SAFETYADVISOR

Common Safety Methods CSM

A common safety method on risk evaluation and assessment

- Directive 2004/49/EC, Article 6(3)(a)
- Presented by: matti.katajala@safetyadvisor.fi / www.safetyadvisor.fi

Motivation

"Directive 2004/49/EC, Article 6"

- The safety management system shall include procedures and methods for
  - carrying out risk evaluation and
  - implementing risk control measures
  - whenever a change of the operating conditions or new material imposes
    - new risk on the infrastructure or on operations
- Common approach for demonstrating
  - compliance with the safety levels and
  - requirements of the railway system
- Recognition of risk acceptance principles
  - Codes of practice
  - Comparison with similar parts of the railway system
  - Using of explicit risk evaluation

Purpose

- The purpose of the CSM is to maintain and improve the level of safety.
- The CSM should facilitate the access to the market for rail transport services through harmonisation of:
  - the risk management processes used to assess the safety levels and the compliance with safety requirements;
  - the exchange of safety-relevant information between different actors in order to manage safety across the different interfaces
  - the evidence resulting from the application of a risk management process

Scope

- The CSM shall apply to any change of the railway system
  - Technical
  - Operational
  - Organisational (operating conditions)
- The systems concerned
  - Risk assessment required by the relevant TSIs
  - To ensure safe integration of the structural subsystems to which the TSIs apply

Definitions.1

- ‘risk’ means the rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm
- ‘risk analysis’ means systematic use of all available information to identify hazards and to estimate the risk
- ‘risk evaluation’ means a procedure based on the risk analysis to determine whether the acceptable risk has been achieved
- ‘risk assessment’ means the overall process comprising a risk analysis and a risk evaluation

Definitions.2

- ‘safety’ means freedom from unacceptable risk of harm
- ‘risk management’ means the systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risks
- ‘interfaces’ means all points of interaction during a system or subsystem life cycle, including operation and maintenance where different actors of the rail sector will work together in order to manage the risks
- ‘actors’ means all parties which are, directly or through contractual arrangements involved
- ‘safety requirements’ means the necessary safety characteristics (qualitative or quantitative) of a system and its operation (including operational rules) in order to meet legal or company safety targets
- ‘safety measures’ means 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

Definitions.3

- ‘proposer’ means
  - the railway undertakings or the infrastructure managers in the framework of the risk control measures they have to implement in accordance with Article 4 of Directive 2004/49/EC;
  - the contracting entities or the manufacturers when they invite a notified body to apply the “EC” verification procedure in accordance with Article 18(1) of Directive 2008/57/EC;
  - or the applicant of an authorisation for placing in service of vehicles;
- ‘safety assessment report’ means the document containing the conclusions of the assessment performed by an assessment body on the system under assessment
- ‘hazard’ means a condition that could lead to an accident
- ‘assessment body’ means the independent and competent person, organisation or entity which undertakes investigation to arrive at a judgement, based on evidence, of the suitability of a system to fulfil its safety requirements;

Definitions.4

- ‘risk acceptance criteria’ means the terms of reference by which the acceptability of a specific risk is assessed. These criteria are used to determine that the level of a risk is sufficiently low that it is not necessary to take any immediate action to reduce it further
- ‘hazard record’ means the document in which identified hazards, their related measures, their origin and the reference to the organisation which has to manage them are recorded and referenced;
- ‘hazard identification’ means the process to find, list and characterise hazards
- ‘risk acceptance principle’ means the rules used in order to arrive at the conclusion whether or not the risk related to one or more specific hazards is acceptable
- ‘code of practice’ means a written set of rules that, when correctly applied, can be used to control one or more specific hazards
- ‘reference system’ means a system proven in use to have an acceptable safety level and against which the acceptability of the risks from a system under assessment can be evaluated by comparison;

