Risk assessment and Safe integration of railway sub-systems – Process and formalism

TSI and Data Digitalisation Workshop

Dragan JOVICIC | 27 March 2025| Hybrid - Portugal

EUROPEAN UNION AGENCY FOR RAILWAYS

Overall architecture of the railway system

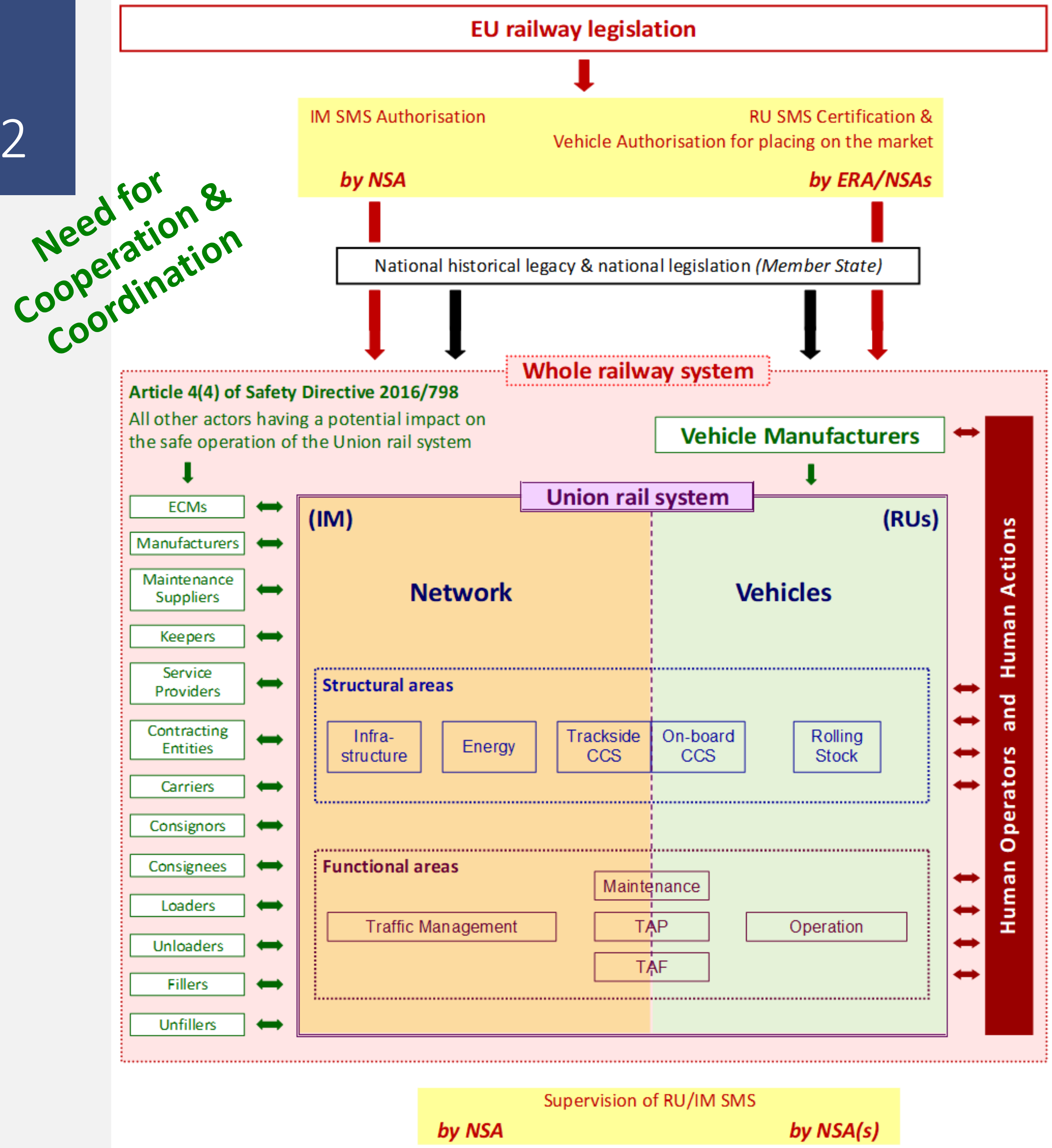


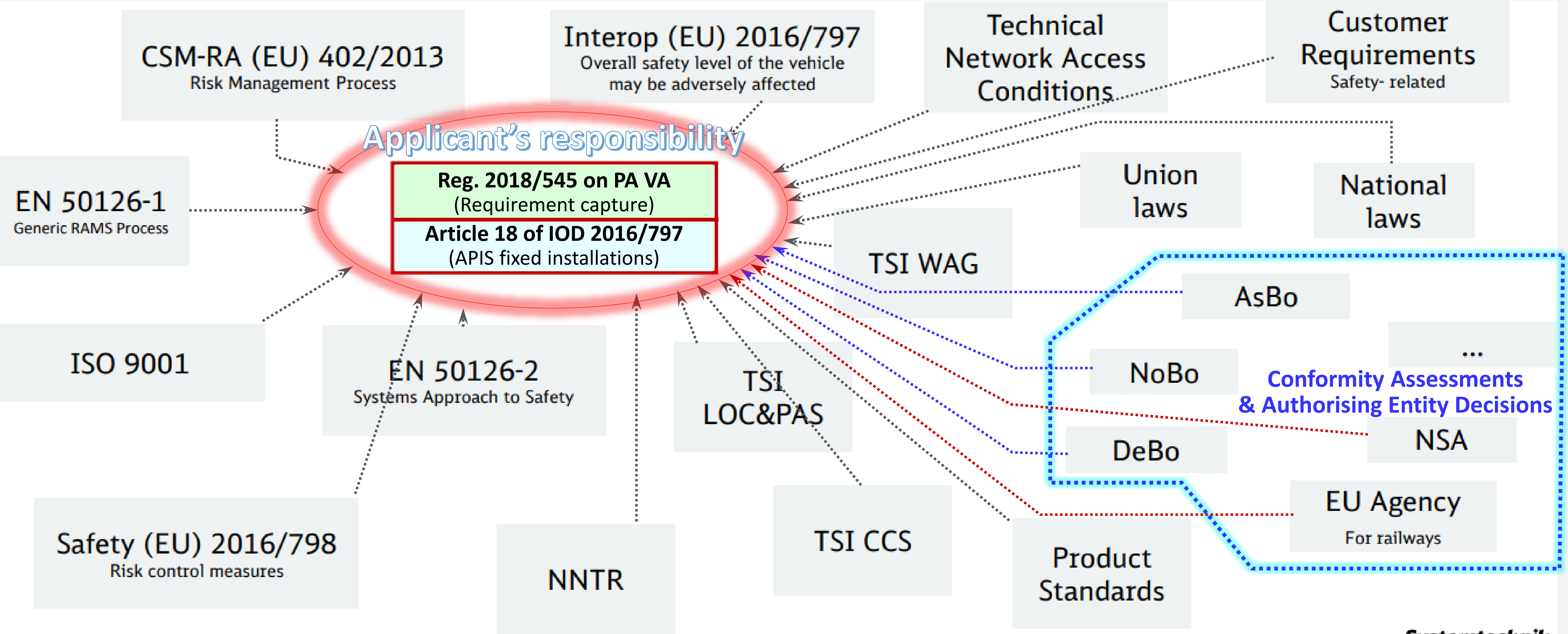
Figure 2 built based on:

1) definitions (1), (3), (4) and (5) in Article 2 and Annexes I and II of Interoperability Directive (EU) 2016/797, and
2) Article 4 of Safety Directive (EU) 2016/798

Railway undertakings (RUs) and infrastructure managers (IMs) main actors **responsible for**:

1) safety of railway system, and
2) safety of railway traffic management, operations

Example of legal and process requirements a Proposer (or an Applicant) must comply with for the placing of a vehicle on the market or a line into service



Systemtechnik

EUROPEAN UNION AGENCY FOR RAILWAYS

Usual railway sector perceptions regarding railway market opening legislation

1) Introduction of new concepts and terminology

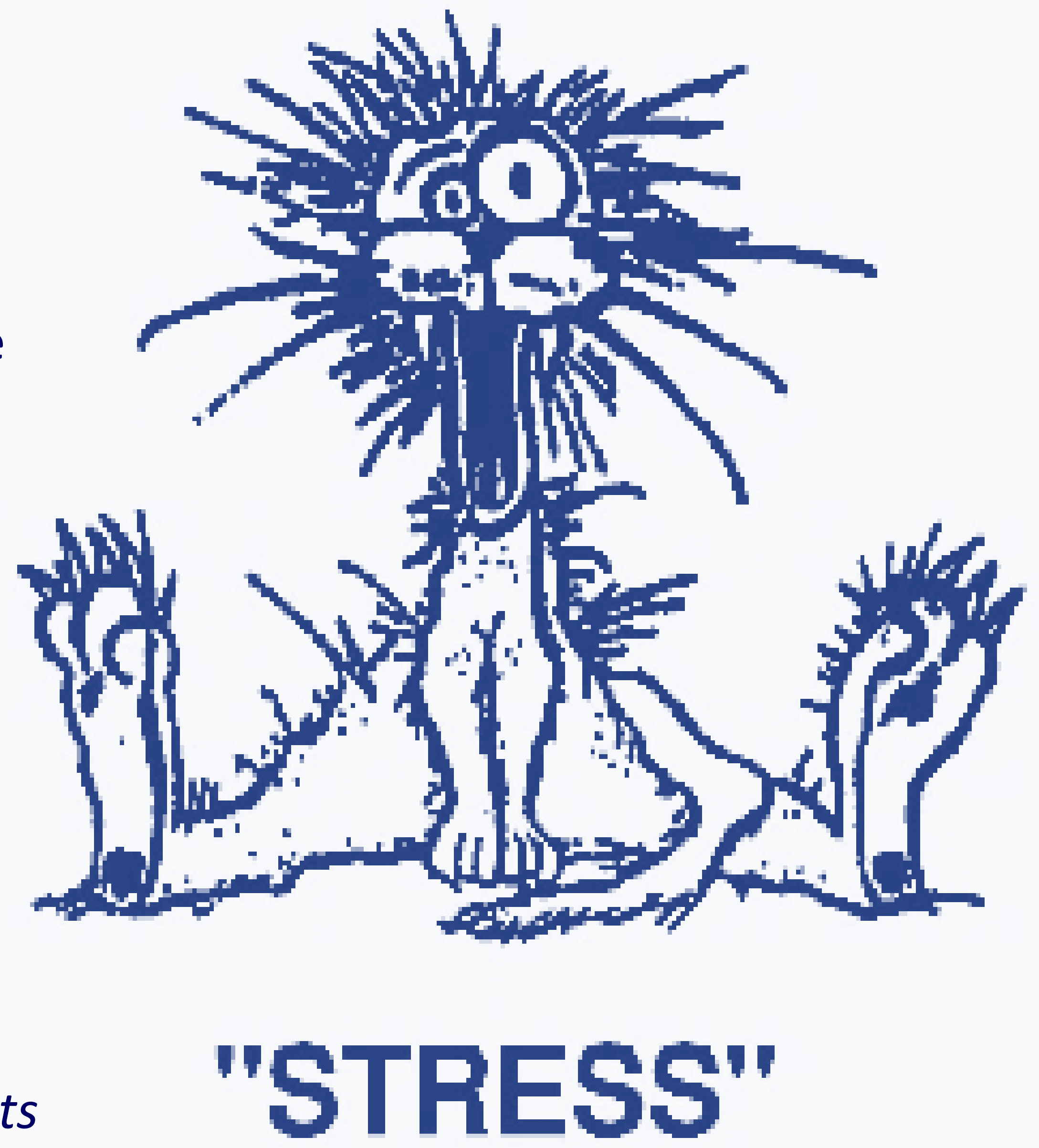
2) New sharing of roles and responsibilities between existing but also new railway stakeholders/actors

3) Need for certification by an Authorising Entity of the capability of railway undertakings, infrastructure managers and ECMs to manage safely their railway activities **+** regular supervision by NSA

4) Need for verification by independent conformity assessment bodies (CABs) (NoBos, DeBos, ECM CBs, AsBos) of the compliance with applicable legislation

5) Authorisation of placing on the market mobile sub-systems *based on CABs' independent assessments*

6) Authorisation of placing into service of fixed installations *based on CABs' independent assessments*



Main changes:

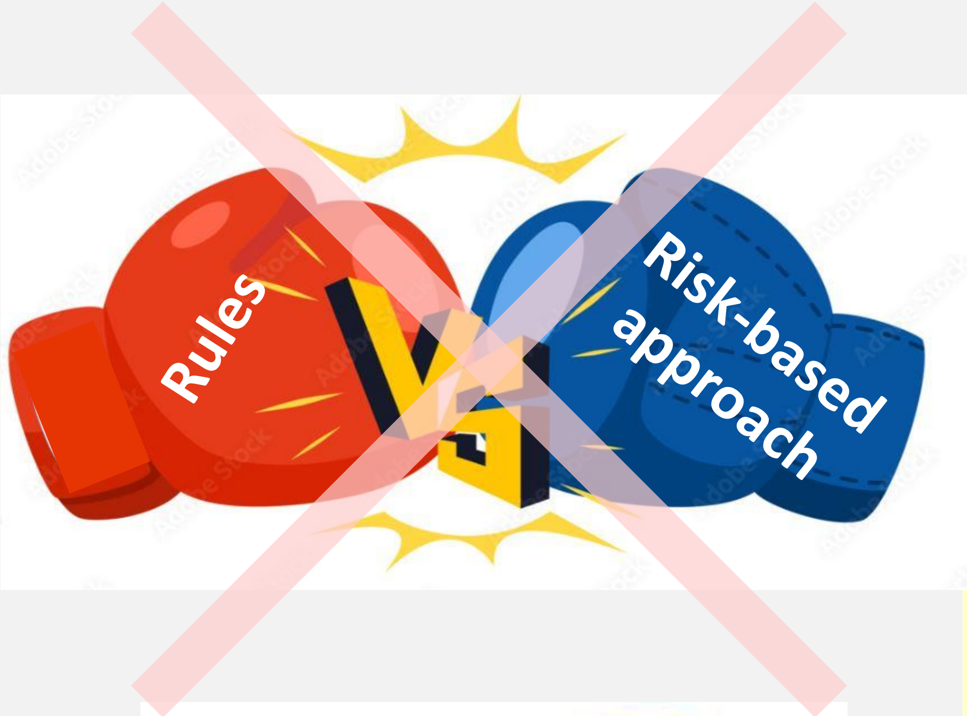
1) organisational changes separating operations and infrastructure
2) new actors, roles and responsibilities (ERA, NSA, ECMs, RUs, IMs, NoBos, DeBos, AsBos, etc.)
3) harmonisation of technical specifications for interoperability
4) harmonisation of safety regulatory framework

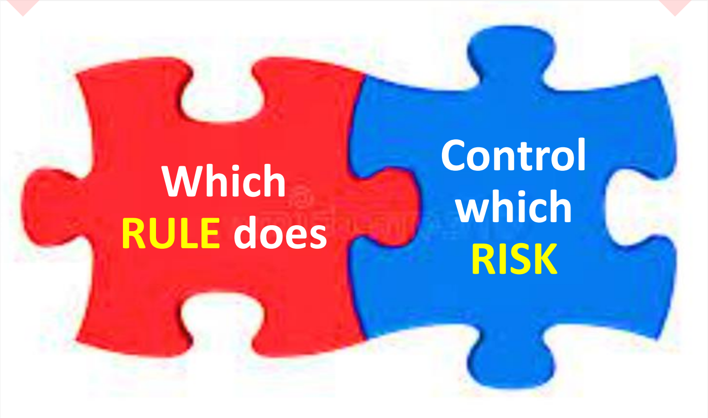
Examples of other novelties:

1) Moving from “blind” **compliance to predefined Rules/Standards** to a risk-based approach with **Proactive Risk Identification, Risk Management and Risk Monitoring**
2) Obligation to cooperation for identifying and managing jointly risks shared at interfaces between several sub-systems/actors
3) Necessity for a systematic top-down approach for identifying, allocating and managing implementation and validation of intended functions and requirements
4) **Safe integration of changes into railway system and demonstration of absence of unsafe impacts of those changes (non-regression) on non-modified parts of railway system**

EUROPEAN UNION AGENCY FOR RAILWAYS

Perception of the concepts





- In general lack of understanding and many fears arising from new concepts and new terminology (in English)
- Most people perceive Risk Identification and Risk Management as a **boring task** that almost nobody likes and **nobody is happy to deal with it**
- Wrongly understood as replacing rules historically used to control risks experienced in past
- No matter we like or dislike it, all risks a company is exposed to must be:
  - identified/known and understood
  - controlled to an acceptable level by appropriate (risk control) measures
  - monitored to verify effectiveness of those measures
  - If necessary, other measures identified & implemented

