Hazard Analysis and Risk Assessment

Safety critical systems

- 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.

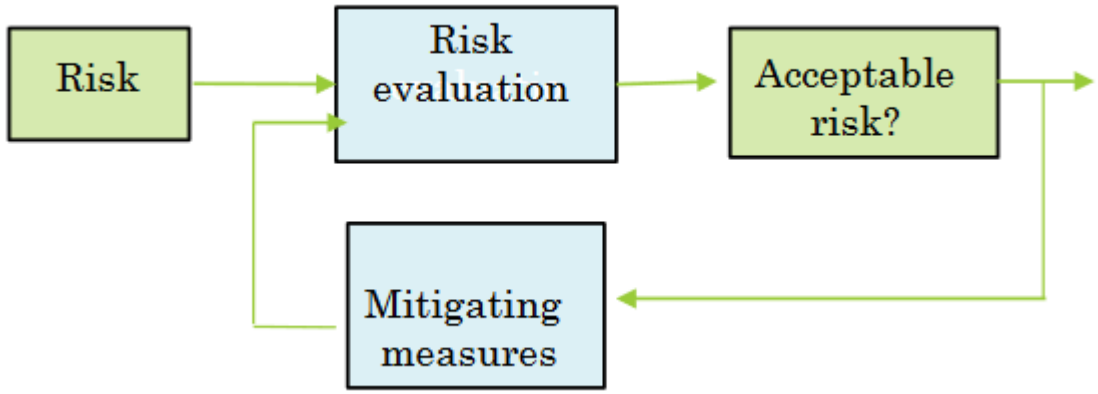
- In particular, **functional safety** is a concept applicable across all industry sectors. It is fundamental to the enabling of complex technology used for safety-related systems.
  It provides the assurance that the safety-related systems will offer the necessary **risk reduction** required to achieve safety in presence of malfunctions.

- 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

Standards enforce rules of conduct. Documentation must be open to external inspection and audit.

Safety critical systems development must comply to certification standards

Hazard analysis and Risk assessment



Hazard identification

Qualitative/Quantitative evaluation of the risk

Risk reduction

IEC 61508: Functional Safety

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

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

- 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

IEC 61508

- 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 **consequenc**e, 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

Risk analysis

identification of hazardous events and determination of the necessary risk reduction for these events.
Risk analysis has been extensively applied in safety critical systems

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.

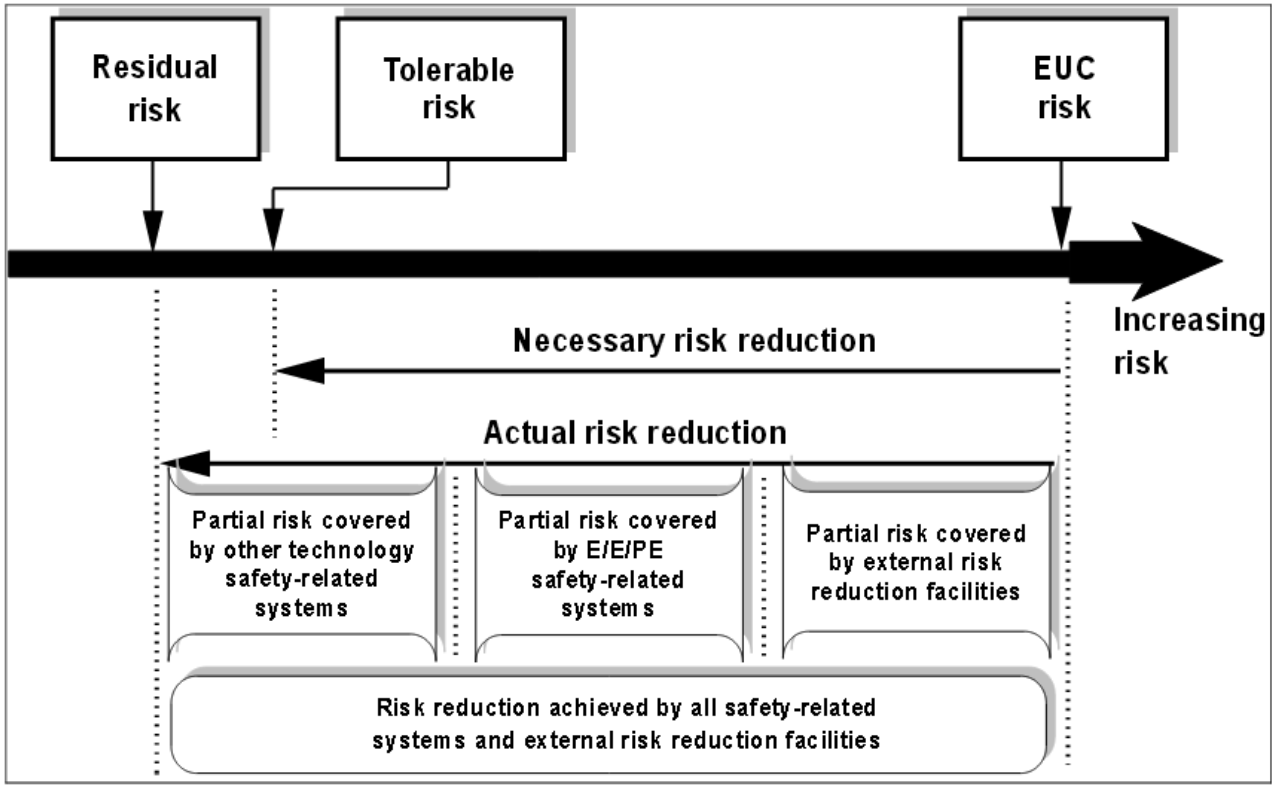
Tolerable risk: risk which is accepted in context based on the current values of society

Determining Risk Reduction

E = hazardous event
EUC=Equipment under control
EUC risk = risk araising from EUC or from its interaction with the EUC control system

EUC risk of E > Tolerable risk of E

→ **take steps to ensure that the risk of E in the overall system S is reduced to the tolerable risk (by introducing functions that reduce the risk of E)**



Let S' = EUC enhanced with the introduced functions
The risk of E in the operation of the system S' 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

Techniques and tools suggested to evaluate risks:

HAZOP – **Haz**ard and **Op**erability study

FMEA – **F**ailure **M**ode and **E**ffect **A**nalysis
document the system being considered using a systematic approach to identify and evaluate the effects of componet failures and to determine what could reduce or eliminate the chance of failure

FMEDA – **F**ailure **M**ode and **E**ffect **D**iagnostic **A**nalysis
extends the FMEA technique to include on-line diagostic techniques and identify failure modes relevant to safety instrumented system design

ETA – **E**vent **T**ree **A**nalysis
FTA – **F**ault **T**ree **A**nalysis
and others

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

A fundamental disquiet with the notion of SIL used in the standard is the association of a SIL with a set of reccomended development techniques, for example whether the use of formal methods is or is not recommended.

