability really works

– **E**xploitability
Effort required to exploit the vulnerability (a number) e.g. authentication is considered

– **A**ffected users
number of instances of the system that would be affected if an exploit became widely available

– **D**iscoverability Measures
the likelihood that a vulnerability will be found by hackers

DREAD risk assessment method

$$\text{Risk} = \frac{\text{Damage} + \text{Reproducibility} + \text{Exploitability} + \text{Affected Users} + \text{Discoverability}}{5}$$

Rating scale for each category: 0-10

1 being the least probability of the occurrence and the least damage potential

Common Vulnerability Scoring System (CVSS) - open framework

CVSS is comprised of three different metric groups:
Base, Temporal, and Environmental.

Each one consists of their own set of metrics.

Base:
- Access Vector
- Access Complexity
- Authentication
- Confidentiality Impact
- Integrity Impact
- Availability Impact

Temporal
- Exploitability
- Remediation Level
- Report Confidence

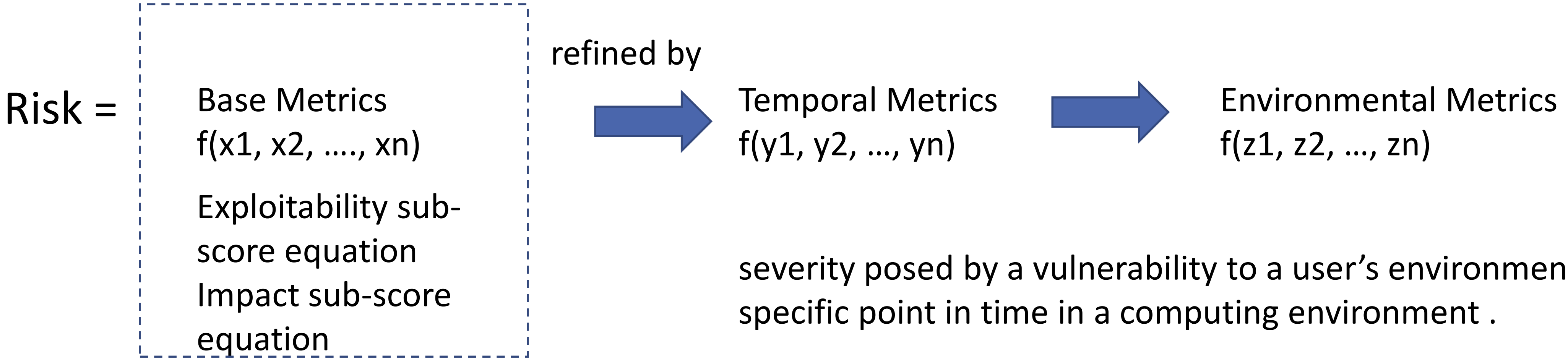
Environmental
- Collateral damage potential
- Target distribution
- Confidentiality requirement
- Integrity requirement
- Availability requirement

CVSS : example

Category	Subcategory	Value
Access Vector (AV)	- L (Local) accessible only on device	0.395
	- A (Adjacent network) accessible via directly attached bus	0.646
	- N (Network) accessible via any number of networks	1
Authentication (Au)	- M(Multiple) multiple auth. steps	0.45
	- S (Single) one auth. step	0.56
	- N (None) No authentication is required	0.704

Score: 0 – 10

Common Vulnerability Scoring System (CVSS) - open framework



Risk =

Base Metrics
f(x1, x2, …., xn)

Exploitability sub-score equation
Impact sub-score equation

refined by

Temporal Metrics
f(y1, y2, …, yn)

Environmental Metrics
f(z1, z2, …, zn)

severity posed by a vulnerability to a user’s environment at a specific point in time in a computing environment .

OWASP risk assessment rating methodologies

Open Web Application Security Project (OWASP)
Estimates both technical and business impact factors

Starts from the standard risk model:

$$\text{Risk} = \text{Likelihood} * \text{Impact}$$

The following methodology is defined, where factors for the likelihood and impact of each risk are considered

From the web: https://owasp.org/
"The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software.
…
The OWASP Foundation is the source for developers and technologists to secure the web."

OWASP risk assessment rating methodologies

Step 1: Identify Risk

Step 2: Factors for estimating likelihood
- Threat Agent Factors
- Vulnerability Factors

Step 3: Factors for estimating impact
- Technical Impact Factors
- Business Impact Factors

Step 4: Determining severity of risk
- Informal Method
- Repeatable Method
- Determining Severity

Step 5: Deciding what to fix

Step 6: Customizing your risk rating model

OWASP top 10 vulnerabilities in web applications
https://www.ibm.com/developerworks/library/se-owasptop10/

Security-Aware Hazard Analysis and Risk Assessment SAHARA

SAHARA method allows the evaluation of the impact of security issues on safety at the system level.

