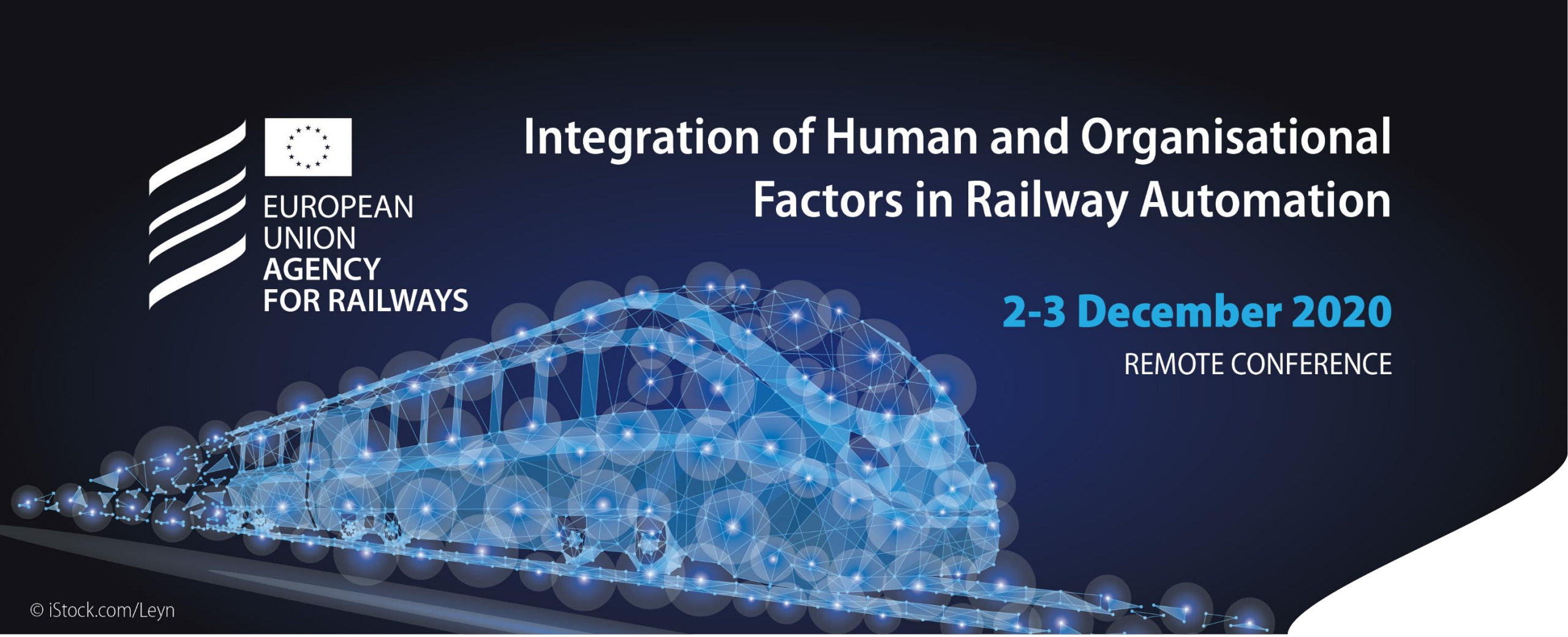


How Human and Organizational factors are addressed in railway safety standards

Roberto SEMPRINI

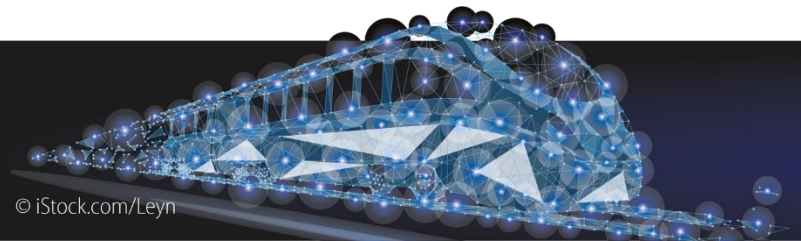
EUROPEAN UNION AGENCY FOR RAILWAYS

How Human and Organizational factors are addressed in railway safety standards

Roberto SEMPRINI

ALSTOM

ALSTOM
• mobility by nature •



© iStock.com/Leyn

Roberto SEMPRINI, Safety Assessment Director, ALSTOM

Master Degree in Electronic Engineering and Professional Engineer. Working in ALSTOM since 25 years in railway safety domain, covering product development and manufacturing, signalling subsystems, overall system integration, vehicles authorization. Contributor to dissemination of safety culture inside the company and in the railway sector.

Currently Safety Assessment Director of the in-house assessment body accredited ISO/IEC 17020. Participated to development of CENELEC safety standards since 2000, and currently Convenor of CENELEC EN 50126 and IEC 62278.

