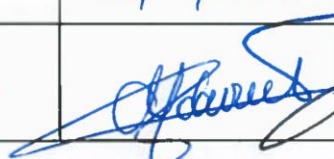
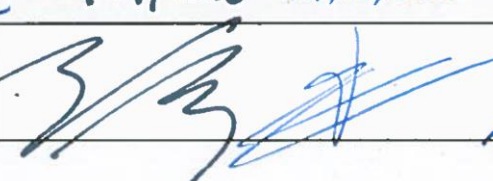
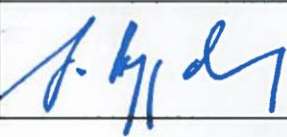


## Clarification Note on *Safe Integration*

	Drafted by	Validated by	Approved by
Name	Dragan JOVICIC	Bart ACCOU Thierry BREYNE	Josef DOPPELBAUER
Position	Project officer	Head of Safety and Operations Unit a.i. Head of PAD Unit	Executive Director
Date	06/01/2020	06/01/2020 14/01/2020	14.1.2020
Signature			

### Document History

Version	Date	Comments
1.0	06/01/2020	First version of the document

*The purpose of this document is to provide the European railway stakeholders with information in regards to the application of the Commission Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment. The clarifications contained in this document may be integrated in the next revision of either the legal text or the associated guidelines without prejudice of the formal process foreseen for updating the guidelines.*

*The present document is a non-legally binding guidance of the European Union Agency for Railways. It represents the views of the European Union Agency for Railways and not those of other EU institutions and bodies. It is without prejudice to the decision-making processes foreseen by the applicable EU legislation. Furthermore, a binding interpretation of EU law is the sole competence of the Court of Justice of the European Union.*

## Table of content

Table of content .....	2
List of Figures.....	2
1. Description of the issue : “concept of safe integration” .....	3
2. Clarifications on safe integration .....	4
2.1. Prerequisites .....	4
2.2. Independent safety assessment of the safe integration.....	4
2.3. Levels of safe integration vs. the architecture of a system.....	5
2.4. Architecture of the railway system and responsibilities for the safe integration.....	7
2.5. Risk assessment, risk management and safe integration at the level of the whole railway system .....	11
2.6. Risk assessment, risk management and safe integration at the level of a sub-system (e.g. a structural sub-system or any modified part of the railway system) .....	15
2.7. Conclusion.....	17
3. Legal background .....	19

## List of Figures

<i>Figure 1: Different levels of safe integration within the architecture of a system. ....</i>	<i>6</i>
<i>Figure 2: Overall architecture of the whole railway system and all involved railway actors. ....</i>	<i>8</i>
<i>Figure 3: Global overview of the risk assessment activities according to the Commission Implementing Regulation (EU) 402/2013. ....</i>	<i>13</i>

## 1. Description of the issue : “concept of safe integration”

- 1.1. The EU railway stakeholders have different understandings of the concept of “safe integration”. Safe integration is often and wrongly understood only as the demonstration of the technical compatibility and of the correct technical interfacing between sub-systems [e.g. check of technical compatibility between the vehicle and the network(s)]. In practice, safe integration is an inherent part of a systematic risk assessment and risk management process<sup>(1)</sup>, also within every structural sub-system. The concept of "safe integration" has thus a broader meaning and goes beyond the single check of the technical compatibility, or correct technical interfacing, between several sub-systems brought together. Safe integration applies also at different levels and to the entire life cycle of the design, operation, maintenance and disposal/decommissioning of the railway system and of its components.
- 1.2. These different points of view currently lead not only to different ways of demonstrating the safe integration but also more problematically to different levels of completeness of the demonstration. Consequently, this inevitably leads to difficulties in mutually recognising the results of the safe integration of a change to the railway across the Member States of the European Union.
- 1.3. The purpose of this document is to :
- (a) provide a harmonised understanding of the “concept of safe integration”;
  - (b) explain how to use the Commission Implementing Regulation (EU) No 402/2013 on the common safety method for risk assessment to demonstrate the safe integration of a change;
  - (c) lay the foundation for mutual recognition of the demonstration of safe integration across the EU.
- 1.4. Indeed, generally speaking, whenever a new element is introduced into a system<sup>(2)</sup>, or an existing element is modified<sup>(3)</sup>, regardless of the significance of that change, the safe integration and the risk assessment and risk management must always be performed. They have to 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) where applicable, the impacts of human and organisational aspects on the operation and maintenance of that element and on the system 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 unintended, adverse and unacceptable effects on the safety of the resulting system into which it is being incorporated.
- 1.5. Safe integration of a change is therefore not a separate and additional set of tasks to the regular risk assessment and risk management activities.