EUROPEAN UNION AGENCY FOR RAILWAYS

Solution to overcome perceived complexity

Nothing really new, as for a **complex and safety related system,** to fulfil all applicable requirements **(Outputs)**, applicant must have:

1) an organisation/**Structure** with competent **staff** (personnel)
2) supporting safety and quality **Processes** for:
   a) correct capture (identification) of all requirements to be fulfilled
   b) allocation of requirements to functions or sub-systems
   c) management of implementation of all requirements
   d) tests, verification and validation to demonstrate correct implementation of all requirements (**Outputs**) throughout development process

Known in existing standards as "**system engineering and functional safety engineering**", i.e. a structured and systematic top-down approach for identification and management of requirements to be fulfilled by **complex and safety related systems**

Tools in EU railway legislation

1. **Reg. 402/2013** on CSM for risk assessment

   Further developed in:

   "ERA1209-063 Clarification note on safe integration"

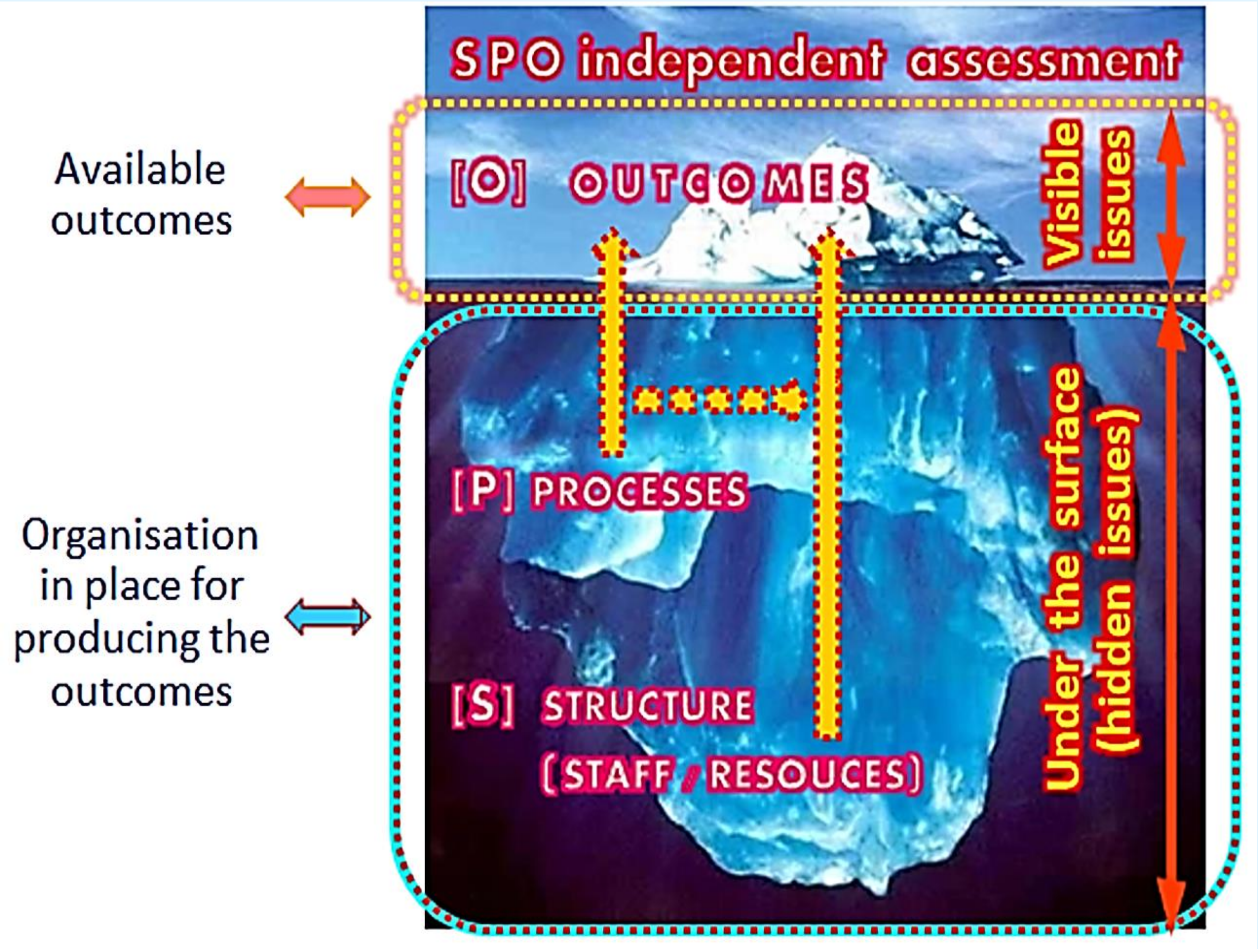
2. Requirement capture process in Article 13 of **Reg. 2018/545 on PA VA**

3. Concepts in these two tools [1 & 2] also apply to **infrastructure projects**

EUROPEAN UNION AGENCY FOR RAILWAYS

What to remember regarding independent safety assessments by an AsBo?

Proposer's/Applicant's organisation and processes for change and risk management activities



AsBo working method

1. **Understand** context and scope, proposer's organisation and processes supporting the project and risk management activities
2. **Plan and Prioritise** independent assessment *(including selection of samples for vertical slice assessment)*
3. **Assess** correct application by the proposer of risk management process and suitability of results
4. **Conclusions & Independent Assessment Report** to the proposer

EUROPEAN UNION AGENCY FOR RAILWAYS

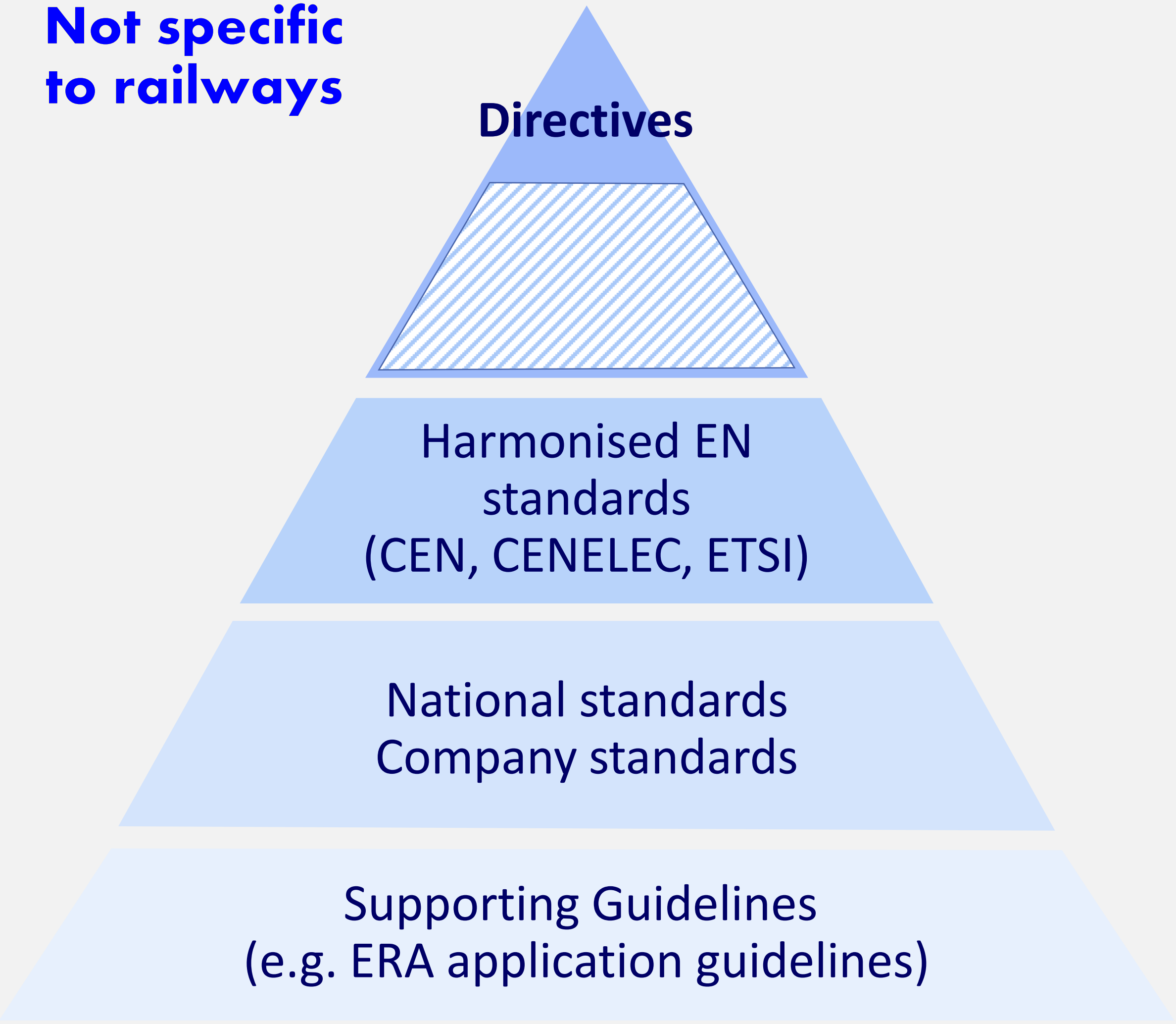
Application of EU new approach to free circulation of products across the EU to specific case of railway market opening

EUROPEAN UNION AGENCY FOR RAILWAYS

General principles within EU New Approach/Global Approach that products must meet to benefit from free movement across EU

Check of compliance with standards by accredited/recognised (CAB)

Not specific to railways



Political decisions – Primary legislation that **needs to be transposed in national laws**

Harmonisation requirements (usually in Directives) define mandatory **essential requirements that products must meet**

EN Standardisation: technical specification for products - Application voluntary unless made mandatory in EU legislation

Other standards or technical specifications permitted (unless mandatory through Notified National Rules)

Voluntary supporting documents

Products manufactured in compliance with harmonised standards & assessed by accredited/recognised CABs benefit from presumption of conformity with essential requirements without further checks

EUROPEAN UNION AGENCY FOR RAILWAYS

Principles of EU New Approach and Global Approach applied to railways
Essential requirements specified not only in directives

Check of compliance with standards by accredited/recognised (CAB)

Directives	IOD 2016/797 SD 2016/798 ERA Reg. 2016/796	Political decisions – Primary legislation that **needs to be transposed in national laws**
Safety Regulatory framework / TSIs	**Specific to railway needs**	Commission Regulations and Decisions (TSIs) which application is mandatory **(without any transposition)**
Harmonised EN standards (CEN, CENELEC, ETSI)		Standardisation: application is voluntary **unless made mandatory in EU legislation** (e.g. ISO 17020 in CSM for risk assessment)
National standards Company standards		Standardisation: voluntary **unless made mandatory through Notified National Rules**
Supporting Guidelines (e.g. ERA application guidelines)		Voluntary supporting documents

Compulsory use of CABs with defined R&R

Authorisation for placing on market of Mobile sub-systems [by ERA or NSA]
Authorisation for placing into service of Fixed installations [NSA]

EU safety regulatory framework for railways

Main novelty in EU railway market opening legislation
Introduction of a harmonised way of thinking in terms of risks

For many railway stakeholders, major shift in manner to manage safety of railway operation, traffic management and maintenance activities

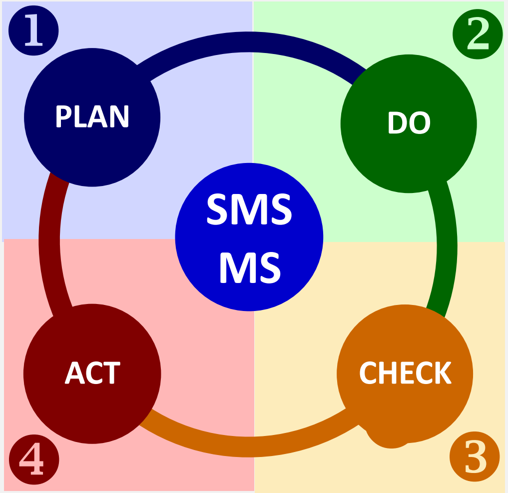
1) **PAST:**
   a) sufficient to comply with well-established national rules, standards and legislation
   → technical differences, <u>and approach to safety</u>, among countries
   b) International traffic made possible only thanks to (voluntary) <u>international or multilateral agreements</u> (COTIF, RIV, bilateral agreements,…)

2) **NOVELTY:** EU railway market opening legislation requires stakeholders to fully take themselves the responsibility for the safe management of their activities through a **risk based approach**

→ New concepts and new obligations/responsibilities that generate many fears

EUROPEAN UNION AGENCY FOR RAILWAYS

Main novelty in EU railway market opening legislation
Proactive and continual risk identification, management and monitoring



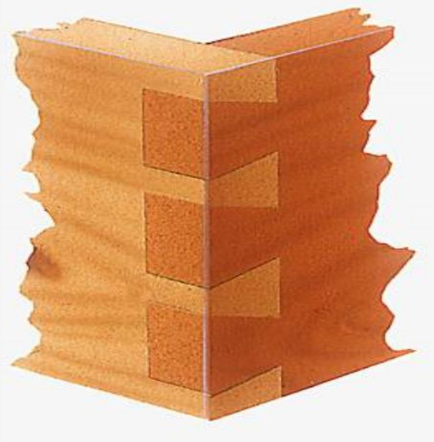
- Instead of **«reacting and fixing»** only the events that occurred in past, the Safety Directive requires RUs, IMs & ECMs to put in place:
  - **(Safety) Management System (SMS/MS),** and;
  - **proactive** way of thinking in **«predicting and preventing»** possible unwanted events (risks) that may happen;
- To ensure safe **Operation & Maintenance** of railway system, Safety Management System [System of Maintenance] [**SMS/MS**] shall look both FORWARD and RETROSPECTIVE in order to IDENTIFY and CONTROL (all) risks associated with RU, IM & ECM activities. This implies to:
  - **«predict»** unwanted events that can happen during operation & maintenance;
  - **«identify and implement»** risk control measures [i.e. SMS processes, procedures, & rules] in order to **«prevent»** them to happen or, if the risk cannot be eliminated, to **«protect»** against the consequences of those unwanted events;
  - **«monitor»** continually the effectiveness of predictive and preventive measures

EUROPEAN UNION AGENCY FOR RAILWAYS

Cornerstones/Pillars processes of an effective Safety Management System [System of Maintenance]

1

CSM for risk assessment



3

CSM for monitoring

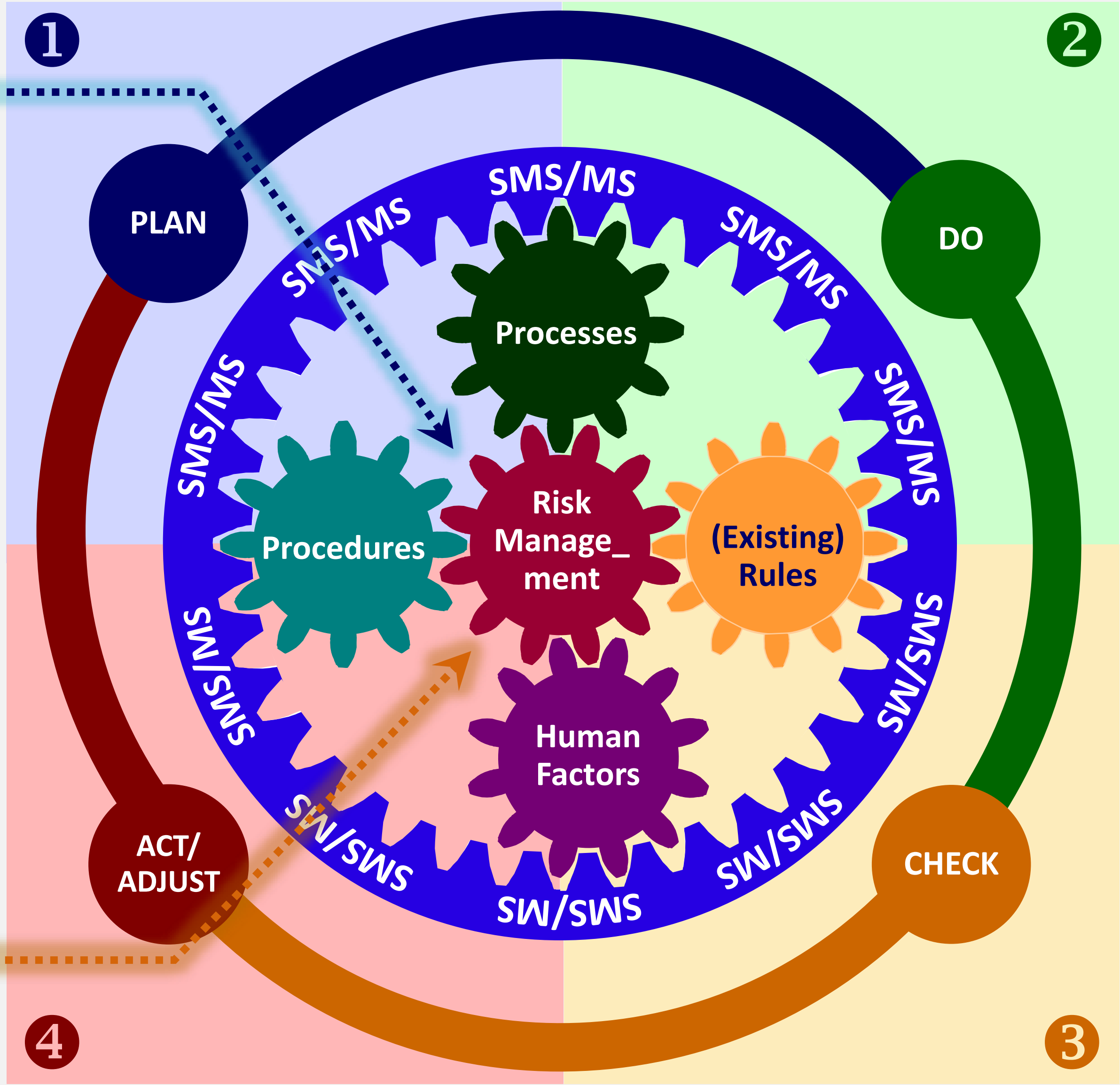
cannot be separated from each other

Implementation of "Technical, Operational & Organisational" changes can be safe & effective only if **Change Control Management** process of RU/IM SMS is based on a continual and combined use of these two other key processes