Definitions.5

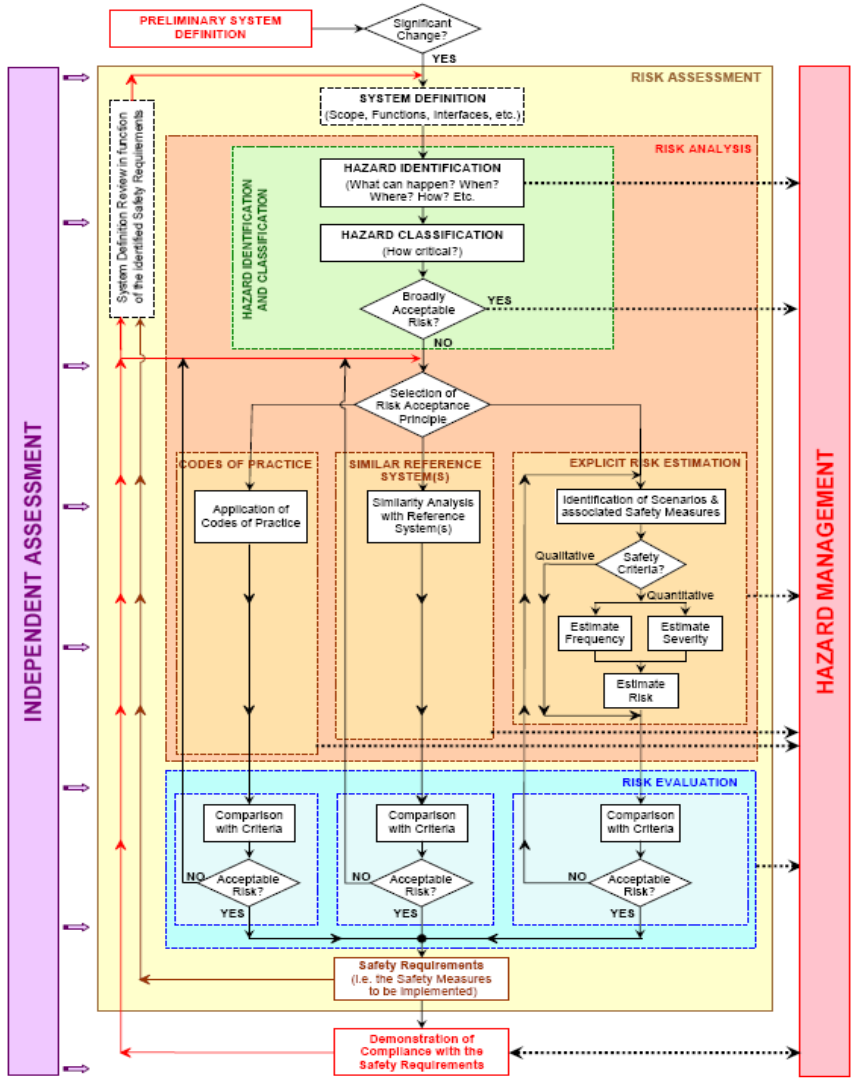
- ‘risk estimation’ means the process used to produce a measure of the level of risks being analysed and consists of the following steps: frequency, consequence analysis and their integration
- ‘technical system’ means a product or an assembly of products including the design, implementation and support documentation. The development of a technical system starts with its requirements specification and ends with its acceptance. Although the design of relevant interfaces with human behaviour is considered, human operators and their actions are not included in a technical system. The maintenance process is described in the maintenance manuals but is not itself part of the technical system.
- ‘catastrophic consequence’ means fatalities and/or multiple severe injuries and/or major damages to the environment resulting from an accident
- ‘safety acceptance’ means status given to the change by the proposer based on the safety assessment report provided by the assessment body
- "system" means any part of the railway system which is subject to a change
- "notified national rule" means any national rule notified by Member States under Directives 96/48/EC, 2001/16/EC, 2004/49/EC and 2008/57/EC.

