Agency clarification note on safe integration

Support to dissemination, March 2020

Dragan JOVICIC, EU Agency for Railways

EUROPEAN UNION AGENCY FOR RAILWAYS

Contents

Existing and known concepts on safety: "1°) Make a system safe; 2°) Ensure it does not damage other systems & 3°) Ensure it remains safe"

- Concepts standing behind "safe integration" are well-known and applied in various industrial fields, but they are not explicitly known with the same terminology

- Every safety-related system or service is characterised by:
  - the safety functions and requirements it fulfils → **WHAT the system does**
  - the safety integrity requirements of those functions, i.e. likelihood of functions to be achieved satisfactorily, without failure → **HOW the safety function is implemented**

- EU legislation on *General Product Safety (Dir. 2001/95, where product includes services)* and on *Liability for Defective Products (Dir. 1985/0374)* require to:
  - demonstrate that products placed on the market are safe
  - demonstrate that the product does have adverse effects on other products
  - identify conditions for the safe use and safe maintenance of the product

- IEC 61508, CENELEC 50126 & 50129 and ISO 26262:
  - define "functional safety as the absence of unreasonable risk due to hazards caused by malfunctioning behaviour of the product/service"
  - define rigorous requirements for development and engineering process of safety-related systems - The higher levels of safety integrity, the greater the rigour shall be
  - Functional Safety is embedded in Product Safety

Examples of “Functional and Technical Safety” principles well-known and applied since long in many industrial disciplines

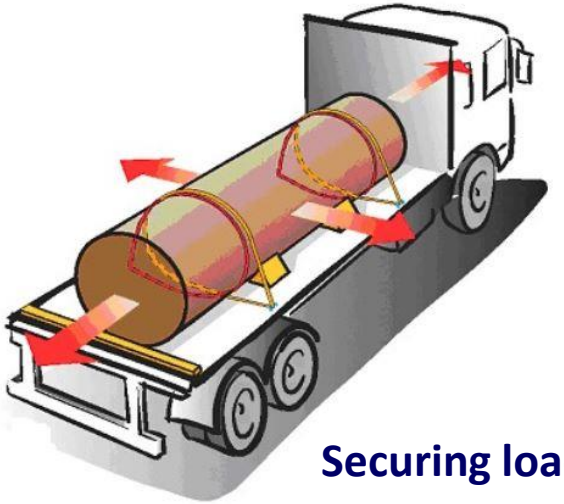
Securing wooden joints

Reinforcing chevron

Castle nut & securing cotter pin

Securing mechanical assemblies

Railway tanks vs. type of transport



Securing loads

Nut & securing bearing circlips

Achievement and demonstration of safety at the level of the Railway System

Considering that the Railway System safety is to be achieved by an extremely high number of various types of safety measures that depend on:

- complex **Organisational & Operational** arrangements at RUs' & IMs‘ levels, which have to take into account all other actors who have a potential impact on the safe operation of the Railway System (including manufacturers, maintenance suppliers, keepers, service providers, contracting entities, carriers, consignors, consignees, loaders, unloaders, fillers and unfillers), and;
- complex architectural breakdown structures with complex **Technical** constituents/ equipment and continual technological innovations and improvements,

No matter whether a hazard/risk at the level of the Railway System can be caused by:

- an E/E/PE sub-system/equipment (*covered by functional safety standards*), or
- a mechanical, hydraulic or pneumatic constituent/equipment, or
- human (HOF) impacts on the operation and maintenance of any equipment

as they could all result in safety concerns, Railway System safety requires a systematic & rigorous development engineering process to identify and manage properly all risks

Safe Integration in the scope of Directives 2016/797 and 2016/798
Fears, misunderstandings and consequences

1) Different understandings → generates much fear and wrong beliefs

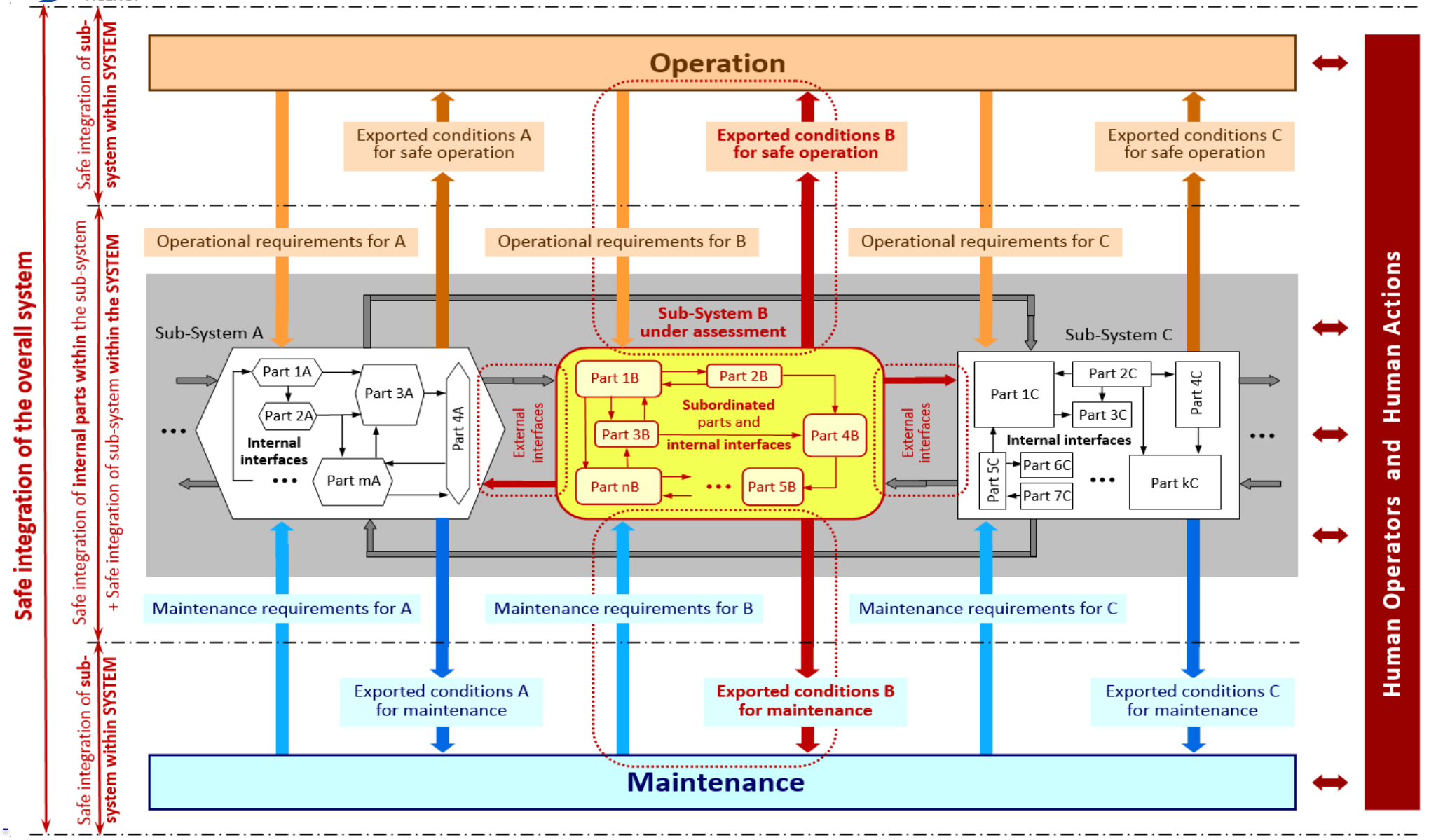
2) Often and wrongly understood only as demonstration of the technical compatibility and correct technical interfacing between sub-systems

3) In practice, it is an inherent part of a systematic risk assessment process [§1.2.7 in Ax I of 402/2013: "*… the* ***proposer is responsible for ensuring*** *that the* ***risk management covers*** *the system itself and its* ***integration into the railway system*** *as a whole*"]

4) Safe integration has a broader meaning and goes beyond single checks above → applies at different levels and to entire life cycle of design, operation, maintenance and disposal/decommissioning of railway system and of its components

5) **Consequences:** different ways of demonstrating safe integration, in particular different levels of completeness of safety demonstration result unavoidably in difficulties to mutually recognise the results of safe integration across the EU

Safe Integration takes place at every level of the Railway System



Agency clarification note on safe integration, March 2020

Safe Integration takes place at every level of the Railway System

1) Whenever a new element is introduced into a system, or an existing one is modified, **regardless of significance**, safe integration and risk management must ensure that:

   a) the new or modified element is technically compatible, and thus correctly interfaces, with the other parts of the system into which it is introduced;

   b) the new or modified element is safely designed and fulfils all the intended functional and technical objectives;

   c) the impacts of humans on the operation and maintenance of that element and on the system where it is incorporated are assessed and properly addressed;

   d) the introduction of that new or modified element into its physical, functional, environmental, operational and maintenance context does not have adverse and unacceptable effects on safety of resulting system into which it is incorporated

   → **Therefore, every actor is responsible for the risk assessment and the safe integration of its contributing part to the overall railway system**

2) **Safe integration of a change is therefore not a separate and additional set of tasks to the regular risk assessment and risk management activities.**

Consequences of the railway market opening and restructuring

1) Past, before market opening: usually one integrated state railway company per country