Threats are **quantified** according to

- **Required Resources**
- **Know-How** that are required to define threats
- Threats **Criticality**

The impact of the threat on the system determines whether the threat is safety-related or not.
If the threat is safety-related, it will be analysed and the resulting hazards will be evaluated.

Georg Macher, et al.. SAHARA: A Security-Aware Hazard and Risk Analysis Method. DATE 2015
https://past.date-conference.com/proceedings-archive/2015/pdf/0622.pdf.

Security-Aware Hazard Analysis and Risk Assessment SAHARA

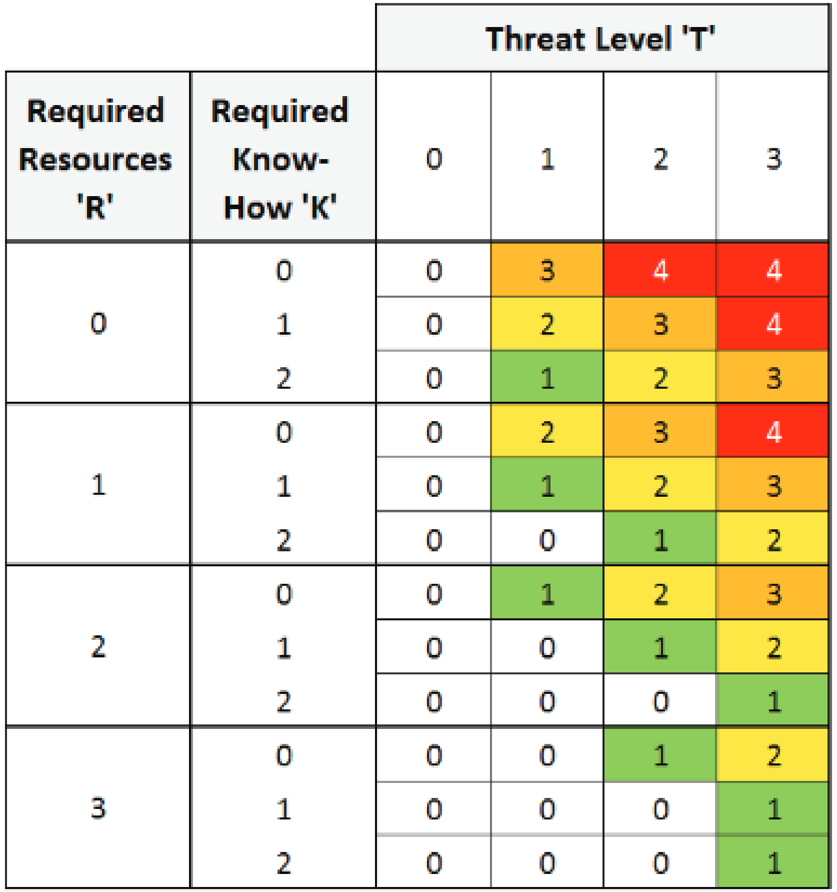
Level	**Required resourse**	Example
0	no additional tool or everyday commodity	randomly using of user interface
1	standard tool	screwdriver, coin
2	simple tool	CAN sniffer, oscilloscope
3	advanced tool	debugger, bus communication simulator …

Level	**Required Know-How**	Example
0	no prior knowledge (black-box approach)	Unknown internals
1	Technical knowledge (gray-box approach)	Electrician, mechanic basic understanding of internals
2	Domain knowledge (white-box approach)	person with technical training, internal disclosed

Security-Aware Hazard Analysis and Risk Assessment SAHARA

Level	**Threat Criticality**	Example
0	no security impact	No security impact
1	Moderate security relevance	Reduced availability
2	High security relevance	non availability, privacy intrusion
3	High security and possibly safety relevance	Life threatening abuse possible

Security Level Determination matrix



		Threat Level 'T'			
Required Resources 'R'	**Required Know-How 'K'**	0	1	2	3
0	0	0	3	4	4
	1	0	2	3	4
	2	0	1	2	3
1	0	0	2	3	4
	1	0	1	2	3
	2	0	0	1	2
2	0	0	1	2	3
	1	0	0	1	2
	2	0	0	0	1
3	0	0	0	1	2
	1	0	0	0	1
	2	0	0	0	1

Classification of hazards according to the matrix
4 is the highest security class