Significant changes

- The proposed change has an impact on safety:
  - Failure consequence: credible worst case scenario
  - Novelty: new to railway sector; new for the organisation
  - Complexity
  - Monitoring: Inability of monitoring throughout the life-cycle
  - Reversibility: Inability to revert to the system before the change
  - Additionality: significance of a set of changes
- The proposer shall keep adequate documentation to justify his decision

Risk management process

- Significant change and placing in service of sub-systems
- TSI refers to use
- Applied by the proposer
- Proposer ensures the risks are managed by:
  - Suppliers
  - Service providers



General principles and obligations

- Definition of the system
- Iterative risk management process
- Hazard record maintained by the proposer
- Compatible risk assessment methods allowed
- Risk assessment process is responsibility of the proposer
- Proposer maintains the process in a documented way
- Evaluation of the correct application (risk management process) is responsibility of the assessment body

Interfaces management

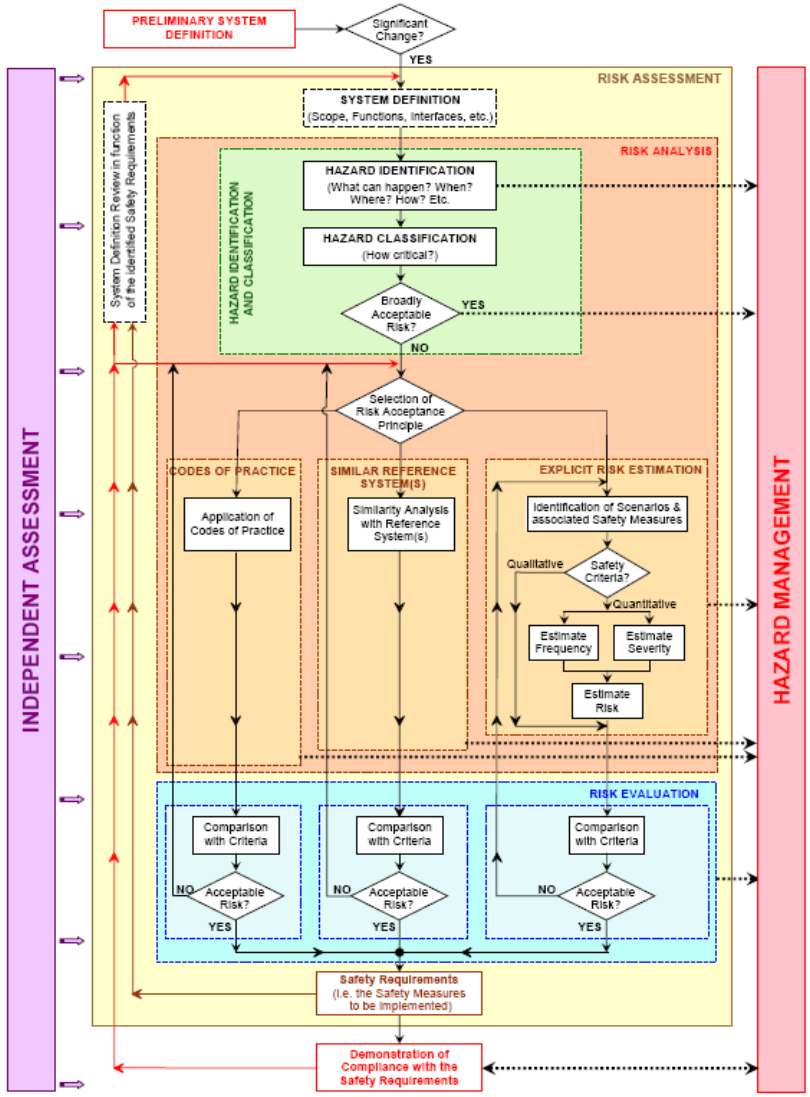
- Proposer co-ordinates the cooperation of the actors identifying jointly:
  - Hazards and related safety measures
- Recognised safety measures
  - Shall be handled by the appropriate actor
- Non-compliance of the safety measures
  - Shall be notified to the proposer by any actor
  - Information shall be distributed as needed for external actors
- Proposer has the responsibility to solve potential situations where agreement between two actors can not be found
- When a requirement in a notified national rule can not be fulfilled by an actor, the proposer shall seek advice from the relevant competent authority
- Proposer is responsible for ensuring that the risk management covers the system itself and the integration into the railway system as a whole