<sup>(1)</sup> *In order to identify, control and manage all risks arising from a change, section § 1.2.7 in Annex I of Commission Implementing Regulation (EU) 402/2013 on the CSM for risk assessment requires that safe integration is systematically an inherent part of the proposer’s risk assessment and risk management process.*

<sup>(2)</sup> *In the present sentence, the term “system” is used under the same meaning as in Article 3(25) of Commission Implementing Regulation (EU) 402/2013 where it is defined as :  
“system means any part of the railway system which is subjected to a change whereby the change may be of a technical, operational or organisational nature”.*

<sup>(3)</sup> *Modifications of the railway system could be technical, operational or organisational. They could be either the introduction of a new element, or the modification of an existing one, such as modifications to vehicles, network projects, structural sub-systems, operational or maintenance procedures, or to any part, component or constituent of those ones.*

## 2. Clarifications on safe integration

### 2.1. Prerequisites

- 2.1.1. An exhaustive “system definition” of the intended change is the most pertinent and most critical for a comprehensive risk assessment, risk management and safe integration. With reference to section § 2.1.3. below, the system definition of the change shall describe clearly and completely all interfaces between the “change/system under assessment” and the human operators and the different parts, components, constituents or sub-systems to which it interfaces<sup>(4)</sup>.
- 2.1.2. When incorporating a new element into the railways, or modifying an existing one (e.g. use of new technology involving a new actor or requiring new human interventions/actions), the proposer must pay attention to describe clearly and completely the change, as well as the limits of the railway system where the change is integrated. The “system definition of the change” must thus identify and describe clearly and completely :
- (a) all new/modified physical and functional interfaces between the new/modified element and the external world, i.e. the rest of the railway system;
  - (b) the precise extent of the “railway system” as it depends on the area of operations. Indeed, the railway system to consider can include parts of railways outside the borders of a country (e.g. cross-border operations or train operation until the border station of a neighbouring state).
- 2.1.3. The definition of the element, i.e. of the system under assessment, has also to identify and describe unambiguously all physical, functional, environmental, operational, and maintenance interfaces. Section § 2.1.2 in the Annex I of the Commission Implementing Regulation (EU) 402/2013 explicitly requires that the following points are properly addressed :
- (a) the objectives (intended purpose) of the system under assessment;
  - (b) the functions and elements, where relevant (including technical, human/organisational and human/operational elements) of the system under assessment;
  - (c) the boundaries of the system under assessment, including other interacting sub-systems;
  - (d) the physical (interacting sub-systems) and functional (input and output) interfaces with the external world. This has to include :
    - (1) the interfaces with the other sub-systems and humans interacting with the system under assessment;
    - (2) the operational and maintenance interface requirements with the system under assessment (e.g. for preventive and corrective maintenance);
  - (e) the environment (for example energy and thermal flow, shocks, vibrations, electromagnetic interference, operational use) of the system under assessment;
  - (f) the existing safety measures and, after the necessary relevant iterations of the identification of hazards and risk control measures, the safety requirements identified by the risk assessment process;
  - (g) the assumptions that determine the limits of the risk assessment.

### 2.2. Independent safety assessment of the safe integration

- 2.2.1. Regardless of whether the change under consideration is significant or not, the safe integration of the change into the railway system is necessary. Thereby, the proposer must demonstrate that the risk assessment and risk management of the change include also the safe integration.

---

<sup>(4)</sup> See points § 1.1.1 and § 2.1.2 in Annex I of Commission Implementing Regulation (EU) 402/2013.

2.2.2. When the change under assessment is considered significant by the application of Article 4 of the Commission Implementing Regulation (EU) 402/2013, the proposer must also appoint an independent assessment body<sup>(5)</sup> (AsBo). The AsBo is responsible for the independent assessment of :

- (a) the overall consistency of the proposer's risk assessment and risk management, and;
- (b) the safe integration of the change into the railway system as a whole<sup>(6)</sup>.

By virtue of sections § 1.1.7 and § 1.2.1 in Annex I of the Commission Implementing Regulation (EU) 402/2013, the verification of the correct consideration of all interfaces in the proposer's risk management<sup>(7)</sup> is to be subject to in-depth independent assessment.

### 2.3. Levels of safe integration vs. the architecture of a system

2.3.1. The construction of any new equipment composed of multiple smaller parts, or the introduction of a new or a modified element into an existing system<sup>(8)</sup>, is a common development activity. Regardless of the level at which such development takes place, safe integration is necessary at every level to ensure the safe achievement of the expected functionality and to demonstrate that the change does not create unintended, adverse and unacceptable effects on the safety of the overall system.