The use of formal methods such as CCS, CPS, HOL, LOTOS, OBJ, temporal logic, VDM, Z is **recommended** but **only exceptionally, for some very basic components only** for SIL 3.

Documentation

Sample Documentation Structure (Annex A)

The documentation has to contain enough information to
- effectively perform each phase of the safety lifecycle, manage functional safety, and allow 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 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

An example

Personnel Competency and compliance to the standard

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.

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."

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)

Sector specific standards

- **The Nuclear Power Plant Application Field**
  IEC 61513 Nuclear power plants - Instrumentation and control important to safety - General requirements for systems

- **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.

……

Functional Safety (FuSa) standards

Standard in automotive field
ISO 26262 - Road Vehicles: Functional Safety

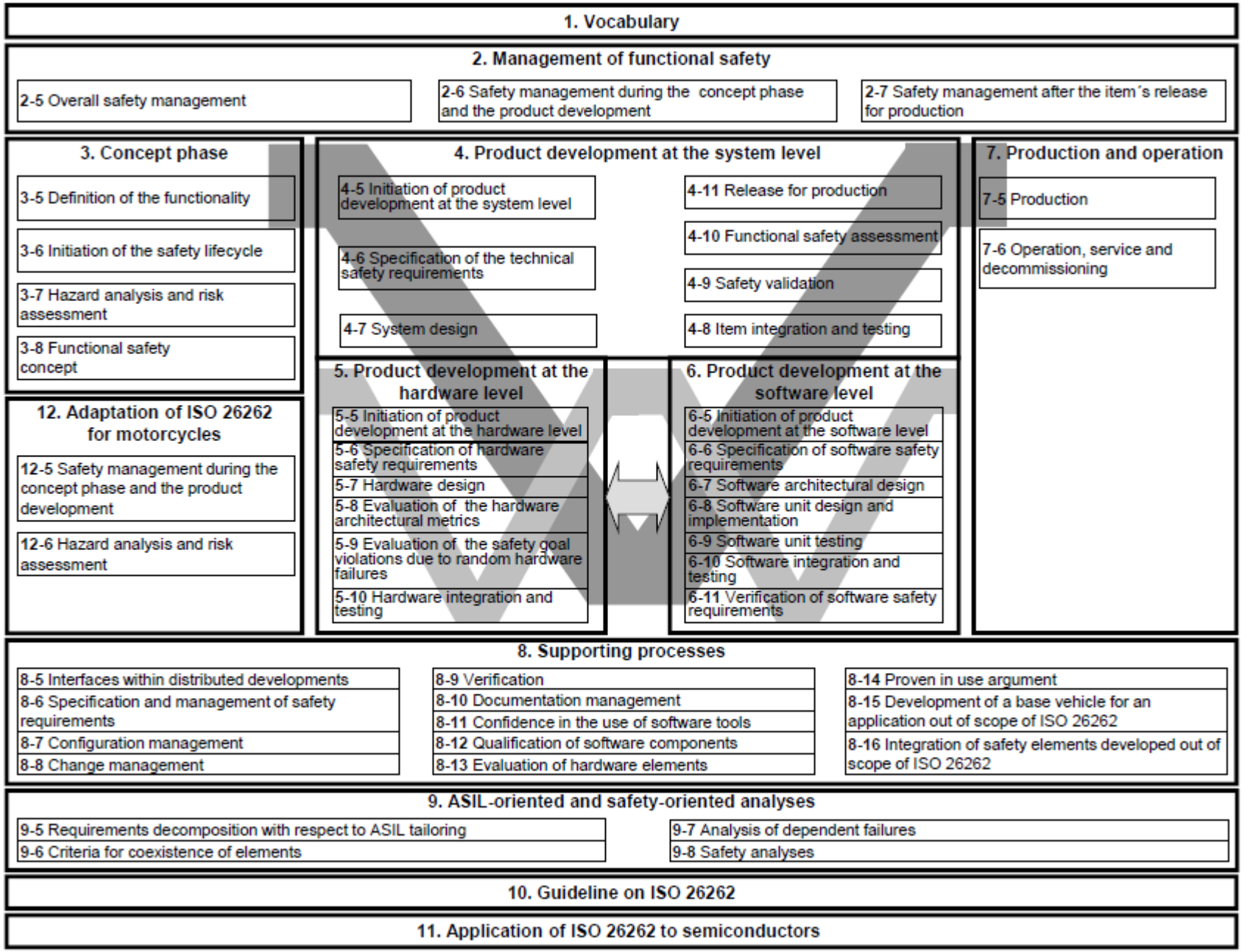
Functional safety:
absence of unreasonable risk due to hazards caused by malfunctioning behaviour of Electric/Electronic/Programmable Electronic systems

- the ability of the system to deliver the expected functionality during its operational life in presence of malfunctions of the E/E/EP components

- reduce the probability of failures at a given acceptable rate in presence of E/E/EP malfunctioning behaviors (using established techniques for dependability)

Applies to systems as enging control, braking or airbags.
For these systems, safety is ensued by mitigating the risk of system failure

Overview of ISO 26262



Vocabulary

- **Hazard**
  potential source of harm (e.g., AIRBAG random explosion)
- **Hazardous event**
  combination of hazard and an operational situation (scenario that can occur during the system life. Automotive: e.g., Driving, Parking, Maintenance) (e.g., AIRBAG explosion during Driving)

- **Risk**
  combination of the probability of occurrence of harm and the severity of that harm
- **Unreasonable risk**
  risk judged to be unacceptable in a certain context according to the current values of society
- **Residual risk**
  risk remaining after the deployment of safety measure