General description

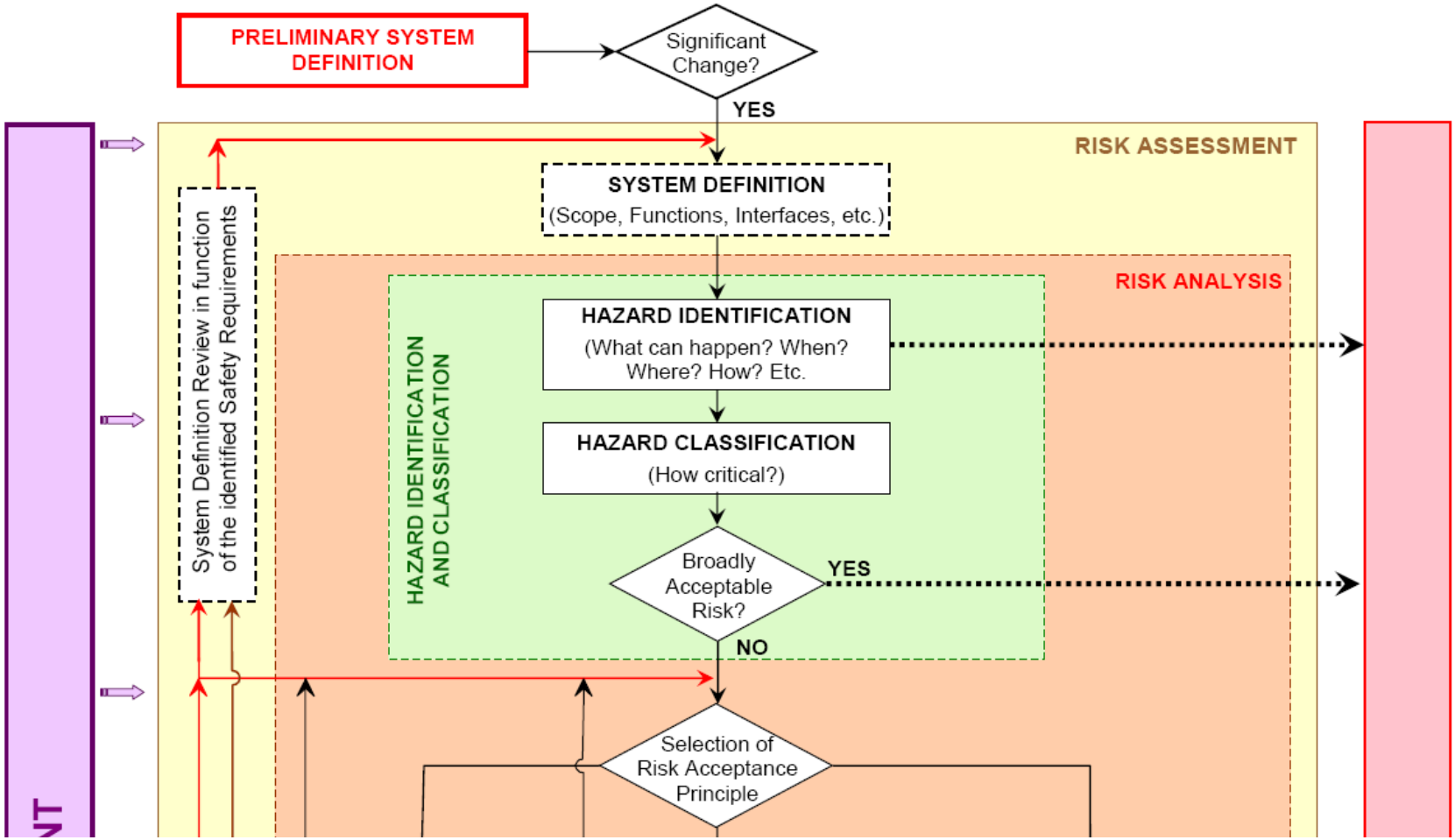
- Iterative process comprises
  - System definition
    - System objective
    - System functions and elements
    - System boundary including other interacting systems
    - Physical and functional interfaces
    - System environment
    - Existing safety measures and after iteration definition of the safety requirements
    - Assumptions which shall determine the limits for the risk assessment
  - Risk analysis and hazard identification
  - Risk evaluation
    - Risk acceptance principles
      - Application of codes of practice
      - Comparison with similar systems
      - Explicit risk evaluation
    - Risk acceptance principles shall identify possible safety measures which make the risk of the system under assessment acceptable
      - Safety requirements
  - Process can be considered as completed when it is demonstrated that all safety requirements are fulfilled and no additional reasonably foreseeable hazards have to be considered