2.3.2. Figure 1 here below illustrates this later concept. It gives an example where :

- (a) a sub-system B is part of a system. The sub-system B is modified;
- (b) the designer of the sub-system B must be allocated by the actor in charge of the system :
  - (1) the operational and maintenance requirements in order to take them into account in the design of the sub-system B;
  - (2) the interface requirements with the sub-systems A and C, i.e. the information the sub-system B is expected to deliver to sub-systems A and C, and the information the sub-system B is expected to receive from sub-systems A and C;
- (c) the sub-system B is composed of multiple smaller internal parts :  $P_{1B}, P_{2B}, P_{3B}, P_{4B}, P_{5B}, \dots, P_{nB}$ ;
- (d) all those internal parts must be safely integrated at the level of the sub-system B;
- (e) the risk assessment and risk management of sub-system B have to identify all requirements necessary for :
  - (1) the safe integration and the safe use of the sub-system B with the sub-systems A and C to which it interfaces;
  - (2) the safe integration, the safe operation and safe maintenance of the sub-system B within the overall system into which it is incorporated.

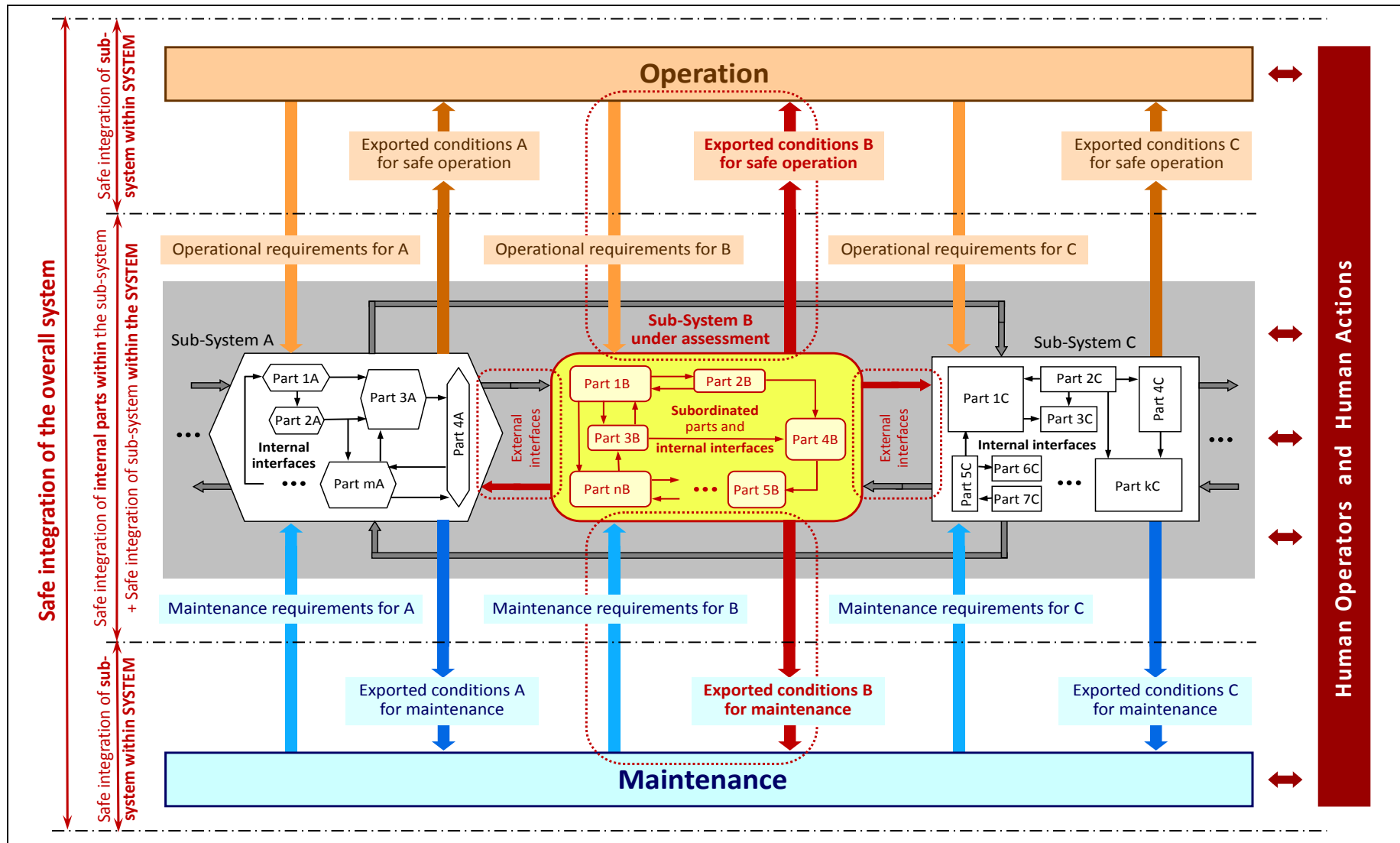
(5) In the framework of the Commission Implementing Regulation (EU) 2018/545 on the practical arrangements for the railway vehicle authorisation and railway vehicle type authorisation process, the independent assessment body (AsBo) is referred to as "assessment body (CSM RA)". Those two wordings designate thus the same body.