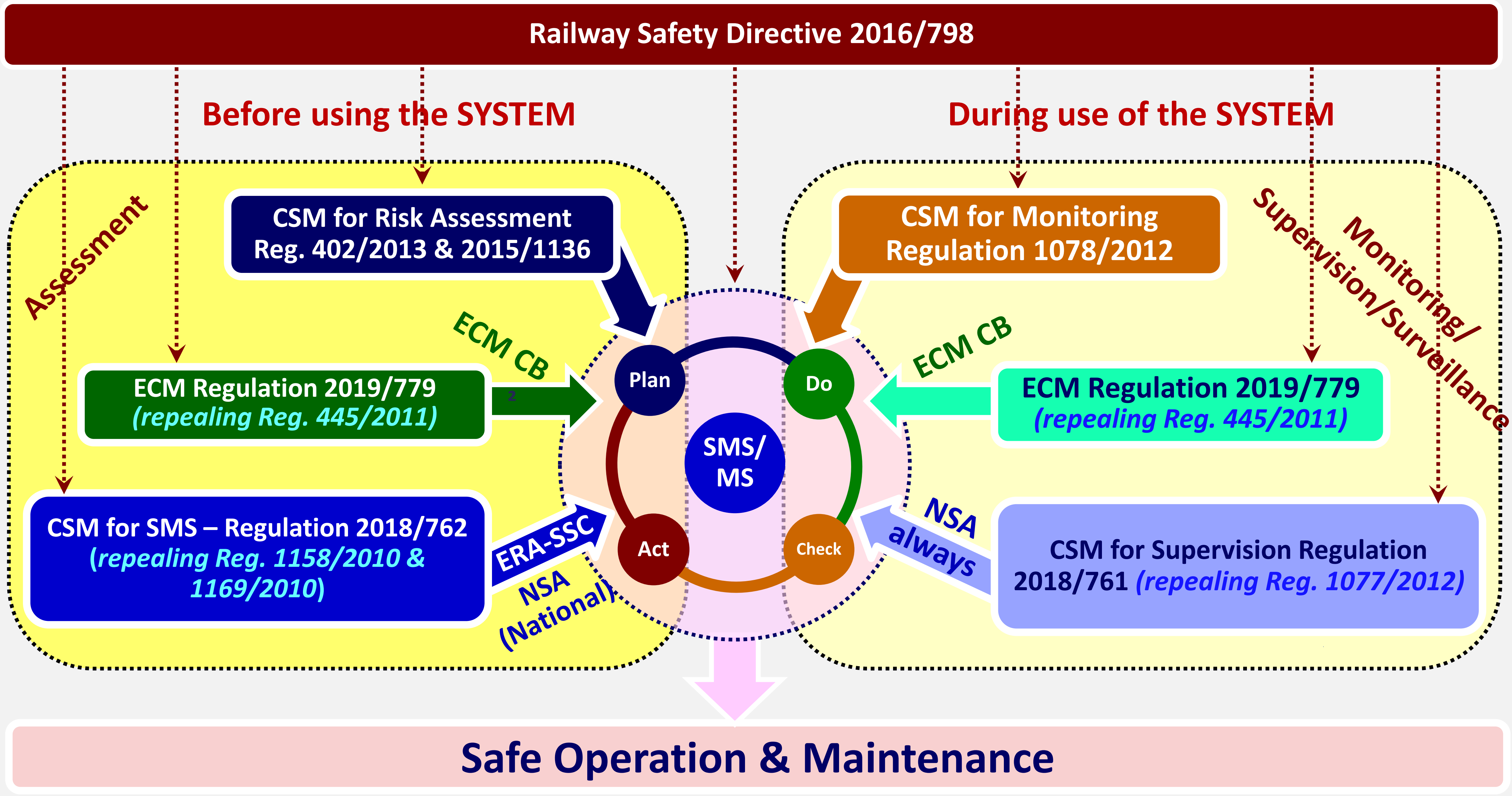
1. CSM for risk assessment (Reg. 402/2013 and 2015/1136), and
3. CSM for monitoring (Reg. 1078/2012)

EUROPEAN UNION AGENCY FOR RAILWAYS

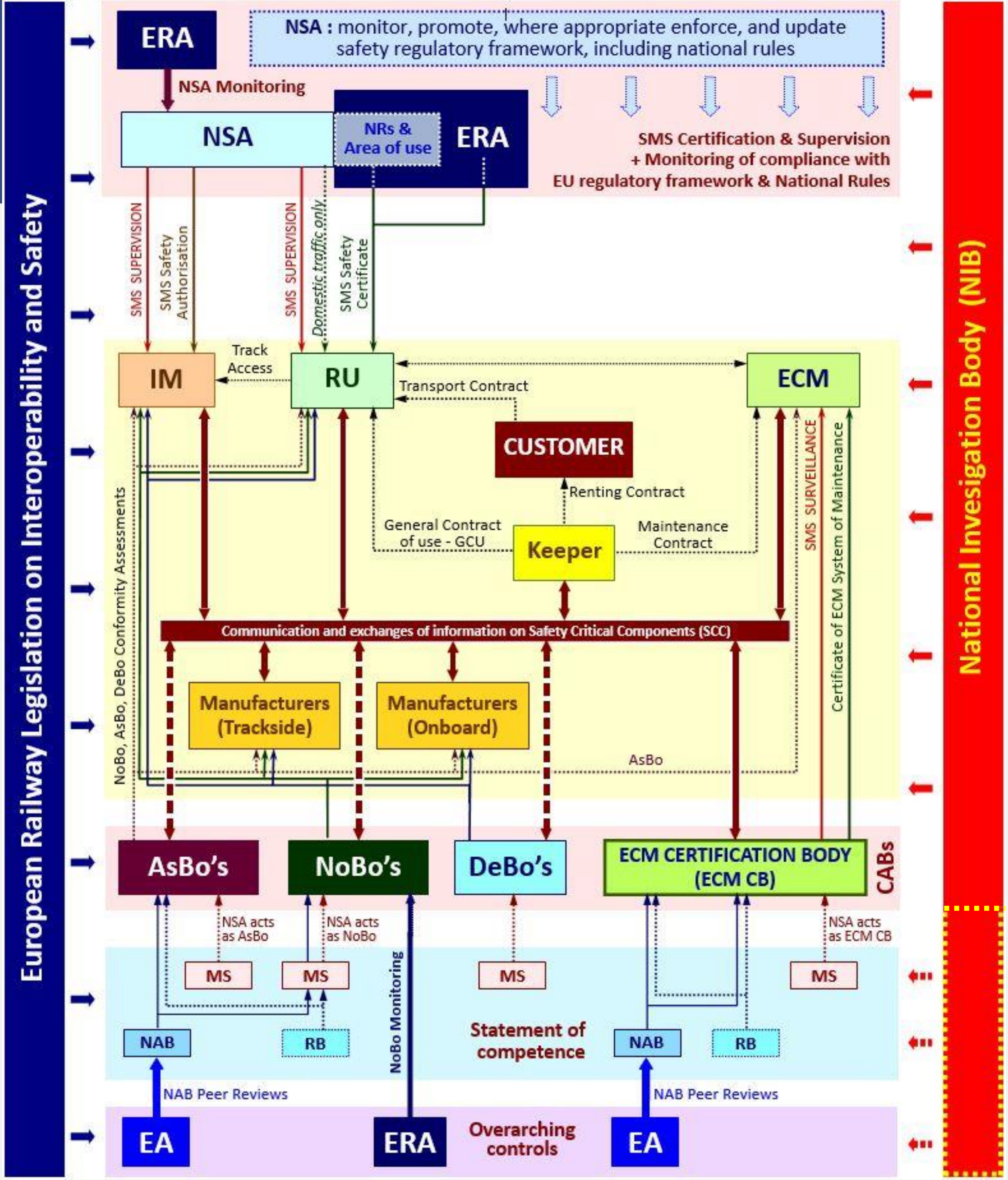
Relation of CSM RA and CSM for monitoring with other processes of the Safety Management System [System of Maintenance]



Legal texts in European Railway Safety Regulatory Framework



Overall picture of main railway actors and control mechanisms foreseen in EU railway legislation



SMS/MS Certification and Authorisation
Mutual recognition across the EU

- ❑ RU SMS must be certified by ERA, or where relevant by NSA, **and supervised by NSA**
- ❑ IM SMS must be certified & supervised **by NSA**
- ❑ ECM system of maintenance must be certified & supervised **by ECM certification body**

Independent conformity assessment bodies (CABs) responsible for verification of conformity:

1) **by NoBos** of ICs and structural sub-systems with Interoperability Directive 2016/797 and TSIs
2) **by DeBo** with National Rules
3) **by AsBo** with CSM for risk assessment

Overview of the CSM for risk assessment

(Regulation 402/2013 & Regulation 2015/1136)

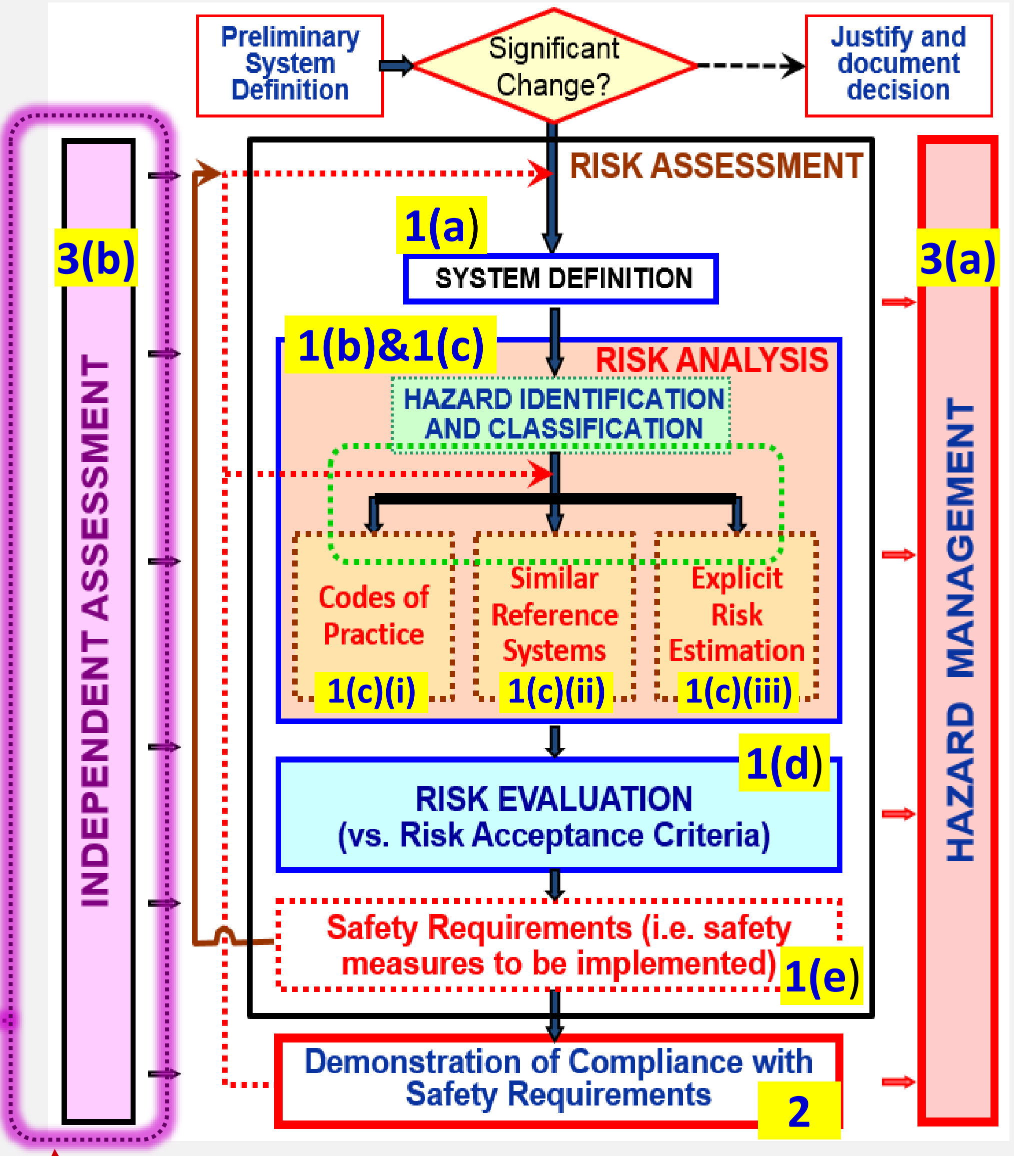
EUROPEAN UNION AGENCY FOR RAILWAYS

Overview of CSM RA - Flowchart in Annex I

1) Common PROCESS for risk assessment of **changes of Technical, Operational & Organisational nature (TOO)**, including:
   - (a) System definition
   - (b) Identification of hazards/risks & associated safety measures
   - (c) Risk analysis based on exiting risk acceptance principles (**CoP, Ref. Syst, Explicit Risk Estimation - no priority**)
   - (d) Risk evaluation for checking acceptance of risk(s)
   - (e) Definition of safety requirements from identified safety measures

2) Demonstration of system compliance with identified safety requirements

3) **Requirements for mutual recognition:**
   - (a) Hazard Management via a Hazard Log
   - (b) **Independent Assessment (AsBo) of correct application of general requirements of a PROCESS + of suitability of results**



Iterative Risk Management Process "triggered" by a Significant Change

Roles & Responsibilities

- Proposer responsible for applying CSM RA:
  - carry out risk assessment of **all safety related changes**
  - document/justify all decisions and results

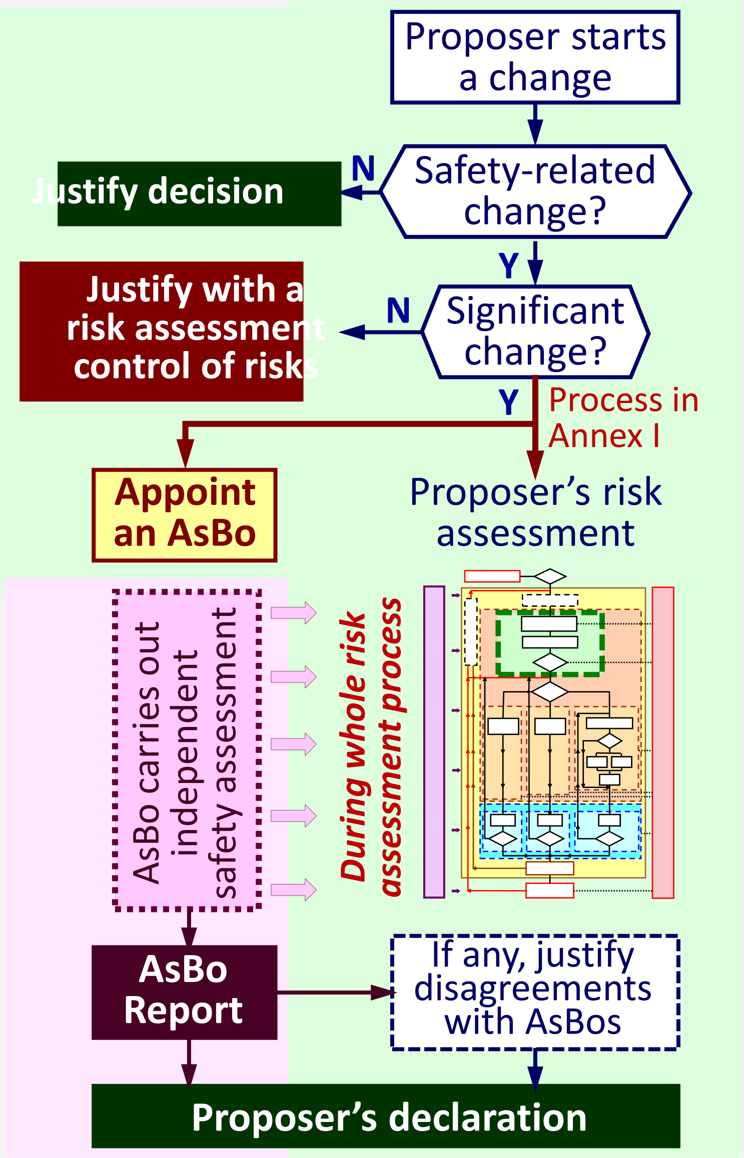
- **When change significant**, Proposer must appoint an AsBo for:
  - independent assessment of both correct application of risk management process and suitability of results from that process
  - deliver an **Independent Safety Assessment Report** to Proposer