The risk management process

- Risk assessment
  - System definition
  - Risk analysis and hazard identification
  - Risk evaluation
  - Safety requirements
- Independent assessment
- Hazard management



Risk management process picture.1



Hazard identification

- The proposer shall systematically identify,
  - using wide-ranging expertise from a competent team
  - all reasonably foreseeable hazards for the whole system under assessment,
  - its functions where appropriate and its interfaces.,:
- All identified hazards shall be registered in the hazard record
- Hazards shall be classified according to the estimated risk
- Safety measures may be identified
- Needs to be carried out at a level of detail necessary to identify where safety measures are expected to control the risks
- Whenever a code of practices or a reference system is used hazard identification can be limited to:
  - verification of the relevance
  - identification of the deviations

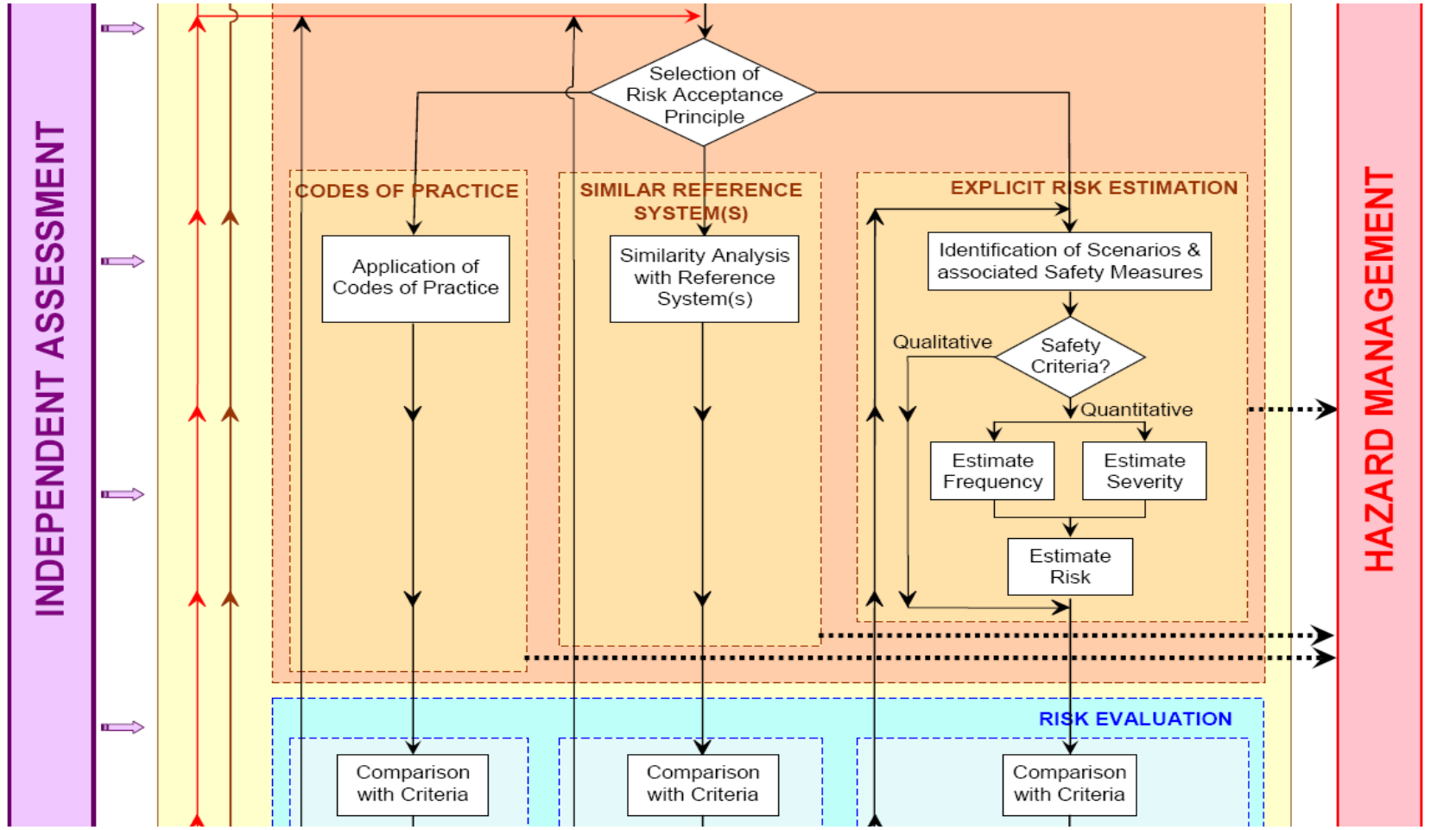
Hazard management

- Hazard record(s) shall be created or updated (where they already exist) by the proposer during the design and the implementation and till the acceptance of the change or the delivery of the safety assessment report.
- The hazard record shall track the progress in monitoring risks associated with the identified hazards.
- The hazard record shall be further maintained by the infrastructure manager or the railway undertaking in charge with the operation of the system under assessment as an integrated part of its safety management system. (In accordance with point 2(g) of Annex III to Directive 2004/49/EC, once the system has been accepted and is operated.)
- The hazard record shall include all hazards, together with all related safety measures and system assumptions identified during the risk assessment process.
- In particular, it shall contain a clear reference to the origin and to the selected risk acceptance principles and shall clearly identify the actor(s) in charge of controlling each hazard.

Exchange of information

- All hazards and related safety requirements which cannot be controlled by one actor alone shall be communicated to another relevant actor in order to find jointly an adequate solution.
- The hazards registered in the hazard record of the actor who transfers them shall only be “controlled” when the evaluation of the risks associated with these hazards is made by the other actor and the solution is agreed by all concerned.

Risk management process picture.2



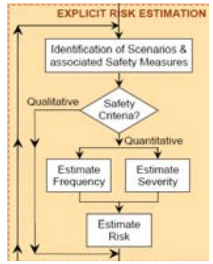
Codes of practice

- shall satisfy at least the following requirements