(6) Requirements in Article 6, point 1.1.7 in Annex I and point 3 in Annex II of Commission Implementing Regulation (EU) 402/2013.

(7) The AsBo has to independently assess that the proposer's risk assessment and risk management systematically identify :

- (a) all impacts and risks arising across the interfaces with other subsystems and with other impacted actors (i.e. both impacts on the existing risks and the new risks);
- (b) the sub-system/actor which has to control each of those shared risks.

(8) The concepts of the breakdown structure of a system into its constituent parts are explained in section § 5.2.1. of the CENELEC EN 50126-1:2017 standard.



**Figure 1: Different levels of safe integration within the architecture of a system.**

## 2.4. Architecture of the railway system and responsibilities for the safe integration

2.4.1. Taking into account the general principles above, every railway actor<sup>(9)</sup> who is involved in the design, operation, maintenance or disposal/decommissioning of any part of the railway system is also responsible for the safe integration of its part of the railway system. Demonstration of safe integration and of correct risk assessment and risk management are thus needed at any level of the railway system :

- (a) for any new or modified element, component or constituent of a system;
- (b) for a new or modified existing structural or functional sub-system;
- (c) for changes of the overall railway system.

2.4.2. The architecture of the railway system is however quite complex, and the safe operation and the safe traffic management are highly dependent on :

- (a) the safety of the contributing technical sub-systems, and;
- (b) the safe organisation and correct sharing of roles and responsibilities between the various stakeholders defined in the European railway legislation;

2.4.3. A correct risk assessment and risk management, and therefore a comprehensive safe integration of a change in the railway system, strongly depend on the correct understanding of :

- (a) the physical, functional, environmental, operational and maintenance context of the change;
- (b) all interrelations and dependencies of the change with the rest of the railway system;
- (c) the roles and responsibilities of every involved stakeholder.

2.4.4. The European legislation on the railway market opening, and the subsequent restructuring of the European railway sector, have changed<sup>(10)</sup> significantly the organisation and the sharing of roles and responsibilities between the (new) railway actors (see Figure 2 here below) : national safety authority (NSA - usually the former safety authorisation department of the state railway company), separation between the infrastructure manager(s) and the railway undertakings, definition of entities in charge of maintenance, manufacturers, service providers, contracting entities, etc.

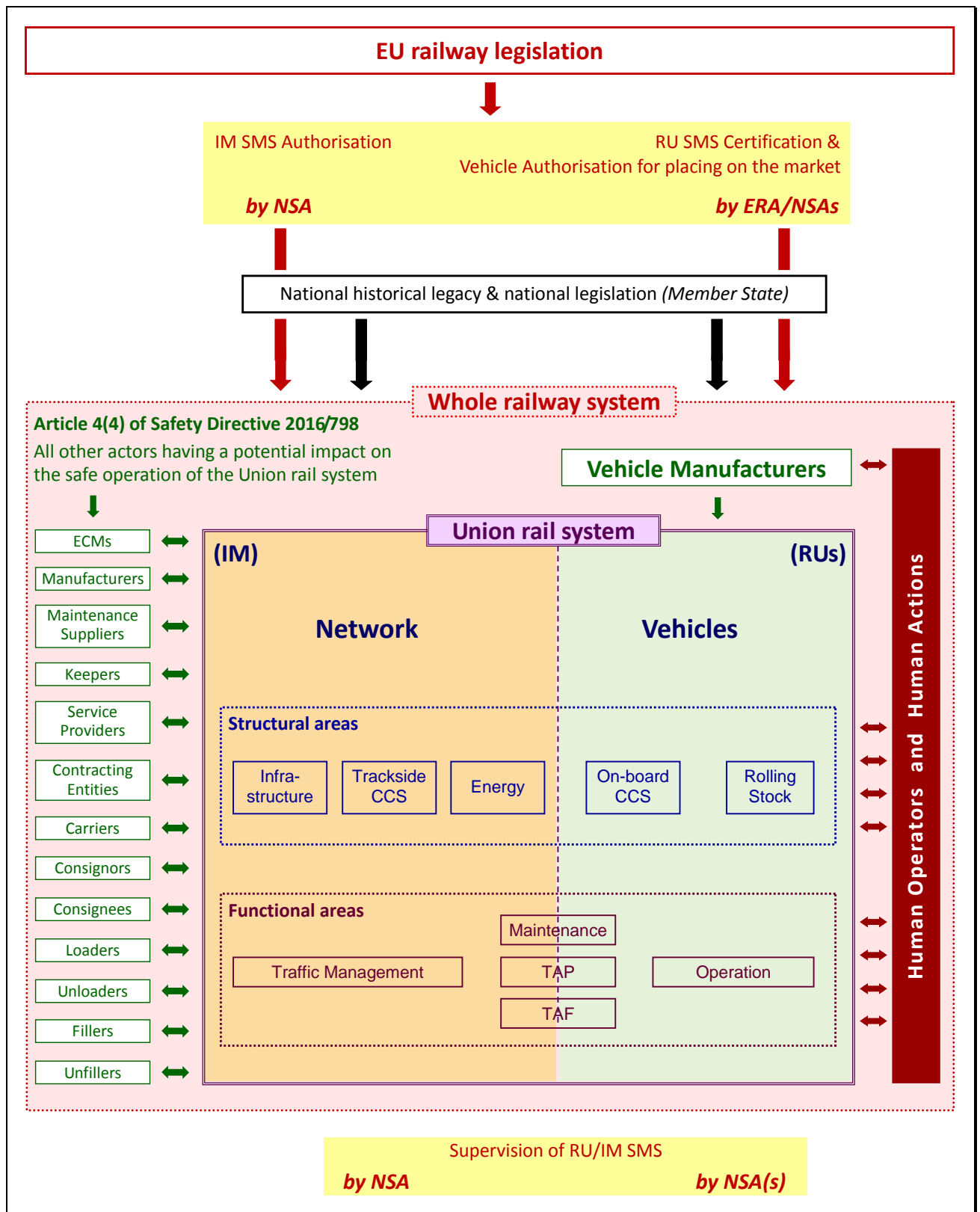
The responsibility for the safe operation and safe traffic management of the former railway system of a country, and the proper control of the associated risks, **does not rest on a single railway actor**. The infrastructure manager and all railway undertakings operating on its network are sharing, each one for its part of the system, that responsibility.