- Proposer responsible for determining **<u>if and how</u>** to take into account conclusions of AsBo Report for accepting change

  If it disagrees with any part of AsBo report, <u>justify and document</u>

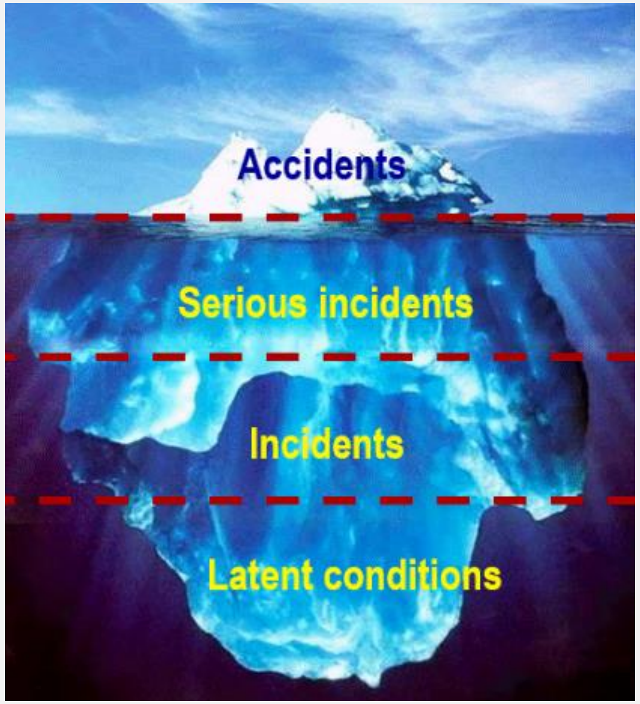
- **Article 16: Proposer's Declaration**

  Based on results of its own risk assessment and on AsBo Report, Proposer must produce a **<u>written Declaration</u>** stating that all identified hazards and associated risks are controlled to an acceptable level



EUROPEAN UNION AGENCY FOR RAILWAYS

Method alone does not lead to successful Risk Management



- Risk Assessment is not always a ton of paper – It could be short
- The most important step in any risk assessment is that **hazards can only be controlled if they are IDENTIFIED**
- Risk assessment is a **means to an end**, not an end in itself. The aim is to **keep people safe**, **not only to have good paperwork**
- The risk analysis process depends on:

  - the experience,
  - the knowledge,
  - the imagination,
  - the creativity, and,
  - the integrity

  of the individuals doing the analysis

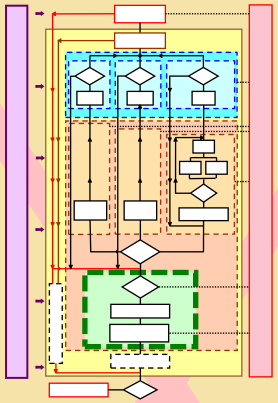
The only application of risk assessment and risk management techniques without appropriately talented/competent staff does not ensure a proper and thorough risk analysis result

EUROPEAN UNION AGENCY FOR RAILWAYS

Successive versions of CSM for risk assessment
Dates of application of the methodology

2005 to 2007

19/07/2010 Technical changes
01/07/2012 TOO changes



RAC-TS [10^{-9} h^{-1}]

Regulation 352/2009
(+ 2 existing Guides)

2010 to 2012

21st May 2015
(Repealing Reg. 352/2009)

R&R CSM AB

Regulation 402/2013

~~**More categories of RAC-TS**~~

2012 to 2014

3rd August 2015
(Amending Reg. 402/2013)

Regulation 2015/1136

CSM DT
[10^{-9} & 10^{-7} h^{-1}]

Regulation 1078/2012 on
CSM for monitoring
applicable since 7th June 2013

EUROPEAN UNION AGENCY FOR RAILWAYS

Associated guides for application of CSM for risk assessment
Complementarities between Guides and Standards

WHAT shall be done?

Regulation 402/2013 on CSM RA and its amendment by Regulation 2015/1163 (repeals Regulation 352/2009)

+

Reg. 2015/1136 on CSM Design Targets (CSM DT)

Existing material

HOW to comply with CSM?

Application Guide on Reg. 352/2009 on CSM for risk assessment

Explanatory Note Roles & Resp. CSM Assessment Body

Application Guide on CSM DT

Examples on **HOW** to apply the CSM

Collection of Examples of risk assessment and Some possible supporting tools

Supporting Standards

IEC61508, IEC/ISO 31000 & 31010
CENELEC 50126, 50128/50716 and 50129 Standards
+ Other Standards (FMECA, FTA, ...)

CENELEC 50126-1:2017, 50126-2:2017, 50716:2023 & 50129:2018

IEC/ISO 31000 & 31010
CENELEC 50126, 50128/50716 and 50129 Standards
+ Other Standards (FMECA, FTA, etc.)

Where is risk assessment necessary/required?

Summary of the legal requirements

Reg. 402/2013 on CSM RA → Manage safely the changes [Art. 4 & 2(2)]

Safety Directive 2016/798
- Art. 6(1)(a) → Reg. 402/2013 on CSM RA
- Art. 9 → RU/IM SMS
- Art. 14 → ECM MS

Interop. Directive 2016/797
- Art. 10 → 'EC' decl. of conformity or suitability for use of ICs
- Art. 15 & 20 → 'EC' decl. of verification of a subsystem
- Art. 18 → Auth. for placing in service of fixed installations
- Art. 15 → 'EC' declaration of verification of onboard and trackside CCS structural sub-system (Regulation 2023/1695)
- Art. 21 → Vehicle authorisation for placing on the market (Regulation 2018/545)

TSIs → Where specifically requested by a TSI (e.g. LOC&PAS, WAG, SRT TSIs)

Safety related changes

- Risk assessment **must always be done**
- Documentary evidence must always exist

Operational & Organisational nature changes
- RU/IM SMS
- ECM MS

Changes of technical NATURE
- 'EC' decl. of conformity or suitability for use of ICs
- 'EC' decl. of verification of a subsystem
- Auth. for placing in service of fixed installations
- **'EC' declaration of verification of onboard and trackside CCS structural sub-system (Regulation 2023/1695)**
- **Vehicle authorisation for placing on the market (Regulation 2018/545)**
- **Where specifically requested by a TSI (e.g. LOC&PAS, WAG, SRT TSIs)**

Non-significant

Justification **must be done by Risk Assessment** (next slide examples of process)

(AsBo optional)

Significant or by law application of

Risk Assessment in **Annex I of CSM is mandatory**

+

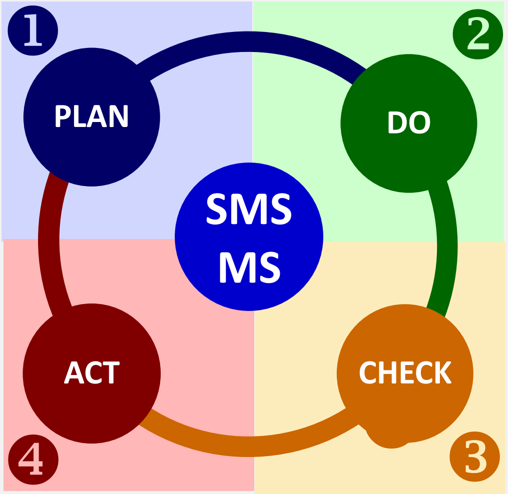
AsBo mandatory

Non-safety related

- Risk assessment not needed
- Keep traceability of changes to justify a proper management of changes

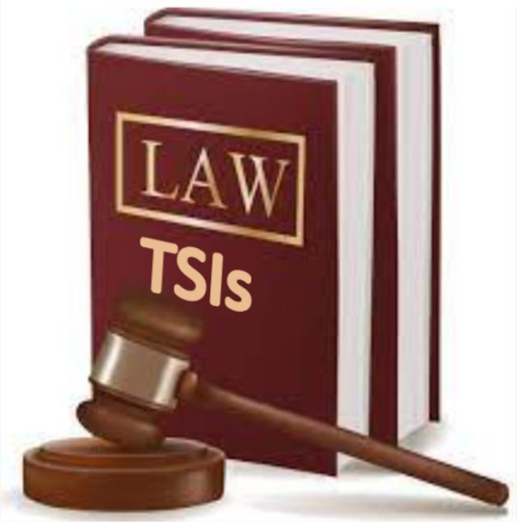
EUROPEAN UNION AGENCY FOR RAILWAYS

Where is risk assessment necessary/required?



Changes to SMS of Operational and Organisational nature

Changes of technical nature



Compliance with TSIs

Authorisation for placing vehicles on the market

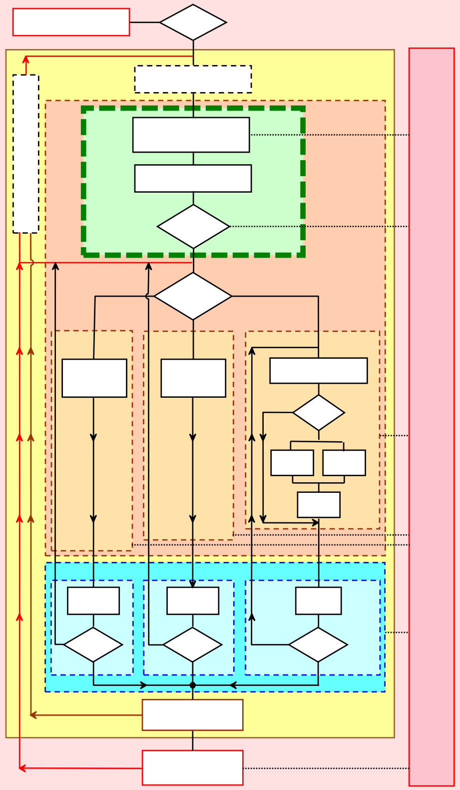
ERTMS - CCS TSI

EUROPEAN UNION AGENCY FOR RAILWAYS

Examples of "processes for risk assessment" and control of risks arising from safety-related non-significant changes

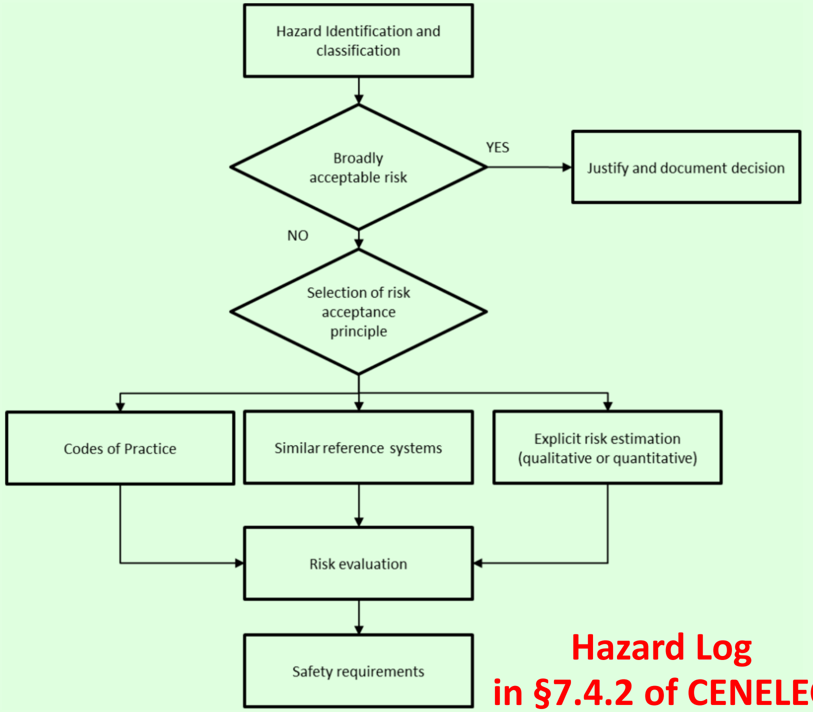
1

Annex I of Reg. 402/2013 without AsBo



2

Figure 8 in CENELEC 50126-1:2017 standard on the process for risk assessment (related to phases 3 and 4 of Figure 6)

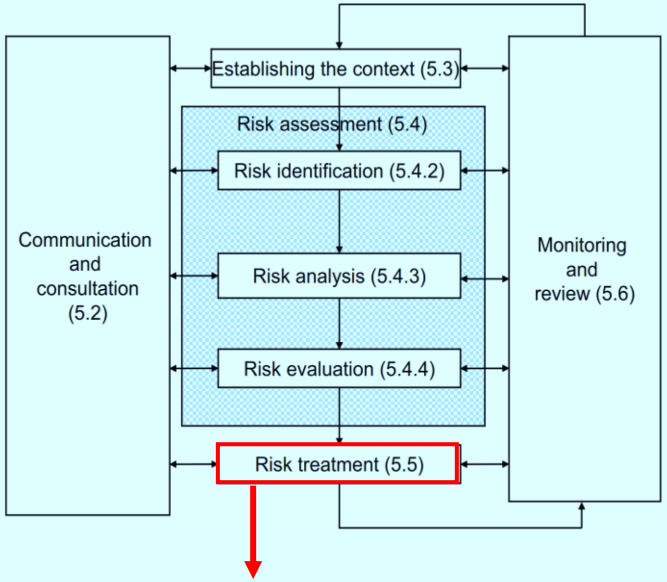


Hazard Log in §7.4.2 of CENELEC

Implementation and demonstration of compliance part of Figure 6 of 50126-1:2017

3

Figure 3 in ISO 31000 standard Risk management process



Includes implementation of control measures that make the risk acceptable/tolerable

Return of Experience [REX] with the CSMs

EUROPEAN UNION AGENCY FOR RAILWAYS

Return of Experience with CSM RA: underestimation of importance of independent assessment of safe management of safety-related changes

PRACTICE: many railway actors misuse concept of "Significant Change" in CSM RA

Return of experience (REX) done in 2018 shows that:

- most of railway stakeholders underestimates **importance of:**
  - **carrying out a formal risk assessment**, when implementing changes in railway system, **and**
  - **independent assessment** by an AsBo of risk assessment and its results
- **less than 5% of changes** considered as **significant**, and lead to:
  - a formal application of risk management process in Annex I of CSM RA
  - an independent assessment by an AsBo of correct application of risk management process and of suitability of results from risk assessment

- In practice, no matter we like or dislike it, proper Risk Identification, Risk Control and Risk Management must be done for both Significant and Non-Significant changes

EUROPEAN UNION AGENCY FOR RAILWAYS

Correct thinking and behaviour

Rather than focussing on demonstration that a "safety-related change" is not significant, and thus wasting crucial time, Proposer shall always:

- carry out a formal & systematic identification of all reasonably foreseeable risks arising from change
- reflect on added the value of independent safety assessment by an AsBo (e.g. need of mutual recognition for an authorisation or customer) → then do not hesitate to:
  - categorise change as significant
  - appoint an AsBo from beginning of project – **Contracting an AsBo at end of project is useless**
- no matter whether safety-related change is significant, or not, ensure risks are acceptable, by either:
  - eliminating risk (*preventive risk control measures*), or
  - reducing either frequency or severity of consequence (*risk mitigation measures*), or
  - accepting risk, if risk is reduced to a sufficiently low level, or
  - transferring to another actor, if the risk is related to an interface shared with another actor
- document formally all results from risk assessment → **evidence of proper risk management**

EUROPEAN UNION AGENCY FOR RAILWAYS

When making a change, when shall start:

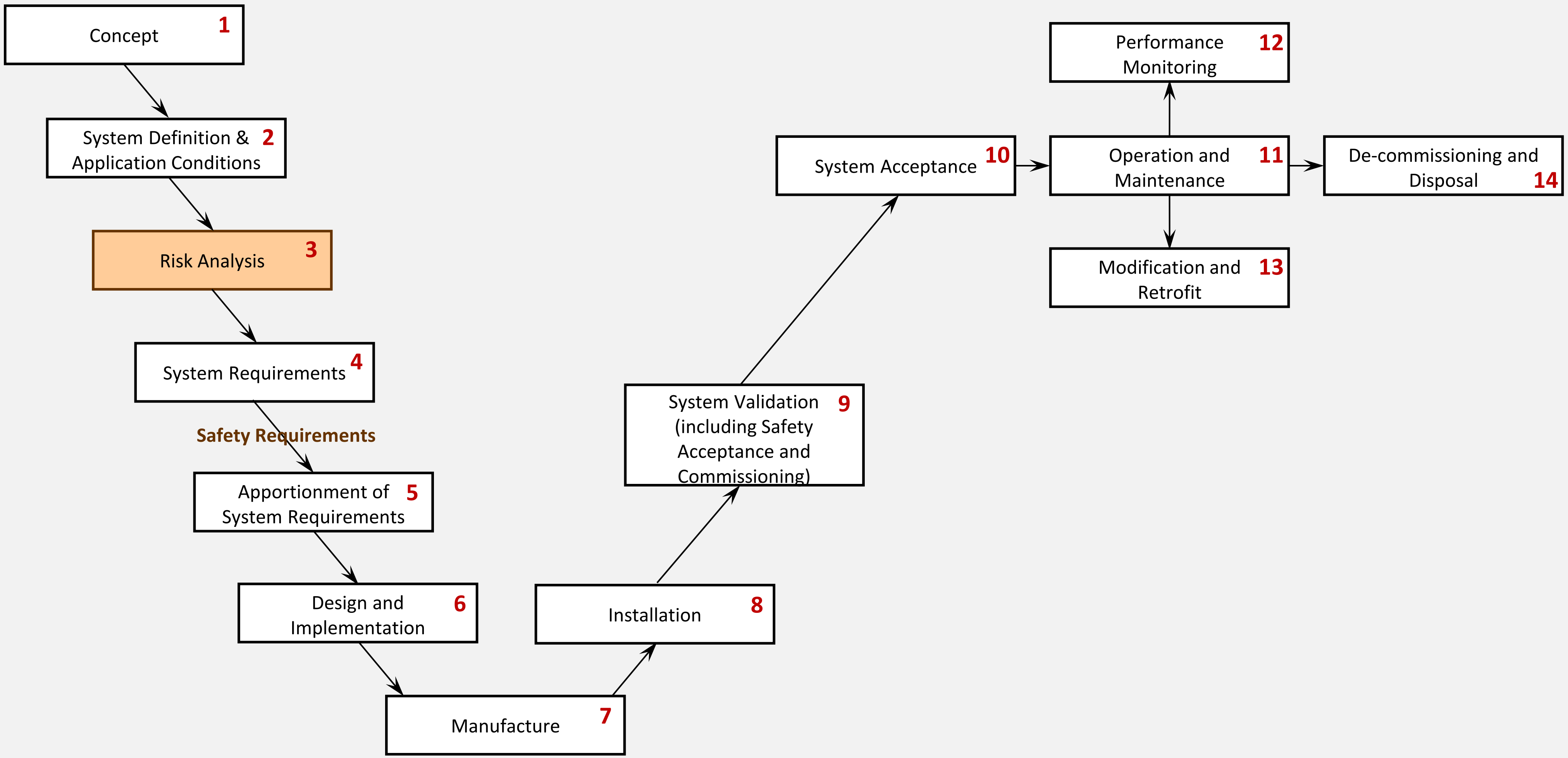
1) Risk assessment and risk management process?
2) Independent safety assessment by an AsBo?

From the VERY BEGINNING of management of a change! – Why?

1) to permit an early identification by applicant's risk management activities and independent safety assessment by an AsBo of potential problems with:
   a) project **organisation** and use of adequate competences for project **staff**
   b) appropriateness and correct application of **supporting safety and quality processes** for:
   c) correct implementation of outcomes of
2) to take timely preventive corrective measures
3) to avoid placing products on market or in service with heavy operational and maintenance constraints

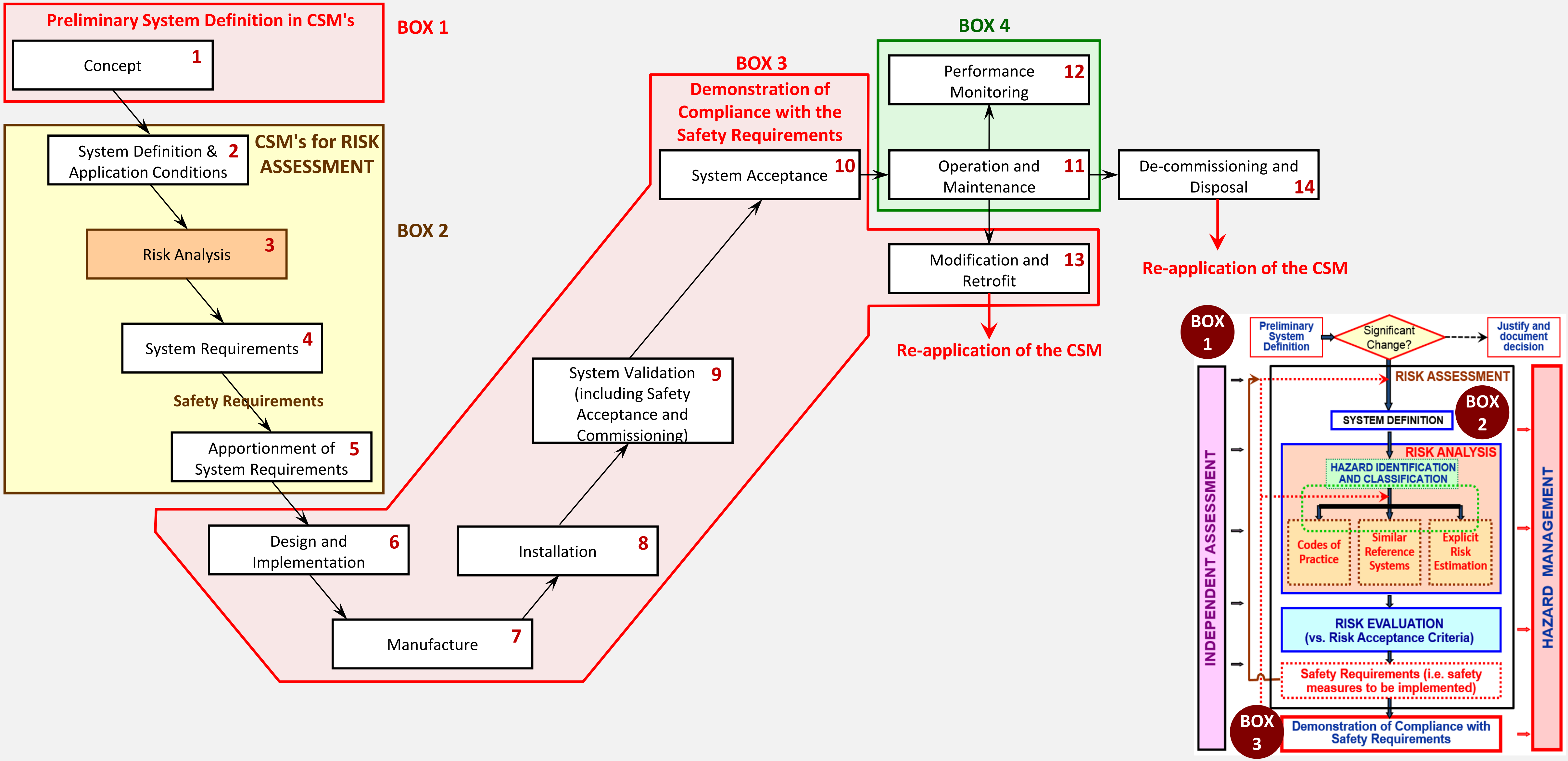
EUROPEAN UNION AGENCY FOR RAILWAYS

Development process or V-Cycle in CENELEC 50126 standard



EUROPEAN UNION AGENCY FOR RAILWAYS

Traceability between CSM and CENELEC



EUROPEAN UNION AGENCY FOR RAILWAYS

EXAMPLE 1 of risk assessment of an ORGANISATIONAL change

(not exhaustive)

System definition of the change

1) A railway company decides to **sub-contract** an activity.

   The organisational change consists in a redesign of the management system where some of the activities previously carried out internally in the company are going to be out sourced. A new interface is going to be created.

2) Remarks

   a) This choice represents an Organisational change that is to be managed according to the procedures of the management system of the company.

   b) This example focuses only on the organisational aspects of the change. Although the technical or operational aspects of the change are also to be covered for a complete management of safety, for the purpose of this example the analysis is not included below.

EUROPEAN UNION AGENCY FOR RAILWAYS

Risk Assessment using human language and sequential writing of outcomes of reflexions

Hazard identification (not exhaustive)

The contractor is not competent to deliver what the railway company requests;

Consequence

Service delivered by the contractor is not compliant with the contractual technical and safety requirements

Risk depends on which activity is sub-contracted

E.g. if sub-contractor fails to report presence of vegetation along the track, could lead to a SPAD

Measures (safety requirement)

Define a company "procedure for selecting qualified contractors according to an internal qualification scheme" including:

(a) assessment of competence;
(b) certifications (e.g. ISO 9001 or ECM certificate);
(c) proven experience in the same type of services or activities for another customer.

EUROPEAN UNION AGENCY FOR RAILWAYS

Same Risk Assessment presented in form of a table
Known in risk management terminology as FMEA (see ISO 31010)

Ref.	Hazard	Consequences	Risk	Safety requirement	Responsible	Exported to	Demonstration of compliance	Status	Monitoring activity
1.	The contractor is not competent to deliver what the railway company requests	1. Service delivered by the contractor is not compliant with the contractual technical and safety requirements	Depends on sub-contracted activity	1. Define a company "procedure for selecting qualified contractors according to an internal qualification scheme" including: (a) assessment of competence; (b) certifications (e.g. ISO 9001 or ECM certificate); (c) proven experience in the same type of services or activities for another customer.	Safety Manager	No	1. A procedure is defined according to both the company document management system and the organisation of the company. 2. Selection of qualified contractors compliant with the defined company procedure	Closed	1. Internal audit for checking the correct application of the selection procedure of qualified contractors and for assessing the contractor competence against the relevant qualification scheme. 2. Check continuous contractor's compliance with the required qualification scheme trough inspections, 3. Request the contractor through contractual arrangements to report the results of any internal or third party audit results and any other issue affecting the validity of the relevant certificate.
				2. Mandatory training for workers employed by the contractor.	Safety Manager		3. The competence management system of the company is updated with a procedure to ensure that: (a) the company training program includes also training of the external staff which is performing safety tasks; (b) a final evaluation of that external staff knowledge is performed.		4. Monitoring of knowledge of contractor's workers is done through the final evaluation exam. 5. Audit the correct application of the process. 6. Use specific indicators to measure the efficiency of the training for the external workers. 7. Direct supervision of the external workers by the railway company is foreseen in contractual arrangements.

EUROPEAN UNION AGENCY FOR RAILWAYS

Same Risk Assessment presented in form of a table
Known in risk management terminology as FMEA (see ISO 31010)

Ref.	Hazard	Consequences	Risk	Safety requirement	Responsible	Exported to	Demonstration of compliance	Status	Monitoring activity
2.	**The contractor is not conscious of the impact of its work on the safety level of the railway system**	1. Service delivered by the contractor is not compliant with the technical and safety requirements 2. Fatalities or (severe) injures of external workers	Depends on sub-contracted activity	1. Inform the contractor in a documented way, supported by bilateral meetings, on possible consequences of contractor workers' mistakes and on the overall impact of its activities on the railway system	Safety Manager	No	1. Contractor warned about impacts of its work on the safety of the railway system 2. Communication on risks through bilateral meetings with contractor's workers		1. Check during internal audits that the contractor's workers were informed about the impacts of their work on the safety of the railway system 2. Check also that bilateral meetings were done
				2. Mandatory training for workers employed by the contractor.	Safety Manager	No	3. The competence management system of the company is updated with a procedure to ensure that: (a) the company training program includes also training of the external staff which is performing safety tasks; (b) a final evaluation of that external staff knowledge is performed		3. Monitoring of knowledge of contractor's workers is done through the final evaluation exam. 4. Audit the correct application of the process. 5. Use specific indicators to measure the efficiency of the training for the external workers. 6. Direct supervision of the external workers by the railway company is foreseen in contractual arrangements.

EUROPEAN UNION AGENCY FOR RAILWAYS

Same Risk Assessment presented in form of a table
Known in risk management terminology as FMEA (see ISO 31010)

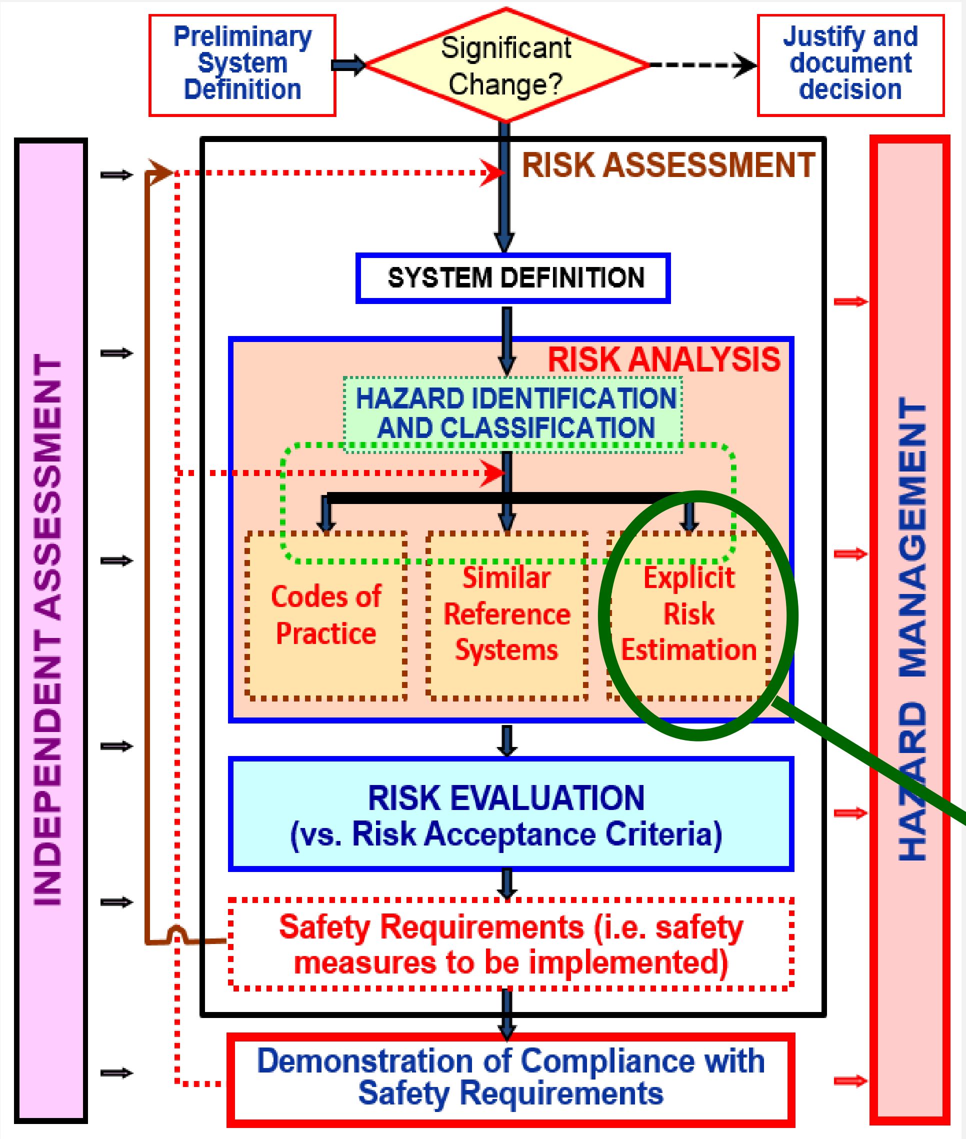
Ref.	Hazard	Consequences	Risk	Safety requirement	Responsible	Exported to	Demonstration of compliance	Status	Monitoring activity
3.	**The workers of the contractor are not aware of the hazards coming from the new working environment**	1. Exposed to accidents	Fatalities or (severe) injuries of external workers	1. Mandatory training for workers employed by the contractor.	Safety Manager	No	3. The competence management system of the company is updated with a procedure to ensure that: (a) the company training program includes also training of the external staff which is performing safety tasks; (b) a final evaluation of that external staff knowledge is performed		3. Monitoring of knowledge of contractor's workers is done through the final evaluation exam. 4. Audit the correct application of the process. 5. Use specific indicators to measure the efficiency of the training for the external workers. 6. Direct supervision of the external workers by the railway company is foreseen in contractual arrangements.
4.	**The railway company produces instructions or contractual arrangements where there is room for interpretation**	1. Contractor not aware of the contractual safety requirements. 2. Contractor is not aware of its responsibilities.	Depends on sub-contracted activity	1. Consultancy for contract definition	Safety Manager	Yes	1. Consultancy contract established		1. No direct monitoring is foreseen for this action
				2. Contract management procedure foresees a continuous improvement of the contract	Safety Manager	No	2. Procedure		2. Collection of feedback related to the issues arising from contract interpretation
5.	•••	•••	•••	•••	•••	•••	•••	•••	•••