How Human and Organizational factors are addressed in railway safety standards

Roberto SEMPRINI

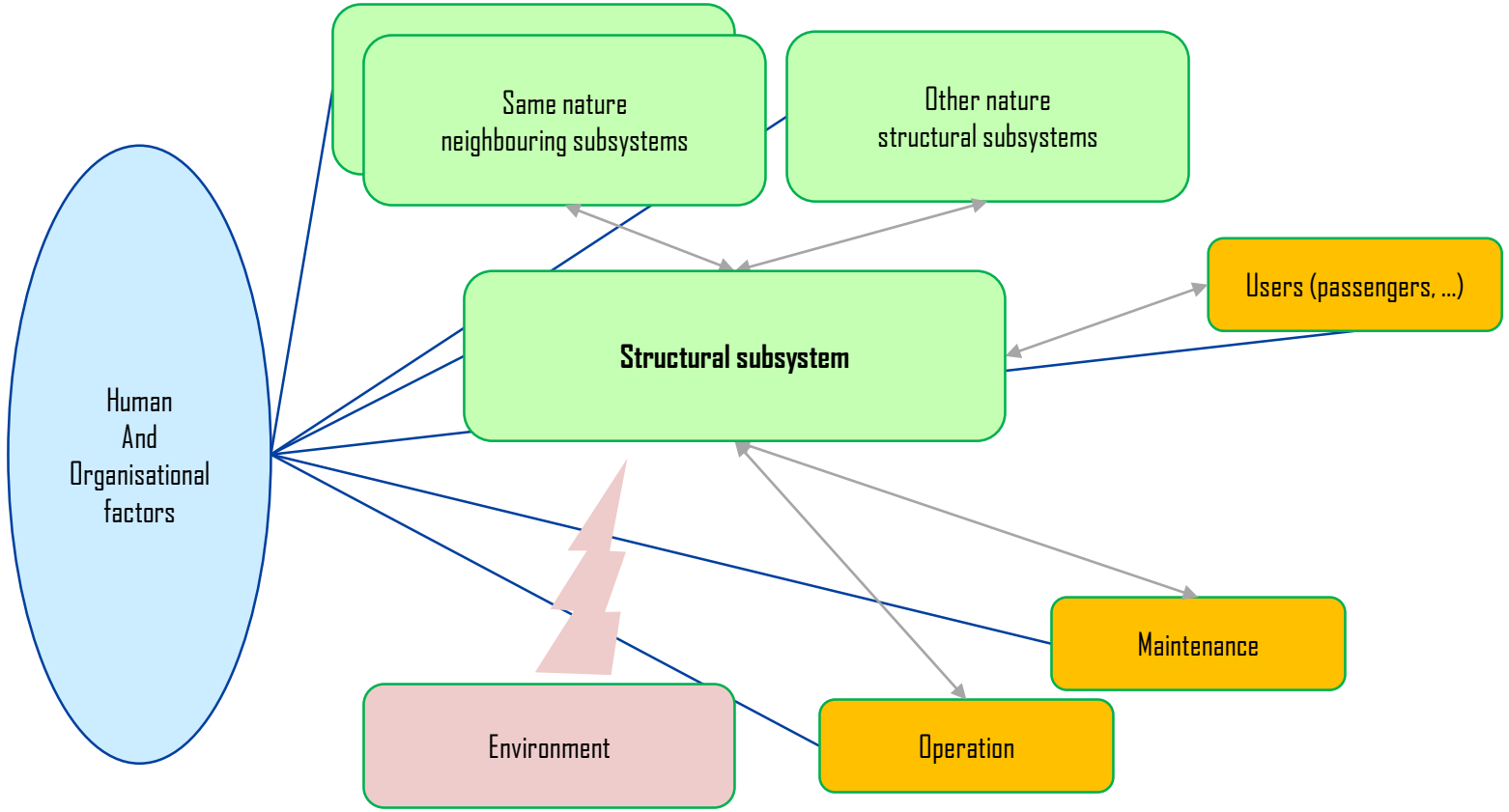
3 December, 2020

ALSTOM
• mobility by nature •

Railway system perspective

Technology

Human and Organisational factors

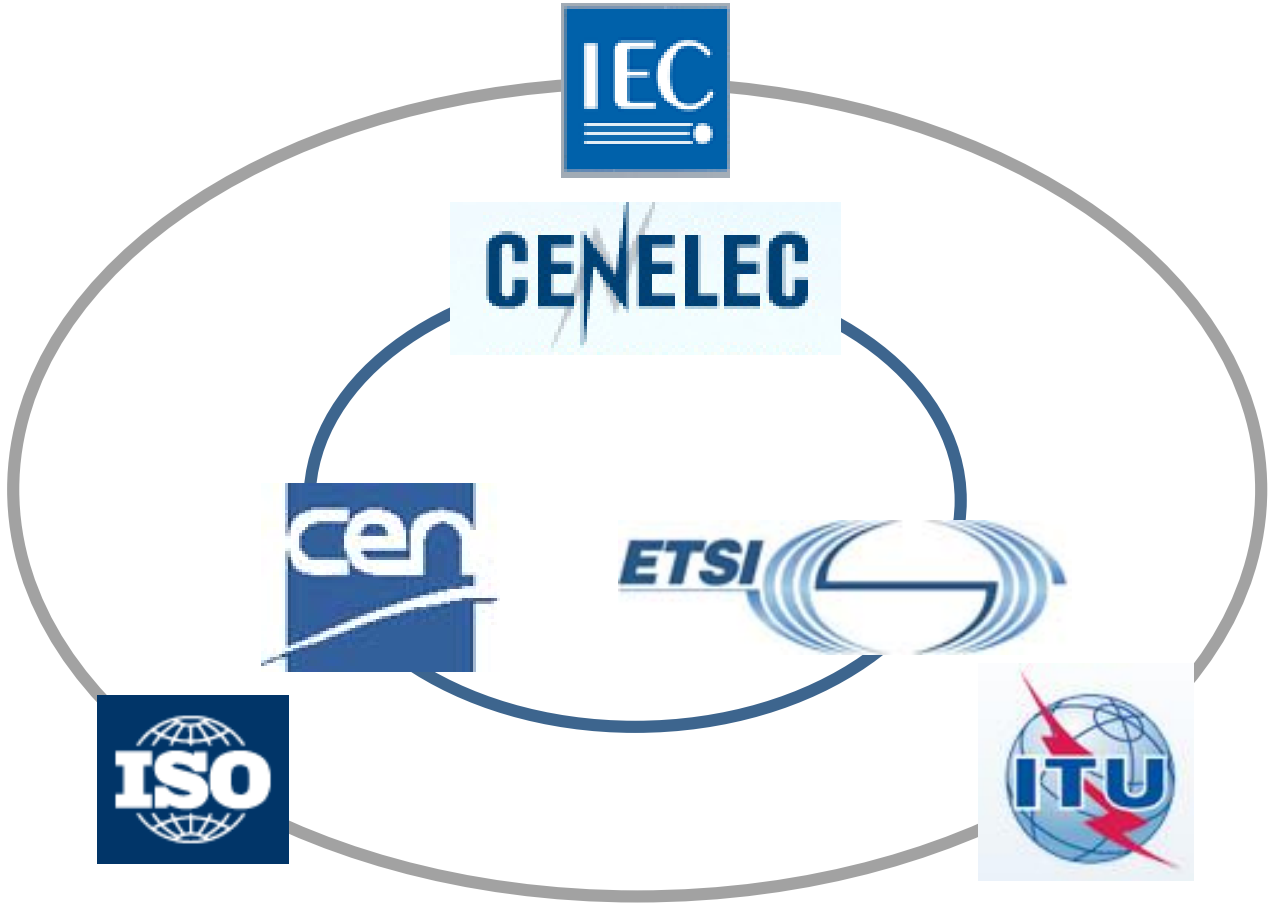


A system comprises not only its technical components but also the interaction with the humans developing, operating, and maintaining it

