universidade de aveiro

Critical software

# Safety (and Security)

Robust Software – Nuno Silva

**Mestrado em Cibersegurança**

# Agenda

- Objectives
- Safety
- How to ensure Safety?
- A Safety lifecycle example
- Risk Management Process
- Safety & Security
- References
- Exercise #7

# Objectives

- Understand the need and the importance of Safety.
- Be able to contribute to a system risk/hazard analysis.
- Be able to contribute to a Failure Modes Analysis.
- Understand the relation between Safety and Security.
- Be able to assess a system based on an international safety standard.
- Robustness in Software must be with the goal to make it Safe and Secure!

# Safety

- A sensor that detects smoke and triggers the activation of a water sprinkler system inside a building.
- The enclosure that is placed around a socket to protect users against accidental contact with electrical parts.
- Train doors automatically close and remain closed during the length of the trip.

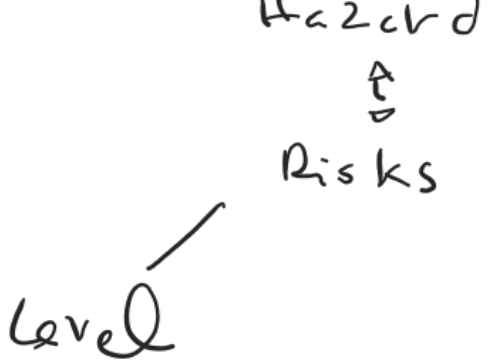
- These are just a few examples of safety measures that are utilized with electrical devices.

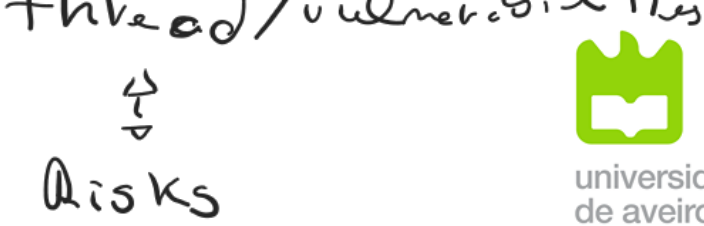
# Safety

- Safety is commonly defined as ***the freedom from unacceptable risk of physical injury***.

- Safety-critical industries are ruled by international standards that provide an extra assurance about the safety level of the systems by promoting safety as an integral aspect of devices and systems, thus protecting people, critical infrastructures, economies and the environment.
- These standards can address aspects of safety that apply to many products or specifically address a single product type or industry.

# Safety




universidade de aveiro

Critical software

- Watch this:
- A calculation that says that 19% of the World is Chinese and 44% is American

- Now imagine using those calcaulators for critical decisions...

# Safety Standards

- Three clear examples of industries that rely on safety:
- Automotive:
  - ISO 26262, "Road vehicles – Functional safety"
- Aeronautics:
  - DO-178C, “Software Considerations in Airborne Systems and Equipment Certification”
- Railway:
  - CENELEC EN 50128, “Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems”
  - CENELEC EN 50657 will take over…

# Safety Standards

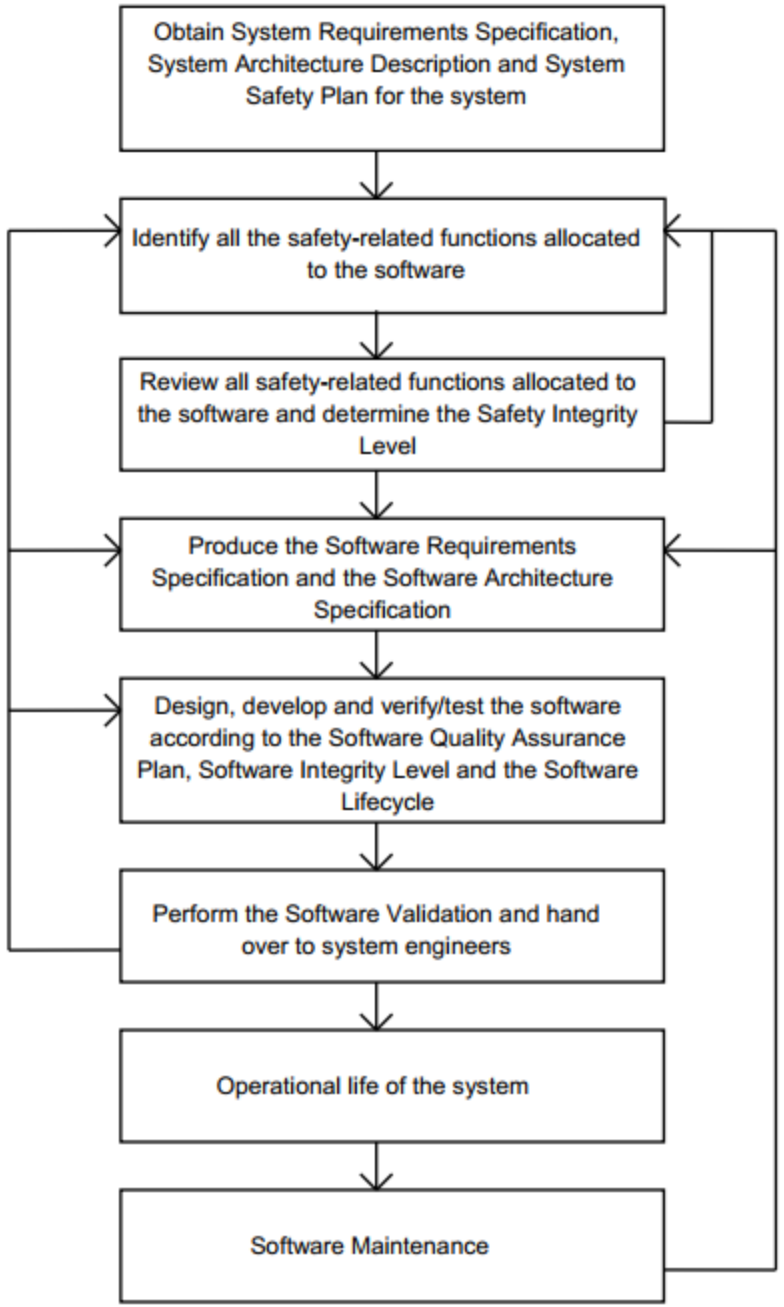
- But there are way more:
  - Think about nuclear power plants, weapons systems, medical devices, manned space vehicles, and so on.
  - Certification is generally mandatory.
  - But is a certification a guarantee?
- A list of EN standards

# How to ensure safety?

- Safety is “ensured” by strict rules, specific analysis and certification/qualification of systems
- We need to be in control, thus a set of clear processes must be planned and applied
- Lifecycle activities as for Security
- Assessments and Analysis (as for Security)