EXAMPLE 2 of risk assessment of a technico-organisational change

(not exhaustive)

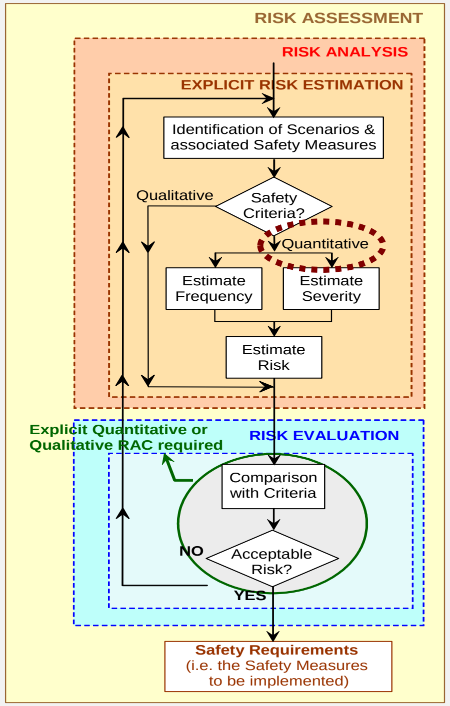
EUROPEAN UNION AGENCY FOR RAILWAYS

Scope of CSM-DT – Related to Regulation 402/2013 on CSM RA
Needed in 3rd risk acceptance principle "explicit risk estimation"



What is Regulation 2015/1136 about:

- A set of new definitions
- An amendment of point 2.5 in Annex I of Regulation 402/2013



Initially RAC-TS renamed into CSM-DT

EUROPEAN UNION AGENCY FOR RAILWAYS

Non legally binding example of risk assessment from

"Guide for the application of the CSM design targets (CSM-DT) [Regulation 2015/1136]"

Annex 5 – Fitting existing passenger trains with an onboard Hot Box Detection system

http://www.era.europa.eu/Document-Register/Pages/Workshop-of-29-30-November-2016-on-the-application-guide-on-CSM-DT.aspx

EUROPEAN UNION AGENCY FOR RAILWAYS

Overview

1. System Definition
2. List of functions (*also part of System Definition*)
3. Scope, assumptions and limits of the risk assessment
4. Hazard Identification and Hazard Classification
5. Applicability of CSM-DT: direct consequence, or presence of external barriers preventing the accident
6. Setting up of applicable category of CSM-DT
7. Allocation of quantitative requirements - Alternative solutions or cases
8. Conclusions from the risk assessment and the allocation of CSM-DT category

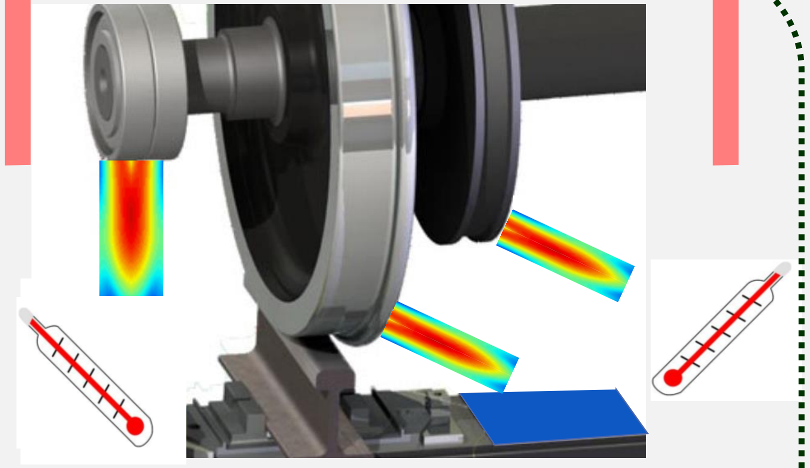
TS under assessment: onboard Hot Box Detection system
1. System definition

Transmit the information to the Train Driver

Detect overheating of wheelsets and axleboxes

Technical system under assessment

Visual and/or audible information on overheating of a wheelset and/or an axlebox



Overheating of wheelsets and/or axleboxes

Train Driver's Cabin

EUROPEAN UNION AGENCY FOR RAILWAYS

TS under assessment: onboard Hot Box Detection system
2. System definition – List of functions

Detection of emerging failures of wheelsets and axleboxes (e.g. wheel bearing fatigue, loss of bearing lubrication in axleboxes, defective brakes, etc.)

Existing System

- Rolling Stock: maintenance and operational procedures [*predeparture checks, periodic planned maintenance inspections and preventive maintenance operations]*
- Trackside "hot box detectors" at regular distances to alarm traffic control center to:
  - inform train driver for stopping train at an appropriate and agreed location
  - reduce speed of trains arriving in opposite direction on adjacent tracks (lateral shock risks caused by blast)

Change under assessment

- Install on existing trains "hot box detectors" which will (**functions**):
  - **monitor overheating of wheelsets and axleboxes**
  - **in case of overheating, lit a lamp in driver's cabin**
- Train driver can stop safely and verify whether additional operational actions might be necessary (e.g. proceed with a speed restriction)

EUROPEAN UNION AGENCY FOR RAILWAYS

TS under assessment: onboard Hot Box Detection system
2. Differences between existing system and change under assessment

- Instead of using a radio communication from Traffic Control Center, “hot box information to driver” is replaced by a “visual and/or audible indication”, using for example a wired connection or a train communication bus.

- Existing infrastructure HB detection system: trackside detectors laid down at regular distances along railway line → in case of failure, “hot box event” detected at next location (e.g. every 25 km, if speed 250 km/h, next HB in 6 minutes)

  Infrastructure detection is fault tolerant – HB event remains undetected only during time needed to reach next trackside HB detector.

- New trainborne HB detection system:
  - HB detection continuous instead of being punctual e.g. every 25 km
  - if HB detector fails, HB event remains undetected until detector is repaired (*info for risk assessment - need for redundancy?*)
  - HB information not automatically available to IM → Traffic Controller cannot thus enforce necessary speed reduction on adjacent tracks to mitigate lateral shock risks caused by blast at crossing of two trains

EUROPEAN UNION AGENCY FOR RAILWAYS

TS under assessment: onboard Hot Box Detection system
3. Scope, assumptions and limits of the risk assessment

- Functions not studied: some HB detection systems might also:
  - indicate increase of temperature gradient which influences operational procedures and emergency of driver's reaction for stopping train safely
  - locate accurately coach number, axle number and side of train where wheelset or axle box is overheating

- **Limitations for the risk assessment:**
  - statistics of hot box occurrences used in the example are dependent on effectiveness of maintenance and operational procedures of RU SMS
  - risk assessment is done by an RU which decides to fit some of its existing trains with a **new trainborne hot box detection** system
  - the existing infrastructure hot box detection system is not removed and continues to be used
  - the manner those two systems are used, with any necessary operational procedures, is not covered by risk assessment below. It needs to be analysed and evaluated in a separate risk assessment

EUROPEAN UNION AGENCY FOR RAILWAYS

TS under assessment: onboard Hot Box Detection system
3. Scope, assumptions and limits of the risk assessment

Limitations for the risk assessment:

- Failures of train driver are neither considered nor associated risk control measures proposed
- Risk assessment only focusses on technical aspects of the change
- It is assumed that associated human factor aspects are properly analysed and controlled through RU SMS
- Since with a trainborne HB detection system, HB detections can occur at any moment of time and at any location of track, operational procedures need to be defined with IM to manage a safe stopping of train at an appropriate and agreed location

Although these considerations impact safe operation of railways, they do not condition setting up quantitative safety requirements for design of trainborne HB detection system → **they must be addressed by a separate risk assessment**

EUROPEAN UNION AGENCY FOR RAILWAYS

TS under assessment: onboard Hot Box Detection system
4(a) Hazard Identification– Use of an FMEA

N°	Function	Functional failure modes	Cause	HAZARD - Consequence at level of technical system	Consequences at train level
1.	Trainborne Hot Box Detection	Detection does not start	• Hot Box Detector failed • Failure of indication system	Hot Box Event not detected by technical system when required	In case of a Hot Box Event, the driver is not informed and cannot stop the train safely.
2.		Detection starts when not required	• Hot Box Detector failed • Failure of indication system	Spurious detection of a Hot Box Event	• Driver required to stop the train whereas not necessary • Traffic operation disturbed
3.		Detection does not stop when required	• Hot Box Detector failed • Failure of indication system	Spurious detection of a Hot Box Event	• Driver required to stop the train whereas not necessary • Traffic operation disturbed
4.		Detection stops when not required	• Hot Box Detector failed • Failure of indication system	Hot Box Event not detected any more by technical system whereas still required	In case of a Hot Box Event, the driver can be misled (e.g. believes it is a false alarm) and could ignore the alarm whereas he shall stop the train safely.
5.		Detection is delayed in response	• Hot Box Detector failed • Failure of indication system	Hot Box Event may not be detected on time to permit actions to be put in place to ensure the safety	In case of a Hot Box Event, the driver is informed too late and might not stop the train safely.
6.		Detection degra-ded (e.g. wrong output level)		Not applicable. The hot box detection is a binary output	Not applicable. The hot box detection is a binary output

EUROPEAN UNION AGENCY FOR RAILWAYS

TS under assessment: onboard Hot Box Detection system
4(b) Hazard Classification – Use of an FMEA

N°				HAZARD - Consequence at level of technical system	Consequences at train level	Potential accident	Potential for at least 1 fatality
1.				Hot Box Event not detected by technical system when required	In case of a Hot Box Event, the driver is not informed and cannot stop the train safely.	• Fire • Derailment	**YES** (i.e. risk not broadly acceptable)
2.				Spurious detection of a Hot Box Event	• Driver required to stop the train whereas not necessary • Traffic operation disturbed	No – Specific operational procedures must be defined to prescribe the actions of the driver when a Hot Box Detector reports a false alarm	**NO** Frequency to be estimated (i.e. risk is broadly acceptable?)
3.							
4.							
5.				Hot Box Event may not be detected on time to permit actions to be put in place to ensure the safety	In case of a Hot Box Event, the driver is informed too late and might not stop the train safely.	• Fire • Derailment	**YES** (i.e. risk not broadly acceptable)
6.				Not applicable. The hot box detection is a binary output	Not applicable. The hot box detection is a binary output	Not applicable	Not applicable

In this example, it is considered that the estimated frequency of event n°2 ensures that the associated hazards are broadly acceptable

EUROPEAN UNION AGENCY FOR RAILWAYS

TS under assessment: onboard Hot Box Detection system
4(b) Hazard Classification – Use of an FMEA

6 identified functional failure modes can be classified in 4 categories:

(a) **failure modes 1 and 4** resulting in “non-detection” of a HB Event and therefore to lack of information to the driver for stopping the train safely;

(b) **failure modes 2 and 3** resulting in a spurious detection of a HB Event and thus disturbing the traffic operation;

(c) **failure mode 5** resulting in a too late “detection” of a HB Event and therefore a late information to the driver for stopping the train safely;

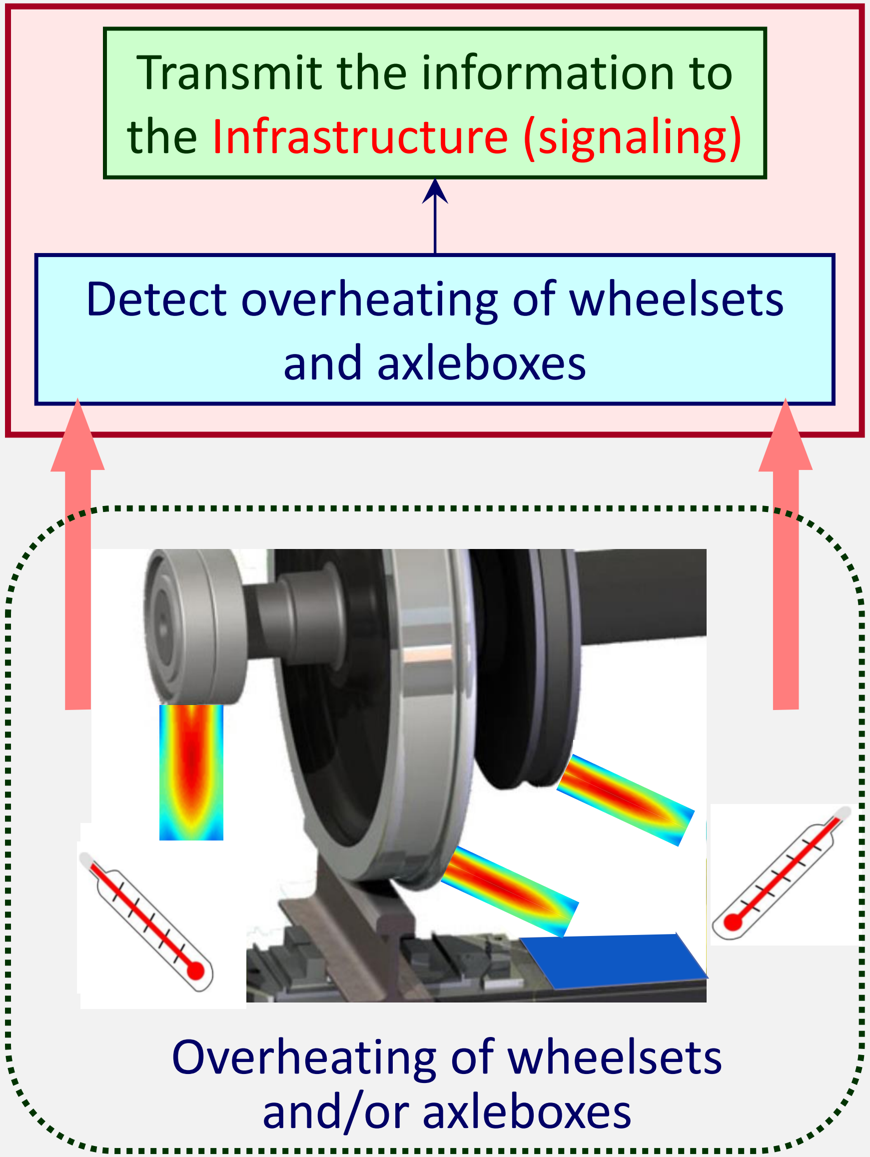
(d) **failure mode 6** which is physically not possible for the system under assessment.