2.4.5. Figure 2 visually represents the overall architecture of the railway system and all actors who have a potential impact on the safe operation of the railway system. It is built from definitions (1), (3), (4) and (5) in Article 2 and information in Annexes I and II of the Interoperability Directive (EU) 2016/797, as well as from Article 4(4) of the Safety Directive (EU) 2016/798.

<sup>(9)</sup> For example safe integration is necessary at the level of :

- (a) an applicant/ manufacturer for a vehicle authorisation for placing on the market;
- (b) a manufacturer for the design and placing on the market of an interoperability constituent, a structural sub-system or any other technical equipment;
- (c) a railway undertaking for the introduction of a new vehicle type into operation or the development of safety management system procedures (e.g. checks of train set compositions, checks of environmental conditions and requirements, pre-departure checks, etc.);
- (d) an infrastructure manager for the design of new infrastructure lines or the upgrade of existing lines;
- (e) an entity in charge of maintenance (ECM) for the development of the processes and procedures of their system of maintenance or for the safe management of the obsolescence of spare parts;
- (f) etc.

<sup>(10)</sup> A single railway company is no more in charge alone of the safe design, safe implementation, safe homologation of vehicles, safe management of railway operation, safe management of the infrastructure and safe maintenance activities of both vehicles and network.



**Figure 2: Overall architecture of the whole railway system and all involved railway actors.**

(\* Figure 2 is built based on the definitions (1), (3), (4) and (5) in Article 2 and the Annexes I and II of the Interoperability Directive (EU) 2016/797, as well as on Article 4 of the Safety Directive (EU) 2016/798.



2.4.6. For the purposes of this document and for proper risk assessment, risk management and safe integration of a change (see section § 1.4.), the terminology “*overall railway system*” or “*railway system as a whole*” designates more than only the “Union rail system” as defined in Article 2(1)<sup>(11)</sup> of the Interoperability Directive (EU) 2016/797. As shown in Figure 2, the whole railway system includes all the interfaces and interrelations between all functional and technical sub-systems, as well as all actors which contribute to the safe operation and the safe traffic management of the railway system, i.e. :

- (a) all elements of the “Union rail system” as defined in Article 2(1) of the Interoperability Directive (EU) 2016/797;
- (b) all other actors who have a potential impact on the safe operation of the railway network and of vehicles (refer to Article 4(4) of the Safety Directive (EU) 2016/798), and;
- (c) the human operators and human actions involved in the safe operation, the safe traffic management and the safe maintenance of the railway system.

As emphasised in bullet (b) of section § 2.1.2. above, the railway system where the change is integrated can include parts of railways outside the borders of a country (e.g. cross-border operations or train operation until the border station of a neighbouring state).

#### 2.4.7. Legal obligations for cooperation between the railway stakeholders

Article 4(1) of the Safety Directive (EU) 2016/798 requires explicitly “ *... that railway safety is generally maintained and, where reasonably practicable, continuously improved*” during and after the market opening. To achieve that goal, the infrastructure manager and railway undertakings are required 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 (e.g. manufacturers of vehicles).