Vocabulary

- **Safety**

  absence of unreasonable risk

- **Safety goal**

  Top level safety requirement as a result of the hazard analysis and risk assessment

- **Safety measure**

  solution to **avoid** or **control** or **detect** failures or **mitigate** their harmful effects

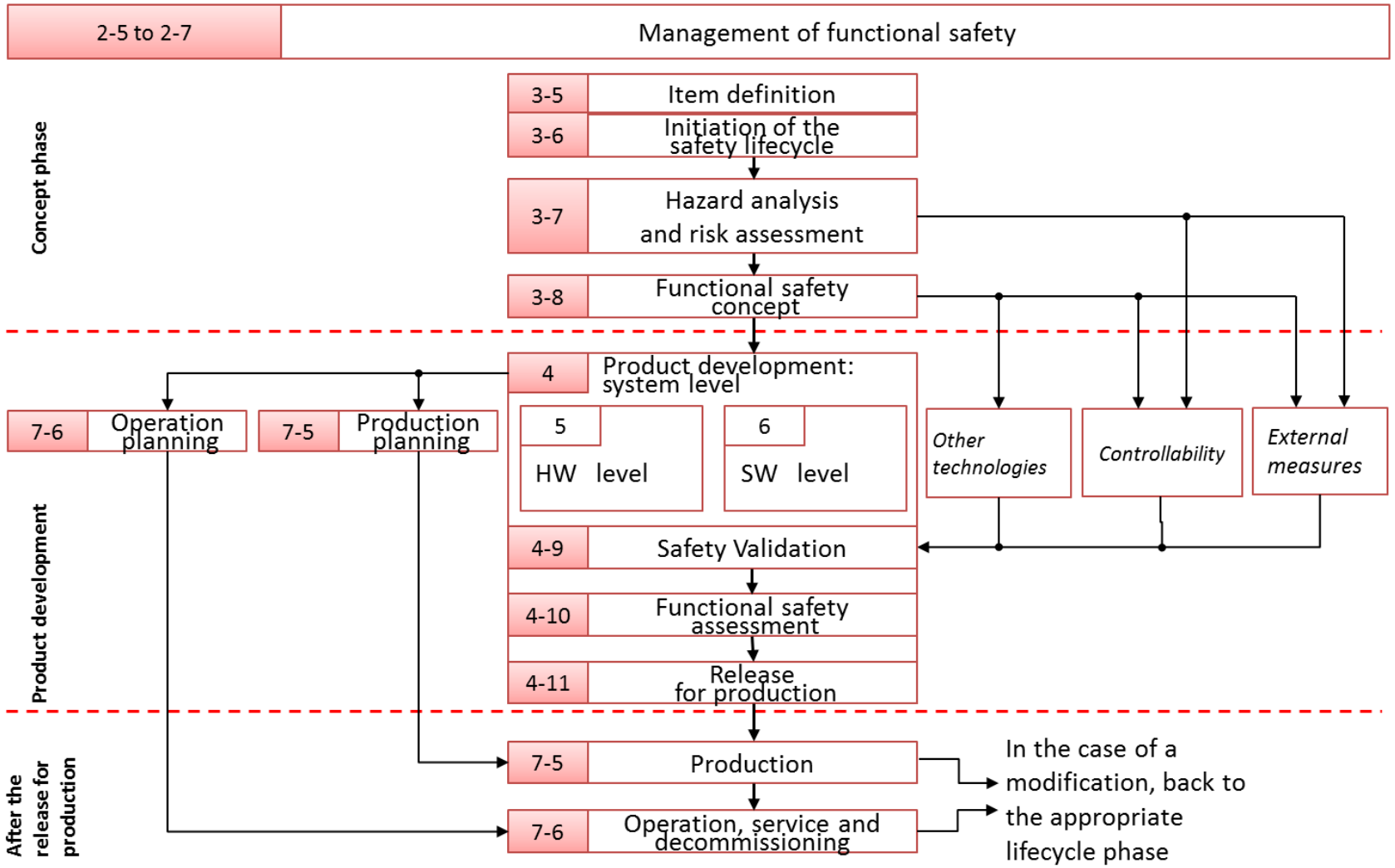
- **Safe state**

  operating mode of a system withouth an unreasonable level of risk which is not the intended operation mode of the system (e.g., switched off system)

- **Safety manager**

  the person responsible for the functional safety management during the system development

2. Management of functional safety



Safety lifecycle

Fig. 2, ISO 26262-2:2018(E)

Vocabulary

Item
system or array of systems to implement a function at the vehicle level

Examples of item:
adaptive cruise control (ACC), braking system (ESC), steering system (EPS), propulsion system, etc

A vehicle function is usually assigned to a single item (ECU, Electronic Control Unit)

Management of functional safety

3-5 Item definition

“The initiating task of the safety lifecycle is to develop a description of the item with regard to its functionality, interfaces, environmental conditions, legal requirements, known hazards, etc. The boundary of the item and its interfaces, as well as assumptions concerning other items, elements, systems and components are determined”

3-6 Initiation of the safety lifecycle

“Based on the item definition, the safety lifecycle is initiated by distinguishing between either a new development, or a modification of an existing item.” We consider a new development

3-7 Hazard Analysis and Risk Assessment

1**. Assignment of ASIL to hazardous events**
“First, the hazard analysis and risk assessment estimates the probability of exposure, the controllability and the severity of the hazardous events with regard to the item.
Together, these parameters determine the ASILs of the hazardous events. “
e.g, AIRBAG random explosion during Driving

2. **Safety goals for the item - top level safety requirements**
All hazardous events with an ASIL have associated a safety goal
e.g., avoid activating the AIRBAG if vehicle not involved in an accident

Safe state: a mode of the item without an unreasonable level of risk
e.g., AIRBAG disabled

Management of functional safety

3. **Derivation of detailed safety requirements from the safety goals**

"… detailed safety requirements are derived from the safety goals. These safety requirements inherit the ASIL of the corresponding safety goals, or, in the case ASIL decomposition has been applied, the ASIL of the corresponding decomposed safety requirement."

Assume the AIRBAG receives object detection by ECU A

Requirement 1: ECU A sends accurate information by proximity sensors to the AIRBAG ECU

Requirement 2: The AIRBAG ECU does not activate explosion if the vehicle speed is 0.