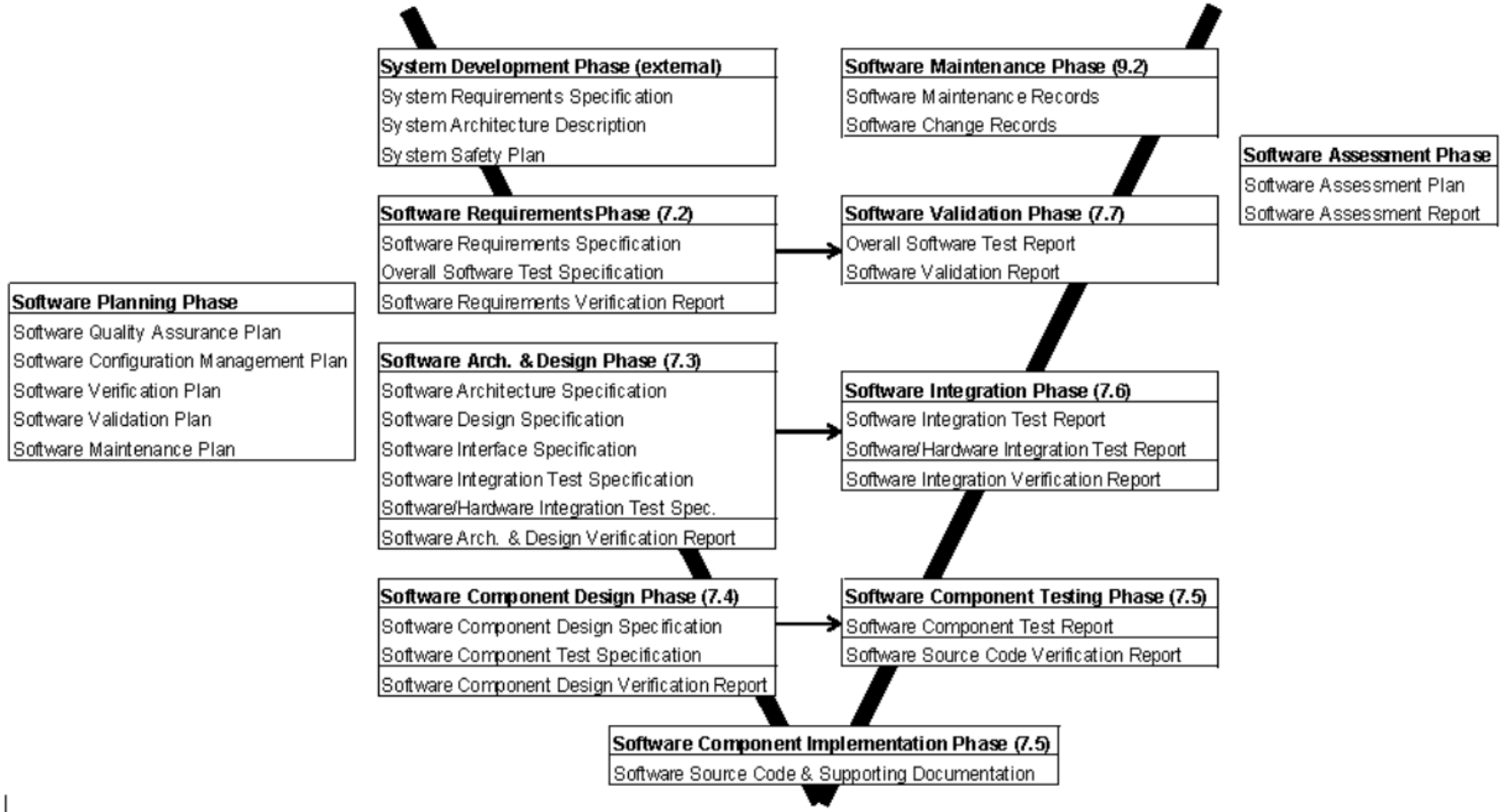
# How to ensure safety?

- Image from EN 50657



# How to ensure safety?

- Image from EN 50657



# How to ensure safety?

- Training or proven experience
- System/Environment knowledge
- Risk/Hazards Analysis
- System and Safety Requirements
- Follow up on development (traceability)
- Verify and Validate
- Build and maintain a Safety Dossier (Safety Case)
- Support external Independent Assessors…

# How to ensure safety?

- Do you remember?

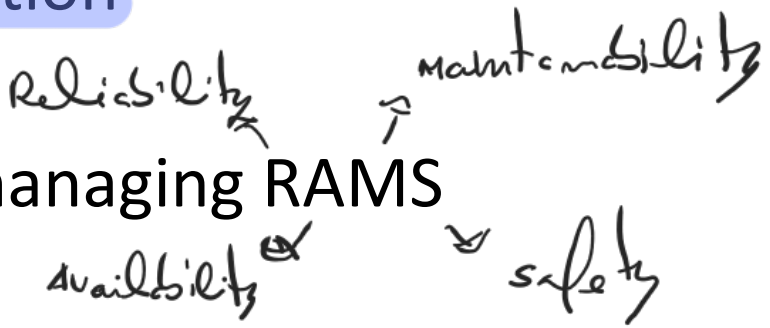
| Security Phase | Safety phase |
|---|---|
| Education and awareness | Training or proven experience |
| Project inception | Project risks/hazards awareness<br>Environment limitations<br>Tool qualification<br>Safety Assessment Plan |
| Analysis and requirements | Hazards Analysis<br>Safety Related Application Conditions (SRAC) incorporation<br>Specifications (System and Safety) |
| Architectural and detailed design | = |
| Implementation and testing | = |
| Release, deployment, and support | Certifications<br>Release, deployment, and support |

# A safety Lifecycle Example

- EN 50126:1999 Railway Applications – The Specification and Demonstration Of Reliability, Availability, Maintainability And Safety (RAMS)
  - Published by CENELEC – European Committee for Electrotechnical Standardisation
  - Provides Railway Authorities and the railway support industry with a process that enables the implementation of a consistent approach to the management of RAMS
  - Can be applied systematically throughout all phases of the lifecycle of a railway application

# A safety Lifecycle Example

- Defines RAMS in terms of reliability, availability, maintainability and safety and their interaction




- Defines a process for managing RAMS
- Enables conflicts between RAMS elements to be controlled and managed effectively
- Defines a systematic process for specifying requirements for RAMS and demonstrating that these requirements are achieved

# A safety Lifecycle Example

- EN 50126 Lifecycle
  - Is a sequence of phases, each containing tasks, covering the life of a system from initial concept through to decommissioning and disposal.

  - The lifecycle provides a structure for planning, managing, controlling and monitoring aspects of a system, including RAMS

# A safety Lifecycle Example

| 1. Concept | 2. System Definition and Application Conditions | 3. Risk Analysis | 4. System Requirements | 5. Apportionment of System Requirements |
|---|---|---|---|---|
| • **Develop a level of understanding of the system** sufficient to enable all subsequent RAMS tasks<br>• Review previously achieved safety performance | • Define the mission profile of the system and its boundaries<br>• Establish the application conditions influencing the characteristics of the system<br>• **Define the scope of the hazard analysis**<br>• Establish the Safety Plan | • **Perform System Hazard & Safety Risk Analysis**<br>• Set-up Hazard Log | • **Specify the overall System Safety requirements**<br>• Establishment of Safety Management | • Define the RAMS acceptance criteria for the designated sub-systems and components<br>• **Apportion System Safety targets and requirements** to designated sub-systems and components |

# A safety Lifecycle Example

universidade de aveiro

Critical software

| 6. Design and Implementation | 7. Manufacturing | 8. Installation | 9. System Validation | 10. System Acceptance |
|---|---|---|---|---|
| • **Create** sub-systems and components<br>• **Demonstrate that sub-systems and components conform to RAMS requirements**<br>• Implement Safety Plan<br>• Prepare Generic Safety Case | • Implement a process which produces RAMS-validated sub-systems and components<br>• Use Hazard Log | • Assemble and install the total combination of sub-systems and components<br>• Initiate system support arrangements<br>• Establish Installation Programme | • **Validate that the total combination of sub-systems, components and external risk reduction measures comply with the RAMS requirements for the system**<br>• Commission the total combination of sub-systems, components risk reduction measures<br>• Prepare, and if appropriate accept, the Application Specific Safety Case | • Assess compliance of the total combination of sub-systems and components with the overall RAMS requirements of the complete system<br>• **Accept the system for entry into service**<br>• Assess Application Specific Safety Case |