Standardization is a key support to address complexity

European and international standardization bodies

with dedicated Technical Committees focussing on railways needs



Safety standards applied since years in the railway industry

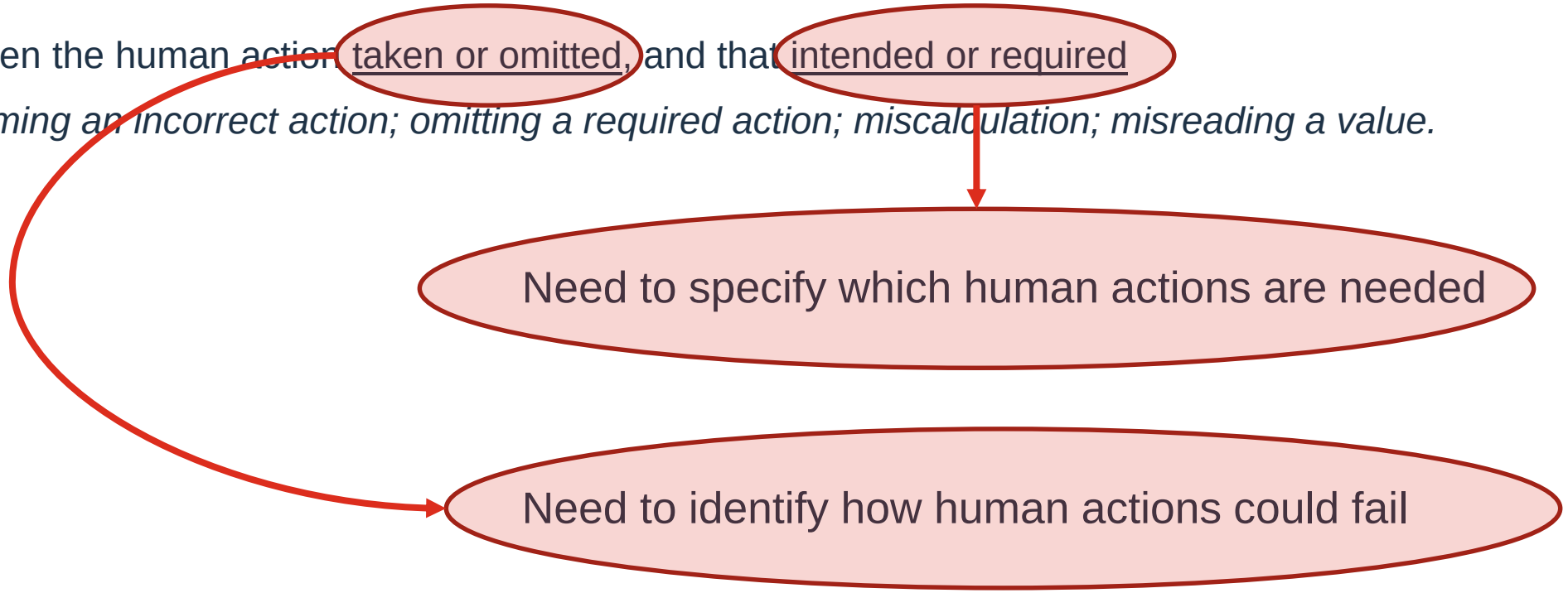
What is a “human error” ?

[source: IEV 60050: 192-03-14]

human error:

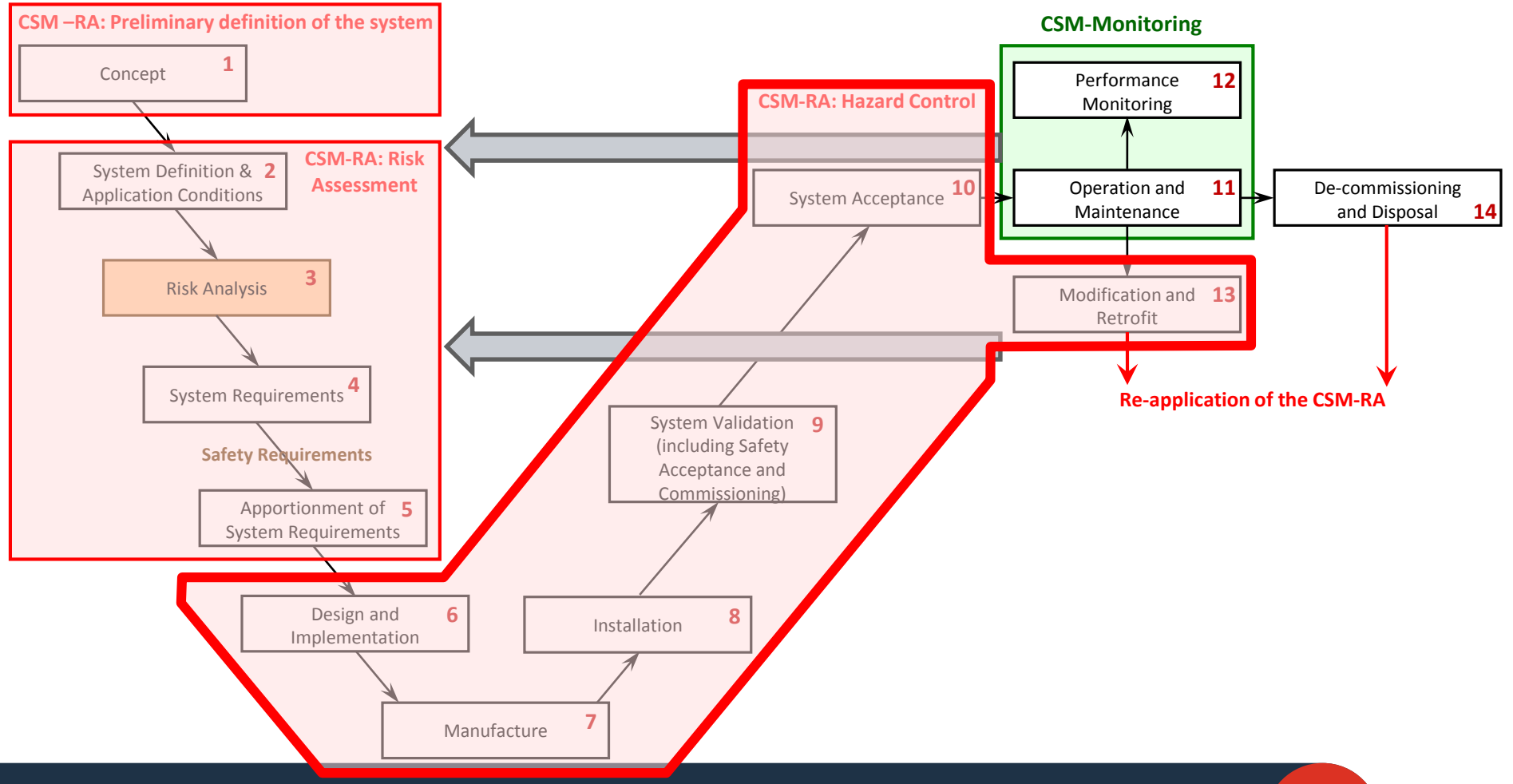
discrepancy between the human action taken or omitted, and that intended or required