In addition to that, the risks associated to failure modes 2, 3 and 6 do not result in an unsafe situation → out of scope of safety assessment

Failure modes 1, 4 and 5 are not broadly acceptable

EUROPEAN UNION AGENCY FOR RAILWAYS

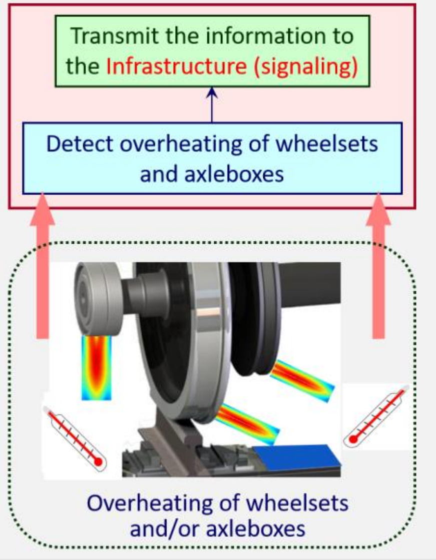
Hot Box Detection function at the trackside level



- Distance between on-track Hot Box Detectors:
  - 30 to 45 km for High Speed Lines
  - 60 to 150 km for Classic Lines
- Functions, involving either a “Monitoring Operator” or “Automated System”:
  - detect side of train with Hot Axle/Wheel
  - axle number from head of train
  - inform Traffic Manager on HB event (track, train, direction)
- When alarm of overheating received, Traffic Manager:
  - manages stopping of train putting signals to RED + informing Train Driver by Track-Train Radio, if possible
  - Train Driver stops train normally, without emergency brakes in a safe place (not in a tunnel or a bridge/viaduct)
  - secures operation on adjacent tracks (e.g. reducing their speed)

EUROPEAN UNION AGENCY FOR RAILWAYS

Hot Box Detection function at the trackside level



- Train Driver actions, once train stopped:
  - after securing himself, inspect train according to procedure of RU SMS
  - if available [side + axle number from train head], inspect it, or entire train
  - after checks, inform Traffic Manager of train status:
    - continue service under conditions, or
    - remove from service to closest parking track or workshop
  - Traffic Manager decides on conditions to release operation of trains on adjacent tracks

- Questions for brainstorming in case of failures of a trackside Hot Box Detector
  - Removal of HBD from service for a SHORT or LONG period of time
  - IM informing RUs operating on the line (track number, km, direction)
  - Acknowledgement by RUs of message received
  - IM measures during HBD unavailability (operational speed limited by signalling or by procedures)
  - Differences between High Speed and Conventional Speed lines
  - Informing RUs once HBD functionality restored

EUROPEAN UNION AGENCY FOR RAILWAYS

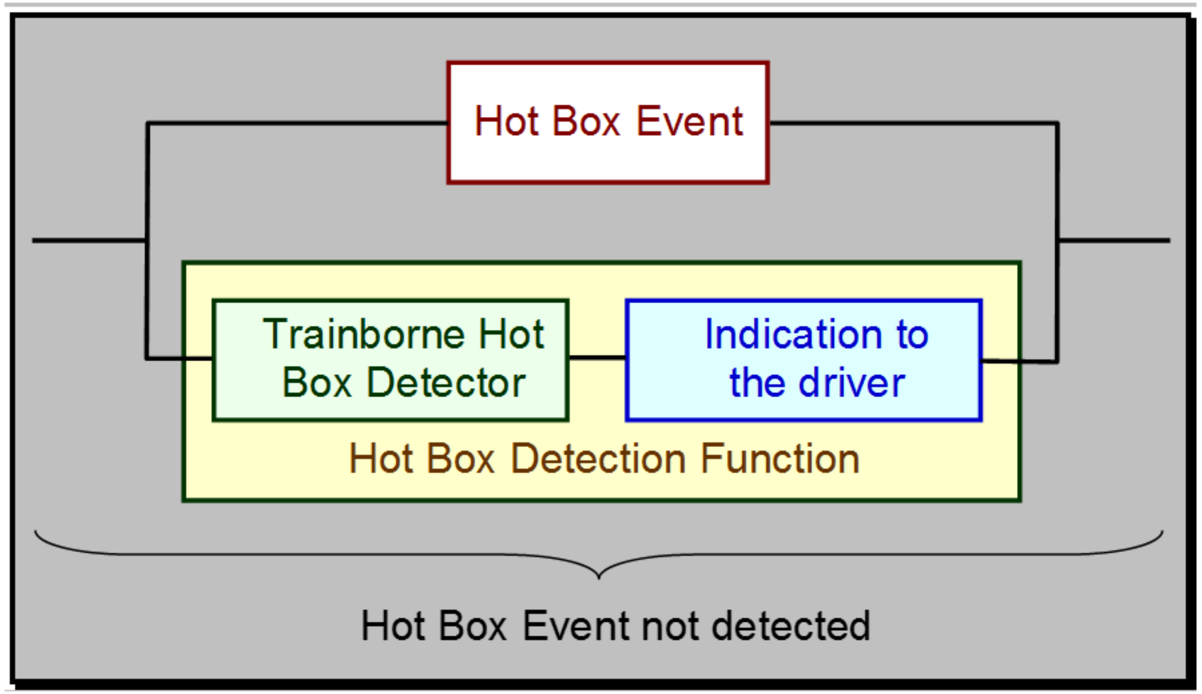
TS under assessment: onboard Hot Box Detection system
5. Applicability of CSM-DT, based on point 2.5.5.

Analysis approached through point 2.5.5. of Reg. 2015/1136

CSM-DT can be used if failure has *"… a credible potential to lead directly to … a catastrophic … or a critical accident"*

In practice

Single failure of HB Detector does not lead directly to an accident



Schematic representation of the events and contributors to the trainborne hot box detection function.

EUROPEAN UNION AGENCY FOR RAILWAYS

What conditions have a credible potential to LEAD DIRECTLY to an accident in case of failure of trainborne Hot Box Detection function?

IF the following two conditions are met **during the same period of time** :

(a) the "trainborne hot box detection function" is failed, i.e.:

(1) either trainborne "HB Detector" is failed, or;
(2) indication of HB Event is not transmitted to driver through communication means (e.g. wired connection or train bus), or;
(3) both do not work any more;

AND

(b) wheelset under supervision of that TS is overheating;

THEN

(c) there is "*a credible potential to lead directly to a catastrophic or a critical accident*" → as driver is not informed about HB Event, he cannot enforce a progressive train deceleration for stopping the train safely

EUROPEAN UNION AGENCY FOR RAILWAYS

TS under assessment: onboard Hot Box Detection system
5. Applicability of CSM-DT, based on point 2.5.9.

Analysis approached through point 2.5.9. of Reg. 2015/1136

“Where the failure of a function of the TS under assessment does not lead directly to the risk under consideration, the application of less demanding CSM-DT shall be permitted if the proposer can demonstrate that the use of barriers … allows the same level of safety to be achieved”

What **barriers external to HB Detector** enable to prevent, detect and, when necessary, correct emerging failures of wheelsets and axleboxes (e.g. wheel bearing fatigue, loss of bearing lubrication in axleboxes, defective brakes or any other cause) that can lead to Hot Box Event hazard?

EUROPEAN UNION AGENCY FOR RAILWAYS

TS under assessment: onboard Hot Box Detection system
5. Applicability of CSM-DT, based on point 2.5.9.

Barriers external to HB Detector:

(a) Appropriate maintenance and operational procedures of SMS (*Predeparture checks, periodic planned maintenance inspections and preventive maintenance operations)*

(b) Those SMS provisions either reduce frequency of occurrence of HB hazard or mitigate the severity of potential consequences of that hazard

(c) Effectiveness of those external barriers has a direct impact on actual frequency of occurrence of HB events → proposer (i.e. RU) has statistics of actual frequency of occurrence of HB events for its fleet

→ Knowledge of frequency of occurrence of HB events can thus be used to derive permissible frequency of occurrence of failures of "**trainborne HB Detector and HB Event indication**"

EUROPEAN UNION AGENCY FOR RAILWAYS

TS under assessment: onboard Hot Box Detection system
6. Setting up of applicable category of CSM-DT

N°				HAZARD – Consequence at level of technical system	Consequences at train level	Potential accident	Potential for at least 1 fatality	Consequence limited to a specific area of train	Associated CSM DT
1.				Hot Box Event not detected by technical system when required	In case of a Hot Box Event, the driver is not informed and cannot stop the train safely.	• Fire • Derailment	YES (i.e. risk not broadly acceptable)	NO (whole train exposed to risk)	$10^{-9}\ h^{-1}$
2.				Spurious detection of a Hot Box Event	• Driver required to stop the train whereas not necessary • Traffic operation disturbed	No – Specific operational procedures must be defined to prescribe the actions of the driver when a Hot Box Detector reports a false alarm	NO (i.e. risk is broadly acceptable)	Not applicable	Not applicable
3.									
4.									
5.				Hot Box Event may not be detected on time to permit actions to be put in place to ensure the safety	In case of a Hot Box Event, the driver is informed too late and might not stop the train safely.	• Fire • Derailment	YES (i.e. risk not broadly acceptable)	NO (whole train exposed to risk)	$10^{-9}\ h^{-1}$
6.				Not applicable. The hot box detection is a binary output	Not applicable. The hot box detection is a binary output	Not applicable	Not applicable	Not applicable	Not applicable

EUROPEAN UNION AGENCY FOR RAILWAYS

TS under assessment: onboard Hot Box Detection system
6. Setting up of applicable category of CSM-DT

In conclusion, if following **"logical condition"** is met:

(a) the wheelset or axlebox under the supervision of the HB Detector is overheating (i.e. there is "Hot Box Event');

AND during the same period of time[14]

(b) either HB Detector is defective and does not report the event **OR** there is a failure of "indication of HB Event to driver" or both of these failures;

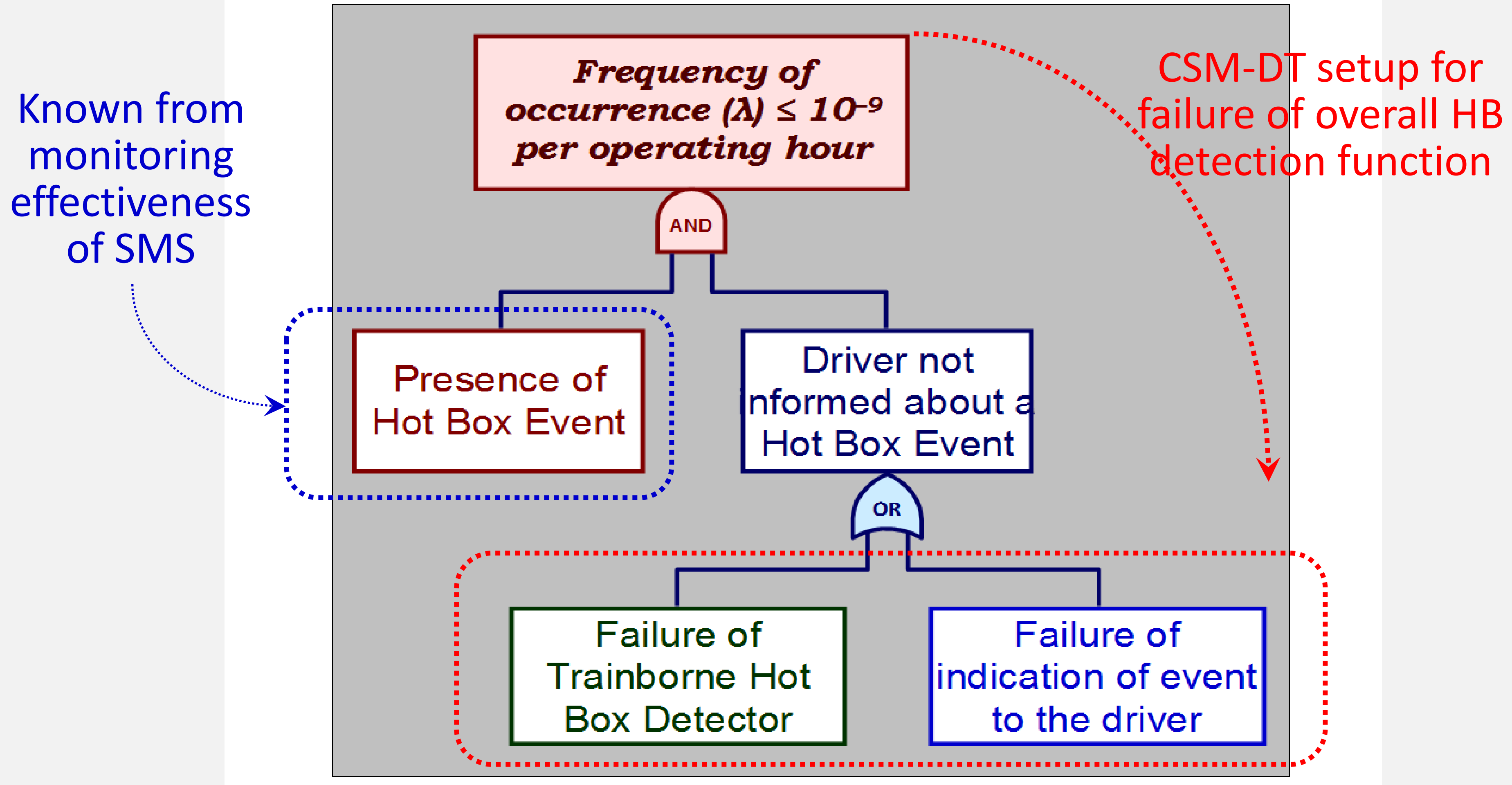
there is "*a credible potential to lead directly to a catastrophic accident*" … "*typically affecting a large number of people and resulting in multiple fatalities*"

Derailment, fire

The associated risk is acceptable if the frequency of occurrence of that logical condition is "*… demonstrated to be less than or equal to 10^{-9} per operating hour*".

The most credible CSM DT category applicable to that logical condition is therefore 10^{-9} h^{-1}

TS under assessment: onboard Hot Box Detection system
6. Setting up of applicable category of CSM-DT



Logical condition leading directly to a failure of the trainborne hot box detection function.

EUROPEAN UNION AGENCY FOR RAILWAYS

TS under assessment: onboard Hot Box Detection system
7. Allocation of quantitative requirements

Use of Faut Trees (FTA) for Quantitative Allocation

Assumption for the risk assessment

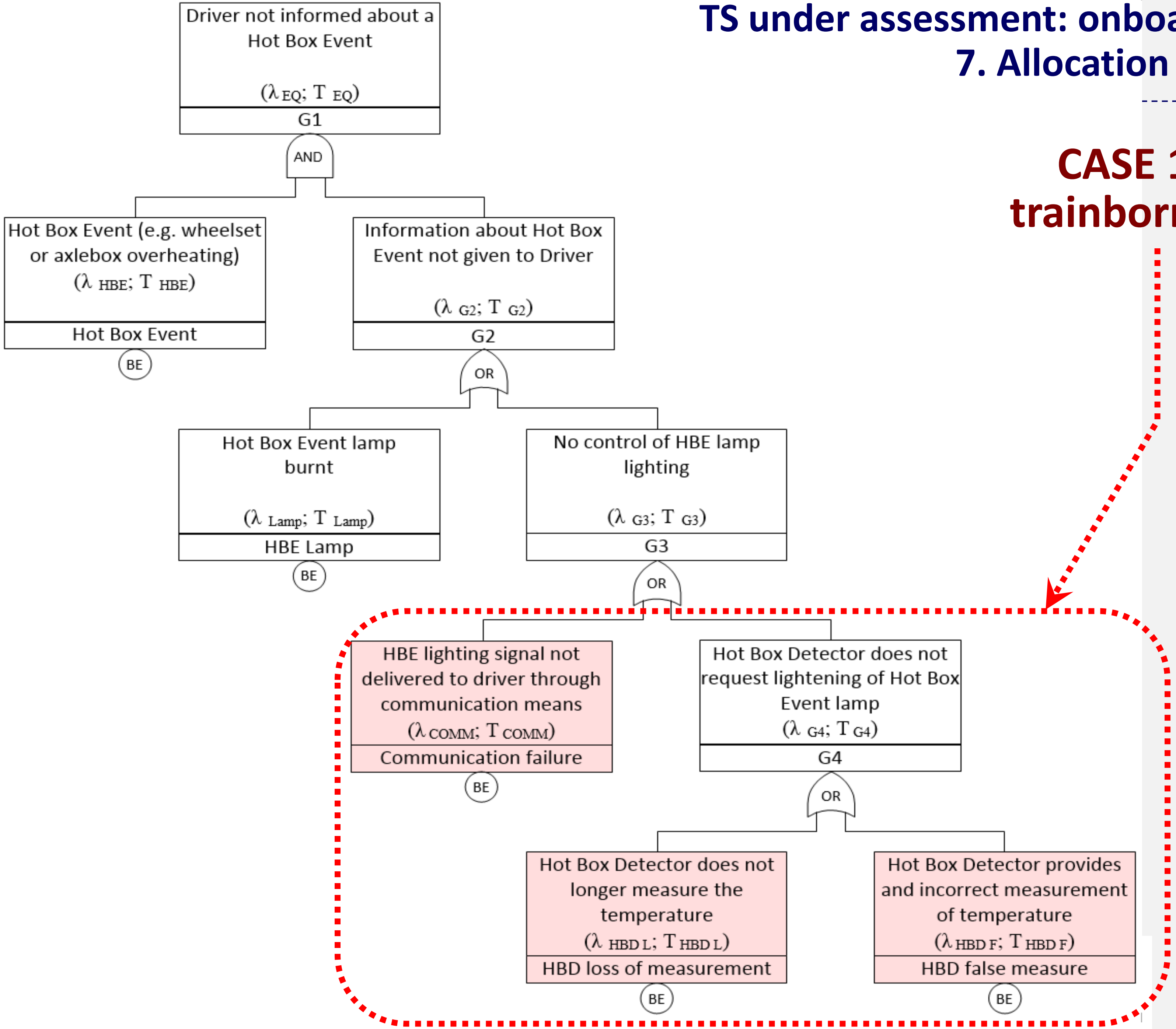
(a) trains operated 10 hours a day

(b) trains operated 30 days a month
(i.e. regular monthly maintenance every 300 hours of operation)