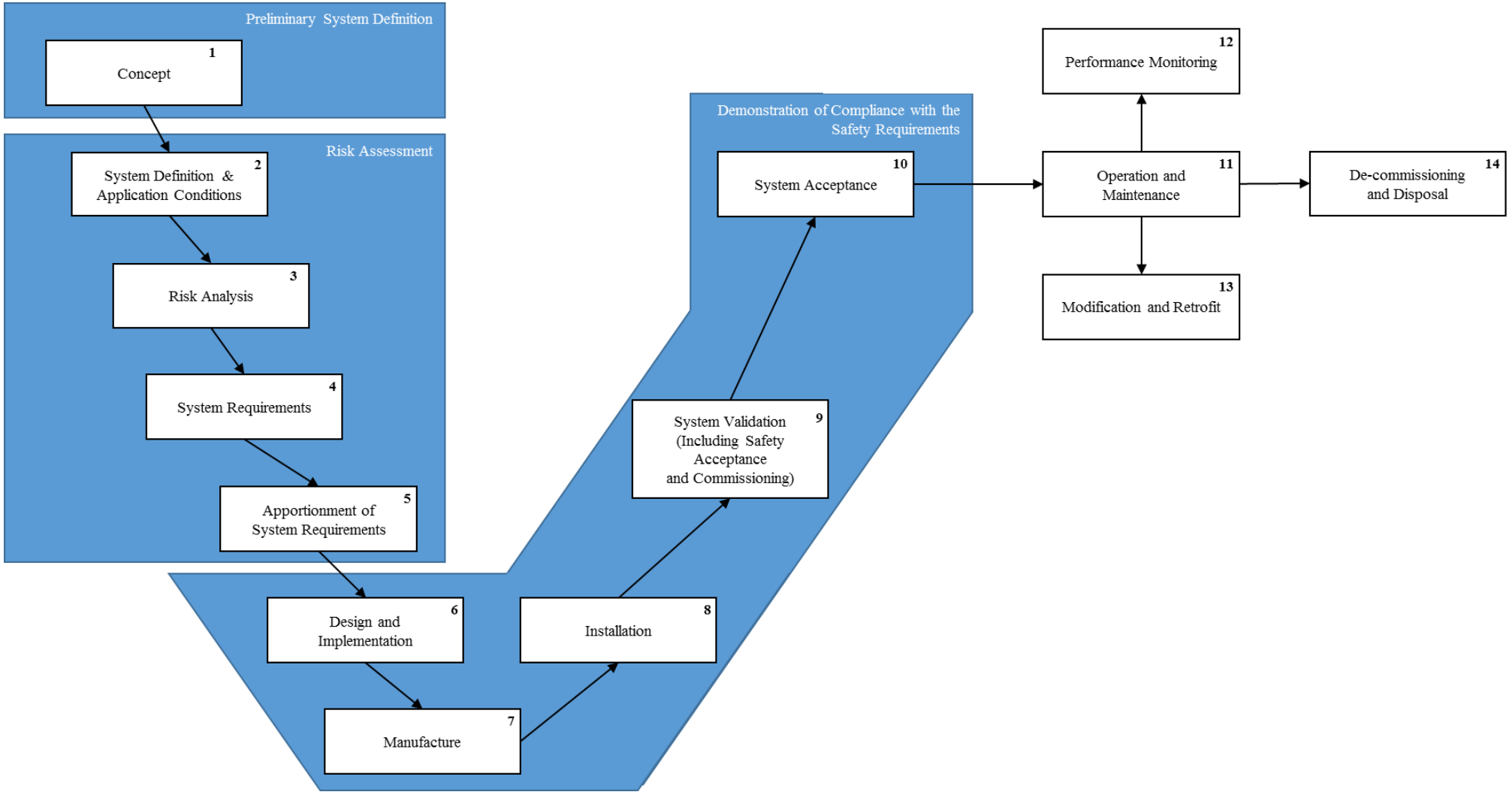
# A safety Lifecycle Example

RAMS in safety lifecycle

| 11. Operation and Maintenance | 12. Performance Monitoring | 13. Modification and Retrofit | 14. Decommissioning an Disposal |
|---|---|---|---|
| • **Operate** maintain and support the total combination of sub-systems and components such that compliance with system RAMS requirements is maintained | • Maintain confidence in the RAMS performance of the system<br>• **Collect, analyse, evaluate and use performance and Safety statistics** | • Control system modification and retrofit tasks to maintain system RAMS requirements<br>• **Consider safety implications for modification and retrofit** | • Control system decommissioning and disposal tasks<br>• Perform hazard analysis and risk assessment |

No certification ?

# A safety Lifecycle Example



# Risk Management Process

- Organized around five major areas
  - System Definition
  - Hazard Identification and Classification
  - Risk Evaluation and Risk Acceptance
  - Safety Requirements and Hazard Management
  - Independent Assessment

# System Definition

- Must address at least: ,
  - system objective (intended purpose);
  - system functions and elements (including human, technical and operational elements);
  - system boundary including other interacting systems;
  - physical (interacting systems) and functional interfaces;
  - system environment (e.g. energy and thermal flow, vibrations, electromagnetic interference, operational use);
  - existing safety measures – and the definition of any additional identified safety requirements;
  - assumptions that determine the limits for the risk assessment.

# Hazard Identification and Classification

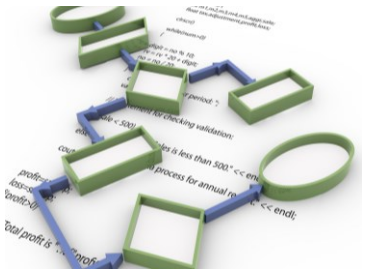
- Systematic activity by a team with a wide-ranging expertise

- Identify all foreseeable hazards for
  - the whole system under assessment
  - its functions where appropriate
  - its interfaces

- Everything shall be registered in the hazard record

# Desk-based Hazard Identification

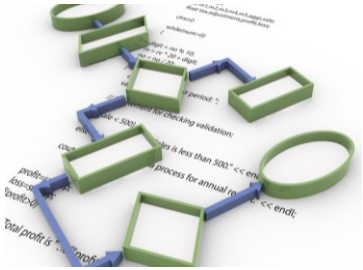
- Desk-based
  - Typically applied by a single experienced person;
  - An individual working alone to apply some structured analysis process;
  - Can be as simple as reviewing data or an existing hazard list;
  - Multi-expertise is, however, recommended.



# Desk-based Hazard Identification

- Typically variants of Failure Modes and Effects Analysis (FMEA)
  - a structured process to identify:
    - the potential failure modes of the elements of a system;
    - the causes of these failures;
    - their effects on larger assemblies and the whole system.
  - FMEA can be very time consuming

- A Functional Hazard Analysis (FHA)
  - Is a systematic, comprehensive examination of functions to identify and classify failure conditions of those functions according to their severity;
  - Can be applied at system-level;
  - FHA involves less work than FMEA;
  - Can be started earlier than FMEA, because it just needs a specification, and not a design;
  - FHA is not good at finding hazards that are not easily characterised as the failure of a function (such as electromagnetic interference or fuel leakage).



# Workshop-based Hazard Identification

- Helps ensuring completeness by drawing on the collective experience of a group of experts

  Systematic identification, by using wide-ranging expertise from a competent team, of all reasonably foreseeable hazards for the whole system under assessment, its functions where appropriate and its interfaces.

- Various different approaches
  - Structured Hazard and Operability (HAZOP)
  - A more informal ‘brainstorming’ exercise (e.g. based on checklists)

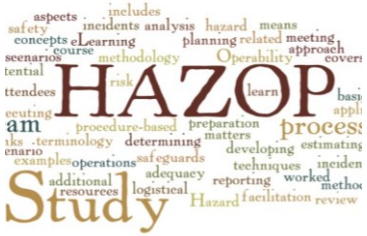
- Some combination of the desk-based and workshop-based

- The approach or combination of approaches should be matched to the complexity and novelty of the system under assessment.