  - be widely acknowledged in the railway domain. If this is not the case, the codes of practice will have to be justified and be acceptable to the assessment body;
  - be relevant for the control of the considered hazards in the system under assessment;
  - be publicly available for all actors who want to use them.
- TSIs and National rules may be considered as codes of practice
- Where not fully compliant with a code of practice, the proposer shall demonstrate that the alternative approach taken leads to at least the same level of safety.
- If the risk for a particular hazard cannot be made acceptable by the application of codes of practice, additional safety measures shall be identified applying one of the two other risk acceptance principles.
- When all hazards are controlled by codes of practice, the risk management process may be limited to:
  - hazard identification
  - registration of the use of the codes of practice in the hazard record
  - documentation of the application
  - An independent assessment

Reference system

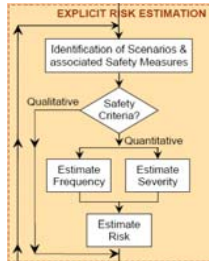
- Similar system could be taken as a reference system
- A reference system shall satisfy at least the following requirements:
  - it has already been proven in-use to have an acceptable safety level and would still qualify for approval in the Member State where the change is to be introduced;
  - it has similar functions and interfaces as the system under assessment;
  - it is used under similar operational conditions as the system under assessment;
  - it is used under similar environmental conditions as the system under assessment
- If a reference system fulfils the requirements listed, then for the system under assessment:
  - the risks associated with the hazards covered by the reference system shall be considered as acceptable;
  - the safety requirements for the hazards covered by the reference system may be derived from the safety analyses or from an evaluation of safety records of the reference system;
  - these safety requirements shall be registered in the hazard record as safety requirements for the relevant hazards
- If the system under assessment deviates from the reference system, the risk evaluation shall demonstrate that the system under assessment reaches at least the same safety level as the reference system. The risks associated with the hazards covered by the reference system shall, in that case, be considered as acceptable.
- If the same safety level as the reference system cannot be demonstrated, additional safety measures shall be identified for the deviations, applying one of the two other risk acceptance principles.