The Safety Directive (EU) 2016/798 also clearly identifies the following requirements (these requirements are not new; they were already part of the Safety Directive 2004/49/EC) :

- (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 – See Figure 3;
- (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...*“;

<sup>(11)</sup> According to Annex I of Interoperability Directive 2016/797, the **elements of the Union rail system** are the “**network**” and “**vehicles**”.

According to the definitions (3), (4) and (5) in Article 2 of the Interoperability Directive (EU) 2016/797 :

- (a) ‘vehicle’ means a railway vehicle suitable for circulation on wheels on railway lines, with or without traction; a vehicle is composed of one or more structural and functional subsystems;
- (b) ‘network’ means the lines, stations, terminals, and all kinds of fixed equipment needed to ensure safe and continuous operation of the Union rail system;
- (c) ‘subsystems’ means the structural or functional parts of the Union rail system, as set out in Annex II of the Interoperability Directive (EU) 2016/797;

According to Annex II of the Interoperability Directive (EU) 2016/797, the system constituting the Union rail system may be broken down into the following subsystems, either :

- (d) structural areas : infrastructure, energy, trackside control-command and signalling, on-board control-command and signalling, rolling stock; or
- (e) functional areas : operation and traffic management, maintenance, telematics applications for passenger and freight services.

- (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 Commission Implementing Regulation (EU) 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***”:
- (1) Article 4(4)(a) : “*implement the necessary risk control measures, where appropriate **in cooperation with other actors***”;
  - (2) 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*”;

#### 2.4.8. Sharing of responsibilities for the risk assessment, risk management and safe integration :

Taking into account the explanations in sections § 2.4.4., § 2.4.5., § 2.4.6. and § 2.4.7. above, and the principles illustrated in Figure 1 above, the responsibilities for the safe integration are the following with respect to the different levels of granularity of the railway architecture listed in section § 2.4.1. :

- (a) the infrastructure manager and all railway undertakings operating on its network share the responsibility, each one for its part of the system, for the **safe management of changes to the “overall railway system” or “railway system as a whole”** (terminology : see section § 2.4.6.).

To do that, according to Article 4(1) of the Safety Directive (EU) 2016/798 (reminded in section § 2.4.7.), the infrastructure manager and railway undertakings must **apply a “system-based approach”** and “**... where appropriate ...” cooperate “... with each other”**. Where necessary, they must also involve all other railway actors who have a potential impact on the safe operation of the railway system.

By virtue of sections § 1.1.5, § 1.2.1 and § 2.2.1 in Annex I of the Commission Implementing Regulation (EU) 402/2013 :

- (1) for a change of the network, or traffic management, the infrastructure manager is the leading proposer. It is responsible for involving all impacted actors, in particular all railway undertakings (contributory proposers) operating on its network, in a joint risk assessment, risk management and safe integration of the change into the overall railway system;
  - (2) for a change impacting the vehicle or the operation and maintenance of vehicles, the railway undertaking is the leading proposer. It is responsible for involving all impacted actors, in particular the infrastructure managers (contributory proposers) of the networks on which it is operating and the entities in charge of maintenance, in a joint risk assessment, risk management and safe integration of the change into the overall railway system;
- (b) for a **new or modified existing structural or functional sub-system**, the responsibility depends on the actor who initiates the change :
- (1) if the **change is part of a vehicle (rolling stock or on-board CCS) or operational**, the railway undertaking is the proposer. It is responsible for defining clearly the requirements to be fulfilled by the vehicle and/or its SMS, regardless whether a manufacturer actually implements the changes to the vehicle. The railway undertaking is also responsible for the safe integration of the change into the whole railway system;

- (2) if the **change is part of the network or traffic management**, the infrastructure manager is the proposer. It is responsible for defining clearly the requirements to be fulfilled by the network and/or its SMS, regardless whether a manufacturer actually implements the changes to the network. It is also responsible for the safe integration of the change into the overall railway system;
- (3) if the **change is a new structural or functional sub-system**, the proposer is the applicant (usually a manufacturer). The proposer/applicant is responsible for:
  - (i) the safe design of the structural sub-system according to the applicable TSIs, national rules, other EU laws, and all requirements identified by the proposer/applicant at the requirement capture stage;
  - (ii) the identification of the necessary operational and maintenance conditions for use;
- (c) for any **new or modified element, component or constituent of a system** (e.g. an internal part of a structural or functional sub-system), the actor<sup>(12)</sup> which initiates the change is the proposer. Depending on the case, the proposer is one or another of the actors listed in bullet point (b) above. Where relevant, that actor shall cooperate with the other impacted actors/sub-systems in order to :
  - (1) identify and manage jointly the hazards and related safety measures to be handled at the shared interfaces, and;
  - (2) identify jointly the potential impacts of the change on the other elements, components, constituents, structural or functional sub-systems of the railway system.