# HAZOP

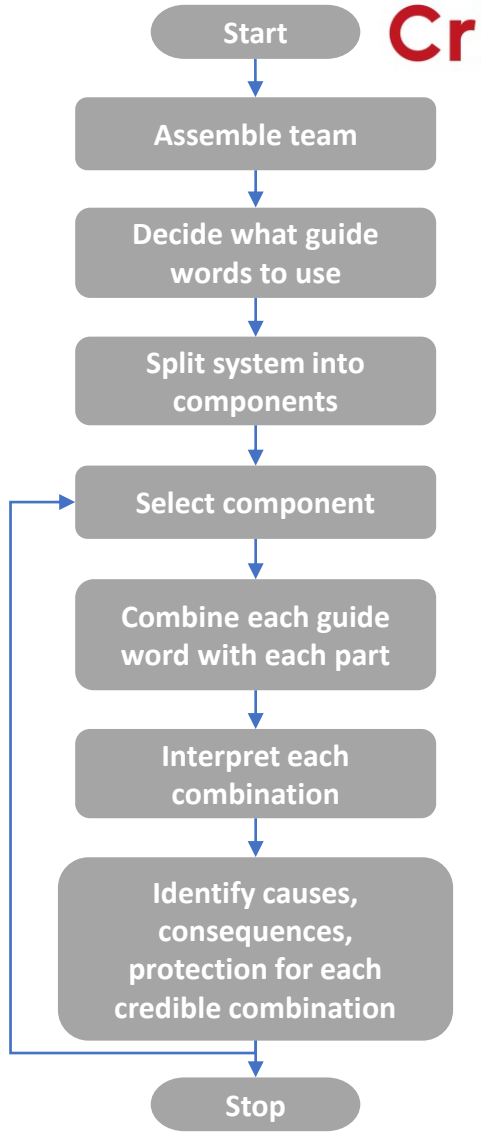
- **Aim**: To determine safety hazards in a proposed or existing system, their possible causes and consequences, and recommend actions to minimise the chance of their occurrence

- Team normally consists of:
  - a study leader
  - a recorder (documents the meeting)
  - a designer (explains the design)
  - users (e. g. train driver, train operator)
  - specialists (expert of the system or the study)
  - and maybe a maintainer

# HAZOP basic guide words

| Guide word | Meaning |
|---|---|
| NO OR NOT | Complete negation of the design intent |
| MORE | Quantitative increase |
| LESS | Quantitative decrease |
| AS WELL AS | Qualitative modification/increase |
| PART OF | Qualitative modification/decrease |
| REVERSE | Logical opposite of the design intent |
| OTHER THAN | Complete substitution |
| EARLY | Relative to the clock time |
| LATE | Relative to the clock time |
| BEFORE | Relating to order or sequence |
| AFTER | Relating to order or sequence |



# Hazard Identification and Classification

- Approaches
  - Desk-based
  - Workshop-based
  - Some combination of the two

- The approach or combination of approaches should be matched to the complexity and novelty of the proposed change

- Any identified safety measures shall be registered in the hazard log

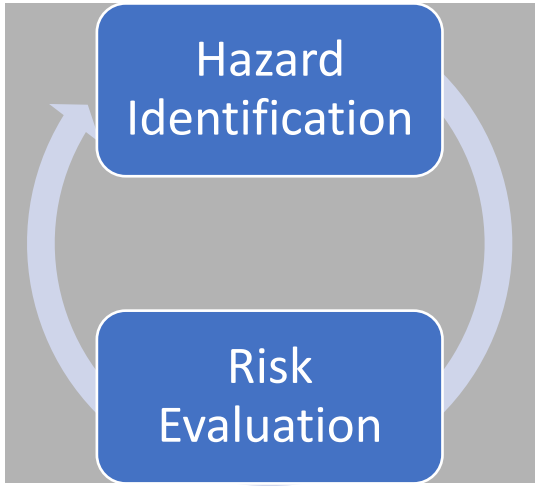
# Broadly acceptable risks

- Risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional safety measure;
- Hazards associated with a broadly acceptable risk need not be analysed further:
  - Based on expert judgement;
  - The classification is justified and recorded;
  - The contribution of all the broadly acceptable risks must not exceed a defined proportion of the overall risk;

# Hazard Identification and Classification

- Carried out only up to a level of detail necessary to identify where safety measures are expected to control the risks in accordance with one of the risk acceptance principles

**‘Hazard Classification’ can be seen as a filtering exercise to remove those hazards that are judged to be of broadly acceptable risk**




- Iteration may be necessary between the risk analysis and the risk evaluation phases

# Risk Evaluation and Risk Acceptance

- **Goal**: assess the acceptability of the risk associated with the proposed system
  - This is done by evaluating the risk associated with each hazard of the system

**The overall risk associated with the system is acceptable when the risk associated with each hazard is acceptable**

# Risk Evaluation and Risk Acceptance

- Risk acceptability is evaluated by using one or more of the following risk acceptance principles:
  - the application of codes of practice;
  - a comparison with similar systems;
  - an explicit risk estimation.

- The assessor shall:
  - demonstrate that the selected risk acceptance principle is adequately applied;
  - check that the selected risk acceptance principles are used consistently.

# Use of codes of practice

- “A written set of rules that, when correctly applied, can be used to control one or more specific hazards.”


- Codes of practice must:
  - be widely acknowledged in the specific domain;
  - be relevant for the control of the considered hazards, meaning that it has been successfully applied in similar situations;
  - be publicly available for all actors who want to use them, not necessarily free of charge.

# Use of codes of practice

- Codes of practice cover documents described as standards, procedures or rule books, for railways, for example:
  - Technical Specifications for Interoperability (TSIs);
  - National Technical Rules and National Safety Rules;
  - Rail Industry Standards;
  - British Standards, Euronorms and other international standards;
  - Network Rail company standards;
  - Association of Train Operating Companies (ATOC) standards;
  - Etc.

**Codes of practice are rarely written just to control hazards – they are normally also written to deliver other benefits such as efficiency, interoperability and reliability**

# Use of codes of practice

When

- Safety measures from the codes of practice appropriately cover the hazard, and
- The codes of practice are fully complied with.


Then

- The safety measures from the codes of practice are considered as safety requirements for the hazard;
- Record the reasons for believing that the safety requirements from the codes of practice appropriately cover the hazard;
- Add the safety requirements in the system definition.

# Use of reference system

- Comparison with reference system(s) principle:
  - Compare a new system against an existing system which is known to be associated with an acceptable level of risk;
  - If the systems are sufficiently similar that there is no additional risk associated with the new system, then the risk from it is considered acceptable;
  - The safety measures from the reference system will be adopted by the new system as safety requirements.

# Use of reference system

- The reference system must:
  - have been proven in-use to have an acceptable safety level and would still qualify for approval in the Member State where the system is to be introduced.
  - have “similar” functions and interfaces as the system under assessment;
  - be used under “similar operational conditions” as the system under assessment;
  - be used under “similar environmental conditions” as the system under assessment.


# Use of reference system

Steps:

1. The risks associated with the hazards covered by the reference system are considered as acceptable;


2. The safety measures from the reference system will be adopted by the new system as safety requirements;

3. These safety requirements are registered in the hazard record as safety requirements for the relevant hazards.

# Deviation from the reference system

- In case of deviation of the systems, the risk evaluation shall demonstrate that the system under assessment reaches at least the same safety level as the reference system;
- One way of carrying out this approach is:
  - Identify all differences between the systems which might affect risk;
  - Identify all differences between the operational and environmental conditions which might affect risk;
  - For each difference in both lists assess if it would make the risk higher or lower;
  - If the results of the previous step demonstrate that the risk associated with the hazard is not greater in the SUA, then the risk associated with that hazard is accepted. The level of risk met by the reference system sets the risk assessment criteria,


# Explicit risk estimation

- Explicit risk estimation can be used where
  - We are unable (or unwilling) to address the hazards via a code of practice or comparison with a reference system;
  - Deviations are necessary from codes of practice or reference systems;
  - We need to explicitly analyse the hazards and evaluate design principles or safety measures.