Explicit risk estimation.1



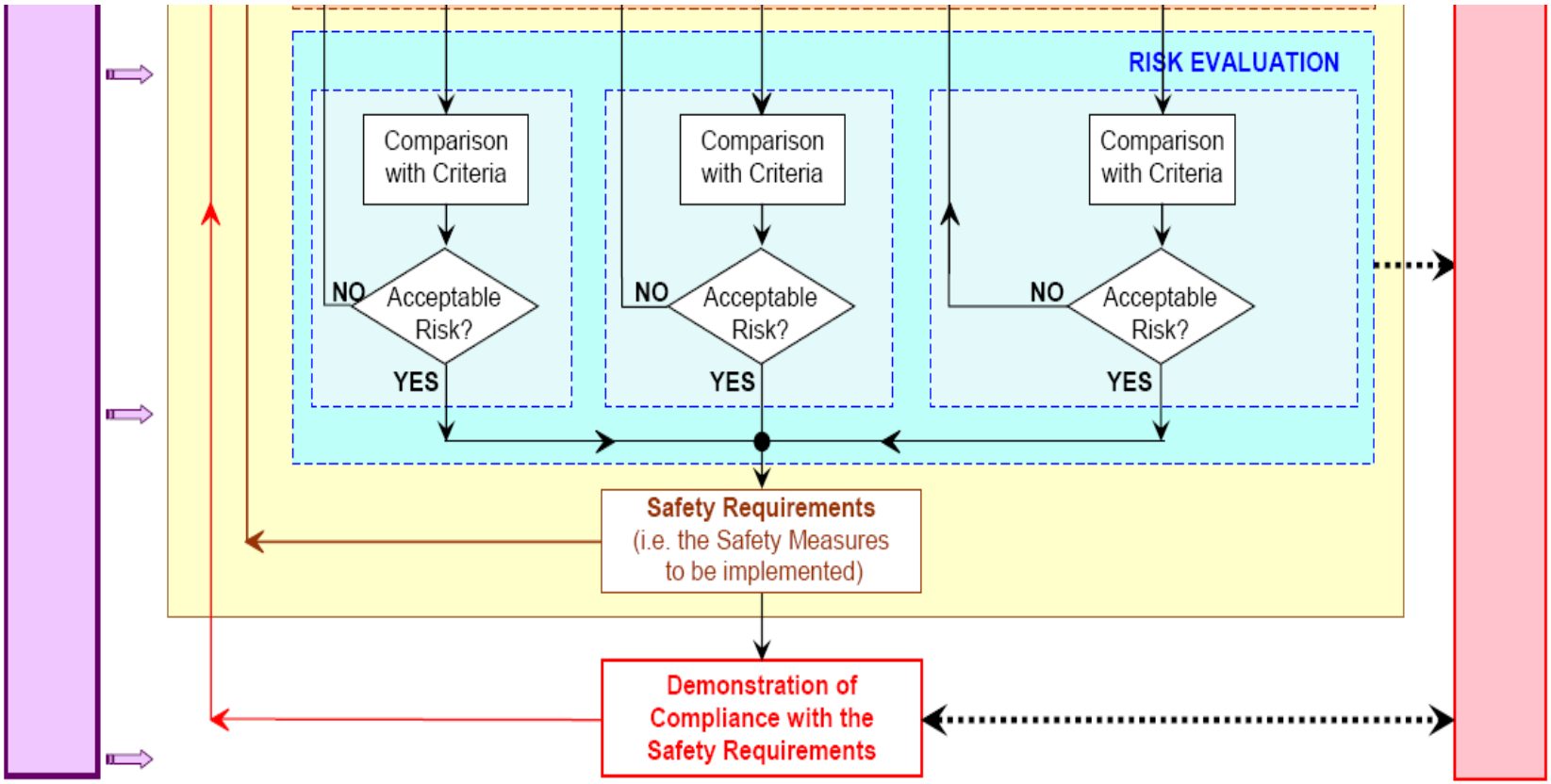
- When the hazards are not covered by codes of practice or reference systems, the demonstration of the risk acceptability shall be performed by explicit risk estimation and evaluation.
- Risks resulting from these hazards shall be estimated either quantitatively or qualitatively, taking existing safety measures into account.
- The acceptability of the estimated risks shall be evaluated using risk acceptance criteria either derived from or based on legal requirements stated in Community legislation or in notified national rules. Depending on the risk acceptance criteria, the acceptability of the risk may be evaluated either individually for each associated hazard or globally for the combination of all hazards considered in the explicit risk estimation.
- If the estimated risk is not acceptable, additional safety measures shall be identified and implemented in order to reduce the risk to an acceptable level.
- When the risk associated with one or a combination of several hazards is considered as acceptable, the identified safety measures shall be registered in the hazard record.