## 2.5. Risk assessment, risk management and safe integration at the level of the whole railway system

2.5.1. As explained above, the safe integration, and its independent assessment by an AsBo, are not separate activities from the proposer's risk assessment and risk management activities.

2.5.2. As represented in Figure 3 below, at the level of the whole railway system the risk assessment and risk management is a "top down process". As explained in section § 2.4.8. here above, the infrastructure manager and the railway undertakings which operate on its network share the responsibility for the coordination of the risk assessment, risk management and safe integration. They play together the role of the proposer defined in the Commission Implementing Regulation (EU) 402/2013

The system risk assessment and risk management shall be based on the definition and the architectural breakdown structure of the railway system (see Figure 2 and section § 2.1.2. above) and its specific environmental, operational and maintenance context (see Figure 1 above). It shall :

- (a) identify the system hazards/risks and the associated safety requirements for the system.

According to point § 1.2.1 in Annex I of the Commission Implementing Regulation (EU) 402/2013, for the interfaces with the operation and maintenance of the railway system, as well as for the interfaces between the different sub-systems and/or rail-sector actors, the proposer has to take care that :

- (1) the concerned actors cooperate in order to identify and manage jointly with the proposer the hazards and the related safety measures that need to be handled at those interfaces;

---

<sup>(12)</sup> *In the framework of Commission Implementing Regulation (EU) 2018/545 on the practical arrangements for the railway vehicle authorisation and railway vehicle type authorisation process, the actor which initiates the change is designated as the "entity managing the change".*

- (2) 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;
  - (3) safety requirements are not assigned to an actor beyond the scope of its responsibility and domain of control;
- (b) according to the architectural breakdown structure of the system, apportion the system functions and those system safety requirements down to the different contributing sub-systems and sub-contractors. *The functions and the safety requirements that cannot be sub-contracted (i.e. that cannot be cascaded down to any constituting sub-system) must clearly be identified as requirements to be fulfilled by the proposer at the level of the railway system;*
- (c) transfer clearly and formally the relevant functions and the apportioned safety requirements (i.e. the sub-hazards associated to the different contributing sub-systems) to every actor in charge of the development of the relevant sub-system. So, every actor is aware of its responsibilities and can take them forward under their own risk management procedures.

2.5.3. The risk assessment and risk management at the level of the whole railway system shall in particular take care of human operators and human actions in order to identify :

- (a) the operational risks and the associated requirements for training;
- (b) the risks associated with the maintenance of the railway system and the requirements for diagnostic functions and training of the maintenance staff;
- (c) in case of a stepwise migration from an existing system, element, constituent or component of it, depending on whether :
  - (1) the new system, element, component or constituent **replaces** the existing one;
  - (2) the new system, element, component or constituent is **superimposed** to the existing one;
  - (3) the new system, element, component or constituent **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 to be implemented.

Those 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.

Usually, a supplier alone, or even all suppliers together, cannot, using the bottom-up approach (see Figure 3 and section § 2.6. below), identify and control alone all those risks without the top-down system approach under the responsibility of the infrastructure manager and the railway undertakings

2.5.4. The actor in charge of the development of every sub-system is then responsible to :

- (a) demonstrate the compliance with the functional, technical and safety requirements apportioned to the sub-system which is under its area of responsibility;
- (b) identify and export all necessary operational and maintenance requirements to be demonstrated for the safe integration, use and maintenance of the considered sub-system : refer also to section § 2.6. here below.