Available information for risk assessment

N°	Basic events	Description in the FTA	Rate of occurrence	Source of information	D&NT	Additional explanations
1.	Hot Box Event	Hot Box Event (e.g. wheelset or axlebox) overheating *(this shall trigger the hot box detection)*	$10^{-5}\ h^{-1}$	Monitoring through experience on similar trains (REX)	10 h	Operational and maintenance provisions are put in place in the RU SMS to permit the detection of wheelset and axlebox failures for the first journey with the train (i.e. pre-departure checks). The driver is also trained for detecting unusual changes of dynamic behaviour of the train and suspicious train vibrations
2.	HBE lamp	Hot Box Event lamp burnt	$10^{-7}\ h^{-1}$	IEC 62380 standard	10 h	The driver's cabin is tested every day, including the good functioning of the Hot Box Event indication lamp. Diversity in the indication can also be envisaged, e.g. use of two lamps – one for indicating a Hot Box Event, the other one for informing that the Hot Box Detection system is defective
3.	HBD loss of measure-ment	Hot Box Detector does not longer detects measure the temperature	**To define by risk asses-sment**	Shall be demon-strated by the supplier of Hot Box Detector	300 h	To be tested once a month during regular maintenance activities. This could be an initial objective in order not to constraint the train operation based on this data. Then depending on the final failure rate allocated by the risk assessment (e.g. if it appears not to be feasible), this number may be changed for example by imposing more constraints on either the train operation or on the maintenance of the Hot Box Detection functionality.
4.	HBD false measure	Hot Box Detector provides an incorrect temperature measurement	**To define by risk asses-sment**	Shall be demon-strated by the supplier of Hot Box Detector	300 h	To be tested once a month during regular maintenance activities
5.	Communi-cation failure	HBE lighting signal not delivered to driver through communication means	**To define by risk asses-sment**	Shall be verified for implement-ation of Hot Box Detection function	300 h	Different technical options are possible for informing the driver. The communication of information shall satisfy the requirements identified in the current risk assessment

CASE 1 – Use of a single trainborne Hot Box Detector



EUROPEAN UNION AGENCY FOR RAILWAYS

CASE 1 – Use of a single trainborne Hot Box Detector

Input data	Iteration of possible values for HBD			Achieved top event
	$\lambda_{HBD\ Total}$ *(100%)*	$\lambda_{HBD\ F}$ *(50%)*	$\lambda_{HBD\ L}$ *(50%)*	$\lambda_{TOP\ EVENT}$
$T_{HBD\ L} = 300\ h$	$2.0*10^{-7}\ h^{-1}$	$1.0*10^{-7}\ h^{-1}$	$1.0*10^{-7}\ h^{-1}$	$3.2*10^{-10}\ h^{-1}$
$T_{HBD\ F} = 300\ h$	$4.0*10^{-7}\ h^{-1}$	$2.0*10^{-7}\ h^{-1}$	$2.0*10^{-7}\ h^{-1}$	$6.3*10^{-10}\ h^{-1}$
$\lambda_{HBE} = 10^{-5}\ h^{-1}$	$\boxed{\mathbf{6.0*10^{-7}\ h^{-1}}}$	$\mathbf{3.0*10^{-7}\ h^{-1}}$	$\mathbf{3.0*10^{-7}\ h^{-1}}$	$\mathbf{9.4*10^{-10}\ h^{-1}}$
$\lambda_{Lamp} = 10^{-7}\ h^{-1}$	$7.0*10^{-7}\ h^{-1}$	$3.5*10^{-7}\ h^{-1}$	$3.5*10^{-7}\ h^{-1}$	$\mathbf{1.1*10^{-9}\ h^{-1}}$
$T_{HBE} = 10\ h$	*(A detected hot box event is repaired within one day)*			
$T_{Lamp} = 10\ h$	*(The HBE lamp is tested every day)*			

Analysis of results - $10^{-9}\ h^{-1}$ target for overall HB function achieved if:

(1) total failure rate of HB Detector less **$6.10^{-7}\ h^{-1}$**
(2) HB Detector tested completely **every 300 h (monthly maintenance)**
(3) HB event lamp tested every day (i.e. every 10 hours of operation)

$6.10^{-7}\ h^{-1}$ for a single HB Detector → SIL 2 requirements for a TS in CENELEC 5012x standards

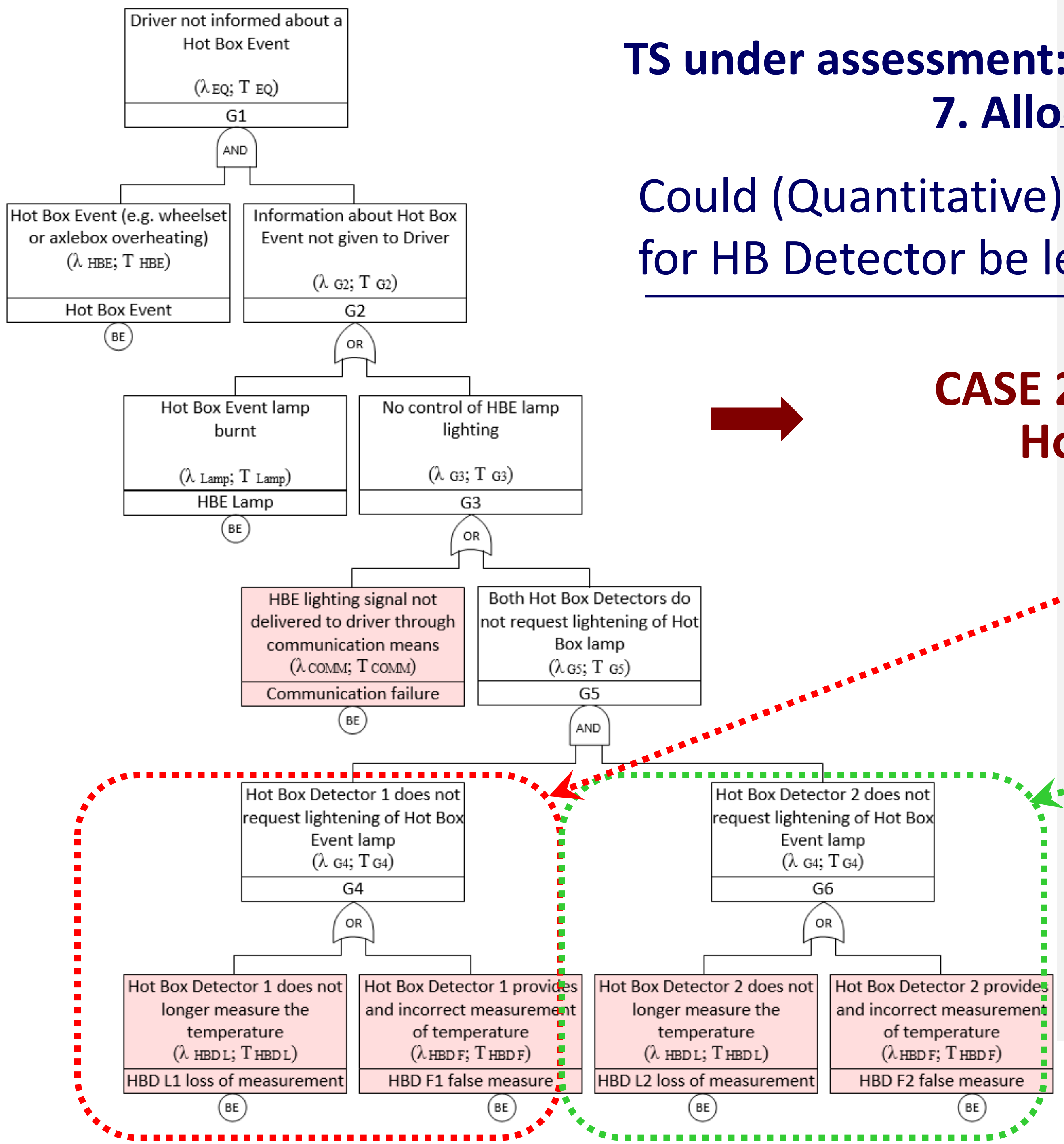
CASE 1 – Use of a single trainborne Hot Box Detector

- If cost of a single HB Detector with demanding safety requirements and short maintenance intervals is unacceptable, or
- If loss of single HB Detector is unacceptable from operational and maintenance constraint points of view [disturbs not only traffic operation but requires also unplanned corrective maintenance to be done]

→ **use of redundant HB detection architecture with higher frequency of occurrence of failure and longer maintenance intervals can be envisaged**

- Reminder:
  - (a) **existing infrastructure HB detection system** is **fault tolerant**: if a detector malfunctioning a HB event remains undetected during time needed to reach next trackside HB detector
  - (b) **new trainborne single HB Detection system** is **not fault tolerant**: if detector fails a HB event can no longer be detected by train equipment as long as detector is not repaired [i.e. at planned monthly maintenance Test Interval]

TS under assessment: onboard Hot Box Detection system
7. Allocation of quantitative requirements



Could (Quantitative) Safety Requirements for HB Detector be less demanding?

CASE 2 – Use of redundant trainborne Hot Box Detector architecture

CASE 2 – Redundant trainborne Hot Box Detector architecture – Monthly maintenance

Input data	Iteration of possible values for HBD			Achieved top event
	$\lambda_{HBD\ Total}$ *(100%)*	$\lambda_{HBD\ F}$ *(50%)*	$\lambda_{HBD\ L}$ *(50%)*	$\lambda_{TOP\ EVENT}$
$T_{HBD\ L} = 300\ h$	$2.0 \cdot 10^{-5}\ h^{-1}$	$1.0 \cdot 10^{-5}\ h^{-1}$	$1.0 \cdot 10^{-5}\ h^{-1}$	$1.06 \cdot 10^{-10}\ h^{-1}$
$T_{HBD\ F} = 300\ h$	$4.0 \cdot 10^{-5}\ h^{-1}$	$2.0 \cdot 10^{-5}\ h^{-1}$	$2.0 \cdot 10^{-5}\ h^{-1}$	$3.94 \cdot 10^{-10}\ h^{-1}$
$\lambda_{HBE} = 10^{-5}\ h^{-1}$	**$6.0 \cdot 10^{-5}\ h^{-1}$**	**$3.0 \cdot 10^{-5}\ h^{-1}$**	**$3.0 \cdot 10^{-5}\ h^{-1}$**	**$8.74 \cdot 10^{-10}\ h^{-1}$**
$\lambda_{Lamp} = 10^{-7}\ h^{-1}$	$7.0 \cdot 10^{-5}\ h^{-1}$	$3.5 \cdot 10^{-5}\ h^{-1}$	$3.5 \cdot 10^{-5}\ h^{-1}$	**$1.19 \cdot 10^{-9}\ h^{-1}$**
$T_{HBE} = 10\ h$	*(A detected hot box event is repaired within one day)*			
$T_{Lamp} = 10\ h$	*(The HBE lamp is tested every day)*			

Analysis of results - $10^{-9}\ h^{-1}$ target for overall HB function achieved if:

(1) total failure rate of HB Detector less **$6.10^{-5}\ h^{-1}$ → SIL 0**
(2) HB Detector tested completely **every 300 h (monthly maintenance)**
(3) HB event lamp tested every day (i.e. every 10 hours of operation)

$6.10^{-5}\ h^{-1}$ 100 times less demanding **BUT** HB Detector must be tested completely, and if necessary restored, every 300 hours [monthly maintenance] → **Test Interval still short**

CASE 2 – Redundant trainborne Hot Box Detector architecture – Maint. every 6 months

Input data	Iteration of possible values for HBD			Achieved top event
	$\lambda_{HBD\ Total}$ (100%)	$\lambda_{HBD\ F}$ (50%)	$\lambda_{HBD\ L}$ (50%)	$\lambda_{TOP\ EVENT}$
$T_{HBD\ L} = 3600\ h$	$2.0*10^{-6}\ h^{-1}$	$1.0*10^{-6}\ h^{-1}$	$1.0*10^{-6}\ h^{-1}$	$1.40*10^{-10}\ h^{-1}$
$T_{HBD\ F} = 3600\ h$	$4.0*10^{-6}\ h^{-1}$	$2.0*10^{-6}\ h^{-1}$	$2.0*10^{-6}\ h^{-1}$	$5.31*10^{-10}\ h^{-1}$
$\lambda_{HBE} = 10^{-5}\ h^{-1}$	$5.0*10^{-6}\ h^{-1}$	$2.5*10^{-6}\ h^{-1}$	$2.5*10^{-6}\ h^{-1}$	$8.25*10^{-10}\ h^{-1}$
$\lambda_{Lamp} = 10^{-7}\ h^{-1}$	$6.0*10^{-6}\ h^{-1}$	$3.0*10^{-6}\ h^{-1}$	$3.0*10^{-6}\ h^{-1}$	**$1.18*10^{-9}\ h^{-1}$**
$T_{HBE} = 10\ h$	(A detected hot box event is repaired within one day)			
$T_{Lamp} = 10\ h$	(The HBE lamp is tested every day)			

Analysis of results - $10^{-9}\ h^{-1}$ target for overall HB function achieved if:

(1) total failure rate of HB Detector less **$5.10^{-6}\ h^{-1}$ → SIL 1**
(2) HB Detector tested completely, and maintained if needed, **every 6 months**
(3) HB event lamp tested every day (i.e. every 10 hours of operation)

$5.10^{-6}\ h^{-1}$ 10 times less demanding than CASE 1 **– Advantage:** HB Detector must be tested completely, and if necessary restored, every 6 months **[i.e. Much longer TI]**

Final decision on allocation of quantitative safety requirements

- Several alternative technical options analysed → several sets of safety requirements with corresponding acceptable maintenance intervals:

  CASE 1: one HB detector [$\lambda < 6.10^{-7}\ h^{-1}$] – Monthly complete maintenance

  CASE 2(a): 2 HB detectors [$\lambda < 6.10^{-5}\ h^{-1}$] – Monthly complete maintenance

  CASE 2(b): 2 HB detectors [$\lambda < 5.10^{-6}\ h^{-1}$] – Complete maintenance every 6 months

- Decision on technical solution to use, and thus necessary maintenance intervals, will be taken based on balance between:

  (a) Product cost of HB Detector → high quantitative safety requirements imply more expensive TS

  (b) Frequency, testability and **maintenance costs** of HB Detector

  (c) Availability of HB Detector and acceptability of disturbing Traffic Operation in case of loss of a single HB Detector

EUROPEAN UNION AGENCY FOR RAILWAYS

(Un)completeness of risk assessment

- Quantitative requirements applicable only to random hardware failures
- Although it seems extensive, risk assessment is not complete. For example, to install and integrate safely HB detection function in train, additional (safety) requirements, need to be defined by an overall risk assessment:

  a) point 2.5.7(b) of Reg. 2015/1136 requires that *"the risks associated with the systematic failures and systematic faults…"* need also to be *"… controlled in accordance with safety and quality processes commensurate with the harmonised design target …"*

  Application of EN 50126 (-1 & -2) & EN 50657 (& EN 50128 & EN 50129 for onboard signalling equipment)

  b) mechanical constraints (size, weight, etc.) + physical interface requirements with train to be specified and communicated to manufacturer

(Un)completeness of risk assessment (continuation)

- Overall risk assessment should determine, based on rolling stock architecture, installation constraints (e.g. most appropriate location on bogies):
  a) to enable detection of overheating of all four wheelsets of bogy;
  b) control risks of damaging either HB Detector housing, or wiring interface for indication to driver of a detected HB Event, or both, by projections of ballast, snow and ice in winter conditions that can occur due to dynamic turbulences underneath train created at high speeds
  c) relevant operational procedures defining actions to be taken in case of loss of communication between HB detectors and Driver's Cabin
  d) Human Factor aspects related to operational rules in case of HB Event to be analysed and controlled through RU SMS
  e) etc.
- **All relevant requirements for HB Detector, including allocated quantitative safety targets, must be transferred to manufacturer**

EUROPEAN UNION AGENCY FOR RAILWAYS

TS under assessment: onboard Hot Box Detection system
8. Conclusions from the risk assessment and CSM-DT allocation

Predictive risk assessment demonstrates that occurrence of hazard “HB event being undetected by TS when required” is acceptable if:

(a) allocated quantitative requirement is used for design of HB Detector

(b) HB detection lamp is tested every day (i.e. every 10 hours) in accordance with a dedicated procedure to be included in Train Driver’s Manual

(c) HB Detector is tested in accordance with appropriate maintenance procedures at time intervals commensurate with defined quantitative requirement

Those procedures need to be clearly written and part of RU SMS

(d) HB detection function is safely integrated within train in compliance with requirements to be identified by additional risk assessment

All safety requirements from risk assessment are registered in Hazard Record in compliance with Reg. 402/2013

EUROPEAN UNION AGENCY FOR RAILWAYS

Additional information needed

More information on Safe Integration can be found in

ERA Clarification Note on Safe Integration (ERA1209-063)

available on the ERA web page:

https://www.era.europa.eu/domains/common-safety-methods/risk-evaluation-assessment-csm_en

Any question can be sent to CSM.risk_assessment@era.europa.eu

Disclaimer

THANK YOU

Moving Europe towards a sustainable and safe railway system without frontiers.

Follow us: