Use of the CSM for risk assessment (Reg. 402/2013) for Fixed Installations and for their Safe Integration

ANSF Workshop, 29 May 2020

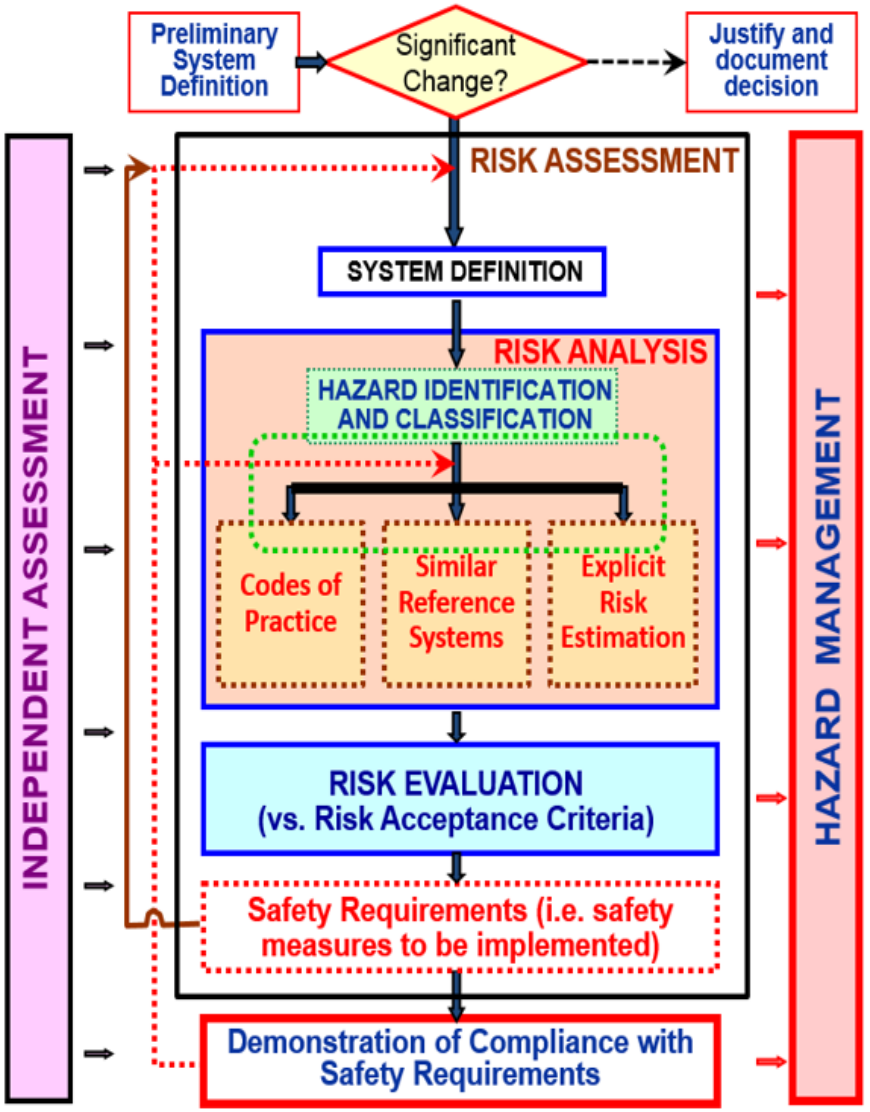
Dragan JOVICIC, EU Agency for Railways

EUROPEAN UNION AGENCY FOR RAILWAYS

Contents

1) Regulation 402/2013 : reminder, versions, guidance material
2) Safety related systems: need for a rigorous management of safety
3) Technical and organisational complexity of the railway system
4) Complementarity between Interoperability and Safety Directives
5) Risk assessment and demonstration of system safe integration
6) Levels of railway system architecture where safe integration required
7) Challenges and complexity arising from the railway market opening
8) System top-down approach and Sub-system bottom-up approach
9) Responsibilities for railway safety & Threats to correct safety management
10) Application of Reg. 402/2013 to infrastructure projects (Example)

Reminders about Regulation 402/2013

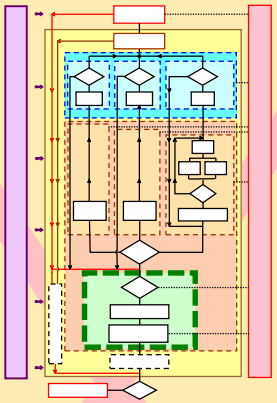


- **WHAT** is the CSM for risk assessment?
  [Common Method & Process in Annex I]
- **WHY** a CSM?
  [Mutual recognition of a Controlled and Safe Management of Changes based on:
  - documented & traceable risk management
  - Independent Assessment **(2nd pair of eyes)**]
- **WHO** shall apply it?
  [Proposer (RU/IM) main responsible]
- **WHEN** shall it be applied?
  [Whenever making a significant change]
- **WHAT** shall it be applied to?
  [Technical, Operational & Organisational changes]
- Keep in mind why risk assessment needed
  (Not for good paper work but **keep people safe**)

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}]

… to be used in combination with

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

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

WHAT shall be done?

Regulation 402/2013 on CSM for risk assessment (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

Translated in all EU Languages

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 and 50129 Standards
+ Other Standards (FMECA, FTA, ...)

CENELEC 50126 & 50129 revised in 2017

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

Safety related systems: existing legislation/standards: Require a rigorous and traceable management of safety

- Every safety-related system or service, including railways, is characterised by:
  - the safety functions and requirements it fulfils
    → this characterises WHAT the system does
  - the safety integrity requirements of those functions, i.e. likelihood of the functions to be achieved satisfactorily, which means without failure(s)
    → this conditions the way on HOW to implement the safety functions

- Systems requiring higher levels of safety integrity require greater rigour in "**system & functional safety engineering**", and imply stringent Q&S processes for:
  - a complete system definition and requirement specification
  - design, implementation and integration processes
  - correct Verification & Validation processes
  - configuration/parametrisation processes, where relevant
  - controlled production and safe servicing processes (i.e. maintenance & repairs)
  - correct evidence of proper risk assessment and risk management
  - stringent demonstration of meeting all requirements

Complexity of the railway system

Railway System safety is achieved by an extremely high number of various types of safety measures dependent on:

- **complex Organisational & Operational** arrangements at RUs' & IMs‘ levels, involving many other actors who have a potential to impact safe operation and safe management of traffic (*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 can be caused by:

- an E/E/PE sub-system/equipment (*covered by functional safety standards*), or
- civil work deficiencies, failures of mechanical, hydraulic or pneumatic equipment,
- 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

Interoperability Directive 2016/797 – Meeting essential requirements and NR's

1) With exception of Vehicles, there is no authorisation for constructing, placing on the market, or placing into service "IC's and structural sub-systems":
   a) **IC's:** placing on the market based on an 'EC' declaration of conformity or suitability for use attesting compliance with corresponding TSI
   b) **structural sub-systems:** placing on market based on an 'EC' declaration of verification attesting compliance with corresponding TSI & national rules

2) Vehicles need an Authorising Entity authorisation for **placing on the market** for defined areas of use and attesting compliance with the relevant TSIs and national rules

3) Fixed installations need an NSA authorisation for **placing into service** attesting that they are designed, constructed and installed in such a way as to meet the essential requirements and national rules

Safety Directive 2016/798 – Changes must also be safe (not only interoperable)

Sole compliance with TSIs does not ensure safety is fully covered. TSIs contain essential requirements related to safety that are necessary to reach interoperability

Development Process of IC's and structural sub-systems must be rigorous and demonstrate through **risk assessment & risk management** (**Regulation 402/2013**) that IC's and structural sub-systems placed on the market:

1) are safe
2) are technically compatible with the other sub-systems to which they are intercommected and with the system into which they are incorporated
3) do not have adverse and unacceptable effects on safety of resulting system into which they are incorporated (**i.e. they will not degrade safety of system**)

   → can be safely incorporated or integrated into physical, functional, environmental, operational, and maintenance context of system where they will be used

1) identify all conditions (SRACs) for their safe use (operation) & safe maintenance

Regulation 402/2013 on CSM for risk assessment and Safe Integration
Fears, misunderstandings and consequences

1) Different understandings of safe integration generates fears and wrong beliefs

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

3) In practice, safe integration is an inherent part of a systematic risk assessment process [§1.2.7 in Ax I of **Regulation 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*"]

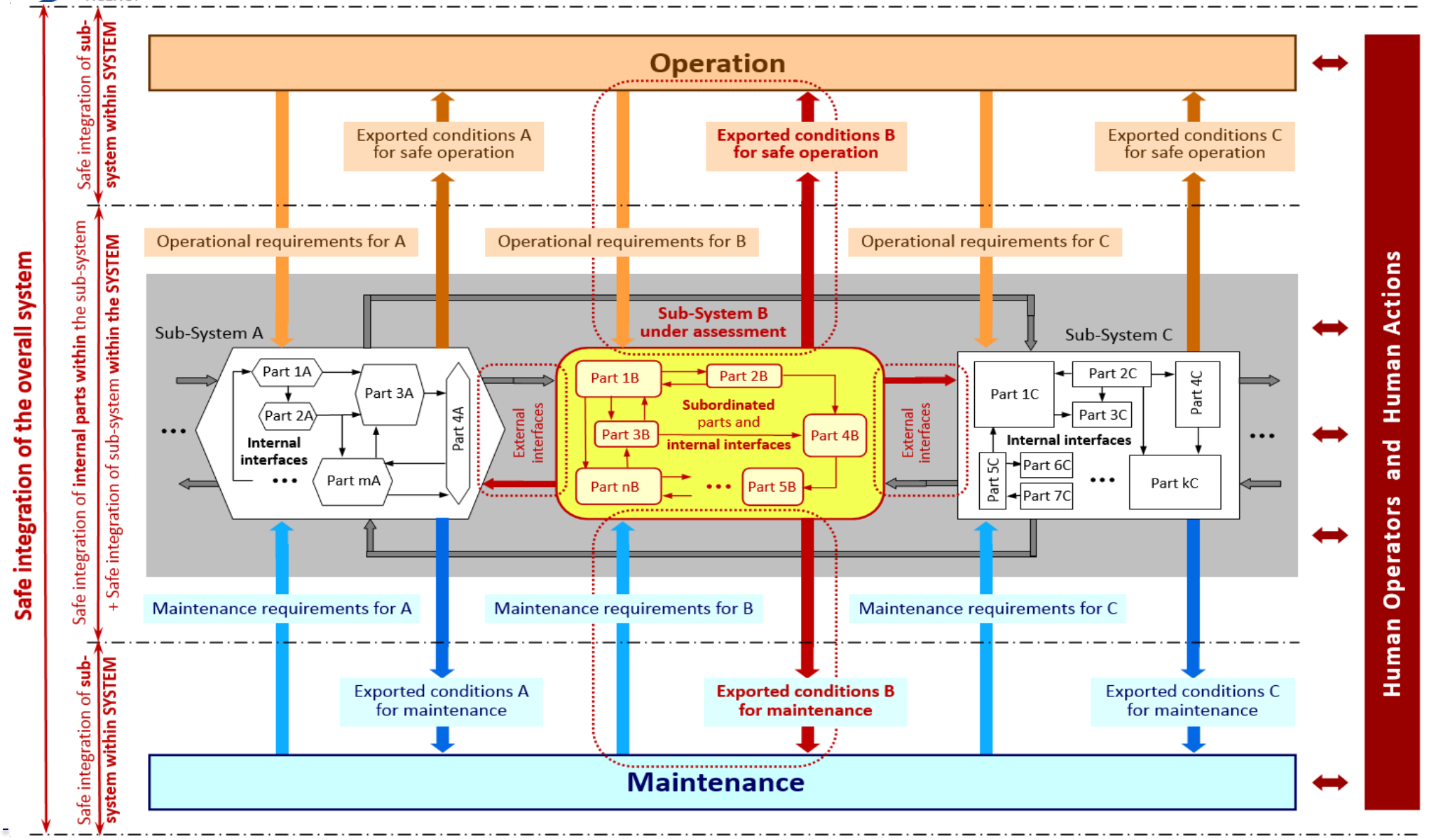
4) Safe integration has a broader meaning and goes beyond single checks above → applies at different levels and to entire life cycle of design, operation, maintenance and disposal/decommissioning of railway system and of its components

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 **without requesting additional risk assessments and additional checks**

Agency clarification note on safe integration (available on the website) – **Purposes of the document**

1) Provide a common understanding of the concept of safe integration
2) Identify levels where safe integration is necessary in architecture of railways
3) Explain how to demonstrate safe integration with application of a systematic system based and top-down approach structured around Regulation 402/2013
4) Lay down the basis for mutual recognition of demonstration of safe integration
5) Highlight big challenges and usual difficulties to overcome for a proper top-down risk assessment, risk management and safe integration
6) Summarise in one document requirements from different European legal texts:
   a) Main roles & responsibilities of RUs & IMs in top-down system engineering (system requirement specification and allocation of relevant ones to suppliers & contractors)
   b) Bottom-up process at levels of sub-system and service suppliers
   c) Emphasise necessity for cooperation between RUs, IMs and all other actors who can impact safe design, operation and maintenance of railway system
   d) Roles of independent safety assessment by AsBos at all levels of architecture
7) **Threats to a systematic & top-down approach to a systematic preventive risk identification, risk control and risk management**

Safe Integration takes place at every level of the Railway System whenever a change is made somewhere



Challenges and difficulties to overcome
Consequences of the railway market opening and restructuring

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

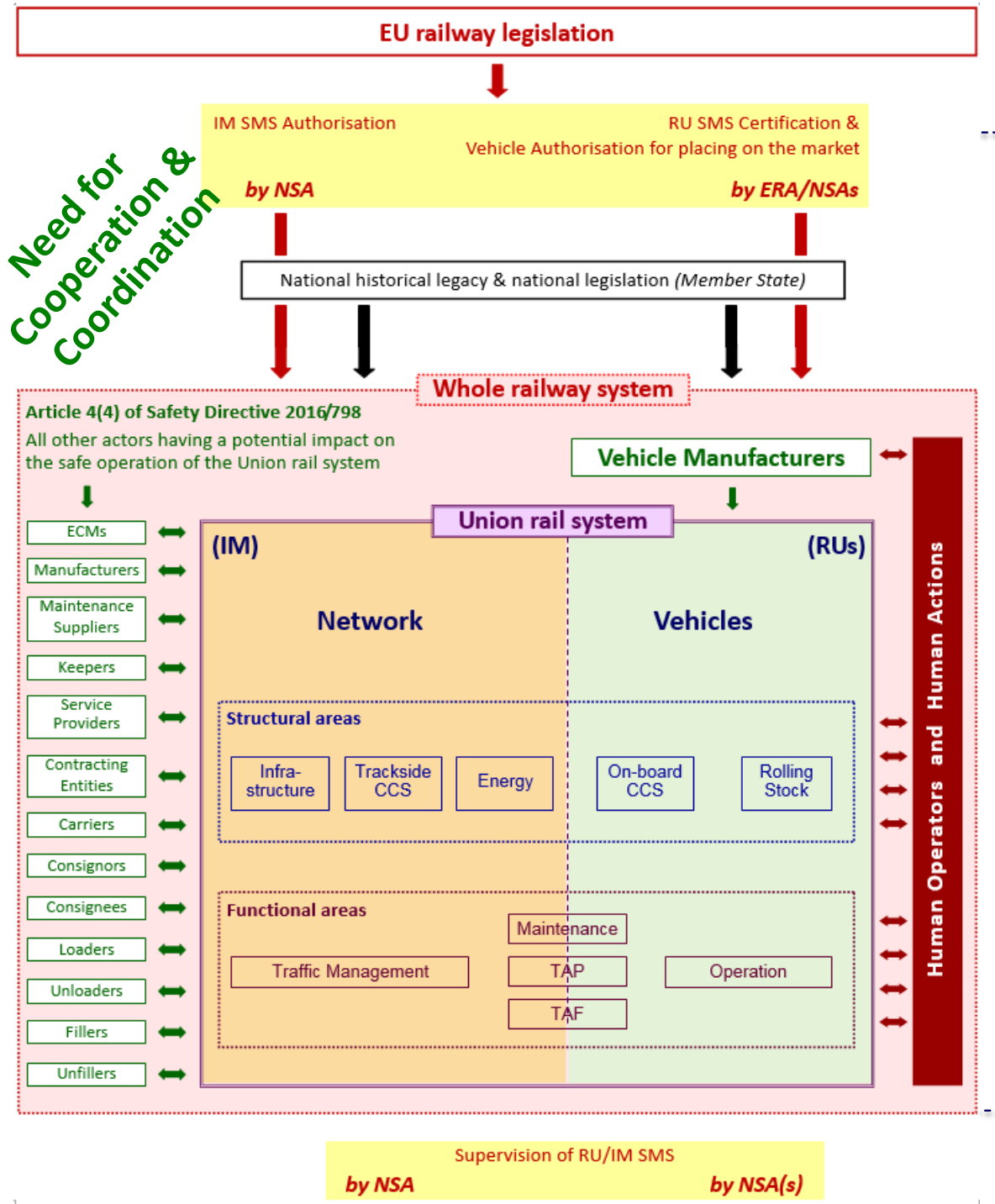
   So, usually one single actor was in charge of safe design, implementation, authorisation and safe management of railway operation, infrastructure and traffic management and all maintenance activities (vehicles and network) → **it had the full knowledge and responsibility for proper control of all railway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

SYSTEM level

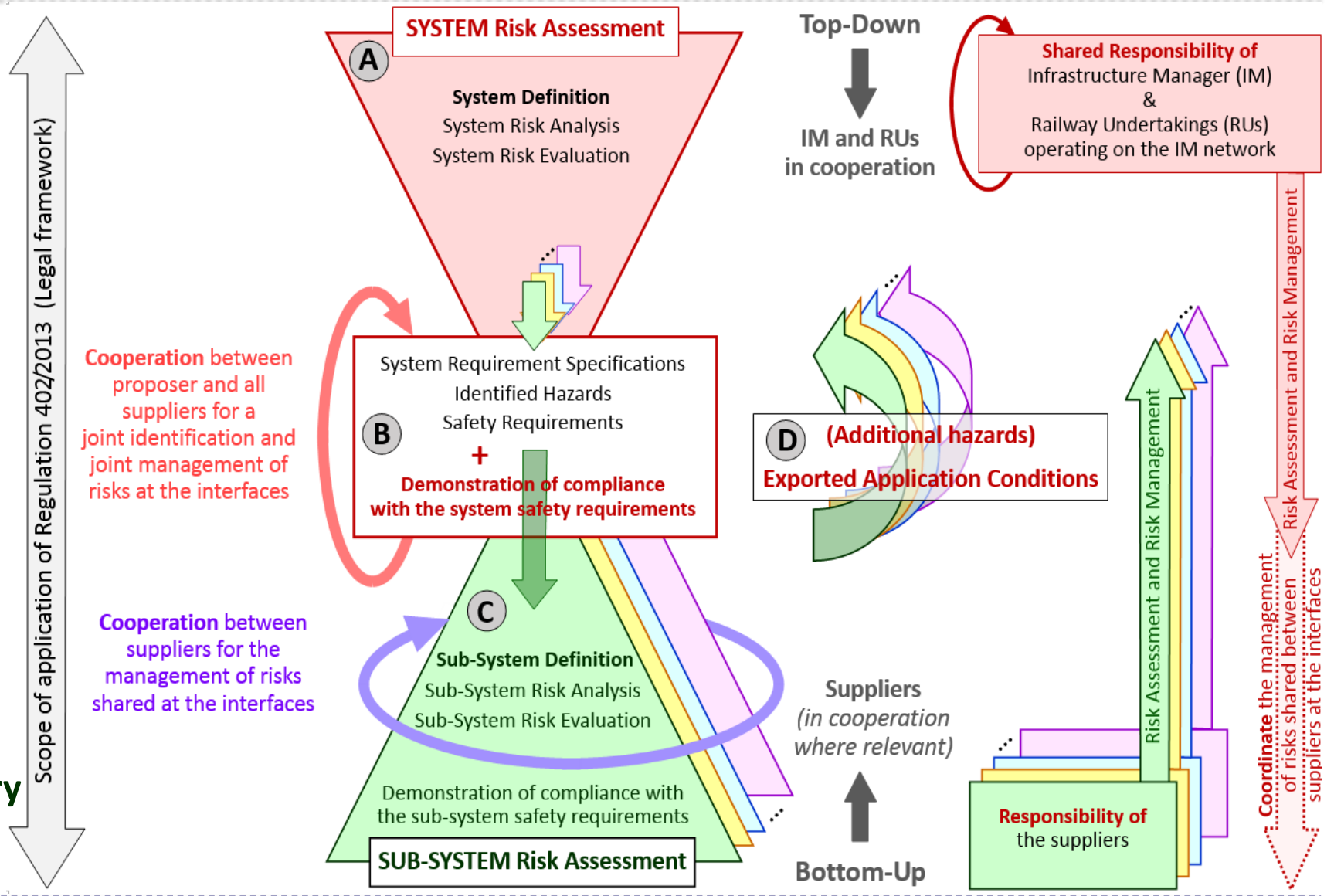
Concepts from

Figure 1 of CENELEC 50126-2:2017

&

Figure A.2 of CENELEC 50129-2:2018

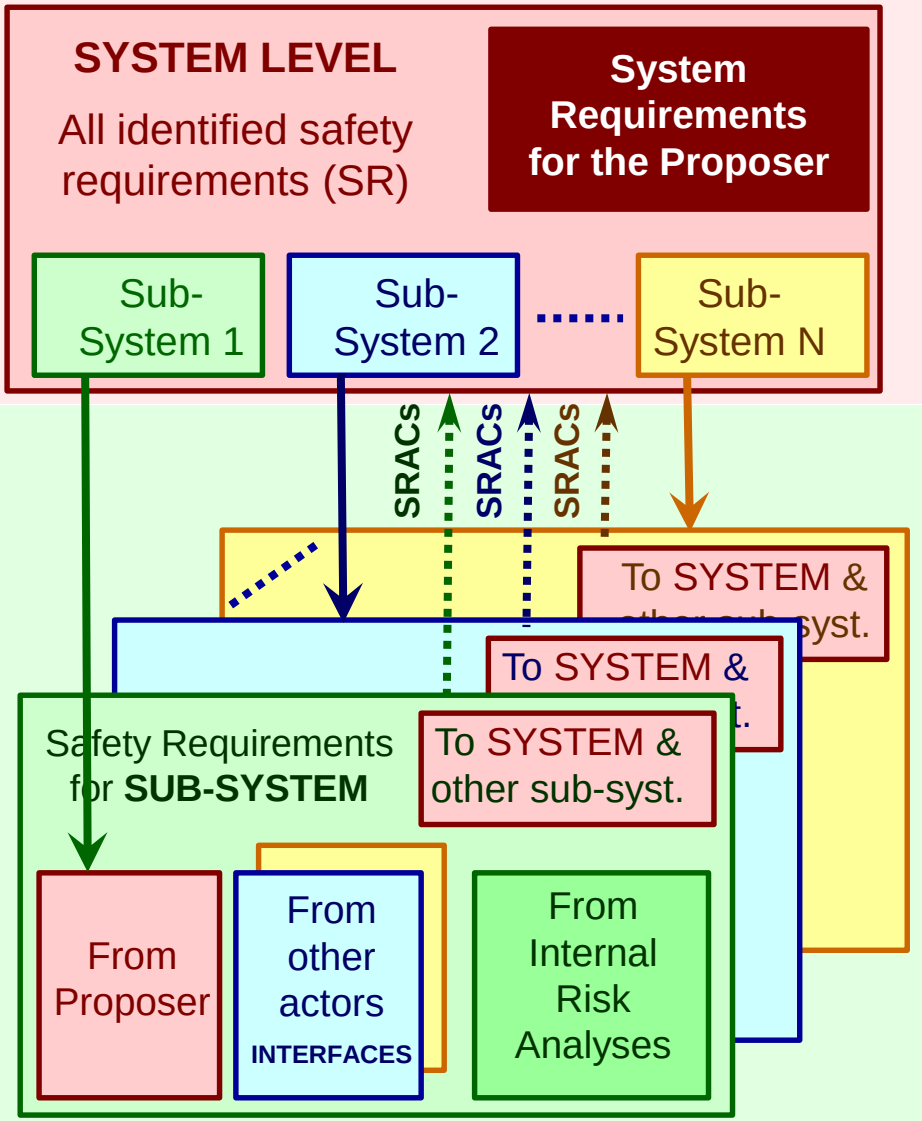
At level of every SUB-SYSTEM



System Risk Assessment (*top-down approach*) and Sub-System Risk Assessments (*bottom-up approach*)

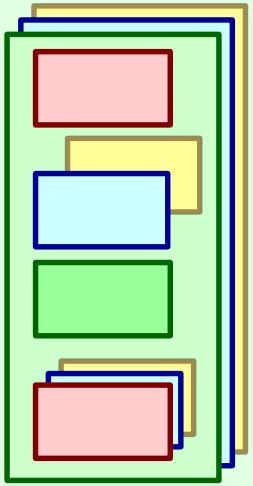
At the level of the RAILWAY SYSTEM, systematic top-down "system based approach":

- 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**

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**

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

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

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**

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

AsBo

Compliance is mandatory

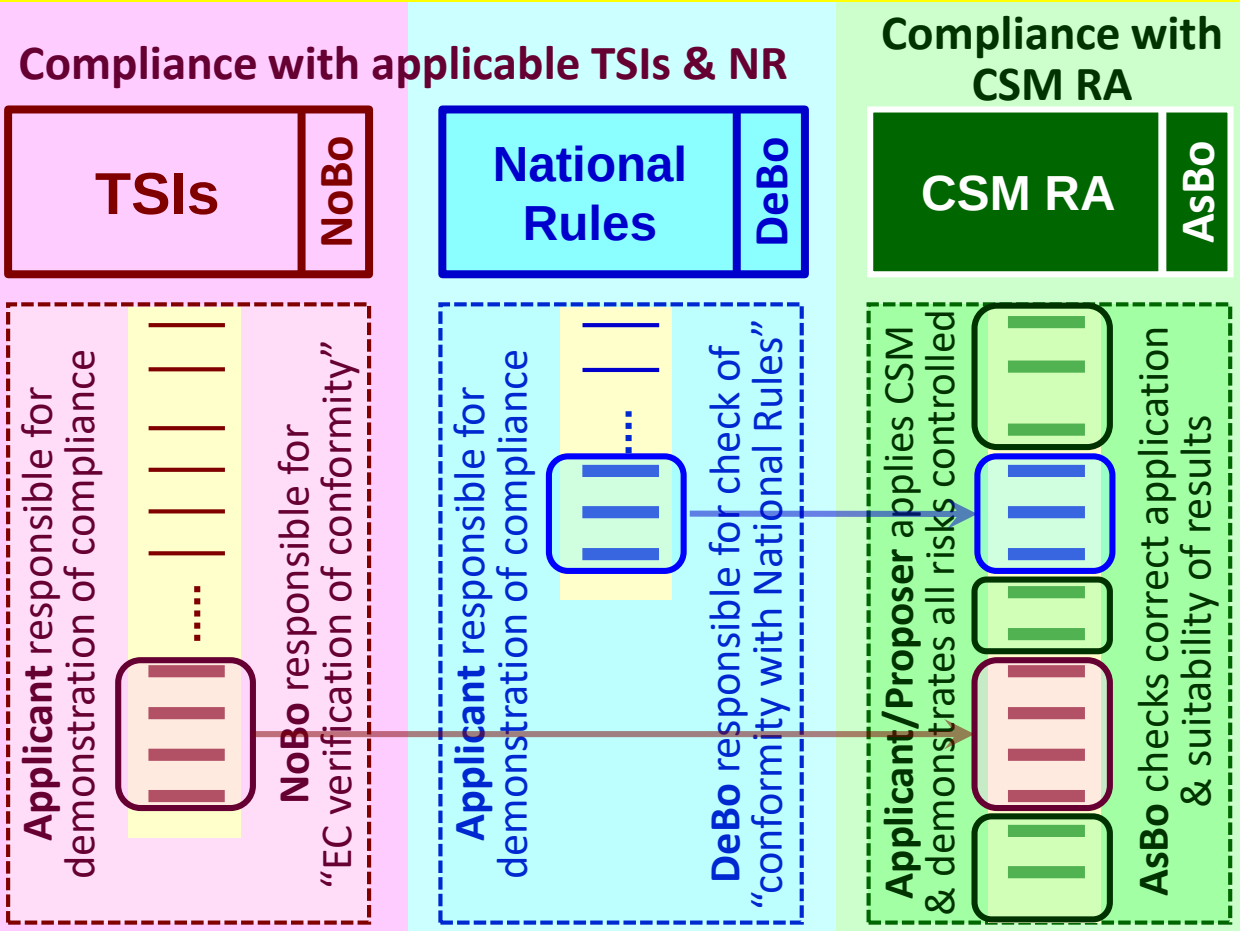
- TSIs contain essential requirements related to safety **as far as they are necessary for interoperability**
- Sole compliance with TSIs **does not ensure safety is fully covered** → additional risk assessment necessary
- **Only where necessary for interoperability purposes**, TSIs request application 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



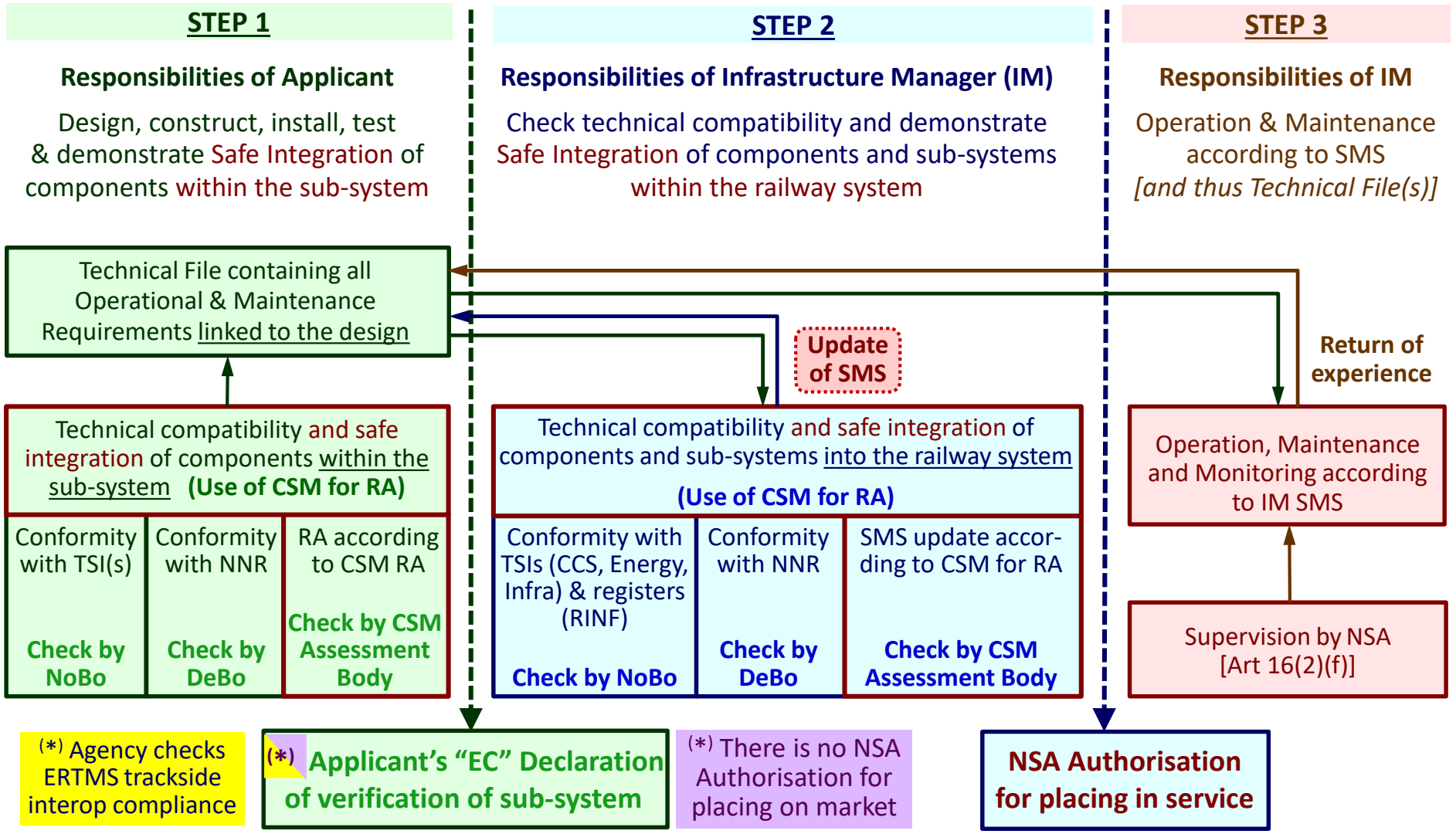
Applicant/Proposer applies its processes and demonstrates:

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

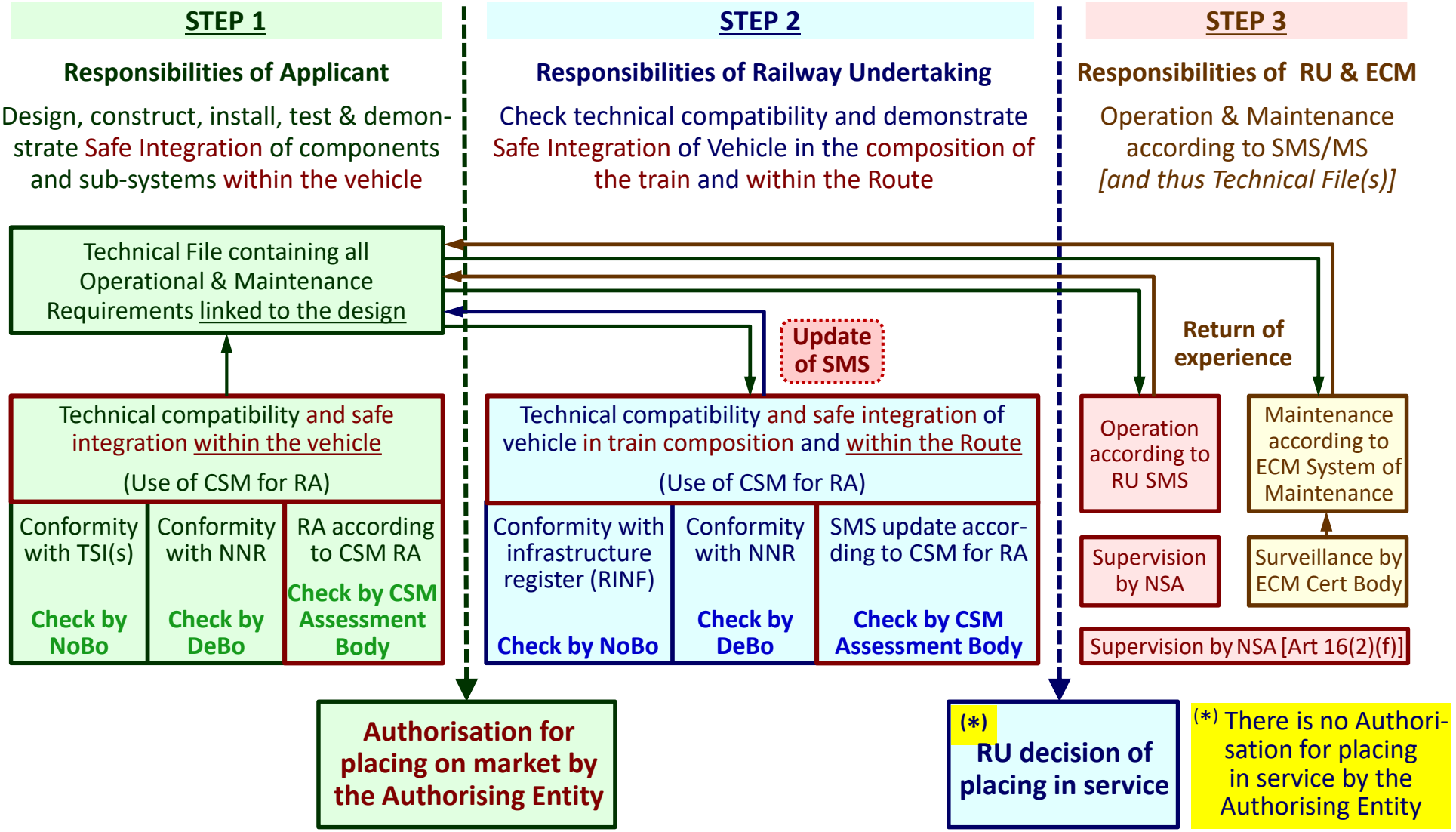
Authorising Entity (e.g. NSA) issues authorisation based on evidences of:

- 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 in service of fixed installations – Safe Integrations



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



Example of an Infrastructure Project

fitting a line with ERTMS

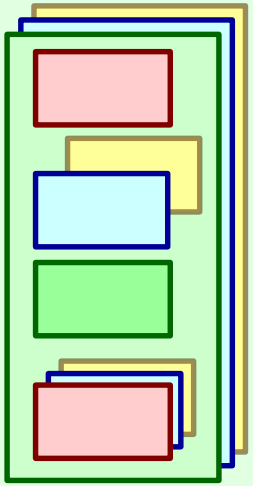
System Risk Assessment (*top-down approach*) and Sub-System Risk Assessments (*bottom-up approach*)

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**)



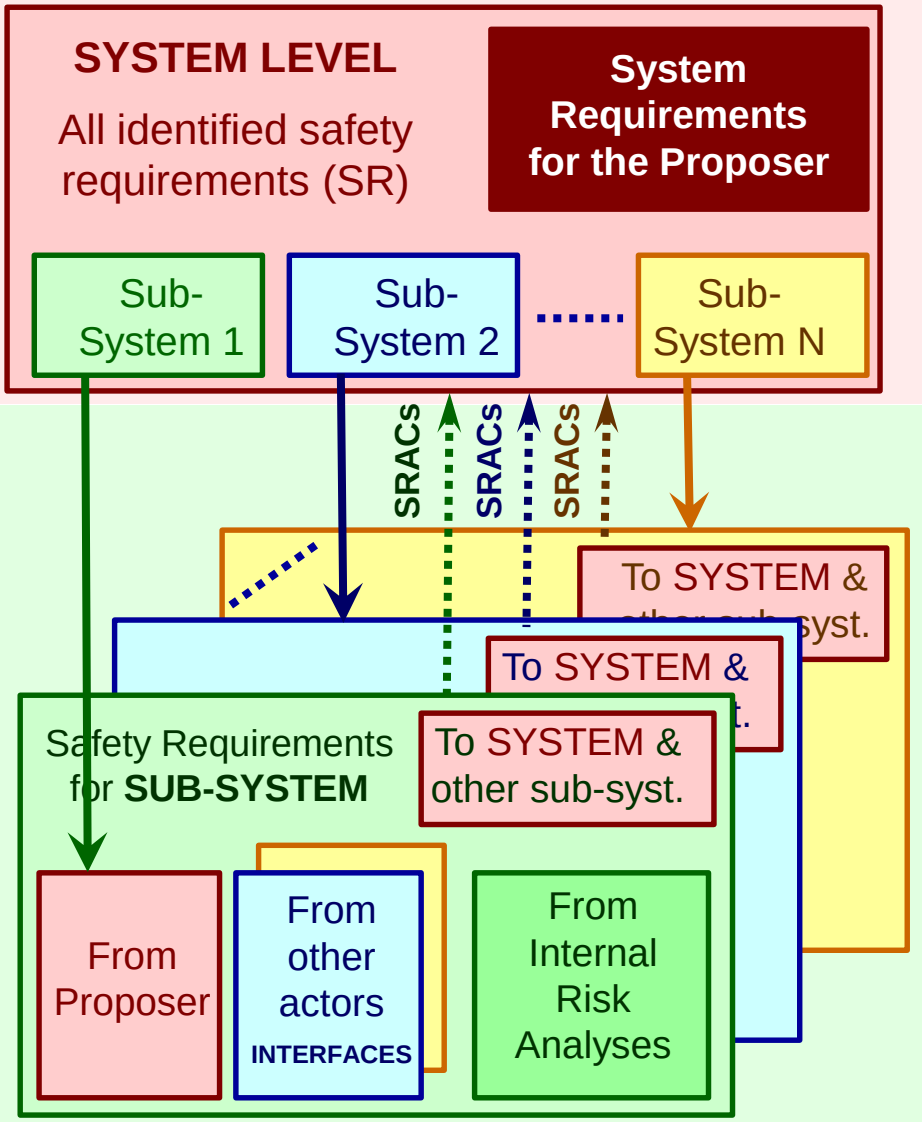
Requirements allocated to sub-system from the SYSTEM level

Requirements imported from other actors through shared interfaces

Internal requirements from own sub-system risk assessment

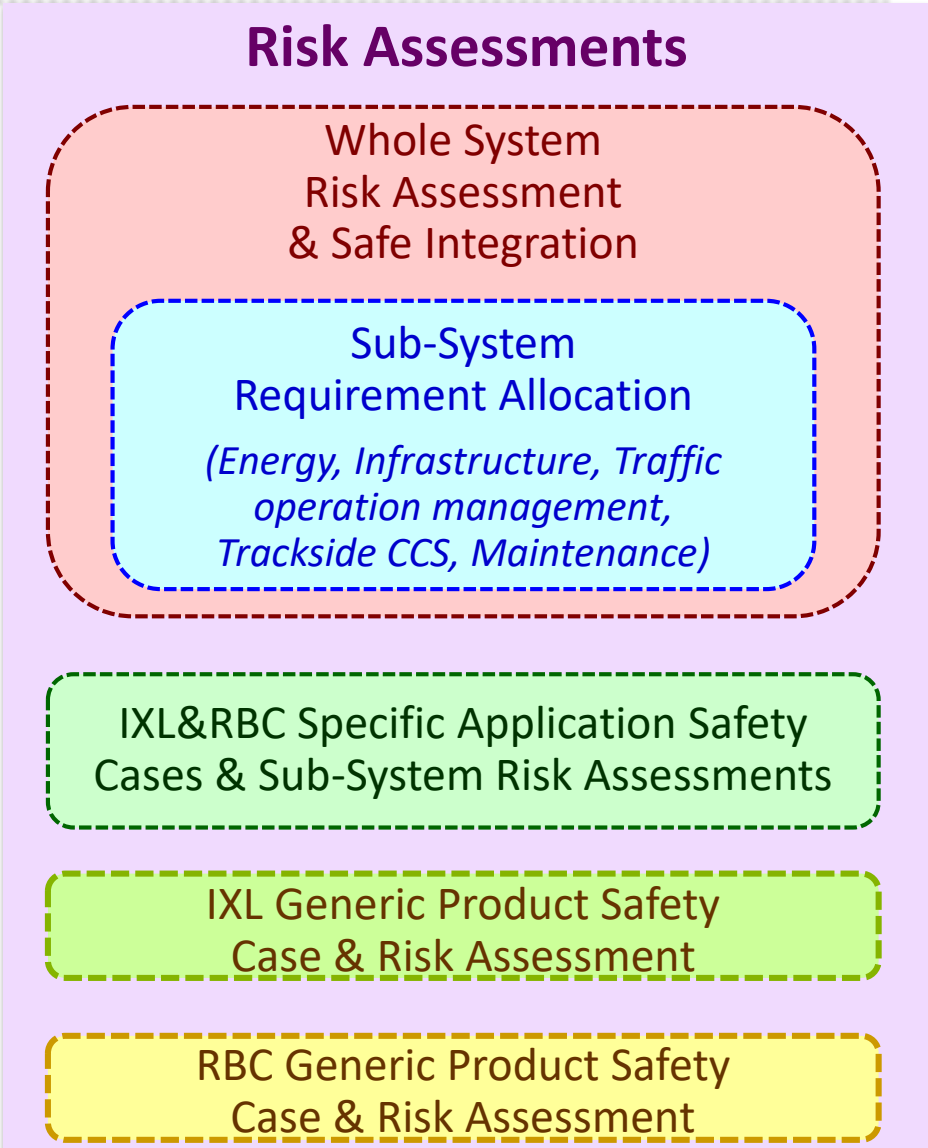
Requirements exported to SYSTEM (SRACs) and to other sub-systems (/actors) through shared interfaces

- **Sub-System AsBo**



System: build a new line fitted with ERTMS

- **Structural and functional sub-systems:**
  - Energy
  - Infrastructure
  - Traffic operation management
  - Trackside CCS
  - Maintenance
- **Existing products on the market:**
  - RBC
  - Interlocking, Track Circuits, Axle Counters
  - etc.



CSM Assessment Bodies (**AsBo**) and Independent Safety Assessment

System Architecture

Independent assessment

SYSTEM AsBo →

- System: new line to be fitted with ERTMS – Structural and functional sub-systems:
  - Energy
  - Infrastructure
  - Traffic operation management
  - Maintenance
  - Trackside CCS matters
  - Sub-System req^{mnt} allocation

Whole System Risk Assessment (including sub-system requirement specification) & Safe Integration

RBC Sub-System AsBo / **IXL Sub-System AsBo** →

- Interlocking + RBC (Level 2) parametrisation (configuration)

Specific Application Safety Cases & Risk Assessments

IXL Product AsBo (ISA?) →

- Interlocking Product

Generic Product Safety Case & Risk Assessment SRACs

RBC Product AsBo (ISA?) →

- RBC Product

SRACs Generic Product Safety Case & Risk Assessment

Mutual recognition of the Independent Safety Assessment Reports from the different CSM Assessment Bodies (**AsBo**)

Independent Safety Assessment Reports

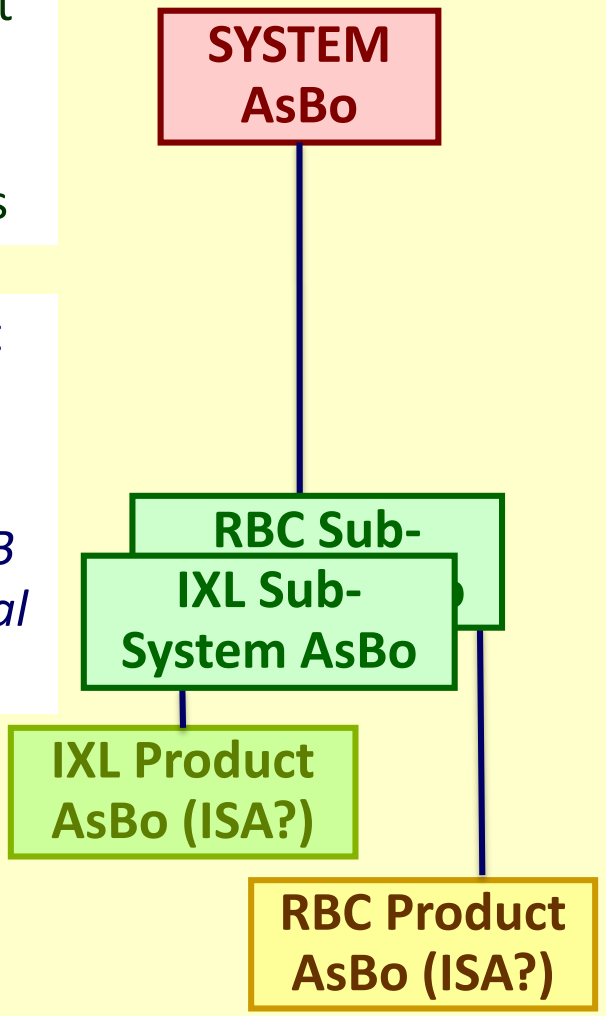
SYSTEM AsBo Report

Mutual recognition obligatory for sub-system AsBo reports

CENELEC ISA Report

Mutual recognition non-obligatory

(Possible but CSM AB can request additional checks)



Independent assessment

Whole System Risk Assessment & Safe Integration

Sub-System Requirement Allocation

(Energy, Infrastructure, Traffic operation management, Trackside CCS, Maintenance)

IXL&RBC Specific Application Sub-System Safety Cases & Risk Assessments

IXL Generic Product Safety Case & Risk Assessment

SRACs

SRACs

RBC Generic Product Safety Case & Risk Assessment

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