ASIL

Risk classification: Automotive Safety Integrity Level (ASIL)

according to three factors Exposure / Severity / Controllability

ASIL D

ASIL C

ASIL B

ASIL A

QM (not safety related)

Severity

	Class			
	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Exposure regarding operational situations

	Class					
	E0	E0*	E1	E2	E3	E4
Description	Incredible	Combination of very low probabilities	Very low probability	Low probability	Medium probability	High probability

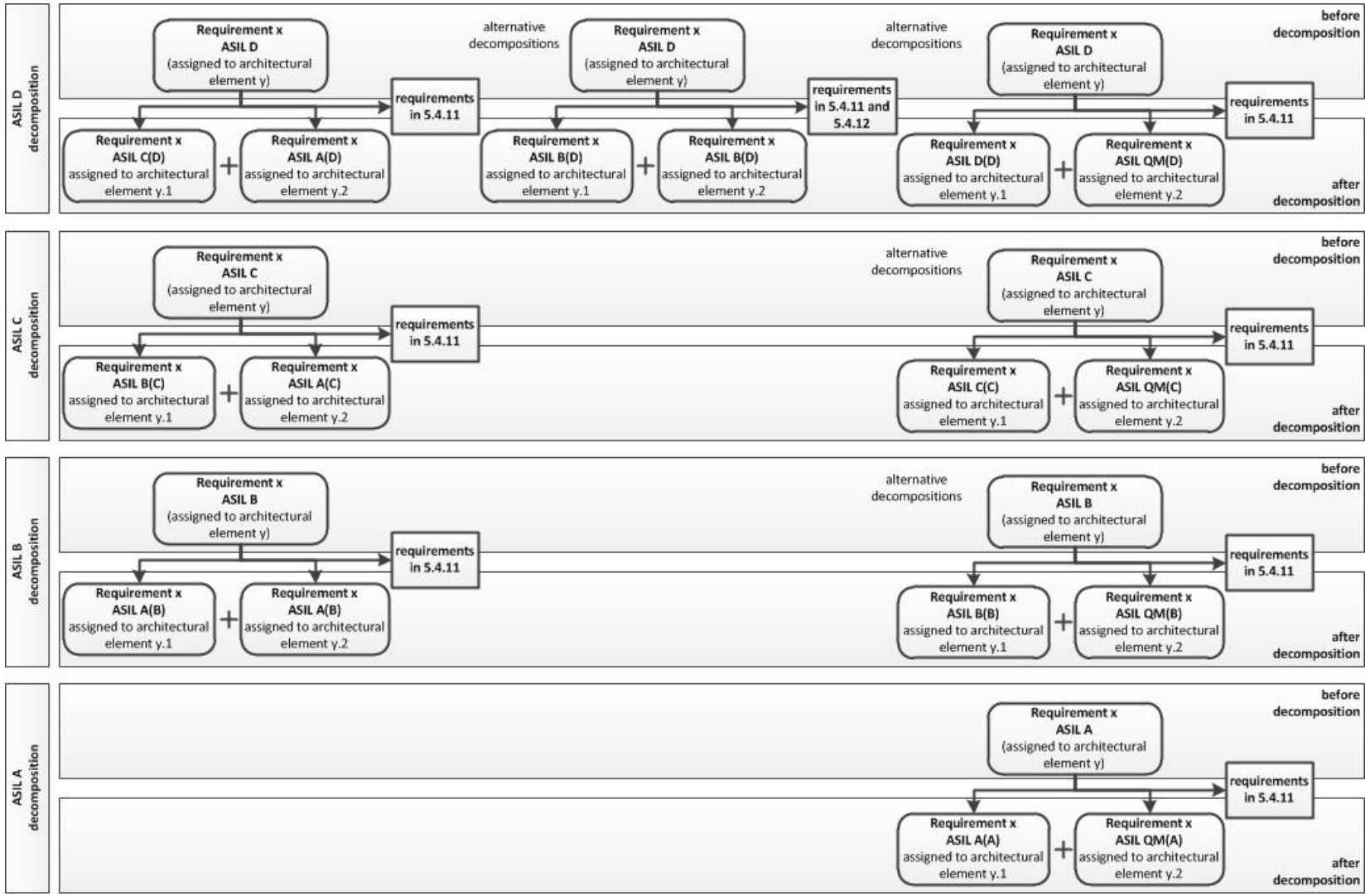
Controllability

	Class			
	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

ASIL determination

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E0*	QM	QM	QM
	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E0*	QM	QM	QM
	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E0*	QM	QM	QM
	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Requirements decomposition

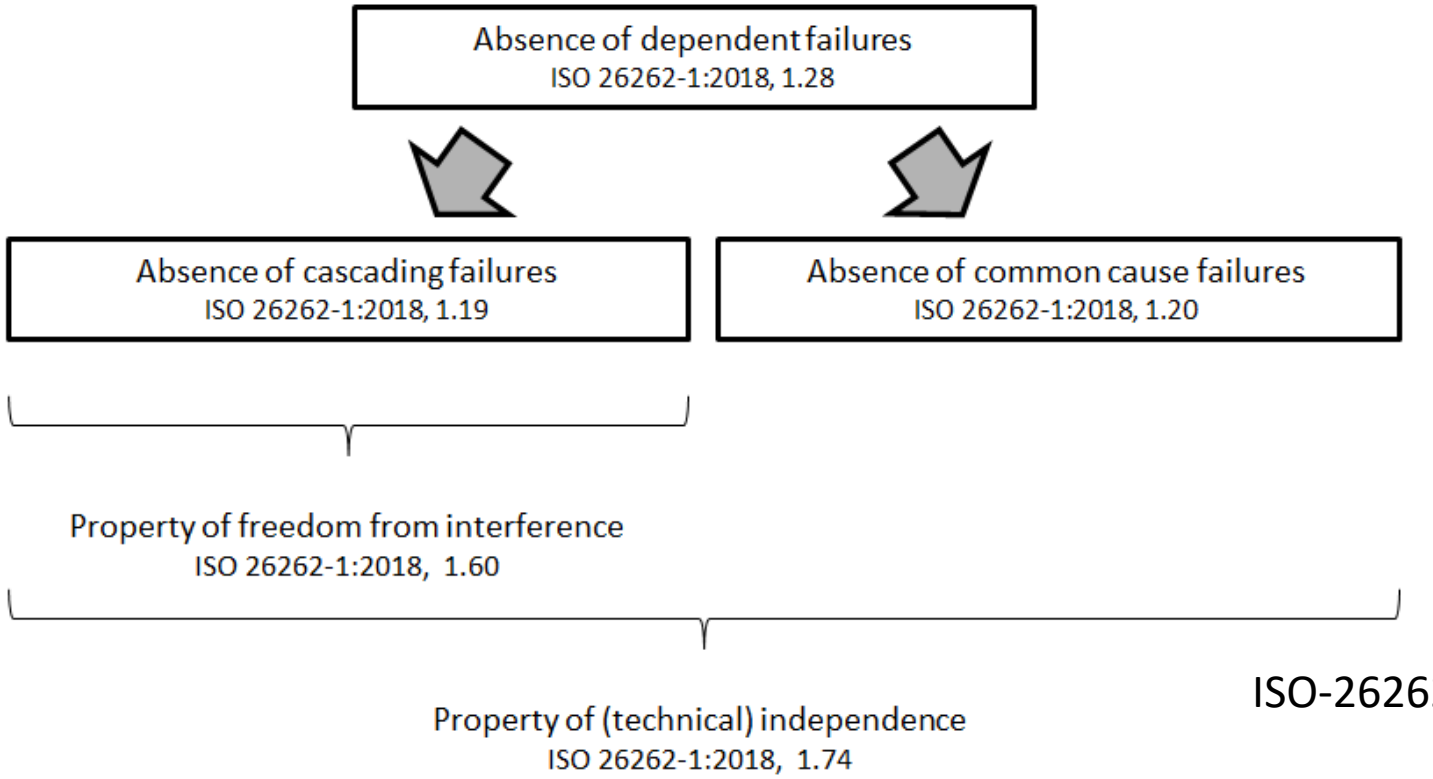


Independence: Independent elements

ISO-26262-9 Fig. 2

Analysis of dependent failures

The analysis of dependent failures aims to identify the single events or single causes or failure modes that could bypass or invalidate a required independence or freedom from interference between given elements and violate a safety requirement or a safety goal.



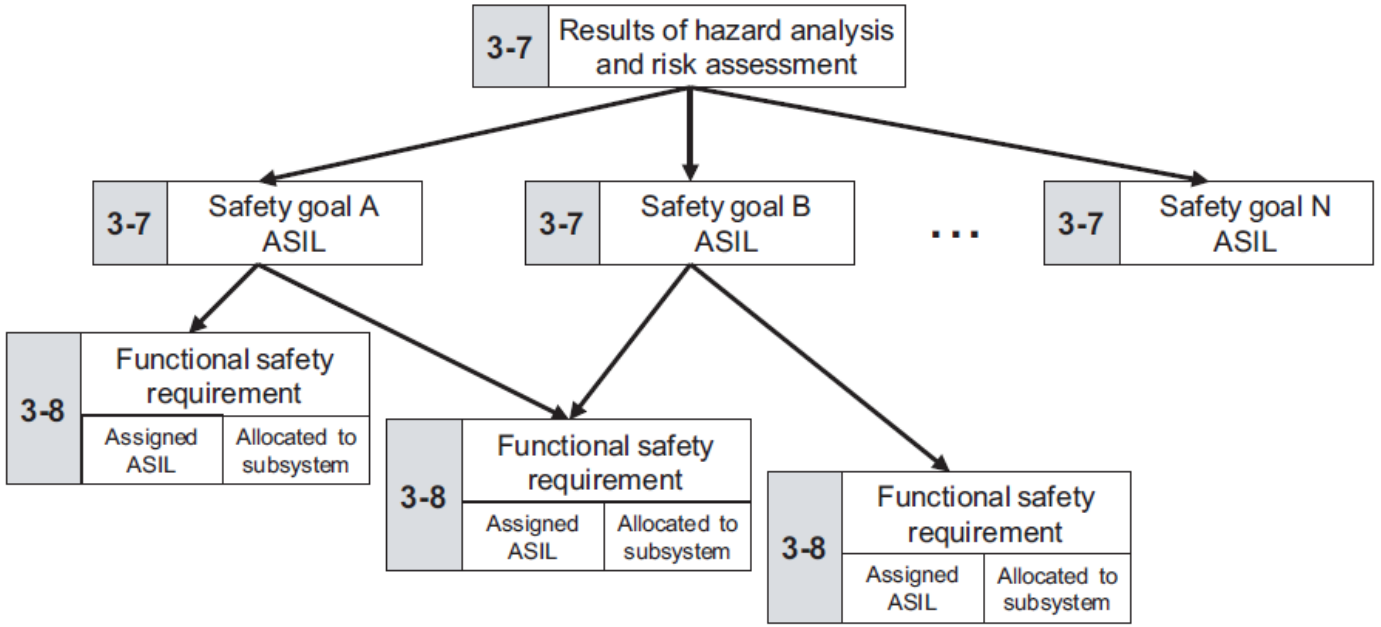
ISO-26262-9 Fig. 3

Management of functional safety

3-8 Funtional Safety Concept
Preliminary architectural assumptions.

The functional safety concept is specified by functional safety requirements that are allocated to the elements of the item.