# Explicit risk estimation

- Explicit risk estimation is an assessment of the risks associated with hazard(s)
- The risk is defined as a combination of
  - The rate of the occurrence of the hazard causing harm (the frequency)
  - The degree of severity of the harm (the consequence)

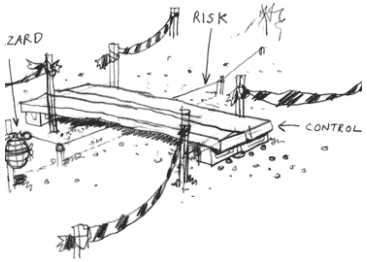
- Explicit risk estimation can be qualitative, semi-quantitative or quantitative
  - Depending on the availability of data and confidence in such data

- The methods used for explicit risk estimation shall reflect correctly the system under assessment and its parameters (including all operational modes)

- The results shall be sufficiently accurate to provide a robust basis for decision-making

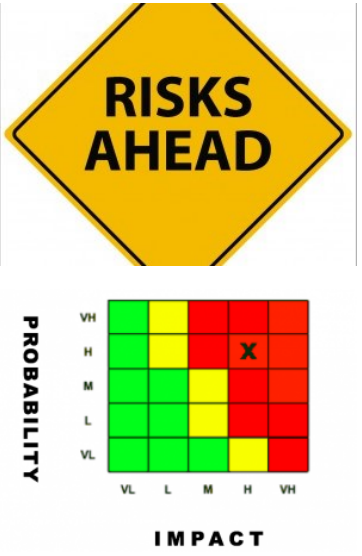
# Qualitative risk estimation

- The classification of an hazard is made on the basis of expert judgement
- In practice, this can be undertaken via the collective opinion of the attendees at an hazard identification workshop
- For a straightforward hazard:
  - Identify the causes of the hazard, and document as a table or short explanation
  - Identify the possible consequences of the hazard and the factors that affect those consequences, and document as a table or short explanation
  - Identify the existing safety measures which control the hazard
  - Identify the practical additional safety measures which might be implemented to control the hazard further

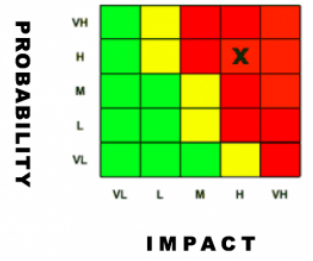

# Semi-quantitative risk estimation

- Used when some data is available, or a good degree of judgment can be applied to estimates of the frequency and consequences of each accident;
- Typically uses a 5 x 5 matrix with the frequency and consequence rankings broadly separated by a fixed factor, but this does not have to be the case;
- The size of the matrix and the factor difference in frequency and consequence rankings should suit a particular stakeholders' operation.



# Semi-quantitative risk estimation

- The main advantages of using a risk matrix:
  - It is an easily understandable representation of relative risk levels;
  - Tie can be applied relatively quickly;
  - It ss readily understandable by those whose inputs and opinions are needed to apply it;
  - It enables the combination of frequency and consequences to be represented in an intuitive visual way.


- The explicit risk estimation involves:
  - Identifying the possible causes of the hazard and estimate the likelihood of each cause resulting in an accident;
  - Identifying the possible consequences of the hazard and assess their severity.

# Likelihood look-up table

| RANKING | CATEGORY | DESCRIPTION |
|---|---|---|
| 5 | Frequent or almost certain | Event occurs many times during the period of the project (or life of the facility). |
| 4 | Likely | Event likely to occur once or more during the period of the project (or life of the facility). |
| 3 | Possible | Event could occur during the period of the project (or life of the facility). |
| 2 | Improbable | Event is unlikely to occur, but it is possible. Means an occurrence of failure at a frequency less than or equal to $10^{-7}$ per operating hour. |
| 1 | Highly improbable | May occur only in exceptional circumstances. Means an occurrence of failure at a frequency less than or equal to $10^{-9}$ per operating hour. |

# Consequence look-up table

| RANKING | CATEGORY | DESCRIPTION |
|---|---|---|
| 5 | Catastrophic | A “catastrophic accident” means an accident typically affecting a large number of people and resulting in multiple fatalities and/or major damage to the environment. |
| 4 | Critical | A “critical accident” means an accident typically affecting a very small number of people and resulting in at least one fatality |
| 3 | Moderate | Small injuries requiring medical treatment and some lost time |
| 2 | Minor | Minor injuries, first aid only required |
| 1 | Insignificant | No injuries or negligible social cultural impacts |

# Frequency/Consequence look-up table

| Frequency / Consequence | | Insignificant | Minor | Moderate | Critical | Catastrophic |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Frequent or almost certain | 5 | 6 | 7 | 8 | 9 | 10 |
| Likely | 4 | 5 | 6 | 7 | 8 | 9 |
| Possible | 3 | 4 | 5 | 6 | 7 | 8 |
| Improbable | 2 | 3 | 4 | 5 | 6 | 7 |
| Highly improbable | 1 | 2 | 3 | 4 | 5 | 6 |

| | | |
|---|---|---|
| 8 – 10 | Intolerable | Risks considered Intolerable shall be eliminated. |
| 7 | Undesirable | Accepted only when risk reduction is impracticable and with the agreement of the Safety Regulatory Authority (SFA), as appropriate.<br>Action plans must be developed with clear assignment of individual responsibilities and timeframes. |
| 5 – 6 | Tolerable | Acceptable with adequate control and with the agreement of the SFA.<br>Risk requires specific ongoing monitoring and review, to ensure level of risk does not increase. Otherwise manage by routine procedures. |
| 2 – 4 | Negligible | Acceptable with/without the agreement of the Safety Regulatory Authority.<br>Risk can be accepted or ignored. Manage by routine procedures, however unlikely to need specific application of resources. |

# Calibrating the risk matrix

- Risk classification matrices are used for ranking and comparing the risk of different hazards
- The matrix must be calibrated so that relative risk of different hazard is preserved across the various risk classifications
  - Achieved by having the same factor difference (a factor of 5) between each frequency and consequence category

| | Once in | No / year | |
|---|---|---|---|
| Frequent or almost certain | 12 days | 31.25 | 5 |
| Likely | 2 months | 6.25 | 4 |
| Possible | 9 months | 1.25 | 3 |
| Improbable | 4 years | 0.25 | 2 |
| Highly improbable | 20 years | 0.05 | 1 |

# Quantitative risk estimation

- Risk in the context of safety can be defined as a measure of the fatalities and weighted injuries (FWIs) that are estimated to occur per year.
- Can be calculated as the product of how often an event is likely to occur per year (the event frequency) and the consequences (injuries, fatalities or incidents of shock / trauma) that could arise should an event occur, that is:

| Frequency of an accident (resulting from a hazard) | X | The consequences of the accident | = | Collective Risk |
|---|---|---|---|---|
| e.g. events / year | | e.g. expected FWIs / event | | e.g. expected FWIs / year |

# Safety measures

- Safety measures are defined as:

  ‘a set of actions either reducing the rate of occurrence of a hazard or mitigating its consequences in order to achieve and/or maintain an acceptable level of risk.’

- Safety measure is a broad term, encompassing:
  - Measures that are in place prior to the system implementation;
  - New measures which might be considered for the application;
  - Safety measures that are to become formal safety requirements.

# Safety requirements

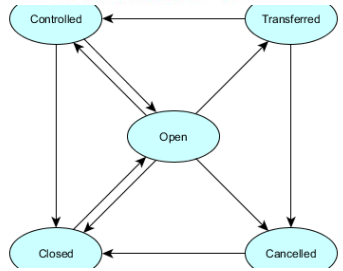
- “’safety requirements’ mean the safety characteristics (qualitative or quantitative, or when needed both qualitative and quantitative) necessary for the design, operation (including operational rules) and maintenance of a system in order to meet legal or company safety targets;”
- Safety requirements may include requirements on the technical system, but also requirements on the operational and maintenance arrangements
  - Safety-Related Application Conditions (SRAC)


# Hazard Management

- Hazard management Process: create and update the Hazard record
  - Track the progress in monitoring risks associated with the identified hazards
  - Includes all hazards, together with all related safety measures and system assumptions identified during the risk assessment process
  - Contains a clear reference to the origin of the hazards and to the selected risk acceptance principles
  - Clearly identify the actor(s) in charge of controlling each hazard
  - After system acceptance, the hazard record is maintained by the infrastructure manager or the railway undertaking

- Exchange of information
  - Communicate all hazards that cannot be controlled by one actor alone and shall be communicated to another relevant actor.

# Hazard life cycle




- Hazard life cycle
  - **Open**: initial status after a hazard has been identified
  - **Controlled**: risk evaluation process has been completed and safety requirements have been established which are sufficient to control risk to an acceptable level
  - **Cancelled**: potential hazard is not an actual hazard or is wholly contained within another hazard so no further action is necessary
  - **Transferred**: hazard has been transferred to another actor who now takes the lead
  - **Closed**: compliance with all safety requirements related to the hazard has been demonstrated

# Independent Assessment

- Independent assessment of the correct application of the risk management process and its results is mandatory by an Assessment Body
- The Assessment Body shall have:
  - Competence in risk management: knowledge and experience of the standard safety analysis techniques and of the relevant standards;
  - All relevant competences for assessing the parts of the system;
  - Competence in the correct application of safety and quality management systems or in auditing management systems.

# Hazard Analysis Example

- Sample Template
- Consider an existing train system with driver and assistant, reduced to one driver only;
- Intended Change: move from two-man operation to DOO(p) – Driver Only Operation for passenger trains;
- Change deemed ‘significant’ because it:
  - Affects safety;
  - Would generally be a novel mode of operation for the train operating company and route and may require the introduction of new technology or equipment;
  - Would be fairly complex because it involves a range of different technical and operational interfaces;
  - Affects organisational structure;

# Hazard Analysis Example

- Four representative scenarios for analysis
  - DOO(p) on a straight platform with the driver performing look-back;
  - DOO(p) on a negatively curved platform with the driver using lineside CCTV cameras to view the doors;
  - DOO(p) on a curved platform with platform staff supporting dispatch (with and without right-away indicators);
  - DOO(p) on a straight platform with a nearby level crossing;

# Hazard Analysis Example

# Hazard Analysis Example

| ID | Hazard |
|---|---|
| HZ-01 | Doors closed with person (or object attached to person) not clear |
| HZ-02 | Train dispatched with person trapped in doors |
| HZ-03 | Train dispatched with person in high risk position of the dispatch corridor |
| HZ-04 | Person returns to train once it has been dispatched |
| HZ-05 | Train dispatched with person fallen between train and platform |
| HZ-06 | Wrongside door release - doors released off platform |
| HZ-07 | Train stopped short: doors released off platform |
| HZ-08 | Long train at short platform: all doors released, some off the platform |
| HZ-09 | Train dispatched against-signal |
| HZ-10 | Train accelerates towards a red signal after being dispatched on a yellow |

No hazards is considered as 'reasonably acceptable'
➔ Continue to the risk evaluation

# Safety & Security

- **Information Disclosure not present...**

| STRIDE Classification | Domain | Threat Description |
|---|---|---|
| Denial of Service | Airborne, Space, Automotive, Railway | Jamming and flooding ground station, VLAN flooding attack, Flooding signals to satellite, Fake correspondent node addresses, Unauthorized Brake, Attacking Active Brake Function, Attacking E-Toll, Head Unit Attack, Flashing per OBD, WLAN Attack, Disturbing passenger Information system, GSM-R Attack (DoS - Denial of service) |
| Elevation of privileges | Airborne, Automotive, Railway | VLAN Tagging attack, Attacking E-Toll, Force Green Wave/Getting traffic lights green ahead of the attacker, Flashing per OBD, E-Call, Manipulate Speed Limits, Manipulate Traffic Flow, Database attack |
| Repudiation | Automotive | Engine DoS-Attack (Engine Refuse to Start) |
| Spoofing | Airborne, Space, Railway | Spoofing attacks on the Automatic Dependent Surveillance – Broadcast (ADS-B) system, Fake correspondent node addresses, Spoofed binding updates, Fake/Modified telecommands delivered to satellites, WLAN Attack |
| Tampering | Airborne, Automotive, Railway, Space | Interference in communications, Tampering GPS coordinates, Tampering attacks on ADS-B, Head Unit Attack, Simulate Traffic Jam, Tamper with Warning Message, Flashing per OBD, Manipulate physical components, Manipulate signalling components, GPS data falsification, Disturbing passenger Information system, Tampering satellite Software updates |

# Safety & Security

- See examples in CECRIS_20150129_WP2_D2.3_IntegrationOfSafetyAndSecurity_R08.pdf

# Apply a Standard to a Project

- Example of ISO/IEC 62443, Security for industrial automation and control systems:
  - IEC TS 62443-1-1:2009 - Terminology, concepts and models
  - IEC 62443-2-1:2010 - Establishing an industrial automation and control system security program
  - IEC TR 62443-2-3:2015 - Patch management in the IACS environment
  - IEC 62443-2-4:2015 - Security program requirements for IACS service providers
  - IEC 62443-2-4:2015/AMD1:2017 - Amendment 1
  - IEC TR 62443-3-1:2009 - Security technologies for industrial automation and control systems
  - IEC 62443-3-2:2020 - Security risk assessment for system design
  - IEC 62443-3-3:2013 - System security requirements and security levels
  - IEC 62443-4-1:2018 - Secure product development lifecycle requirements
  - IEC 62443-4-2:2019 - Technical security requirements for IACS components

# Apply a Standard to a Project

- Standards are expensive
- Shall be applied from the beginning
- Will be certified
- But, known good practices and requirements can/shall always be applied even if no certification is required

- It represents a magnificent log of good design practices
- ISO/IEC 62443 Sample Checklist

# Safety Plan

- Done at the initial planning phase of the project
- Basically defines "Who does what and when“ in the scope of safety management activities
- Is one the project plans and it defines the relation with other relevant plans: Project Management Plan (PMP), Quality Assurance Plan (QAP) and Validation and Verification Plan (VVP)
- Should provide a short description of the system as part of the introduction
- Should define in which artefacts the Safety Requirements and details on how they are to be achieved, namely in terms of:
  - Safety roles, responsibilities and bodies
  - Safety tasks and relation to the project lifecycle phases
  - Hazard identification and analysis
  - Risk Assessment
  - Assurance of safe design
  - Verification and Validations activities
  - Safety Assessment and audits
  - Safety related deliverables
  - Safety assurance processes
  - Constraints and assumptions
- Should define the structure of the Safety Case

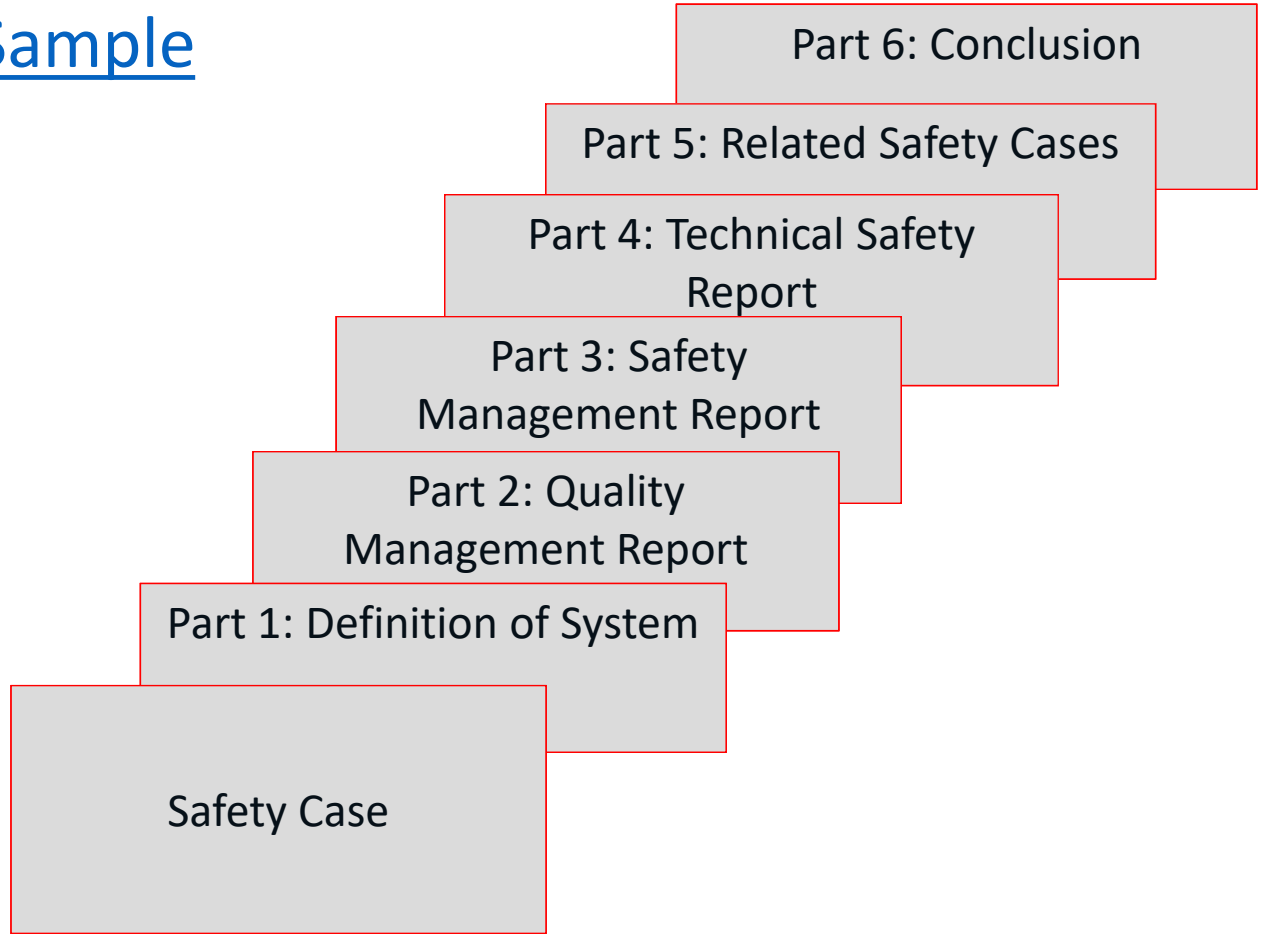
| Lifecycle Phase | Phase related Safety tasks |
|---|---|
| 6. Design and Implementation | Implement Safety Plan by review, analysis, testing and data assessment, addressing:<br>• Hazard Log<br>• Hazard Analysis & Risk Assessment<br>• Justify safety related design decisions<br>• Undertake Programme Control, covering:<br>  • Safety Management<br>  • Control of sub-contractors & suppliers<br>• Prepare Generic Safety Case<br>• Prepare (if appropriate) Generic Application Safety Case |

# Safety Case

- Is the key document that documents demonstration that the product complies with the specified safety requirements
- Evidence can be shown in related documents, all referred in the Safety Case
- Should cover
  - Technical requirements
  - Quality processes
  - Safety Processes
- Concludes unequivocally on if and how the system complies with the expected SIL (Safety Integrity Level)
- Identifies and describes (or points to the description) on all the open points an SRACs

# Safety Case

- Safety Case Sample



# Safety Case :: Quality Management Report

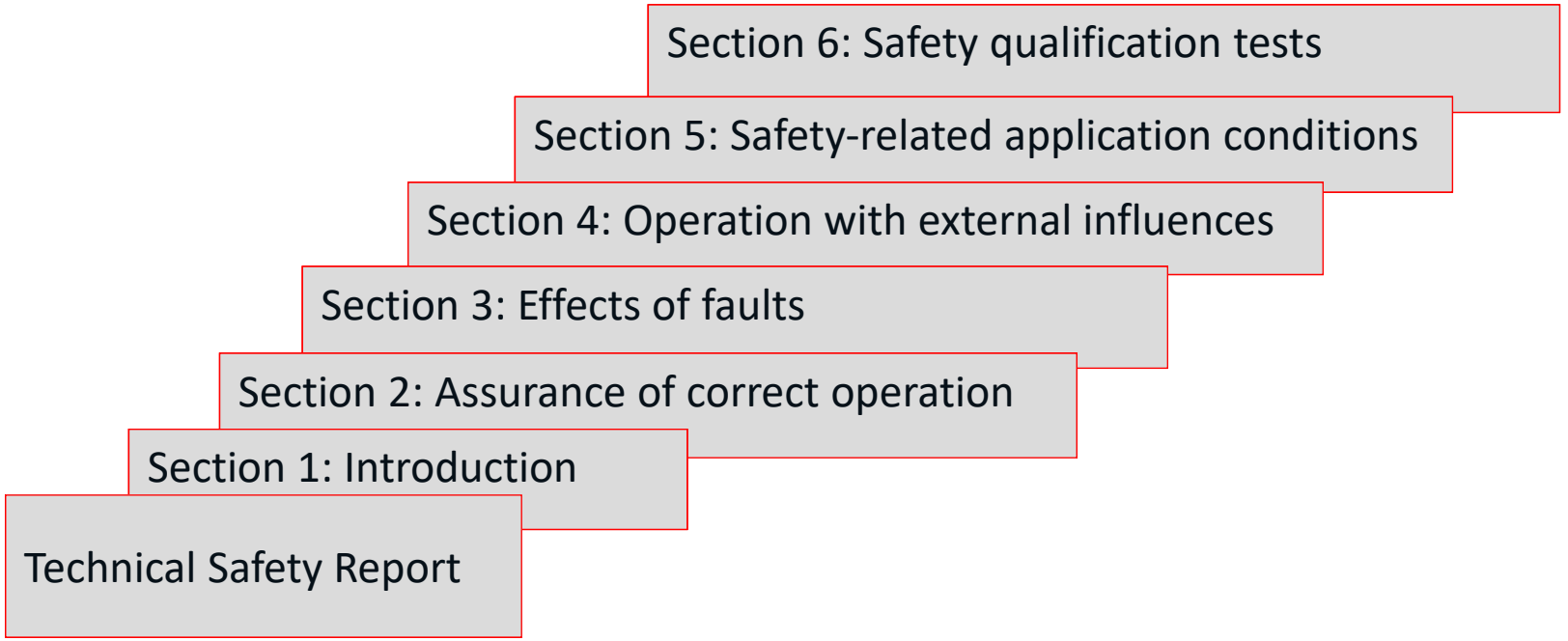
- Shows evidence of the control of quality of the system by an effective Quality Management System (QMS)
- QMS purpose is to minimize the incidence of human errors at each stage of the lifecycle and should be applicable throughout the system lifecycle
- Examples of aspects which should be controlled by the quality management system and included in the Quality Management Report
  - organisational structure;
  - quality planning and procedures;
  - specification of requirements;
  - design control;
  - design verification and reviews;
  - application engineering;
  - procurement and manufacture;
  - product identification and traceability;
  - handling and storage;
  - inspection and testing;
  - non-conformance and corrective action;
  - packaging and delivery;
  - installation and commissioning;
  - operation and maintenance;
  - quality monitoring and feedback;
  - documentation and records;
  - configuration management/change control;
  - personnel competency and training;
  - quality audits and follow-up;
  - decommissioning and disposal.

# Safety Case :: Safety Management Report

- Shows evidence of the managing of safety of the system by an effective safety management process
- Safety management process purpose is to minimize the incidence of safety-related human errors at each stage of the lifecycle
- The Safety Management Report must include all documentary evidence for this process, either directly or by reference to other documents
- The process should be consistent with the defined in EN 50126 in areas like RAMS management, hazard analysis and risk assessment
- Should include, but not necessary limit to, the following elements
  - Safety lifecycle
  - Safety organization
  - Safety plan
  - Hazard log
  - Safety requirements specification
  - System design
  - Safety reviews
  - Safety verification and validation
  - Safety justification
  - System handover
  - Operation and maintenance
  - Decommissioning and disposal

# Safety Case :: Technical Safety Report

- Consists of technical evidence of the safety of the system design (product), complementing the evidence of quality and safety management (process)
- Should explain the technical principles which assure the safety of the design, including supporting evidence (design principles and calculations, test specifications and result, safety analysis)



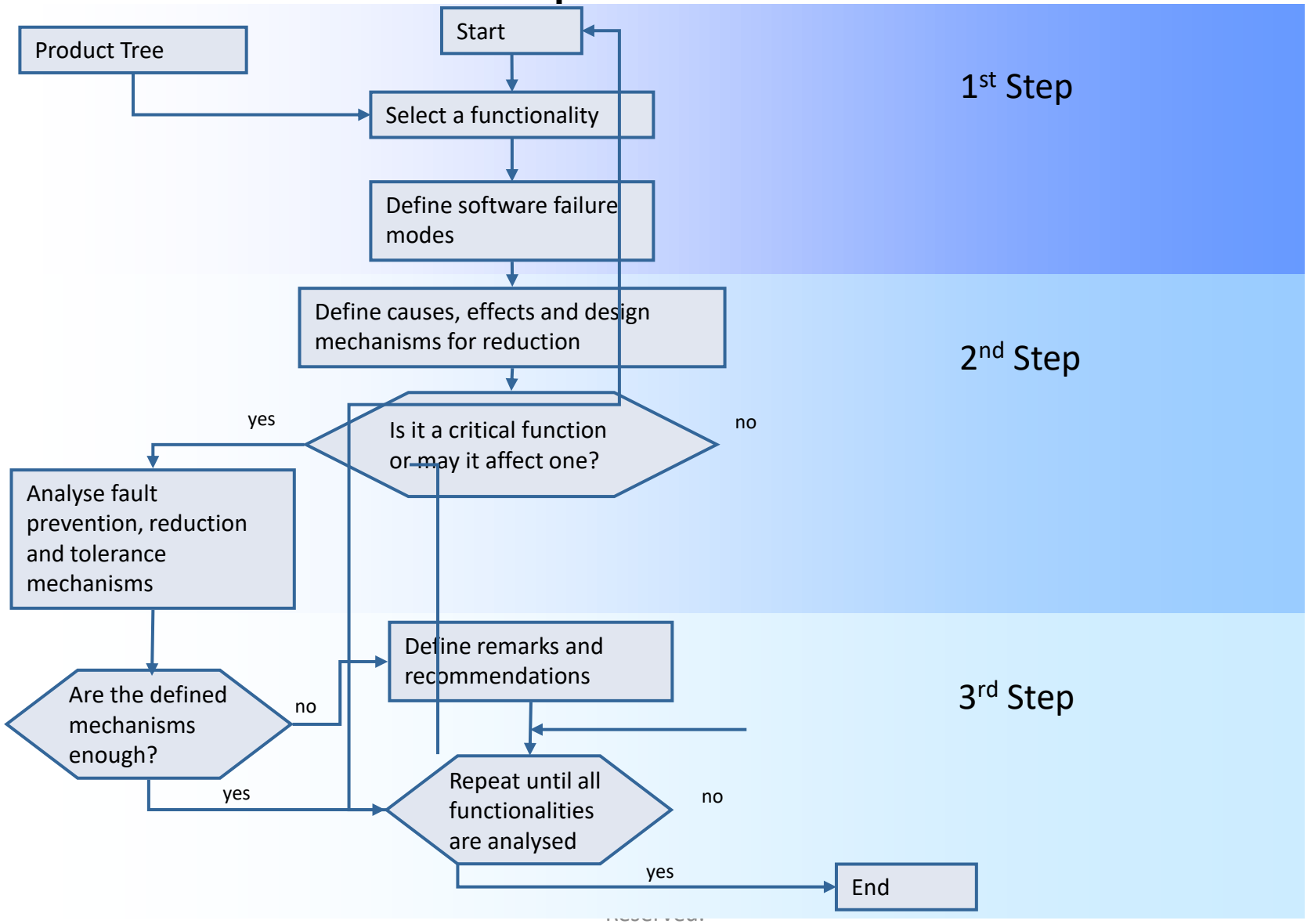
# Safety Case :: Technical Safety Report

- Structure of the Technical Safety Report (full description in EN 50129):
- Introduction: overview description of the system including summary of technical safety principles and the extent to which the system is claimed to be safe. Should also indicate the applicable standards and respective issues
- Assurance of correct operation: evidence on the system correct operation according to its operational and safety requirements, including the following aspects:
  - System architecture description
  - Definition of interfaces
  - Fulfilment of System Requirements Specification
  - Fulfilment of Safety Requirements Specification
  - Assurance of correct hardware functionality
  - Assurance of correct software functionality
- Effects of faults: evidence that the occurrence of random and systematic faults do not reduce the safety of the overall system, including the following aspects:
  - Effects of single faults
  - Independence of items
  - Detection of single faults
  - Action following detection (including retention of safe state)
  - Effects of multiple faults
  - Defence against systematic faults
- Operation with external influence: demonstrate that when subjected to the external influences the system continues to fulfil its specified operational and safety requirements (including fault conditions).
- Safety-related application conditions: specify the rules, conditions and constraints to be observed in the application of the system
- Safety qualification tests: evidence to demonstrate successful completion, under operational conditions, of the Safety Qualification Tests

# FMEA Example

- Failure Modes and Effects Analysis (FMEA)
- Start from the foreseen functions (at system or software level) and ends up at system level with “odd” situations.
- Can be combined with a Fault Tree Analysis
- Generic (but not necessarily the only ones) failure modes:
  - No function
  - Incorrect Function
  - Delayed/too soon Function

# FMEA Example




- FMEA Sheet Sample

# The End

universidade de aveiro

Critical software


# References


- CENELEC EN 50128, Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems, 2011.
- CENELEC EN 50657, Railways Applications - Rolling stock applications - Software on Board Rolling Stock, 2017.
- CENELEC EN 50126, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), 1999.
- RTCA/DO-178C, Software Considerations in Airborne Systems and Equipment Certification, 2012.

# References


- ISO 26262, Road vehicles — Functional safety, 2018.
- https://en.wikipedia.org/wiki/List_of_EN_standards
- https://smallbusinessprogramming.com/safety-critical-software-15-things-every-developer-should-know/
- INTEGRATION OF SAFETY AND SECURITY ASPECTS INTO EXISTING METHODOLOGIES, CECRIS Project, CECRIS_20150129_WP2_D2.3, R08.
- ISO/IEC 62443, Security for industrial automation and control systems, 2009-2018.

# Exercise #4

- #1: By using your application/solution:
  - a) Identify a few hazards (ideally 5 or more) – note: you probably won't find "safety" risks, thus consider a security risk as an hazard, e.g.:
    - denial of service / application blocking;
    - data disclosure;
    - unwanted access;
    - data corruption or tampering;
    - data deletion/removal;
    - …
  - b) (if we reach this part in class) provide the analysis of 2 functions of your application in the form of a FMEA:
    - Consider 3 failure modes per function (no function, wrong function, delayed function)

# Exercise #4

- #2: Use the provided templates:
  - generic-hazard-log-sample.xlsx
  - system_fmea_example.xlsx
- #3: Deadline: 31-Dec-2022

# Exercise #4

- Clarifications:
  - An Hazard is a condition, event, or circumstance that could lead to or contribute to an unplanned or undesirable event.
  - A Failure Mode is a potential failure of an existing system, subsystem, component, assembly, etc…

  - If you master these two, you can work in safety related projects.