A process for engineering dependable system

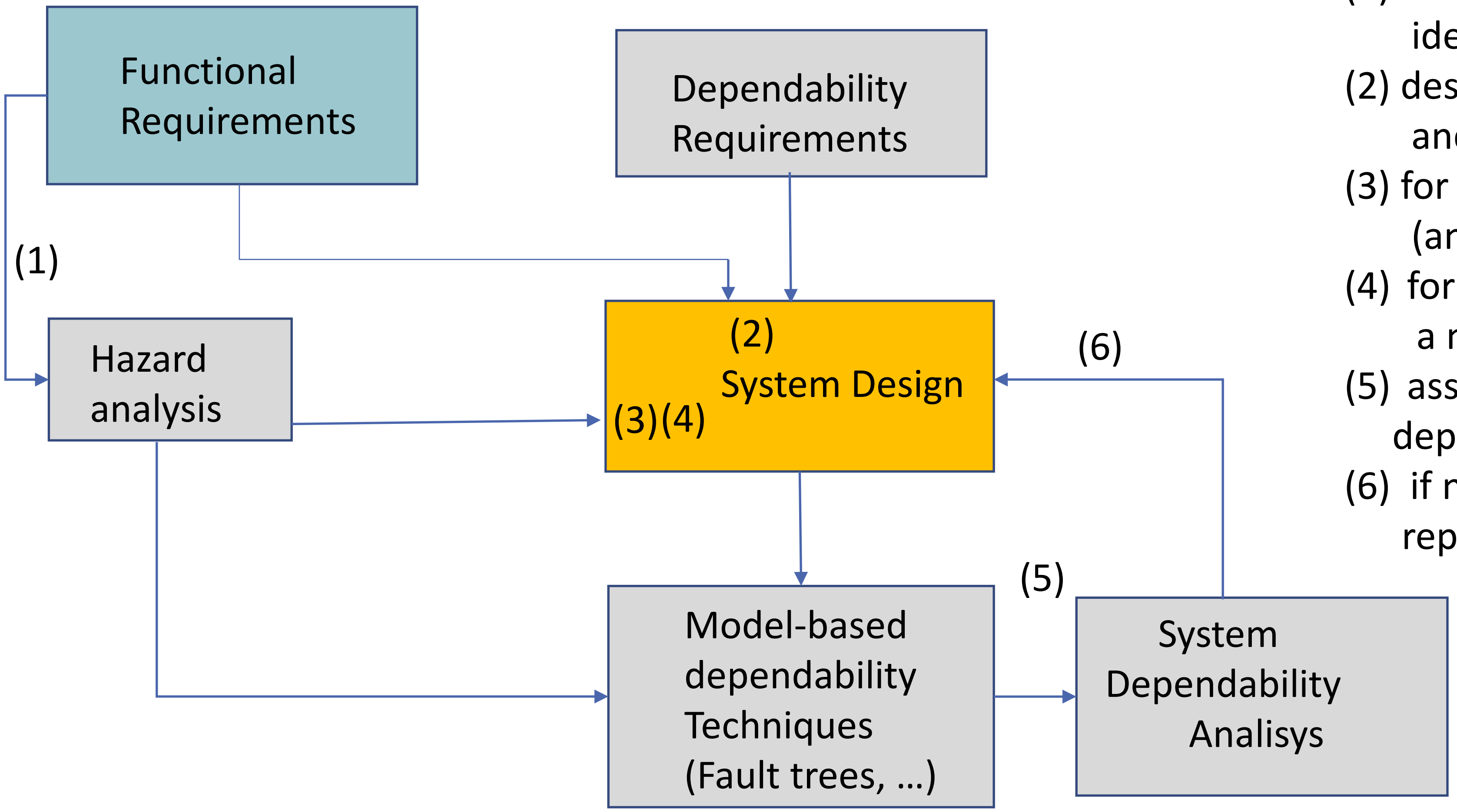
- The functional requirements and the dependability requirements are used to guide the system design process

- Anticipate faults to which the system is subject and deal with it to meet the dependability requirements
  (using fault tolerance techniques, ….)

- Assess the dependability

- Cycle through the process again if dependability requirements are not met

A process for engineering dependable system


Functional Requirements
Dependability Requirements
(1)
Hazard analysis
(2)
System Design
(3)(4)
(6)
(5)
Model-based dependability Techniques (Fault trees, …)
System Dependability Analisys

(1) Starting from functional requirements identify hazards
(2) design the system to meet functional and dependability requirements
(3) for each hazard determine the faults (anticipated faults)
(4) for each anticipated fault, determine a means to deal with the fault
(5) assess the resulting system to check if dependability requirements are met
(6) if needed re-design the system and repeat the assessment process