Functional safety requirements



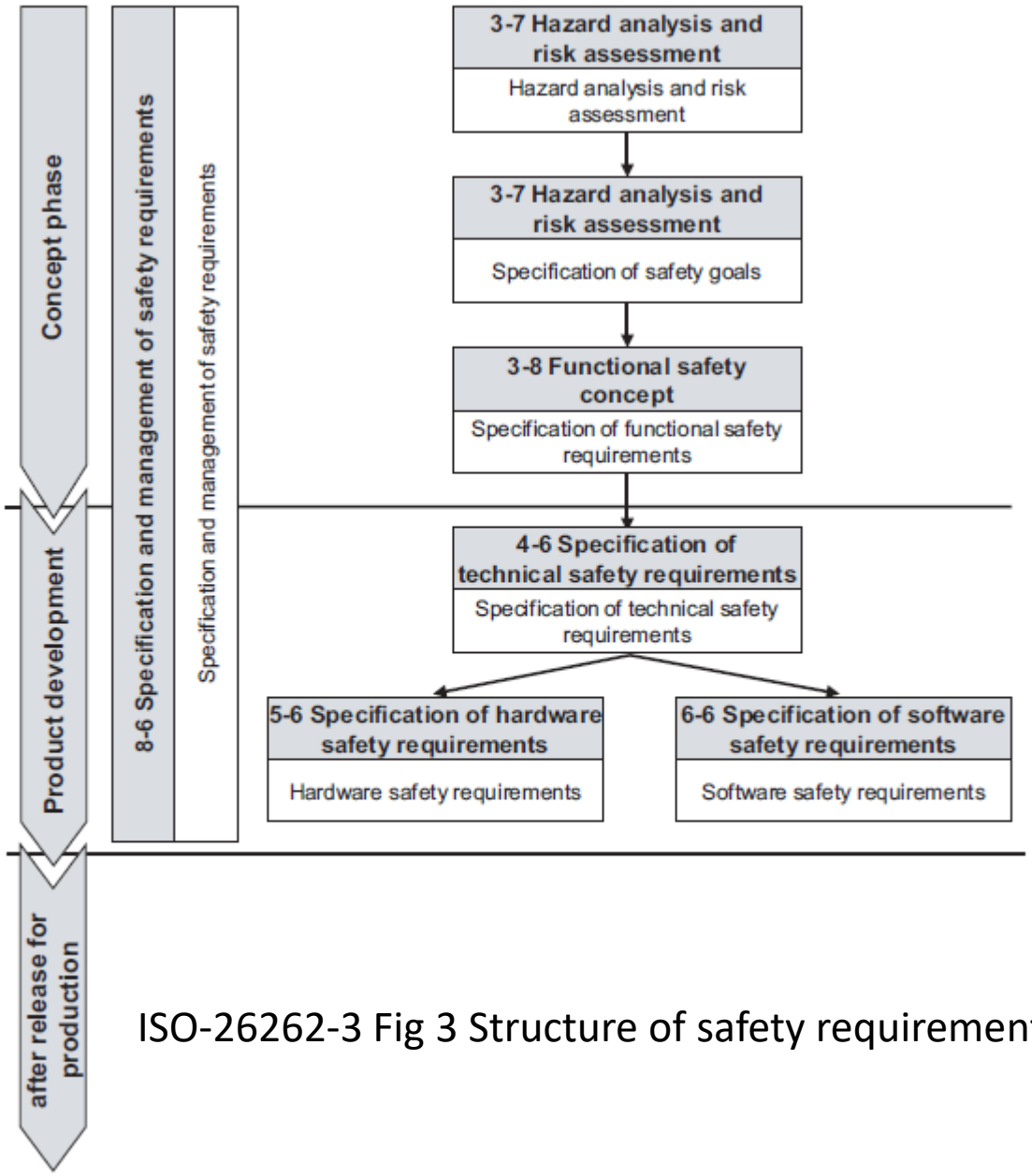
ISO-26262-3 Fig. 2

Management of functional safety

The functional safety requirements are allocated to the elements of the preliminary architecture.

High-level functional safety requirements are refined to low-level technical safety requirements

From Functional Safety Requirements (FSR) to Technical Safety Requirements (TSR)

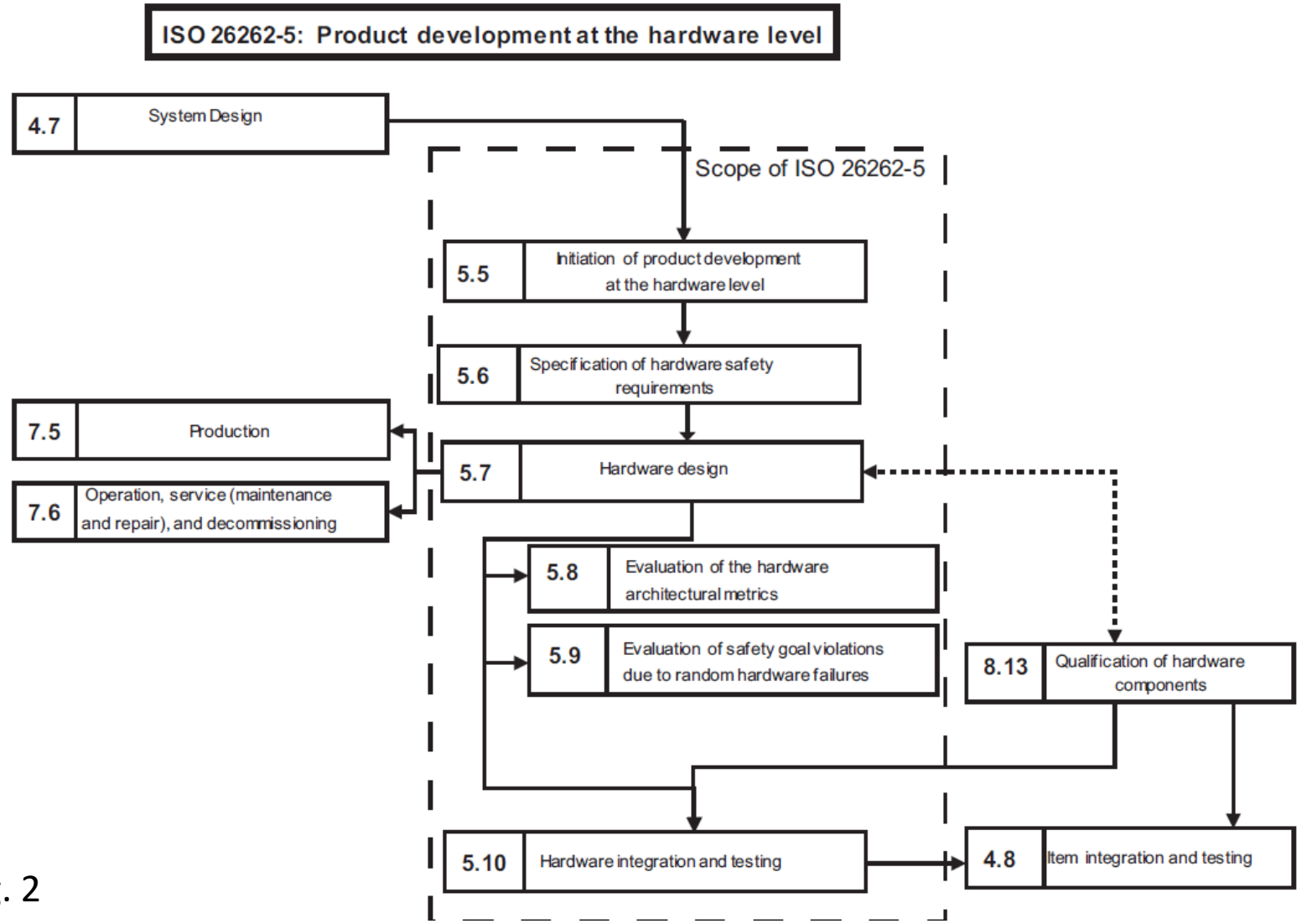


ISO-26262-3 Fig 3 Structure of safety requirements

Reference phase model for the product development at the hardware level

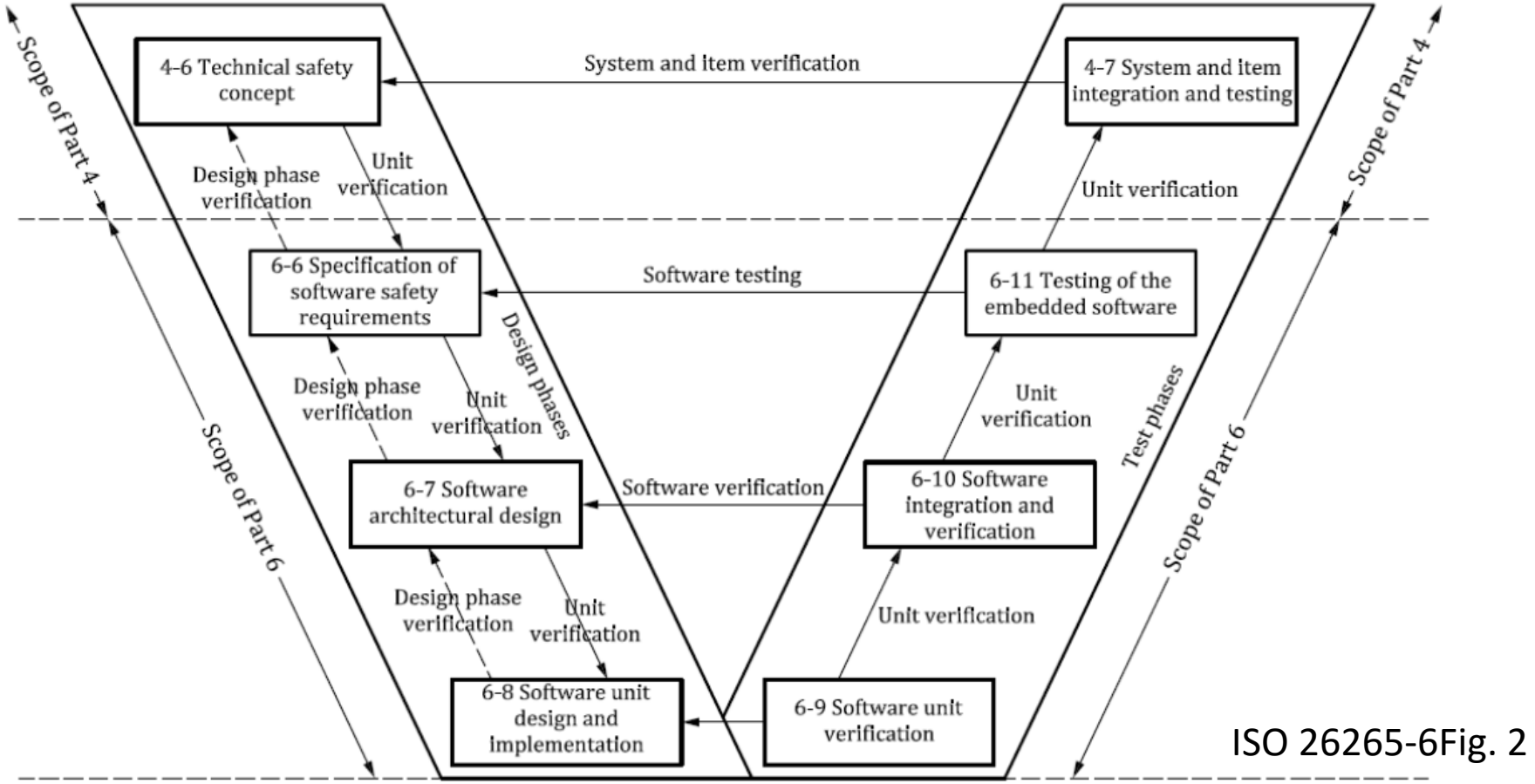
includes

- evaluation of violation of the safety goal due to random hardware failures



ISO 26265-5Fig. 2

Reference phase model for the software development



ISO 26265-6Fig. 2

Minimization of systematic faults during the software development

Safety analysis

The safety analysis includes

- the identification of conditions and causes, including faults and failures, that could lead to the violation of a safety goal or safety requirement;

- the identification of additional requirements for detection of faults or failures;

- the determination of the required responses (actions/measures) to detected faults or failures; and

- the identification of additional requirements for verifying that the safety goals or safety requirements are complied with, including safety-related vehicle testing.

Functional Safety standards

ISO/PAS 21448 Road vehicles — Safety of the intended functionality (SOTIF)
Autonomous (semi-autonomous) driving - standard under development

Applies to functionality that requires proper situational awareness in order to be safe. Guaranteeing the safety of the intended functionality in absence of faults ‘’

The road is icy. Without sensing the icy road condition, a self driving vehicle might drive at a faster speed than is safe for the condition’’ Taking that situation into account.
Safety hazards that result **without** system faillure.

Applies to systems such as emergency intervention systems and advanced driver assistance systems (autonomous and semi-autonomous driving).
These systems could have safety hazards without system failure.

Threat Analysis and Risk Assessment (TARA)

Security: risk assessment tools

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

DREAD risk assessment method

DREAD

qualitative risk analysis previously used at Microsoft.

Classify risk according to 5 categories:

– **D**amage potential

Ranks the extent of damage if a vulnerability is exploited

Consider

- type of data (sensitive/non-sensitive)
- amount of access (level of access, elevation of priviledge)

– **R**eproducibility

Ranks the relative effort and ease of repeatedly exploiting the threat

An exploit that can be performed repeatedly and reliably with little effort: high reproducibility

An exploit that requires additional knowledge and cannot reliably be performed: low reproducibility

DREAD risk assessment method

– **E**xploitability
Only focuses on the effort required to exploit the vulnerability (e.g. authentication is considered)
Remote attacks that do not require authentication and can be executed by automated tools: high exploitability
An attack to a local priviledged user in a private network: low exploitability

– **A**ffected users
estimate the number of users affected compared to the total number of users
Possibly give importance to the type of user or users that may be affected

– **D**iscoverability Measures
the likelihood that a vulnerability will be found by hackers
All vulnerabilities are discoverable with enough effort and discoverability rewards security by obscurity (system security should not depend on the secrecy of the implementation)
Often by convention the maximum value is assigned to discoverability

DREAD risk assessment method

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

Rating scale for each category: 1-10

A different implementation suggested:
rating values as numbers (3-high, 2-medium, 1-low)

Risk rating	Result
High	12-15
Medium	8-11
Low	5-7

Common Vulnerability Scoring System (CVSS)

CVSS is a published standard (CVSS Special Interest Group (SIG))
capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity

CVSS is comprised of three different metric groups: Base, Temporal, and Environmental. Each one consists of their own set of metrics.

"The Base metrics: reflects the severity of a vulnerability according to its intrinsic characteristics which are constant over time and across deployed user environments

The Temporal Metrics: adjust the Base severity of a vulnerability based on factors that change over time, such as the availability of exploit code.

The Environmental Metrics adjust the Base and Temporal severities to a specific computing environment. They consider factors such as the presence of mitigations in that environment."

Common Vulnerability Scoring System (CVSS)

Produced by the organization maintaining the vulnerable product (do not change over time and are common to all environments)

Base

Exploitability metrics

- **Access Vector**
- **Access Complexity**
- **Authentication**

The *vulnerable component* is typically a software application, module, driver, etc. (or possibly a hardware device)

Impact metrics

- **Confidentiality Impact**
- **Integrity Impact**
- **Availability Impact**

The *impacted component* could be a software application, a hardware device or a network resource. This potential for

- **Scopus**

Measuring *the impact of a vulnerability other than the vulnerable component*

Common Vulnerability Scoring System (CVSS)

Changes over time: the presence of a simple exploit kit would increase the CVSS score, while the creation of an official patch would decrease it.

Temporal

- **Exploitability**
  measures the likelihood of the vulnerability being attacked
- **Remediation Level**
  The typical vulnerability is unpatched when initially published. Workarounds or hotfixes may offer interim remediation until an official patch or upgrade is issued. Each of these respective stages adjusts the Temporal Score downwards, reflecting the decreasing urgency.
- **Report Confidence**
  measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details.

Common Vulnerability Scoring System (CVSS)

The Environmental metric group represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

Environmental

Security Requirements

- **Confidentiality requirement**
- **Integrity requirement**
- **Availability requirement**

These metrics enable the analyst to customize the CVSS score depending on the importance of the affected asset to a user's organization, measured in terms of Confidentiality, Integrity, and Availability.

That is, if an asset supports a business function for which Availability is most important, the analyst can assign a greater value to Availability relative to Confidentiality and Integrity. Each Security Requirement has three possible values: Low, Medium, or High

Modified Base Metrics

Modified Access Vector

....

Common Vulnerability Scoring System (CVSS)

Risk =

Base Metrics
f(x1, x2, …., xn)

Exploitability sub-score equation
Exploit()

Impact sub-score equation
Impact()

When the Base metrics are assigned values by an analyst, the Base equation computes a score ranging from 0.0 to 10.0

refined by

Temporal Metrics
f(y1, y2, …, yn)

more accurately reflect the relative severity posed by a vulnerability to a user's environment at a specific point in time in a computing environment.

specified by vulnerability bulletin analysts, security product vendors, or application vendors

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

specified by end-user organizations because they are best able to assess the potential impact of a vulnerability within their own computing environment

Score +

Vector string

https://www.first.org/cvss/calculator/3.0

Common Vulnerability Scoring System (CVSS)

"Note that all metrics should be scored under the assumption that the attacker has already located and identified the vulnerability. That is, the analyst need not consider the means by which the vulnerability was identified.

In addition, it is likely that many different types of individuals will be scoring vulnerabilities (e.g., software vendors, vulnerability bulletin analysts, security product vendors), however, note that vulnerability scoring is intended to be agnostic to the individual and their organization."

https://www.first.org/cvss/specification-document

CVSS : example

Base

Score: 0 – 10

Category	Subcategory	Value
Access Vector (AV)	- L (Local) accessible only on device	0.395
	- A (Adjacent network) attack is limited *at the protocol level* to a logically adjacent topology	0.646
	- N (Network) accessible remotely 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

This metric reflects the context by which vulnerability exploitation is possible.

This metric describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability.

Common Vulnerability Scoring System (CVSS)

Severity rating scale

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Different Metrics Equations:

Base Metrics Equations

Temporal Metrics Equations

Environmental Metrics Equations

https://www.first.org/cvss/specification-document

OWASP risk assessment rating methodologies

https://owasp.org/

Open Web Application Security Project (**OWASP**) web application security
Estimates both technical and business impact factors

Starts from the standard risk model:

Risk = Likelihood * Impact

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

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	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

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

Required Resources 'R'	Required Know-How 'K'	Threat Level 'T' 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

Security Level Determination matrix

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

ISO/SAE 21434 Road Vehicles: Cybersecurity Engineering (2021)

‘’This document addresses the cybersecurity perspective in engineering of electrical and electronic (E/E) systems within road vehicles. By ensuring appropriate consideration of cybersecurity, this document aims to enable the engineering of E/E systems to keep up with state-of-the-art technology and evolving attack methods.

- This document provides vocabulary, objectives, requirements and guidelines related to cybersecurity engineering as a foundation for common understanding throughout the supply chain. This enables organizations to:
- — define cybersecurity policies and processes;
- — manage cybersecurity risk; and
- — foster a cybersecurity culture.

This document can be used to implement a cybersecurity management system including cybersecurity risk management.’’