Explicit risk estimation.2



- Where hazards arise from failures of technical systems not covered by codes of practice or the use of a reference system, the following risk acceptance criterion shall apply for the design of the technical system:
  - For technical systems where a functional failure has credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to 10^{-9} per operating hour.
- A more demanding criterion may be requested, through a national rule, in order to maintain a national safety level.
- If a technical system is developed by applying the 10^{-9} criterion the principle of mutual recognition is applicable
- Nevertheless, if the proposer can demonstrate that the national safety level in the Member State of application can be maintained with a rate of failure higher than 10^{-9} per operating hour, this criterion can be used by the proposer in that Member State.
- The explicit risk estimation and evaluation shall satisfy at least the following requirements:
  - 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 serve as robust decision support, i.e. minor changes in input assumptions or prerequisites shall not result in significantly different requirements.

Risk management process picture.3



Demonstration of compliance

- Prior to the safety acceptance of the change, fulfilment of the safety requirements resulting from the risk assessment phase shall be demonstrated under the supervision of the proposer.
- This demonstration shall be carried out by each of the actors responsible for fulfilling the safety requirements
- The approach chosen for demonstrating compliance with the safety requirements as well as the demonstration itself shall be independently assessed by an assessment body.
- Any inadequacy of safety measures expected to fulfil the safety requirements or any hazards discovered during the demonstration of compliance with the safety requirements shall lead to reassessment and evaluation of the associated risks by the proposer.
- The new hazards shall be registered in the hazard record.

Evidence

- The risk management process used to assess the safety levels and compliance with safety requirements shall be documented by the proposer in such a way that all the necessary evidence showing the correct application of the risk management process is accessible to an assessment body.
- The assessment body shall establish its conclusion in a safety assessment report.
- The document produced by the proposer shall at least include:
  - description of the organisation and the experts appointed to carry out the risk assessment process,
  - results of the different phases of the risk assessment and a list of all the necessary safety requirements to be fulfilled in order to control the risk to an acceptable level.

Independent assessment

- An independent assessment of the correct application of the risk management process shall be carried out by an independent body
- The body may be
  - Identified by Community or national legislation
  - Appointed by the proposer
    - Another organisation
    - Independent department
- Duplication of work between the conformity assessment should be avoided
  - Conformity assessment by notified body or national body
- The safety authority may act as the assessment body in the case of
  - Vehicle placing in service authorizations
  - Safety certificates of railway undertaking and infrastructure managers
  - Harmonisation of safety certificates or in the case of accident and incident investigation

Independent assessment criteria

- The assessment body is not involved in:
  - Design
  - Manufacture
  - Construction
  - Marketing
  - Operation
  - Maintenance
- Professional integrity
  - Competence
  - Independence
  - Liability ensured
  - Confidentiality
- Possess the means required
  - Technical tasks
  - Administrative tasks
  - Access for required equipment
- The staff
  - Proper training
    - Technical
    - Vocational
  - Requirements knowledge
  - Reporting skills

Safety assessment reports

- The safety assessment body shall provide the proposer with a safety assessment report.
- The report shall be taken into account
  - by the national safety authority in its decision to authorise the placing in service of subsystems and vehicles
  - by the notified body in the charge of delivering the conformity certificate
  - by the contracting entity in charge of drawing up the EC declaration of verification

Monitoring CSM practices

- Audits of application of the CSM monitored by the national safety authority
  - Undertakings
  - Infrastructure managers
- The national safety authority reports to Agency
- Agency informs the Commission