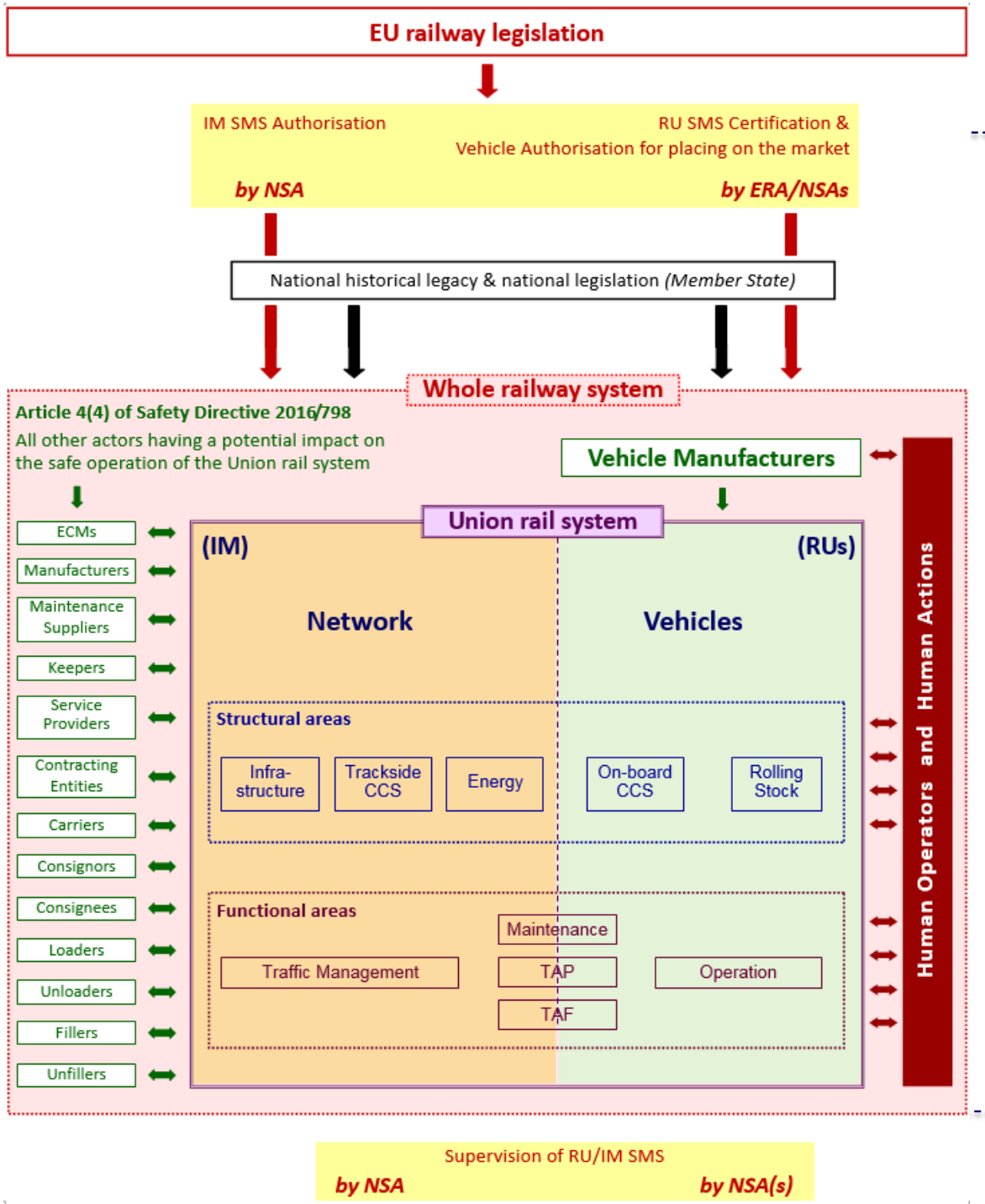
   So, usually one single actor was in charge of safe design, implementation, authorisation and safe management of railway operation, infrastructure and traffic management and all maintenance activities (vehicles and network) → **it had the full knowledge and responsibility for proper control of all railway risks**

2) Now, after market opening: former integrated railway companies, and associated responsibilities, are split into new railway actors: NSAs (usually safety authorisation department of former state railway company), IM(s), RUs, ECMs, manufacturers, service providers, contracting entities, etc.

Responsibility for safe operation and traffic management of former railway system, and proper control of associated risks, does not rest any more on a single railway actor.

IM and all RUs operating on its network share, each one for its part of the system, the responsibility of former integrated state railway company

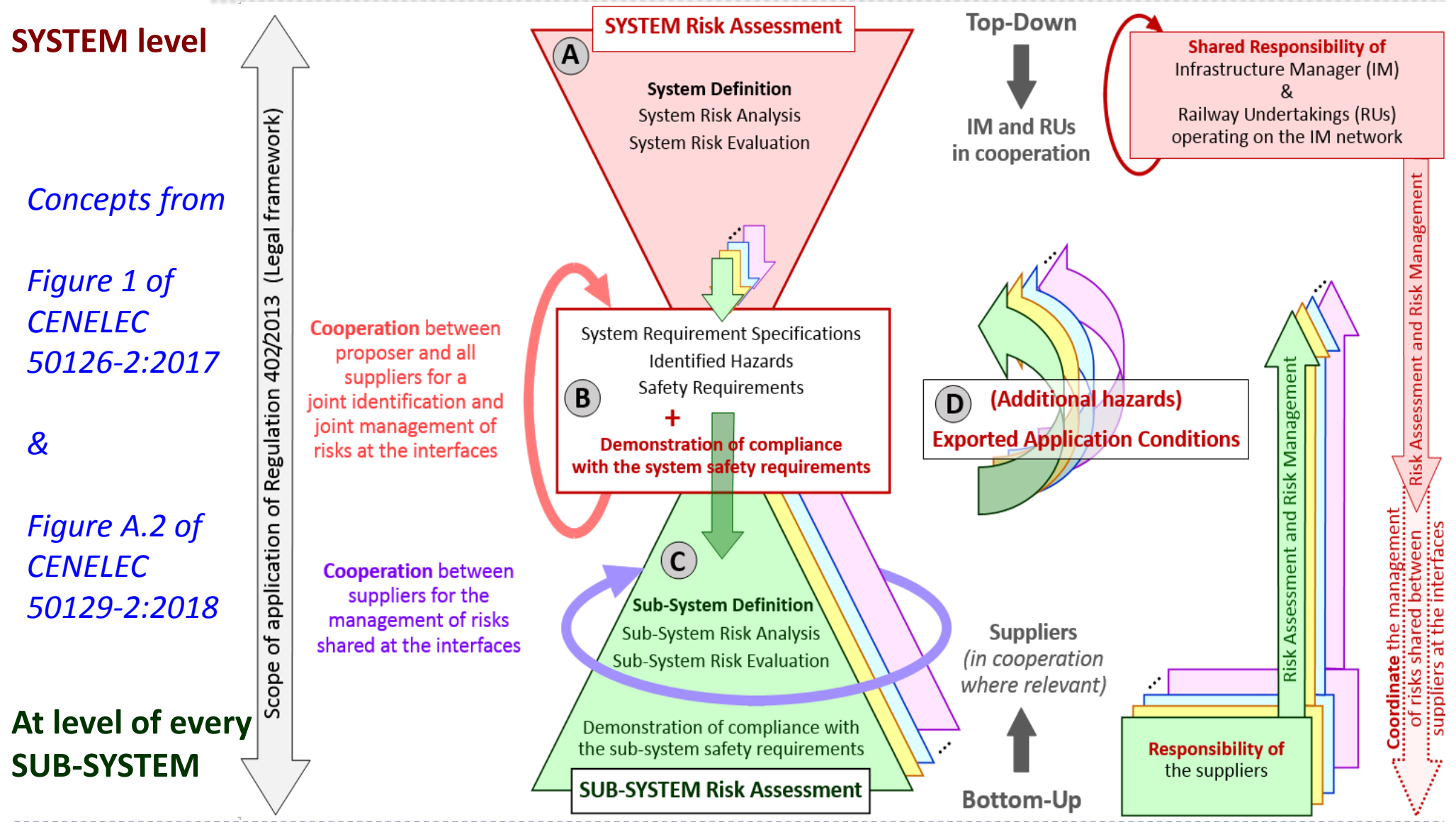
Architecture of the Railway System Responsibilities for Safe Integration



Art. 4 of Safety Directive 2016/798:

- IM & RUs must apply a system-based approach and where appro-priate co-operate with each other
- involve all actors who can impact the safe operation of system
- where appropriate those actors must cooperate with each other
- those actors must ensure that their sub-systems, accessories, equipment and services comply with the specified requirements and conditions for use so that they can be operated and maintained safely by RUs & IMs

Global overview and "system based approach" to risk assessment with Reg. 402/2013 – **Safe Integration at System & Sub-System levels**

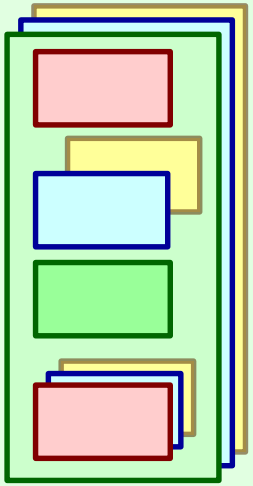


At the level of the RAILWAY SYSTEM, systematic top-down "system based approach":

- Joint System Risk Assessment by IM & RUs, with involvement of all other relevant actors
- apportion requirements to the sub-systems
- **System AsBo**

At level of every Sub-System (i.e. sub-contractor)

- Sub-System Risk Assessment (jointly with other sub-contractors **for shared risks**)



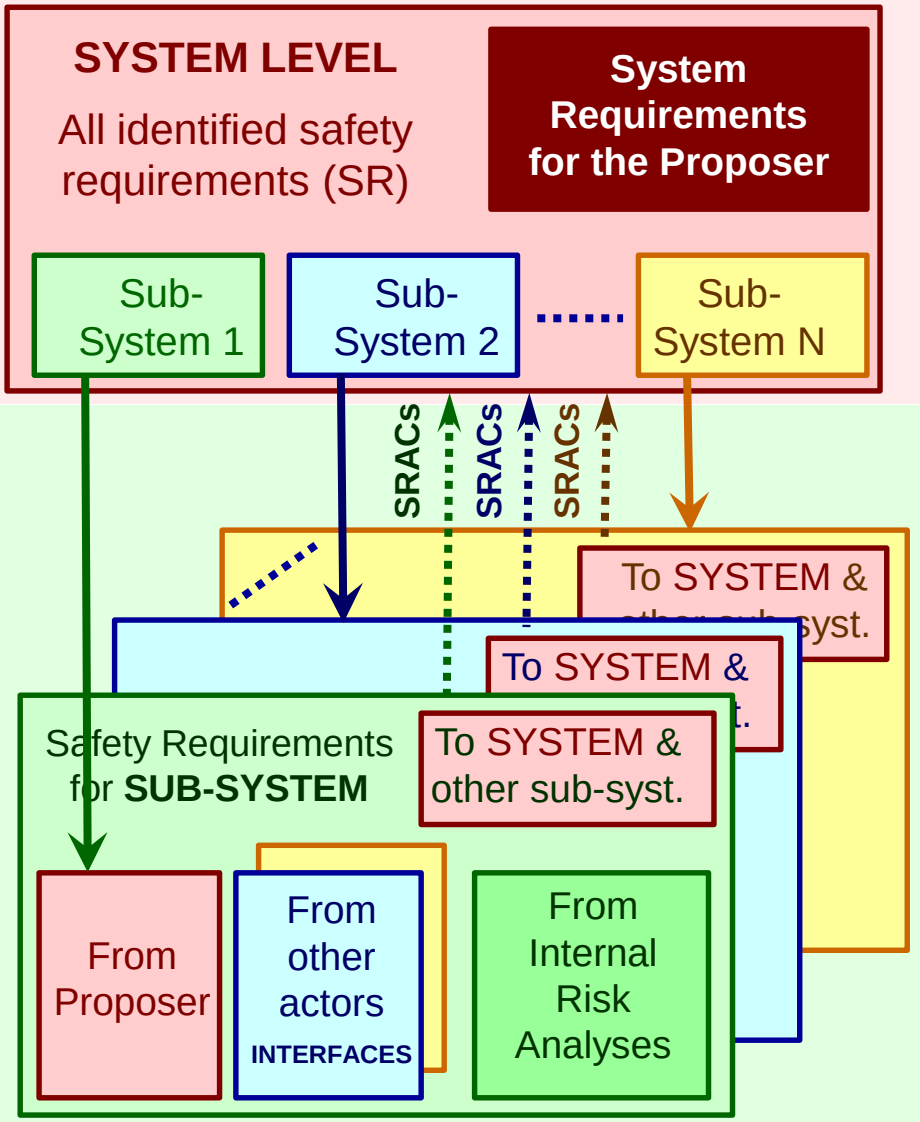
Requirements allocated to sub-system from the SYSTEM level

Requirements imported from other actors through shared interfaces

Internal requirements from own sub-system risk assessment

Requirements exported to SYSTEM (SRACs) and to other sub-systems (/actors) through shared interfaces

- **Sub-System AsBo**



Risk Assessment and Risk management **at level of the Railway System**
System based approach & top-down process

1) **Proposer:** IM & RUs in cooperation, with involvement of other relevant actors

2) **Inputs:** definition and architectural breakdown structure of railway system, including environmental, operational and maintenance specificities + interfaces between contributing sub-systems and with the SYSTEM operation & maintenance

3) **Risk assessment activities:**

   a) joint identification of system hazards/risks & associated safety requirements, including of interfaces with IM/RUs and between sub-systems/other actors

   b) all actors impacted by the change agree jointly on who is in charge of fulfilling each of the safety requirements defined by the risk assessment and risk management;

   c) apportion and transfer formally part(s) of the system functions and system safety requirements down to different contributing sub-systems/suppliers (but not beyond the scope of their responsibility and domain of control)

   d) functions and safety requirements that cannot be sub-contracted (cascaded down) to any constituting sub-system are requirements to be fulfilled by the proposer at the level of the railway system

Independent Safety Assessment by **a SYSTEM AsBo** of the Risk Assessment and Risk management at **level of the Railway System**

1) overall organisation, management and coordination by Proposer of development, risk assessment and risk management at levels of both railway system and different contributing sub-systems
2) relevance and completeness of SYSTEM risk assessment and risk management
3) suitability of the results from the SYSTEM risk assessment and risk management
4) apportionment of system hazards, functional, technical and safety requirements to the different contributing parts/suppliers of the railway system
5) **verification that the Proposer does not allocate requirements outside the scope of responsibility and reasonable domain of control of any sub-contractor**
6) methods and resources deployed for managing, coordinating and demonstrating compliance with functional, technical and safety requirements, including SRACs and sub-system AsBo reports from sub-contractors
7) cross acceptance of sub-system AsBos' reports, if appointed by sub-contractors. If there is no sub-system AsBo, the Proposer can ask the SYSTEM AsBo to assess the risk assessment and risk management of every contributing part/sub-system

Risk Assessment and Risk management at **level of a Sub-System**
Systematic bottom-up process

1) **Proposer:** sub-system contractor, if needed in cooperation with other relevant ones

2) **Inputs:**

   a) part(s) of system hazards, functional, technical and system safety requirements allocated by the RU/IM down to the sub-contractor, including environmental, operational and maintenance specificities of the SYSTEM
   b) interfaces with the other sub-systems/sub-contractors
   c) definition and architectural breakdown structure of the sub-system

3) **Risk assessment activities:**

   a) capture, understand and control system hazards apportioned to sub-system

   b) capture, understand and control hazards, and associated risks, imported through interfaces with other sub-systems/actors

   c) identify systematically, manage and control correctly risks arising from design choices and implementation of sub-system, including safe integration of internal architectural components/parts, and the proper consideration of human and organisational elements

3) Risk assessment activities: :

a) analyse and identify systematically the safety measures for controlling the risks arising from the interactions of the sub-system with the human, technological and organisational factors during design, implementation and use of sub-system

b) identify and manage systematically, where needed jointly with RU/IM, risks arising from operation and maintenance of sub-system within overall system

c) transfer formally to RU/IM hazards/risks and safety related application conditions (SRACs) necessary for safe integration of sub-system into physical, functional, environmental, operational and maintenance context of Railway System

d) identify and manage jointly and systematically risks associated to functions and information shared across interfaces with other sub-systems/actors;

e) transfer and receive risks & safety measures to be controlled/implemented on both sides of interface (with formal acknowledgement and acceptance to control)

Every actor who receives safety requirements for hazards/risks shared across interfaces with a sub-system is responsible to demonstrate appropriate control of shared hazards/risks falling under its area of responsibility. That applies also to SRACs

Independent Safety Assessment by **a sub-system AsBo** of the Risk Assessment and Risk management at **level of a sub-system**

1) overall organisation, management and coordination with other relevant actors of development, risk assessment and risk management at sub-system level and, in particular for the interfaces shared with other sub-systems/actors
2) methods and resources deployed for managing, coordinating and demonstrating compliance with:
   a) functional, technical and safety requirements allocated by RU/IM from System
   b) risks & safety measures across interfaces shared with other sub-systems/actors
3) relevance and completeness of sub-system risk assessment and risk management
4) suitability of the results from the sub-system risk assessment and risk management
5) different parts/components safety integrated in design of sub-system architecture
6) hazards/risks and safety related application conditions (SRACs) are identified and formally communicated to RU/IM, and other relevant actors, for safe integration of sub-system into physical, functional, environmental, operational and maintenance context of Railway System

Essential responsibility of IMs and RUs at the level of the Railway System risk assessment and risk management

System risk assessment must take care of human operators & actions to identify:

1) the operational risks and the associated requirements for training;
2) the risks associated with the maintenance of the railway system and the requirements for diagnostic functions and training of the maintenance staff;
3) **in case of a stepwise migration** from an existing system, depending on whether:
   a) the new system replaces the existing one;
   b) the new system is superimposed to the existing one;
   c) the new system modifies the existing one;

   identify the temporary risks that could arise during every migration step and the necessary risk control measures such as any necessary design solution to handle safely the transition, training requirements or specific protection measures
4) temporary risks must not be neglected; they can exist during weeks, months or years until the next step of the migration is reached. They are usually different from risks of the final system put into service once the migration is complete.
5) **Usually, suppliers cannot identify and manage alone those risks without a structured and top-down system approach under the RU/IM responsibility**

Complementarity of the SYSTEM top-down [IM/RU] and sub-system bottom-up [contractors] risk assessments

1) Operators of the railway system (RUs & IMs) are responsible for managing jointly the safe implementation of changes to the railway system

2) The **integration of changes** into the overall system **is not safe** if RUs/IMs:

   a) cut and sub-contract the overall system into a list of constituting sub-systems
   b) wait for suppliers to develop the different sub-systems and put them together technically
   c) collect the bottom-up exported safety related application conditions (SRACs) from the different constituting sub-systems/suppliers
   d) demonstrate the compliance with those SRACs imported from the risk assessment of every constituting sub-system/involved actor

3) Changes must not be assessed in isolation but through a top-down risk assessment process which systematically assesses and controls any potential impacts on:

   a) all unchanged parts of the railway system
   b) the interfaces with those unchanged parts
   c) the operation and maintenance of the overall railway system

All system hazards/risks **cannot be identified and controlled** by bottom-up analyses

Threats to a systematic top-down approach where **RUs & IMs are not capable to fulfil their Proposer's role**

Typical examples of changes not driven by an RU/IM, where a systematic and top-down approach to SYSTEM risk identification and management is usually lacking

1) Financial consortium, or regional public authority, purchasing a fleet of vehicles or trains without consulting/involving future operators (RUs/IMs)
2) Regional public authority, or Ministry, purchasing to a contractor construction of a new, or extension of an existing, (regional) railway line without involving IM

To manage properly such changes, and improve proactive hazard identification and preventive risk control, it is essential for the "Procurement Entity" either to:

3) apply itself a top-down and system-based approach right from tender stage & beginning of project, involving future operators (RUs) and traffic manager (IM), or
4) sub-contract to future operators (RUs) & traffic manager (IM), proper management of project, including proactive risk assessment and management with manufacturer

That permits to systematically identify early in project potential risks and to control those risks through technical improvements of design instead of obliging the future users to implement afterwards constraining operational and maintenance SRACs

Who is the PROPOSER?
Responsibility for safe integration depends on!

IM, and RUs operating on its network, share responsibility, each one for its part of system, for safe management of changes to "overall railway system"

IM & RUs must apply a "system-based approach" and "***... where appropriate ...***" cooperate "***... with each other***", involving, where necessary all other railway actors who have a potential impact on the safe operation of the railway system

1) **Changes of network, or traffic management: IM is leading proposer**, responsible for involving all impacted actors, especially all RUs (contributory proposers) operating on its network, in joint risk assessment, management and safe integration into railway system

2) **Change impacting a vehicle or operation and maintenance of vehicles: RU is leading proposer**, responsible for involving all impacted actors, especially IMs (contributory proposers) of networks on which it operates and ECMs, in a joint risk assessment, risk management and safe integration of change into overall railway system

Who is the PROPOSER?
Responsibility for safe integration depends on!

A new or a modified existing structural or functional sub-system: responsibility for top-down risk assessment approach depends on the actor who initiates the change:

1) **A part of a vehicle (rolling stock or on-board CCS) or operation is changed**

   RU is proposer responsible for defining clearly requirements to be fulfilled by vehicle and/or its SMS, regardless whether a manufacturer actually implements the changes to vehicle. RU is also responsible for safe integration of change into whole railway system

2) **A part of network or traffic management is changed**

   IM is proposer responsible for defining clearly requirements to be fulfilled by network and/or its SMS, regardless whether a manufacturer actually implements the changes to network. IM is also responsible for safe integration of change into whole railway system

3) **Change is a new structural or functional sub-system:** the proposer is the applicant (usually a manufacturer) responsible for:

   a) safe design of structural sub-system according to applicable TSIs, national rules, other EU laws, and all requirements identified by it at requirement capture stage

   b) identification of all necessary operational & maintenance conditions for use (SRACs)

Conclusions on Safe Integration and a Top-Down Risk Assessment Process

1) Safe integration of a change to railway system is implicitly an integral part of a systematic, comprehensive and consistent risk assessment and risk management process. If does not require additional checks or demonstrations

2) A system based and top-down risk assessment does not assess a change in isolation, or locally. It assesses a change beyond its boundaries within its physical, functional, environmental, operational, and maintenance context and identifies systematically:

   a) the interactions of the change with the external world
   b) the potential direct or indirect impacts (through the interfaces) of the change on the other non-modified sub-systems of the railway system
   c) any necessary requirements for the operation and maintenance of the sub-system itself, as well as for the other sub-systems or railway system as a whole

3) A system based & top-down approach requires risk assessment & risk management:

   a) at level of railway system by IM and RU(s)
   b) at level of every impacted sub-system by actor in charge of its development

4) In absence of a top-down analysis, some system hazards/risks might remain non-identified and uncontrolled; they cannot be compensated by bottom-up analyses

Conclusions on Safe Integration and a Top-Down Risk Assessment Process

1) At the level of the railway system, the IM and RU(s) must:
   a) carry out a "top-down" risk assessment and risk management, "***... where appropriate ...***", in cooperation "***... with each other***", involving all other railway actors who have a potential impact on safe operation of railway system
   b) allocate to every contributing actor and sub-system the associated hazards/risks, functional, technical and safety requirements to be fulfilled and managed by the actor in charge of the development of the sub-system

2) At the level of every impacted sub-system, actor in charge of its development must:
   a) carry out a "bottom-up" risk assessment and risk management, in cooperation with other actors in charge of development of other sub-systems (if needed), to identify and manage jointly the hazards at interfaces shared between them
   b) demonstrate that the sub-system is safely designed and implemented and fulfils safely the intended functional, technical and safety requirements allocated to it
   c) identify, and transfer to RU(s)/IM, the hazards/risks and SRACs necessary for the safe integration of sub-system into physical, functional, environmental, **operational and maintenance** context of Railway System

Safe Integration
of safety-related non-significant changes

Agency position

CSM for risk assessment shall be used for the "safe and controlled" **management of all changes** to the railway system

Legal requirements
Where is risk assessment necessary/required?

Safety Directive 2016/798

Art. 6(1)(a) → **Reg. 402/2013 on CSM RA** → Manage safely the changes [Art. 4 & 2(2)]

Safety related changes

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

Non-safety related

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

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 (Reg. 2019/776 which amends Regulation 2016/919

Art. 21 → Vehicle authorisation for placing on the market (Reg. 2018/545)

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**

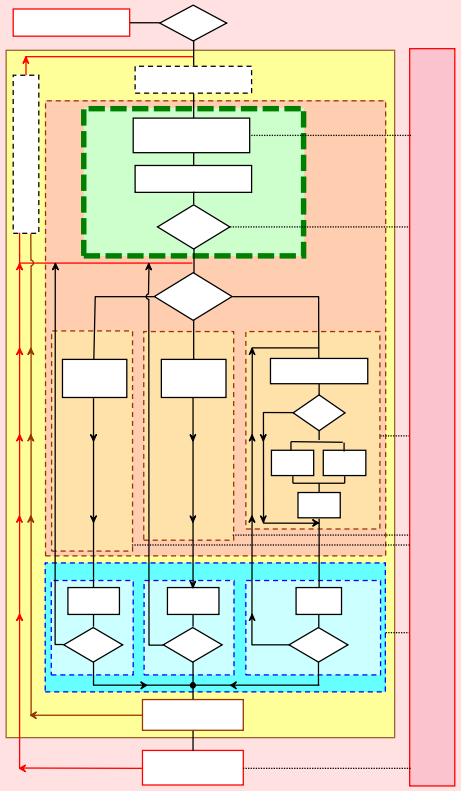
+

AsBo mandatory

Possible “processes for risk assessment” and control of **risks arising from safety-related non-significant changes**

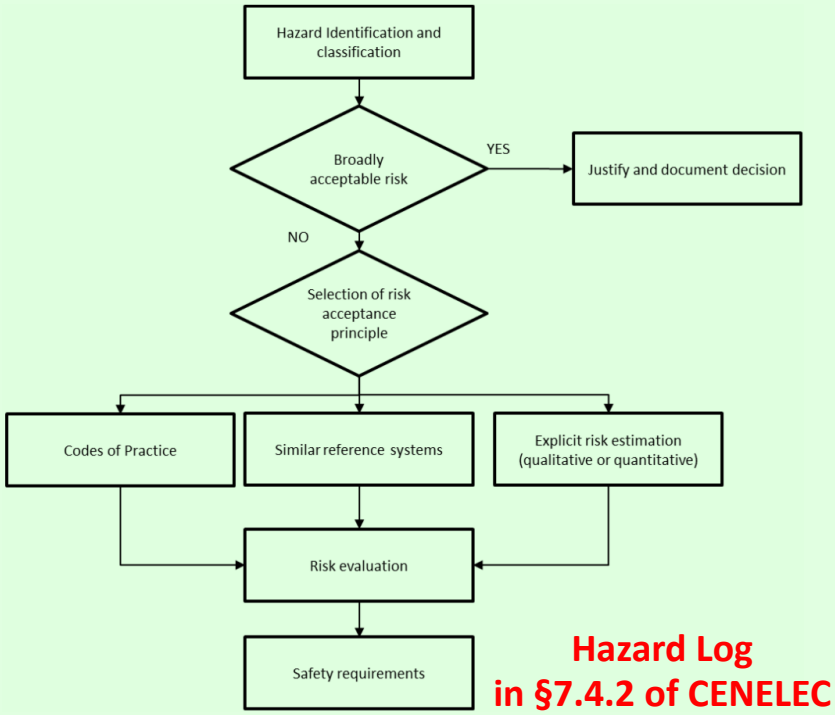
1

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)

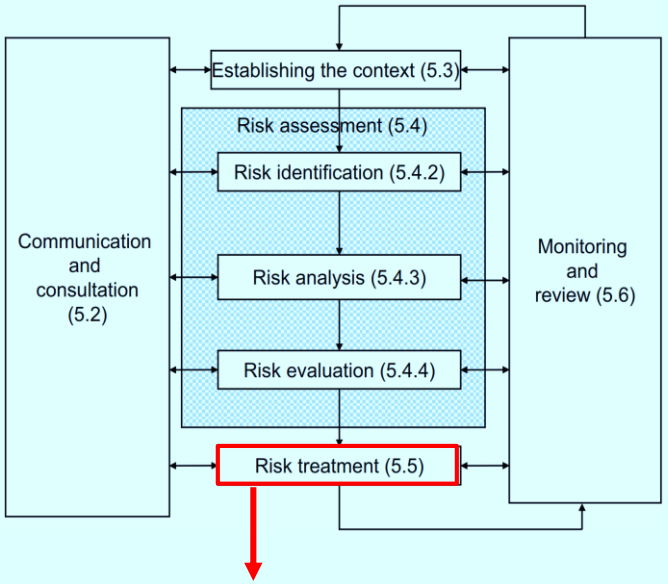


Hazard Log in §7.4.2 of CENELEC

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

Structuring of Development, Verification, Validation and independent Conformity Assessments activities

between the Proposer, NoBo, DeBo & AsBo

Relationship between AsBo and other conformity assessment bodies (NSA, NoBo, DeBo, other ASBOs)

EU legislation requires to avoid duplication of independent assessment work between different conformity assessment bodies *(NoBo, DeBo, NSA, AsBo, etc.)*

⬇

Essential that the Proposer correctly structures the different development, verification and validation activities and independent conformity assessments

Compliance with applicable TSIs & National Rules

and

NoBo "EC Verification of conformity" & DeBo Checks

Compliance with CSM for risk assessment

and

Independent Safety Assessment by an AsBo

Compliance with applicable TSIs and national rules is mandatory

TSIs ≡ **EU law** (Derogations in Art. 7 of ID 2016/797)

NR in force at time of request of Authorisation ≡ **National Law**

Independent Conformity Assessment by **NoBo**

DeBo

- TSIs contain essential requirements related to safety **as far as they are necessary for interoperability**
- Sole compliance with TSIs **does not ensure safety is fully covered** → additional risk assessment necessary
- **Only where necessary for interoperability purposes**, TSIs request application of specific part(s) of CSM RA
- TSIs do not question necessity to apply CSM RA for safe management of changes → **CSM RA must also be applied to demonstrate safety is fully controlled**

Compliance with Regulation 402/2013 is mandatory when carrying out a change

Regulation 402/2013 (CSM RA) ≡ EU law

(when making changes)

Independent Conformity Assessment

AsBo

Compliance is mandatory

BUT

Application of CSM RA shall not lead to requirements contrary to a TSI otherwise TSIs need to be revised or MS shall ask for a derogation

TSIs and Regulation 402/2013 are separate legal texts → compliance with CSM Risk Assessment is also mandatory

TSIs ≡ **EU law** (Derogations in Art. 7 of ID 2016/797)

NR in force at time of request of Authorisation ≡ **National Law**

Regulation 402/2013 (CSM RA) ≡ EU law *(when making changes)*

Independent Conformity Assessment by **NoBo** / **DeBo**

Compliance is mandatory

Independent Conformity Assessment by **AsBo**

Compliance is mandatory

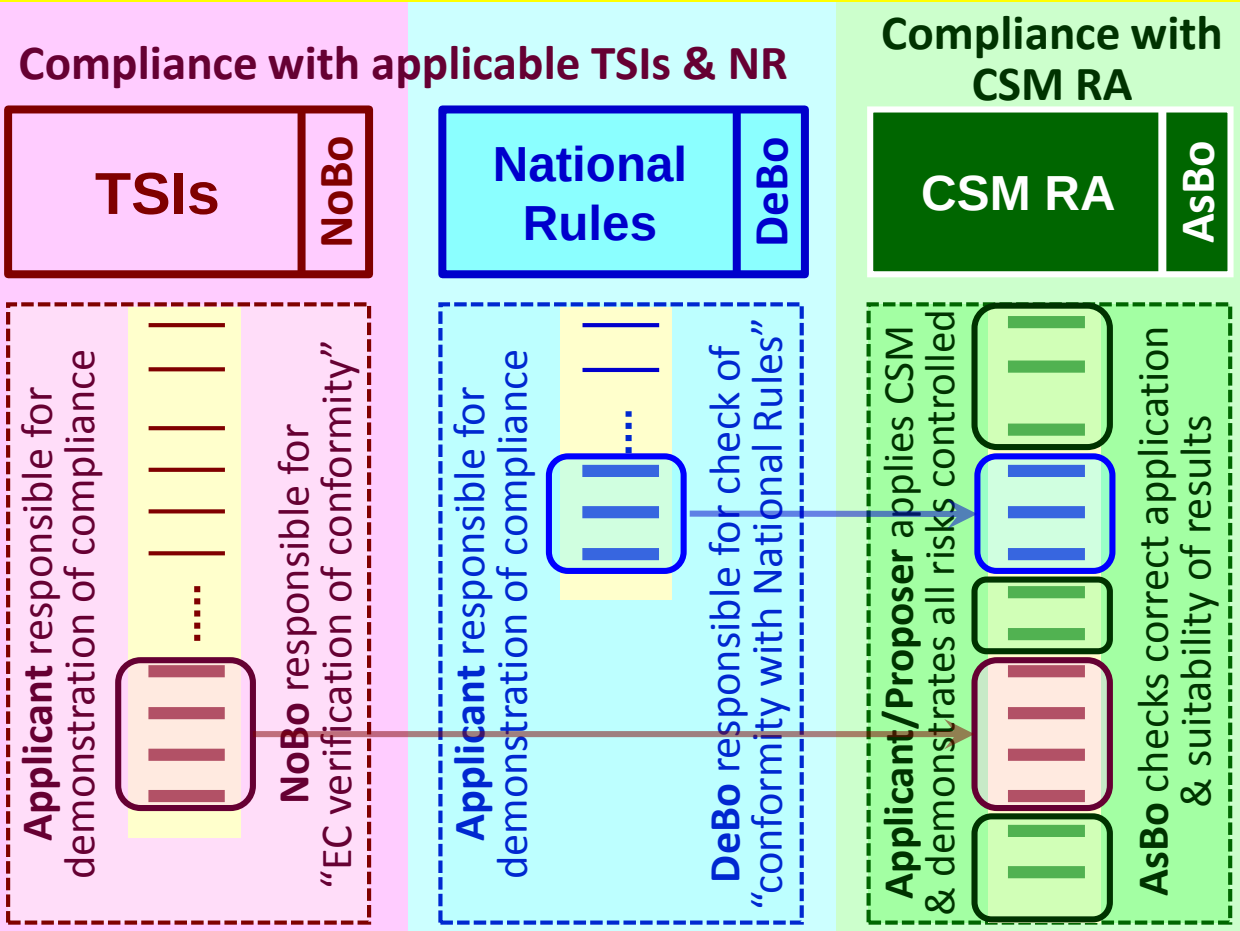
- TSIs contain essential requirements related to safety **as far as they are necessary for interoperability**
- Sole compliance with TSIs **does not ensure safety is fully covered** → additional risk assessment necessary
- **Only where necessary for interoperability purposes**, TSIs request application of specific part(s) of CSM RA
- TSIs do not question necessity to apply CSM RA for safe management of changes → **CSM RA must also be applied to demonstrate safety is fully controlled**

BUT

Application of CSM RA shall not lead to requirements contrary to a TSI otherwise TSIs need to be revised or MS shall ask for a derogation

Compliance with TSIs – Compliance with CSM Risk Assessment
WHAT is the interaction of AsBo with other CABs?

Duplication of independent assessment work between different Conformity Assessment Bodies shall be avoided



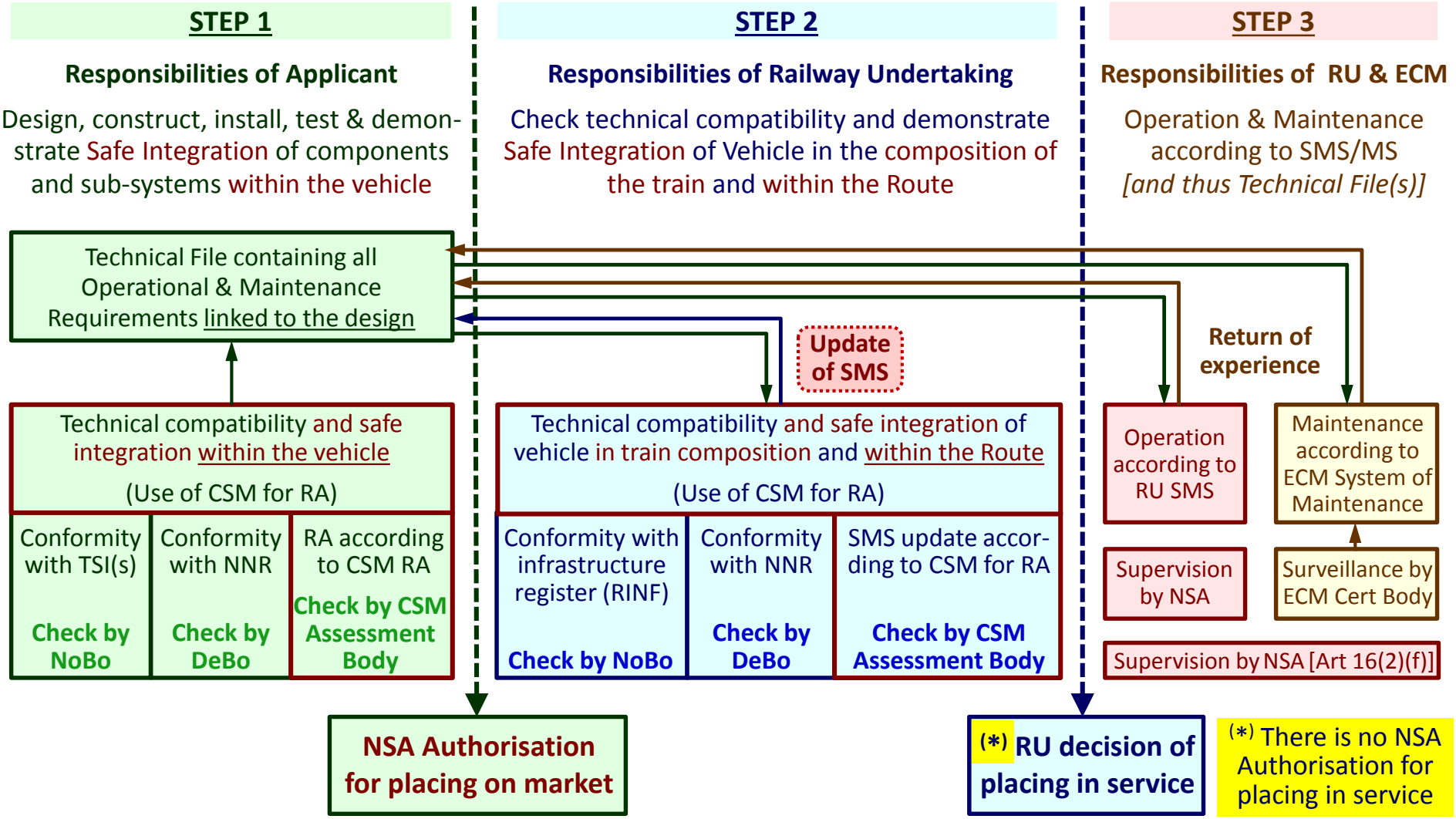
Applicant/Proposer applies its processes and demonstrates:

- compliance with TSIs, NNR & CSM
- all risks identified and controlled to an acceptable level **(Proposer's Declaration – Art. 16)**

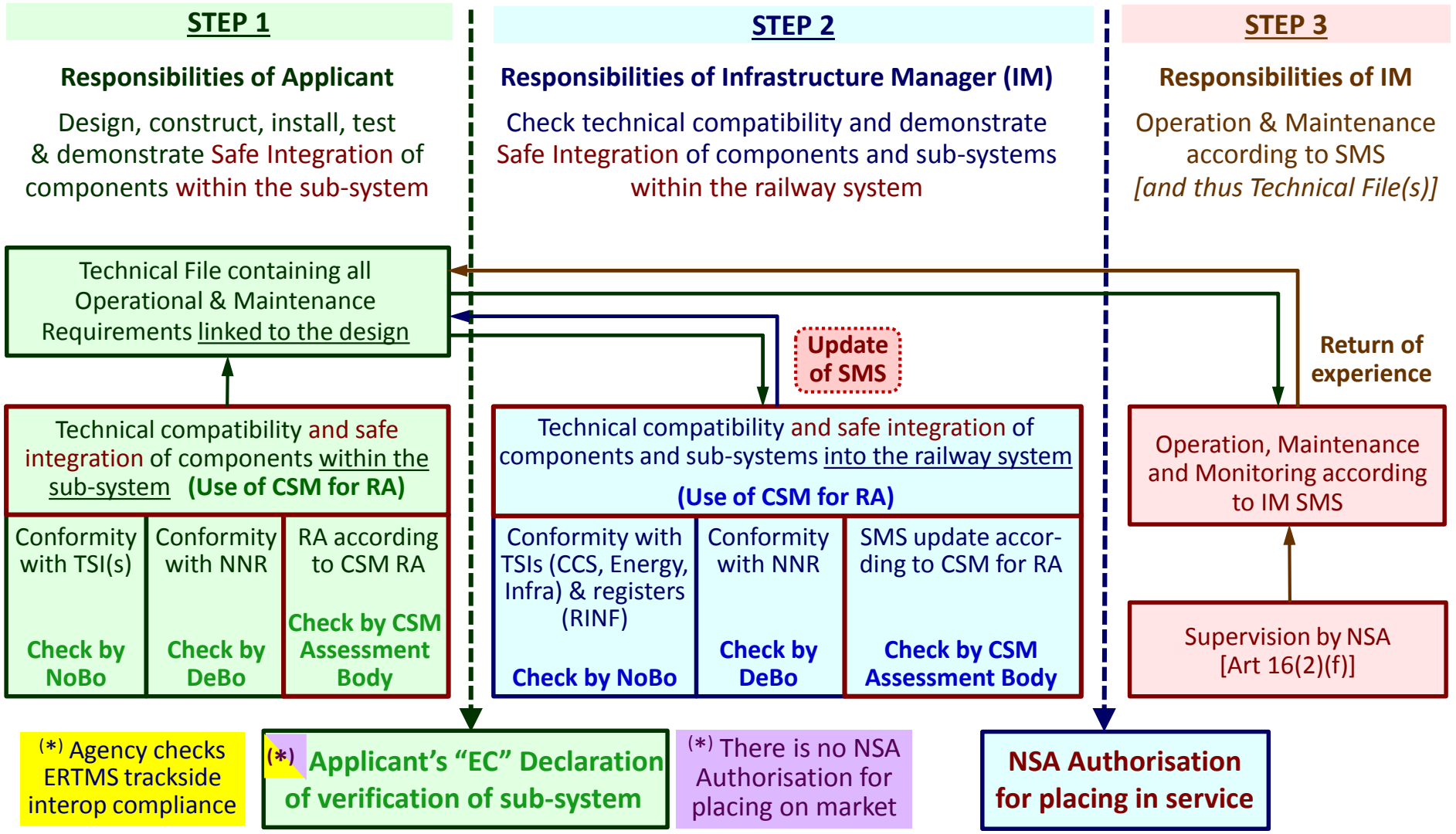
Authorising Entity (e.g. NSA) issues authorisation based on evidences of:

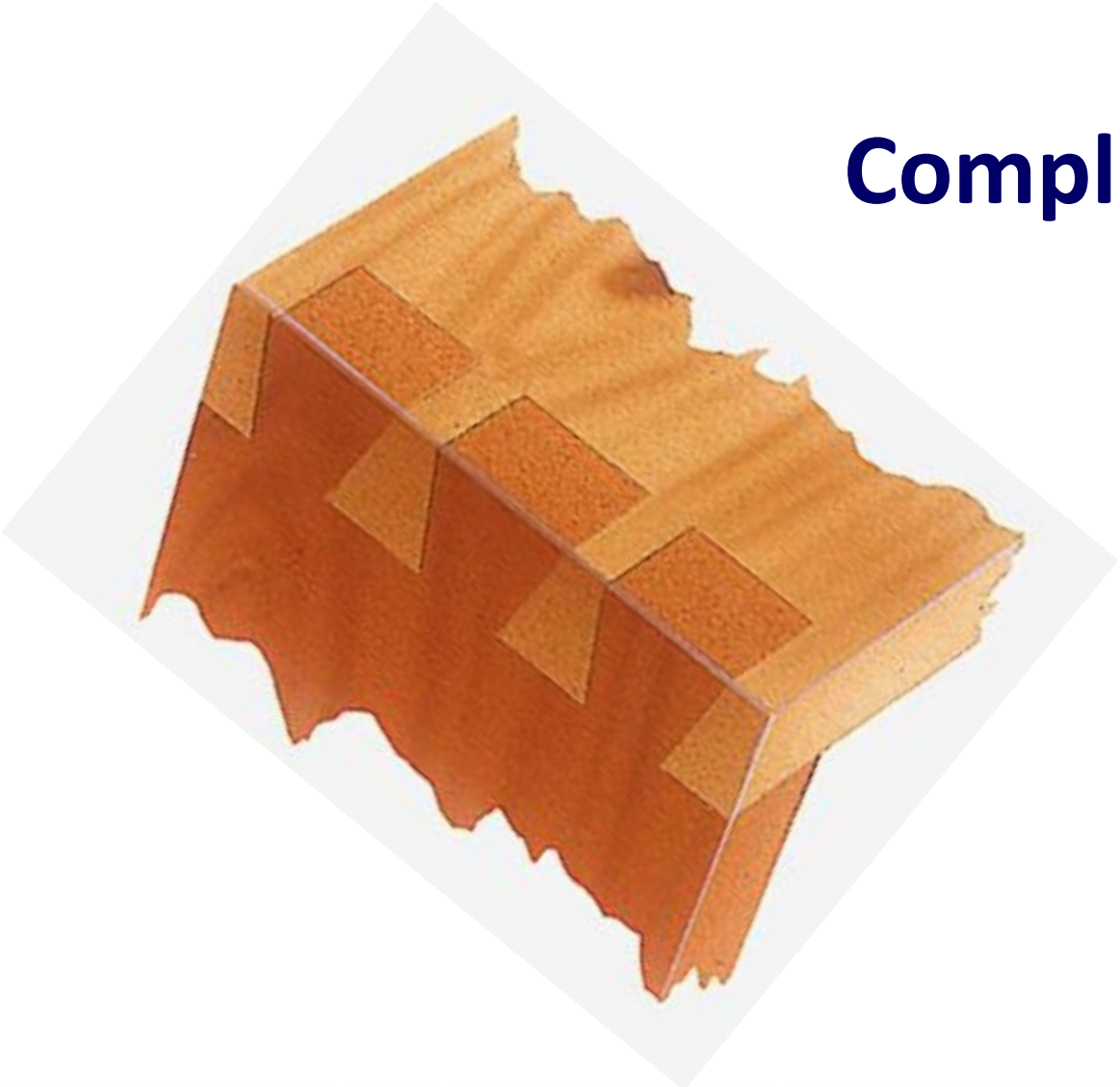
- NoBo EC Verification of conformity with TSIs;
- DeBo verification of conformity with notified national rules;
- **Applicant's EC declaration of verification**;
- AsBo safety assessment report;
- Applicant's declaration of **Article 16 of the CSM RA**;

Roles and responsibilities of different Conformity Assessment Bodies within Authorisation for placing on market Vehicles - Safe Integrations



Roles and responsibilities of different Conformity Assessment Bodies within Authorisation for placing in service of fixed installations – Safe Integrations





Complementary Slides

Existing legislation and standards

incorporate similar requirements to those meant by safe integration in Regulation 402/2013 on the CSM for risk assessment

General European legislation on Product and Service Safety

Directive 2001/95/EC on general product safety requests producers to "***ensure that products placed on the market are safe***". According to Article 2:

- "*product*" means "*… any product – including … a service*" (including thus transport)
- "*safe product*" means "*… any product which, under* ***normal or reasonably foreseeable*** *conditions of use, including …, where applicable, putting into service, installation and maintenance requirements,* ***does not represent any risk or … considered to be acceptable*** *… taking into account*

  (i) the characteristics of the product, including … instructions … for installation and maintenance;

  (ii) the effect on other products, where it is reasonably foreseeable …

  (iii) … any warnings and instructions for its use …"

Have a formal process:

1) to demonstrate product is safe
2) to demonstrate it does have adverse effects on other products
3) to identify conditions for safe use and safe maintenance of product

Directive 1985/0374 concerning liability for defective products requires that "***the producer shall be liable for damage caused by a defect in his product***"

§3.2 IEC 61508-0 standard:

The term “safety-related” is used to describe systems that are required to perform a specific function or functions to **ensure risks are kept at an acceptable level**. Such functions are by definition safety functions. Two types of requirements are necessary to achieve functional safety:

1) safety function requirements, *i.e. **WHAT** the function does/achieves*	→ derived from a Hazard Analysis
2) safety integrity requirements, *i.e. the likelihood of a safety function being performed satisfactorily (without failure) → related to **HOW** the function is implemented*	→ derived from a Risk Assessment

- Any system which carries out safety functions is a safety-related system
- The higher the safety integrity level, the lower the likelihood of a dangerous failure
- Safety-related systems with **higher levels of safety integrity necessitate greater rigour in the engineering** of the safety-related system
- **Functional safety is embedded in Product safety**

Standards on safety-related Products and Services

Standards covering functional safety of electrical/electronic/programmable electronic (E/E/PE) safety-related systems – Functional safety is:

IEC 61508	part of the overall safety that depends on a system or equipment operating correctly in response to its inputs
CENELEC 50126–1 & –2:2017 CENELEC 50129:2018	part of the overall safety that depends on functional and physical units operating correctly in response to their inputs
ISO 26262 **for road vehicles**	absence of unreasonable risk due to hazards caused by malfunctioning behaviour of electrical/electronic systems

Functional safety has to be achieved by a rigorous development process, supported by Safety & Quality management processes, with stringent requirements for:

- requirement specification,
- design, implementation & integration,
- verification & validation,
- configuration/parametrisation,
- production and service processes (maintenance & repairs)
- risk assessment and risk management
- **stringent proof of meeting requirements**

Responsibilities for the Safe Integration

Article 4(1) of Safety Directive 2016/798 requires to "*… ensure that railway safety is generally maintained and, where reasonably practicable, continuously improved*" during and after the market opening. To achieve that goal, Article 4 requires the IM and RUs to apply a "***system-based approach***" and "*… where appropriate …*" **to cooperate** "*…* ***with each other***", involving all other railway actors who have a potential impact on the safe operation of the railway system

The Safety Directive 2016/798 clearly identifies the requirements below. They are not new; they were already part of the former Safety Directive 2004/49.

a) Article 4(1)(c) requires that "*measures to develop and improve railway safety take account of the need* ***for a system-based approach***", i.e. a systematic top down approach;

b) Article 4(1)(d) requires that "*the responsibility for the safe operation of the … rail system and the control of risks associated with it is laid upon the* ***infrastructure managers and railway undertakings, each for its part of the system****…*";

c) Article 4(1)(d)(i) requires that "*railway undertakings and infrastructure managers shall implement the necessary risk control measures…* ", identified by the application of Regulation 402/2013 on the CSM for risk assessment, " … ***where appropriate in cooperation with each other and with other actors***";

d) Article 4(4) requires that "*without prejudice to the responsibilities of railway undertakings and infrastructure managers …, entities in charge of maintenance and* ***all*** *other* ***actors having a potential impact on the safe operation*** *of the Union rail system, including manufacturers, maintenance suppliers, keepers, service providers, contracting entities, carriers, consignors, consignees, loaders, unloaders, fillers and unfillers,* ***shall***":

(i) Article 4(4)(a) : "*implement the necessary risk control measures, where appropriate* ***in cooperation with other actors***";

(ii) Article 4(4)(b) : "*ensure that subsystems, accessories, equipment and services supplied by them comply* ***with specified requirements and conditions for use*** *so that they* ***can be safely operated*** *by the railway undertaking and/or the infrastructure manager concerned*";

Responsibilities for the risk assessment

By virtue of section §1.1.5 in Annex I of Regulation 402/2013:

"Without prejudice to civil liability …, the risk assessment process shall fall within the responsibility of the proposer. In particular the proposer shall decide, with agreement of the actors concerned, who will be in charge of fulfilling the safety requirements resulting from the risk assessment. The safety requirements assigned by the proposer to those actors shall not go beyond the scope of their responsibility and domain of control. This decision shall depend on the type of safety measures selected to control the risks to an acceptable level…"

i.e. there shall be a System Risk Assessment at the level of RU/IM

i.e. apportionment of requirements from the risk assessment to every contributing sub-system or actor (i.e. to supplier and sub-contractors)

i.e. responsibility for the system safety requirements must not be transferred to sub-contractors or other actors, including the acceptance of the system risks

Responsibilities for the risk assessment

By virtue of section §1.2.1 in Annex I of Regulation 402/2013:

"For each interface relevant to the system under assessment and without prejudice to specifications of interfaces defined in relevant TSIs, ***the rail-sector actors concerned shall cooperate*** *in order to* ***identify and manage jointly the hazards and related safety measures that need to be handled at these interfaces****. The management of shared risks at the interfaces shall be* ***coordinated by the proposer****."*

i.e. all actors impacted by the change through the interfaces must cooperation in a joint hazard identification and assignment of the sub-system/actor which must manage the associated risks

i.e. the system proposer (i.e. RU/IM) is responsible for coordinating the risk identification and risk management among the sub-systems/actors across the shared interfaces

Responsibilities for the risk assessment

By virtue of section §2.2.1 in Annex I of Regulation 402/2013:

"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"

i.e. the proposer (RU/IM) must apply a system based approach [Article 4(1) of Safety Directive 2016/798]

i.e. the system based approach must consider all sub-systems and all interfaces with all actors impacted by the change across the interfaces

Global overview and "system based approach" to risk assessment with Reg. 402/2013 – **Safe Integration at System & Sub-System levels**

SYSTEM level

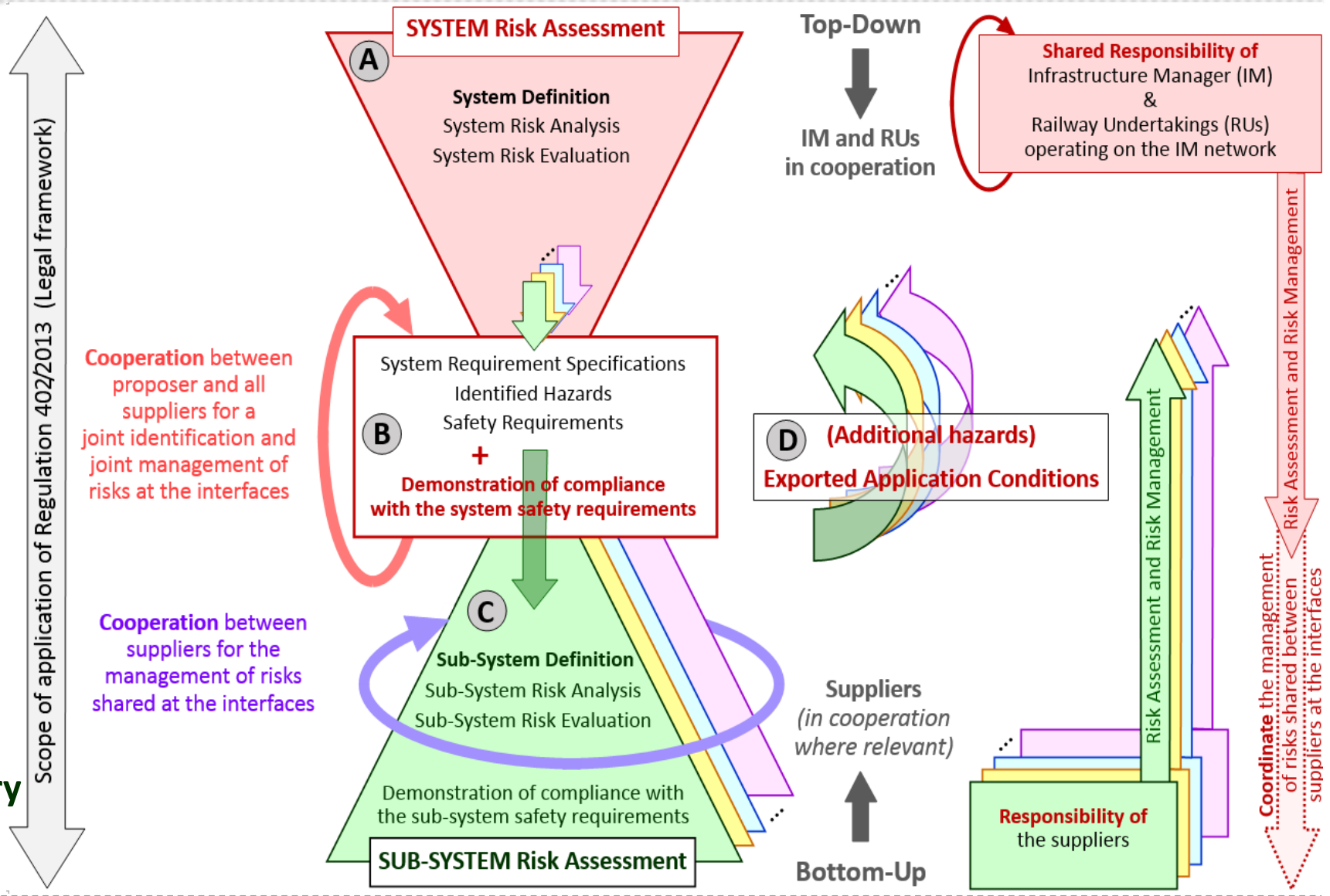
Concepts from

Figure 1 of CENELEC 50126-2:2017

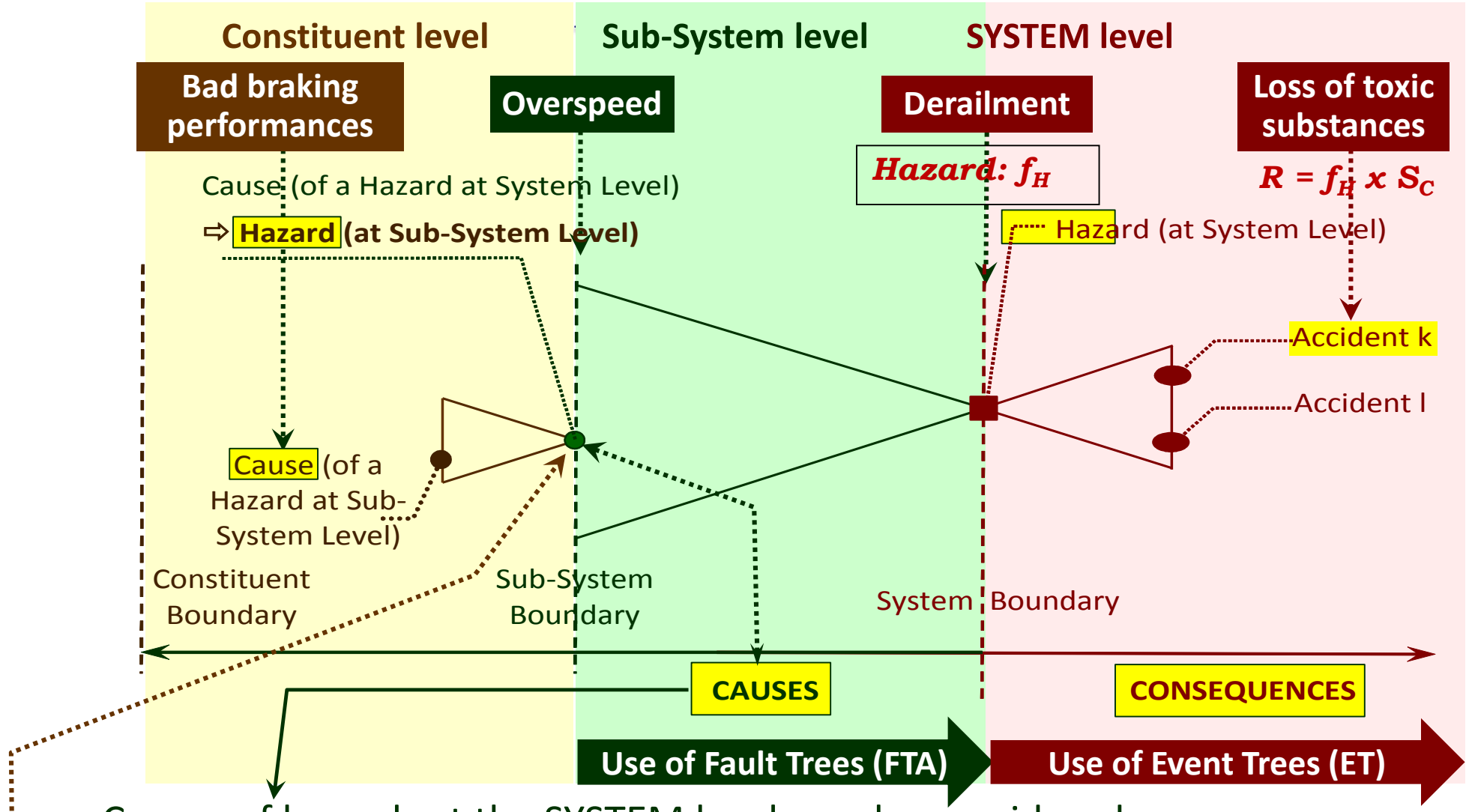
&

Figure A.2 of CENELEC 50129-2:2018

At level of every SUB-SYSTEM



Example of Hazard-Risk-Accident - Bow-Tie diagram in Fig. A.3 of EN 50 129:2018 - Definition of hazards with respect to the system boundary



Causes of hazards at the SYSTEM level may be considered as hazards at the sub-system level (with respect to sub-system boundary).

Example of Hazard-Risk-Accident
Vertical representation of the Cause-Hazard-Consequence Bow Tie

CONSEQUENCES (SYSTEM level)

Risk Analysis

- System Definition
- Hazard Identification
- (Risk) Consequence Analysis
- Risk Estimation
- Tolerable Hazard Rate Allocation (where relevant)

Accidents

Emergency Response Measures

Passive Protection Measures

Active Protection Measures

HAZARD

Hazard Control

- Causal Analysis
- Common Cause Analysis
- Safety Integrity Level Allocation

Technical Safety Measures

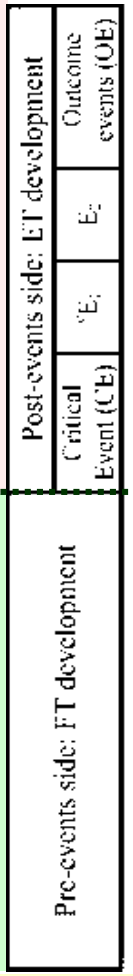
Process Measures

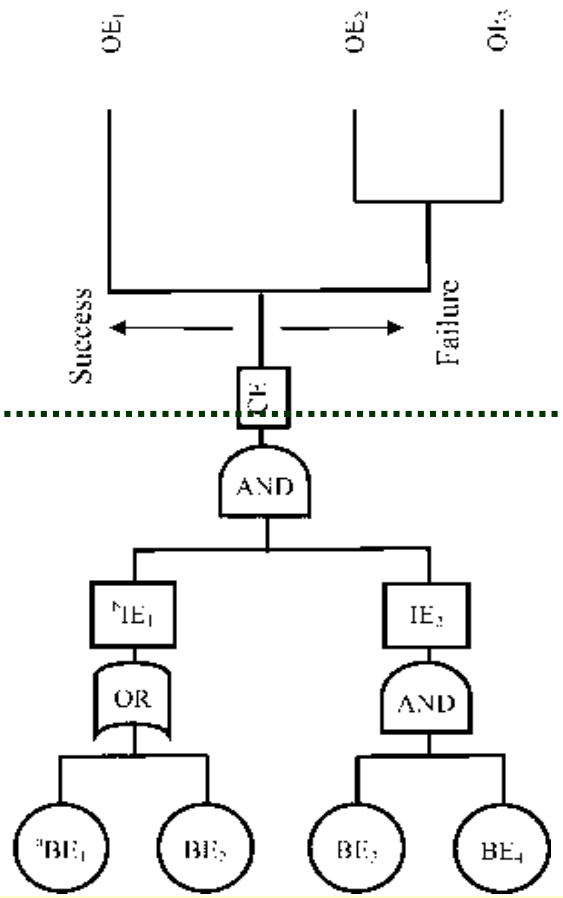
Operational Measures

(Sub-System level) CAUSES

Mitigation RCM

Preventive RCM





Use of Event Trees (ET)

Use of Fault Trees (FTA)

Constituent level Risk Analyses

Making the railway system work better for society.

Follow us on Twitter: @ERA_railways

Questions? → Send e-mail on: CSM.risk_assessment@era.europa.eu