EXAMPLE: Performing an incorrect action; omitting a required action; miscalculation; misreading a value.



How to manage human factors and related risks for a railway system

Definition of a structured lifecycle model



Risks shall be managed all along the system lifecycle

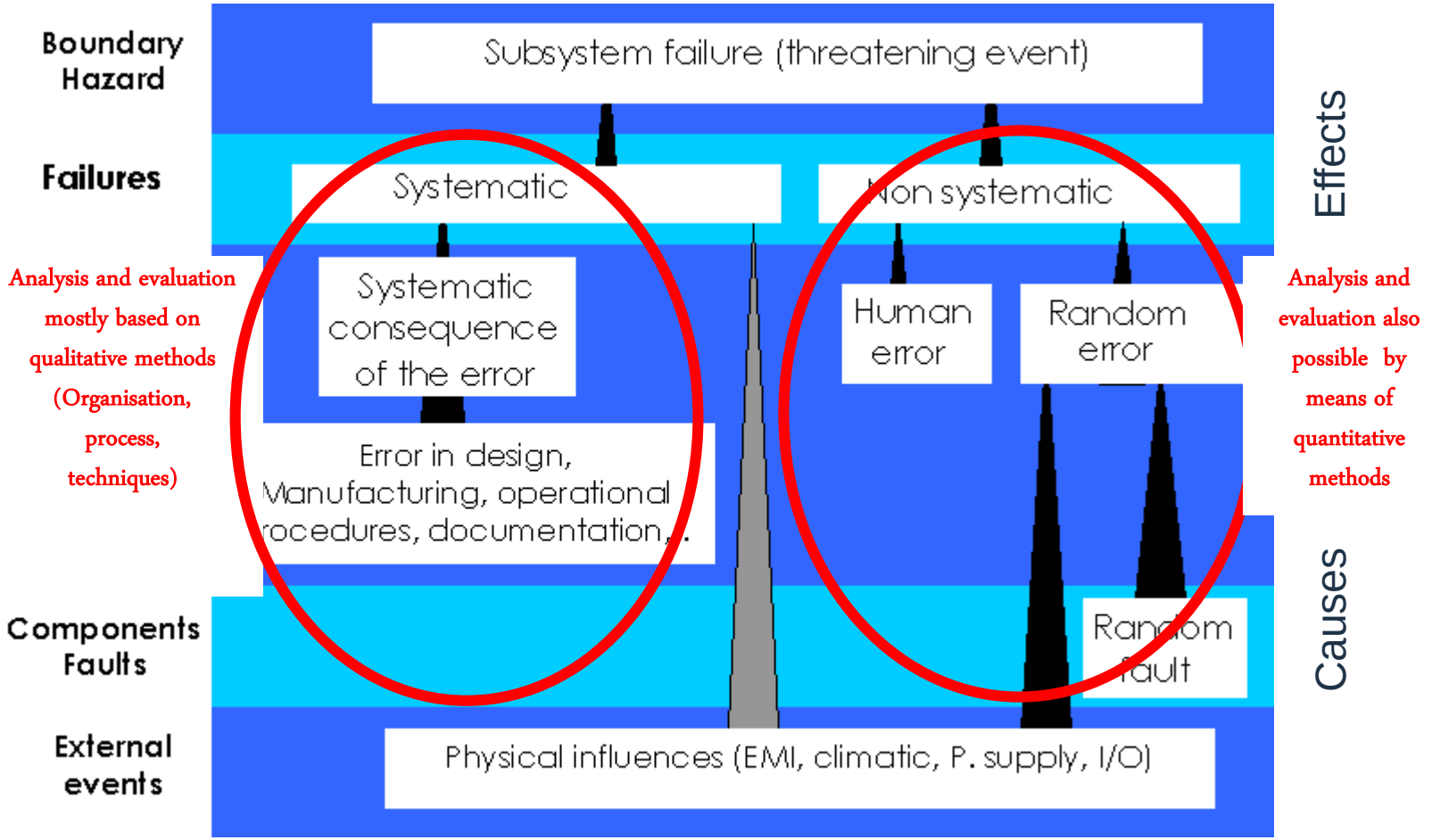
Consideration of human factors at System Definition

- During “System Definition” phase, the operational context shall be considered, defining:
  - functions to be performed by the technical system,
  - relevant interfaces considering interactions with human operators and their behavior,
- Requirements shall include the different modes of operation (i.e. normal, abnormal/degraded, maintenance mode), states and transitions and their interactions, if they could have an impact on the systems functionality and safety;
- Both the maintenance process (described in the maintenance manuals) and the operation are specified.
  - Not considered parts of the technical system itself -> restricted by “**application conditions**”.
- Human factors can be defined as the impact of human characteristics, expectations and behaviour upon a system. These factors include the anatomical, physiological and psychological aspects of humans.
- The precise influence of human factors on RAMS is specific to the application under consideration.

Safety requirements specification and allocation based on Risk Assessment

Analysis of the causes

- All humans are subject to occasional lapses in performance.
- When these occur in the operational and maintenance phases of the system life cycle they tend to result in random failures;
- When they occur in earlier phases of the life cycle they can result in systematic failures in the operational phase.



Human influence can be regarded as having both random and systematic aspects

Human influencing factors – Example of checklist

the allocation of system functions **between human and machine**;

the **effect on human performance** within the system of:

- the human/system interface;
- the environment, including the physical environment and ergonomic requirements;
- human working patterns;
- human competence;
- the design of human tasks;
- human interworking;
- human feedback process;
- railway organisational structure;
- railway culture;
- professional railway vocabulary;
- problems arising from the introduction of new technology

Requirements for the system arising from **human information processing capabilities**, including:

- human/machine communications;
- density of information transfer;
- rate of information transfer;
- the quality of information;
- human reaction to abnormal situations;
- human training;
- supporting human decision making processes;
- other factors contributing to human strain.

Requirements **on the system** arising from:

- human competence;
- human motivation and aspiration support;
- mitigating the effects of human behavioural changes;
- operational safeguards;
- human reaction time and space.

the effect on the system of **human/system interface factors**, including:

- the design and operation of the human/system interface; the provision of user manuals etc.;
- the effect of human error;
- the effect of deliberate human rule violation (e.g. where an operator ignores a rule in order to save time);
- human involvement and intervention in the system;
- human system monitoring and override;
- human perception of risk;
- human involvement in critical areas of the system;
- human ability to anticipate system problems;
- human reaction under different operating modes (e.g. normal, degraded or emergency).

human factors in **all phases of the system lifecycle**, including:

- human competency;
- human independence during design, verification and validation;
- human involvement in verification and validation;
- interface between human and automated tools;
- systematic failure prevention processes (e.g. measures to assure safety integrity)..

Quality and Safety Management System

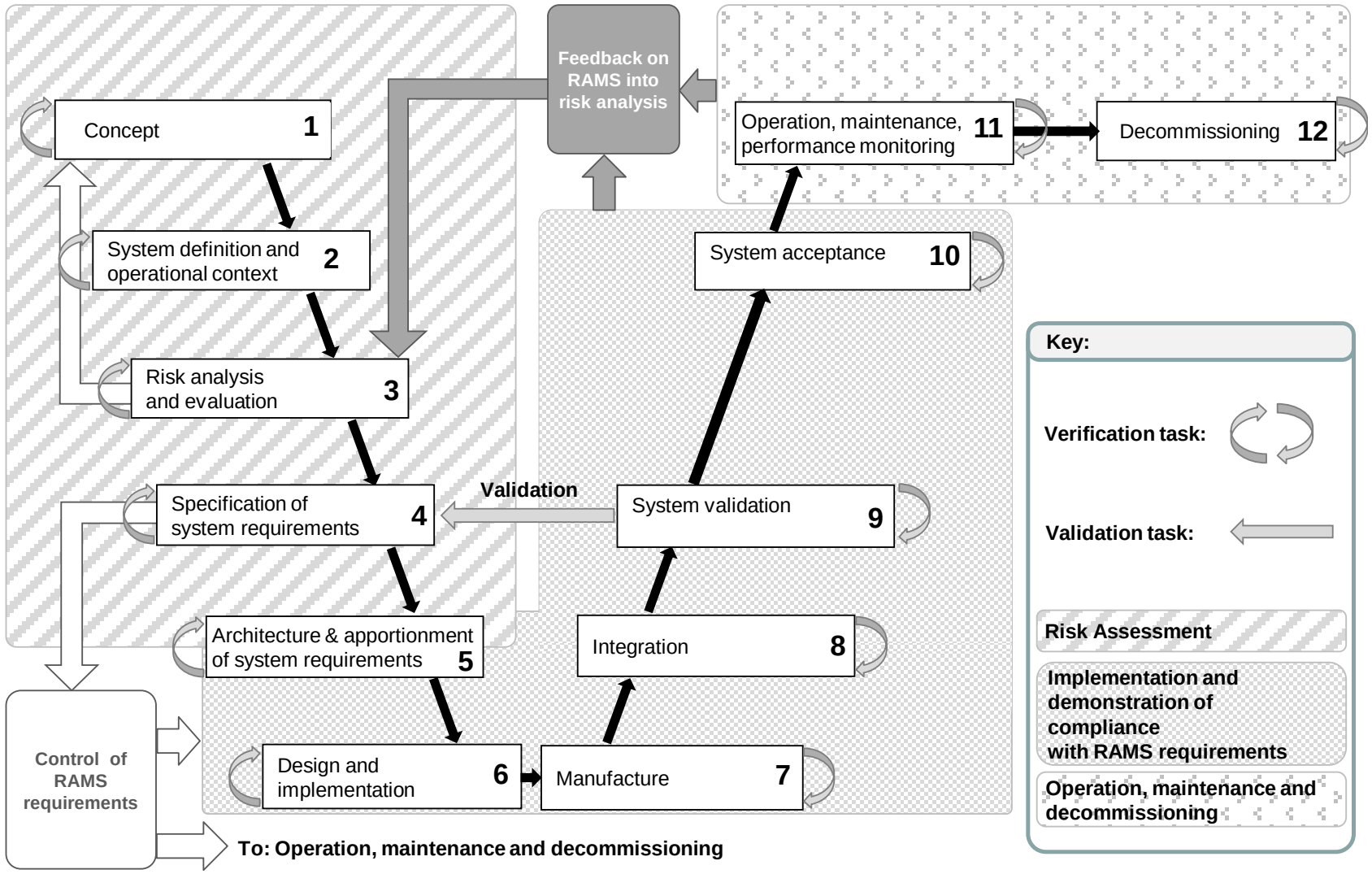
- Systematic faults are caused by human errors in the various stages of the system, subsystem or equipment life cycle.
- EXAMPLE:
  - specification errors;
  - design errors;
  - manufacturing errors;
  - installation errors;
  - operation errors;
  - maintenance errors;
  - modification errors.
- Systematic failure integrity is achieved by means of the quality management system (QMS), safety management system (SMS) and technical defences.
- In addition to the quality and safety management techniques, technical defence measures are taken such that in the event of a hazardous systematic fault it would, as far as reasonably practicable, be prevented from creating an unacceptable risk.

Organisation: Roles, Responsibilities, Competencies, Independence, Impartiality

Policy, Processes and management

Procedures, Methods, Techniques

Systematic integrity: Verification and Validation in the lifecycle



Systematic integrity: Verification and Validation in the lifecycle

- Verification and validation tasks performed along system lifecycle have the aim to detect systematic errors/failures.
- Verification:
  - confirmation, through the provision of objective evidence, that specified requirements have been fulfilled
  - Verification is conducted at various life cycle phases of development, examining the system and its constituents to determine conformity to the requirements specified at the beginning of that life cycle phase
- Validation:
  - confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

Includes confirmation that process and lifecycle activities have been properly performed
Appropriate conditions of use defined and exported

Not only correctness, but also completness

- Verification and Validation are tasks/activities of the lifecyle
- They are based on methods (analysis, checks, inspection, testing, …)

Independent Safety Assessment

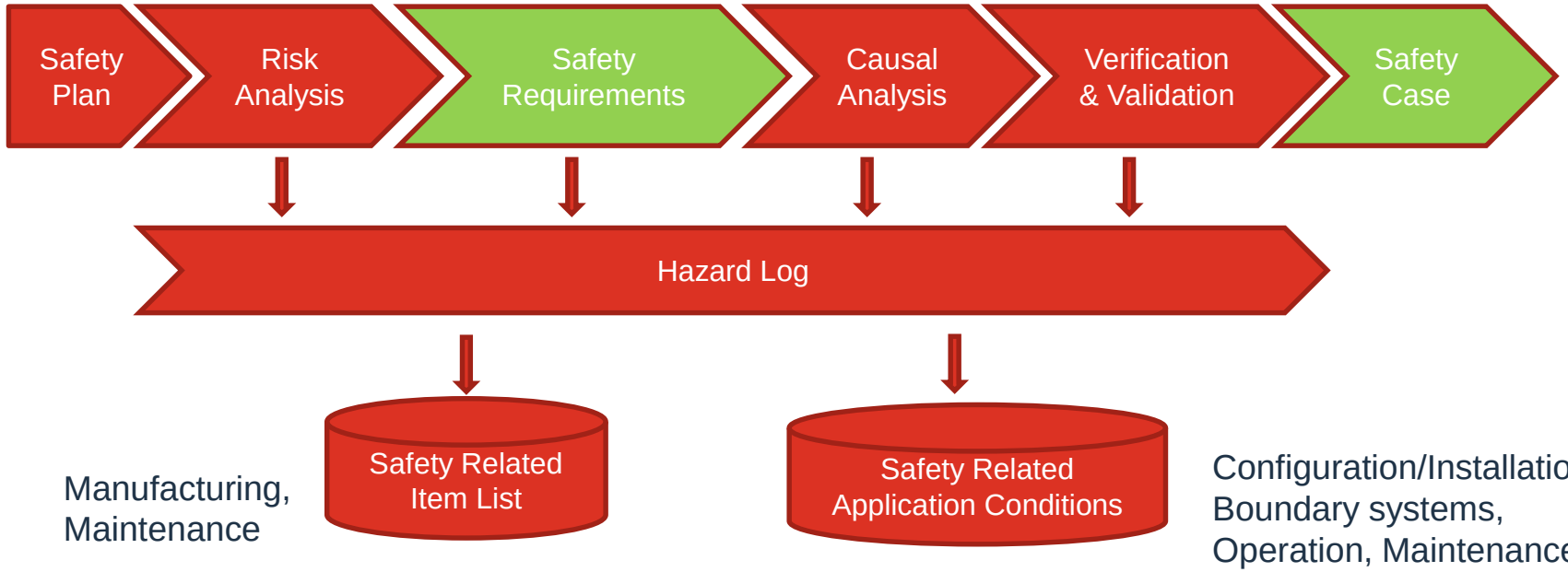
- Process to determine whether the system/product meets the specified safety requirements and to form a judgement as to whether the system/product is fit for its intended purpose in relation to safety
- It's a means to provide additional confidence about the avoidance of systematic failures of the system under consideration which can adversely influence safety
- The role of Independent Safety Assessor (ISA) is in addition to Verification and Validation

- Also the legal framework (CSM-RA) more recently has defined the activity of Safety Assessment to be performed either by accredited internal or external organisation identified as AsBo, fulfilling requirements of inspection bodies according to ISO/IEC 17020 standard.

Safety Assessment is different from Conformity Assessment

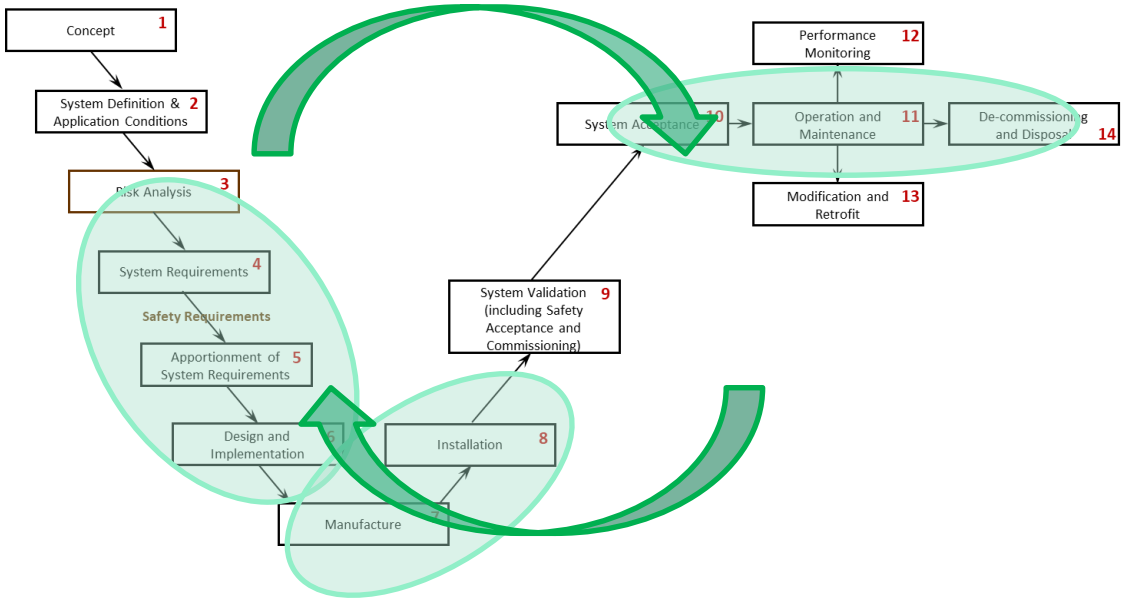
Key activities of the Safety management

- Safety shall be:
  - Planned
  - Specified on the basis of risk assessemnt
  - Controlled on the basis of causal analysis
  - Demonstrated on the basis of appropriate Verification and Validation activities



Human Factors in causal analysis

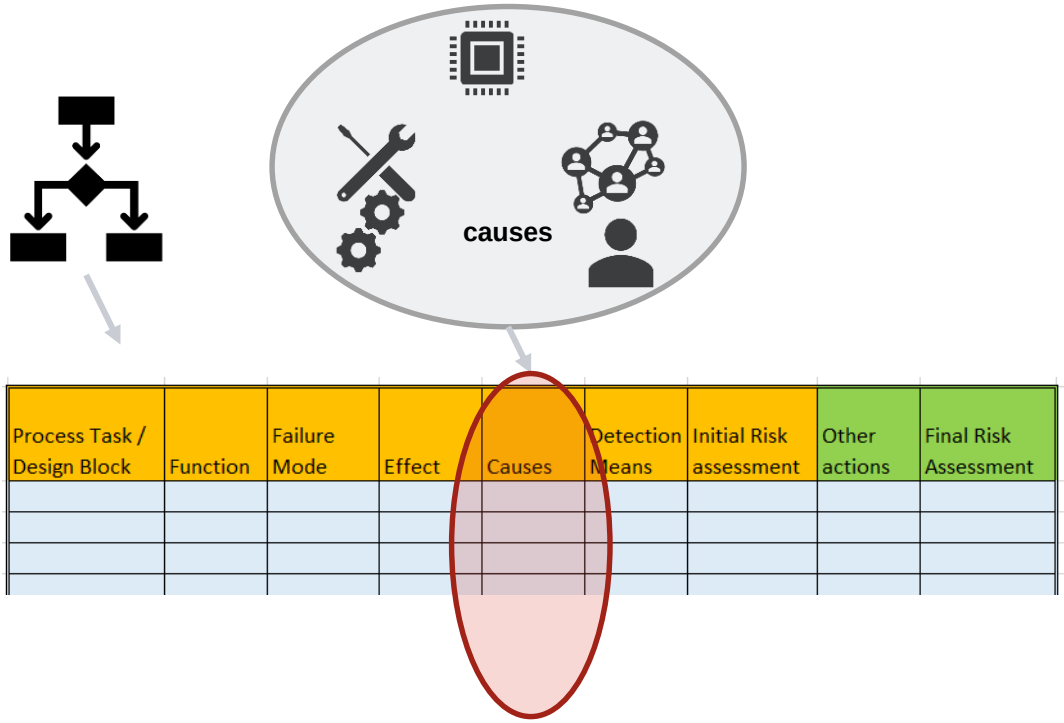
- Hazard control process requires to perform causal analysis identifying events leading to hazardous conditions and defining mitigations to keep the risk at an acceptable level.
- The causal analysis techniques aim to identify the logic sequence of the events developing into a hazard. The maybe top-down or bottom-up techniques or mixed bottom-up and top-down techniques. Typical examples of techniques includes Fault Tree Analysis (FTA), Failure Mode Effects and Criticality Analysis (FMECA), …
- The list of causes shall consider technical as well as all credible human errors
- Causal analysis shall be applied to all lifecycle phases:
  - Development (specification, design, …)
  - Deployment (manufacturing, installation)
  - Operation, Maintenance



Lot of back-and-forth information between analysis of the technical system design and analysis of related design/operation/maintenance processes

Human Factors in causal analysis

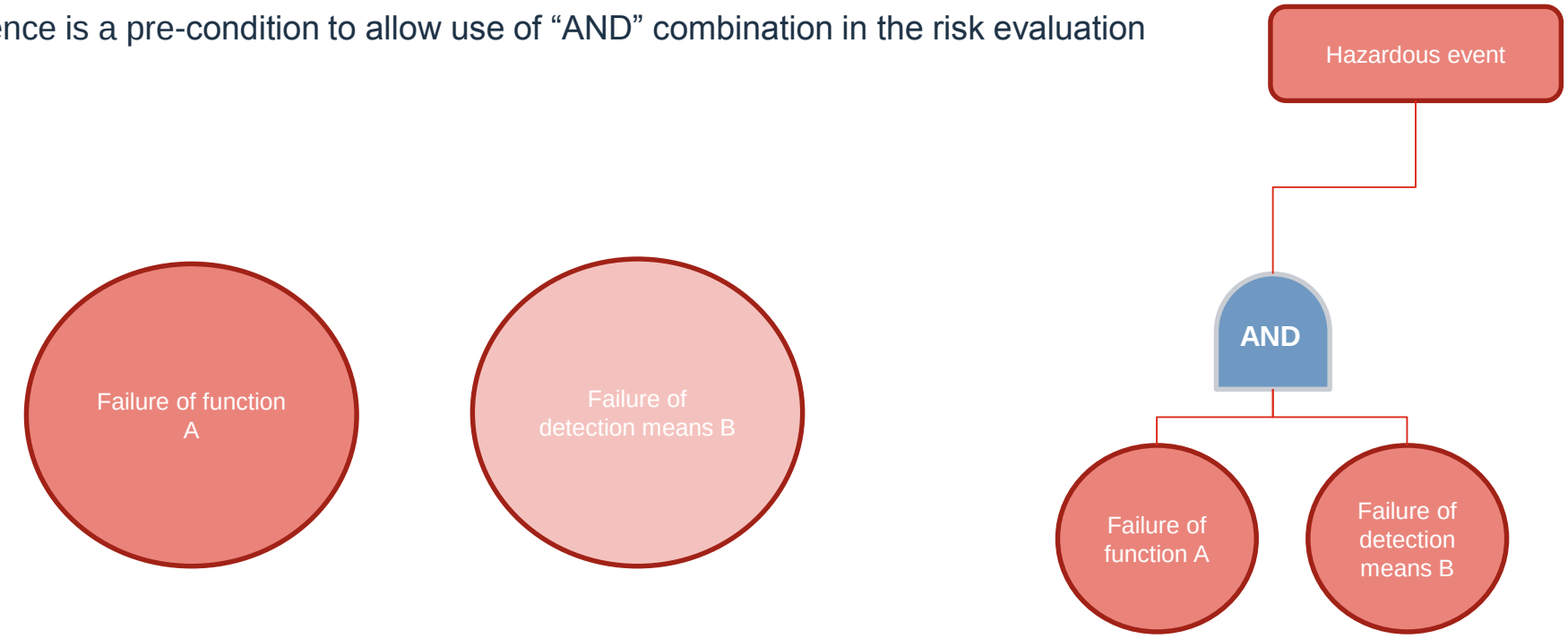
- Example of FMECA
- FMECA applied to Design (also called DFMECA) and to process (also called PFMECA) are based on same method.
- When applied to processes:
  - Structured definition of the process with all the functions and input/output relationships
  - Function is specified action or activity which can be performed by technical means and/or human beings and has a defined output in response to a defined input
  - Causes shall includes Organisation and human factors, i.e. procedures, roles, human errors, … .



Causes shall be tuned to the specific process under consideration

Human Factors in causal analysis

- The acceptable level of risk associated to the hazardous event may be achieved by combination of two functions (technical or process tasks).
- Independence is a pre-condition to allow use of “AND” combination in the risk evaluation

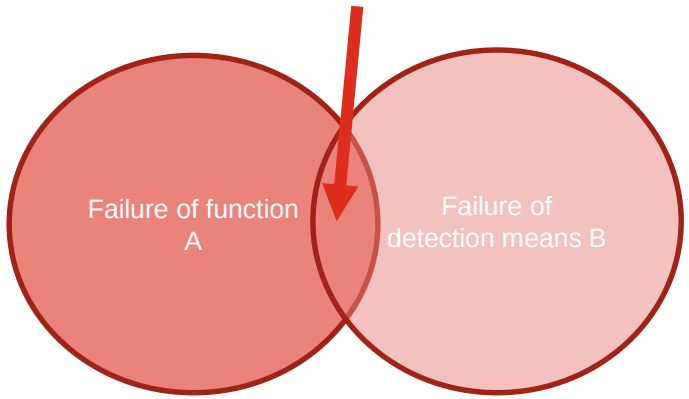


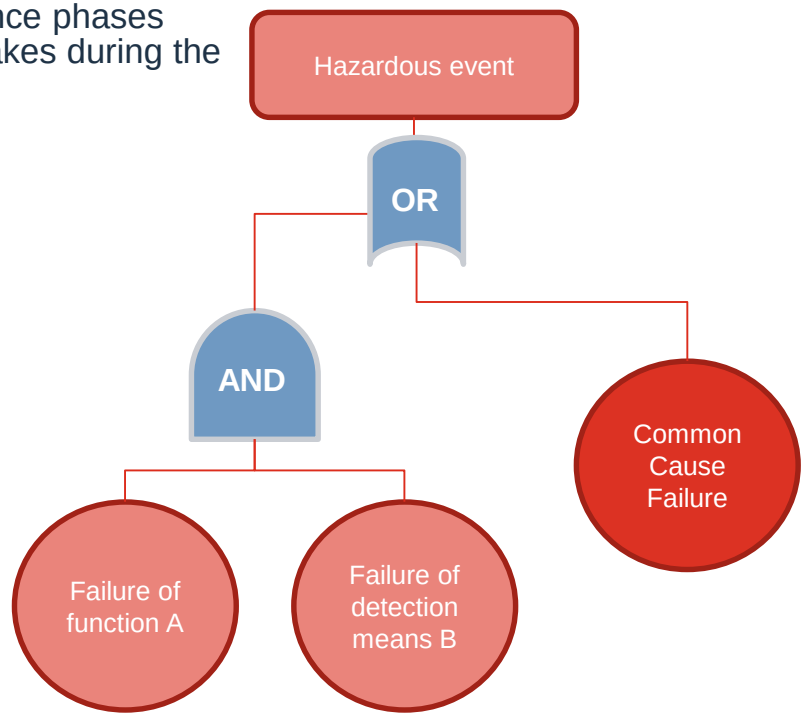
Independence of failure modes

Human Factors in causal analysis

- Organisational independence and diversity in human resource and life-cycle processes are deemed to contribute to higher overall safety integrity
- Any common process activities in the design, manufacturing, installation and maintenance phases (e.g. same human resource, common modelling, etc.) can be a cause of common mistakes during the development phase of the two functions.

Common Cause Failures (CCF)





No process-related causes shall prevent the identification of flaws inheriting the potential for common cause failures

Use of Tools for safety related functions

- Tools can perform or support activities in any of the life cycle phases (design, construction, testing, operation, maintenance, …) helping to minimize the possibility of introducing human errors
- The more the level of automation, the less will be the contribution of human operators. Tools can:
  - directly affect safety: those tools which generate outputs that contribute to the design or implementation of a safety-related function, and whose errors could directly lead to a systematic hazardous fault
  - indirectly affect safety: those tools which support the safety verification of the design or implementation of a safety-related function, and whose errors do not directly lead to a systematic hazardous fault in the product or application, but rather might affect the detection of other errors from other sources.
- Importance to control potential systematic errors becoming the main source of risk:
  - Hazard identification and hazard analysis shall be applied to the tools and the processes
  - Validation of the tool and related processes with methods and techniques commensurate to the required safety integrity

Modifications management

- Whenever needs for modifications are identified, risk assessment and lifecycle shall be re-iterated.
- A Modification management process with related Risk Assessment, including:
  - analysis of the change (technical, organizational, operational)
  - configuration management
  - application of the modification (retrofit/upgrade)

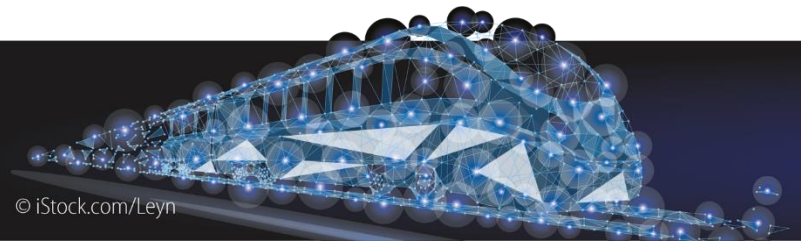
Thank you for your attention

EUROPEAN UNION AGENCY FOR RAILWAYS

Q & A

In the next 20 minutes Mr. Roberto SEMPRINI will reply live to your questions.

- You may wish to write your question in the Teams Live chat, or
- Receive a detailed reply after this conference: use the link provided on the event webpage.



EUROPEAN UNION AGENCY FOR RAILWAYS

Making the railway system work better for society.

Follow us on ERA_railways

Discover our job opportunities on **era.europa.eu**