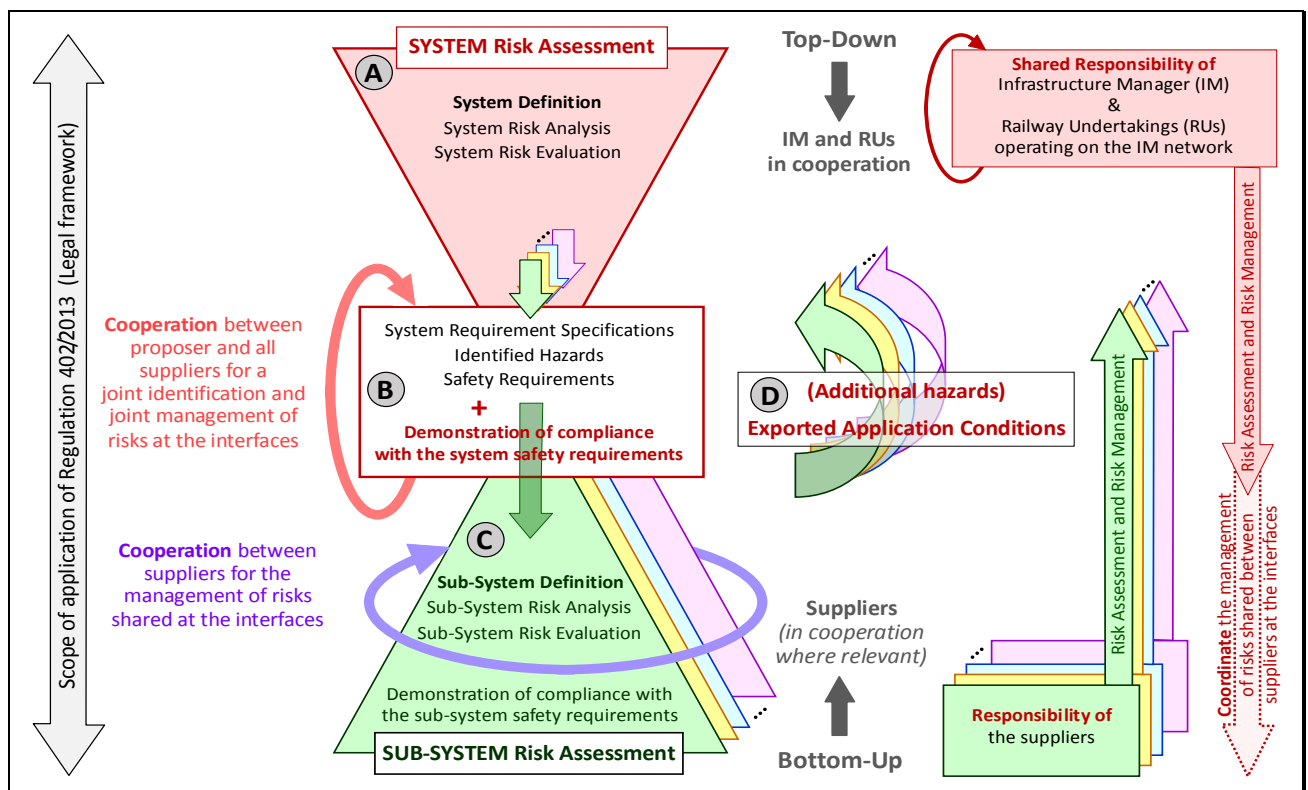
2.5.5. The proposer<sup>(13)</sup> in charge of the development of the railway system as a whole is also responsible for the overall coordination of the risk assessment and risk management : see Figure 3 below. This means that it is in charge of the following :

---

<sup>(13)</sup> The word “proposer” is used with the meaning of Commission Implementing Regulation (EU) 402/2013, i.e. the actor in charge to apply that Regulation and the risk management process defined therein for the part of the railway system falling under its area of responsibility.

- (a) the demonstration of fulfilment of the safety requirements that are not transferred to any supplier, or constituting sub-system, and that were allocated to the design, operation and maintenance of the railway system;
- (b) the coordination of the risk assessment and risk management of the different constituting sub-systems and of the associated results;
- (c) the demonstration of the appropriate risk control of every hazard/risk that is imported into the system from the risk assessments and risk managements of the suppliers and different constituting sub-systems. This can be done by either complying with the imported safety related application conditions/constraints (SRACs) or by defining other risk control measures that make the risk acceptable at the level of the railway system;

**Note:** This set of activities corresponds to the part of the safe integration to be demonstrated at the level of the railway system as a whole.



**Figure 3: Global overview of the risk assessment activities according to the Commission Implementing Regulation (EU) 402/2013.**

(\*) Figure 3 corresponds to the concepts from Figure 1 of CENELEC 50126-2:2017 and Figure A.2 of CENELEC 50129-2:2018 adapted to the risk management process in the Appendix of Annex I of the Commission Implementing Regulation (EU) 402/2013.

2.5.6. In general, the stakeholders responsible for changes of the design of the railway system, i.e. the infrastructure managers and railway undertakings, each one for its part of the system, **cannot thus be satisfied only with** :

- (a) cutting the overall system into a list of constituting sub-systems;
- (b) waiting for the suppliers to develop the different sub-systems and then just putting them together technically;

<p>(c) collecting the bottom-up exported safety related application conditions/constraints (SRACs) from the different constituting sub-systems/suppliers;</p> <p>(d) demonstrating the compliance with those safety related application conditions/constraints imported from the risk assessment of every constituting sub-system/involved actor.</p> <p>2.5.7. They must consider also the potential impacts of the considered change on :</p> <p>(a) the other unchanged elements, components, constituents, structural or functional sub-systems of the railway system;</p> <p>(b) the interfaces with those other elements, components, constituents of the railway system.</p>
<p>2.5.8. In addition to the routine changes of the railway system, there could be other types of changes that are not driven directly by a railway undertaking or an infrastructure manager. Typical examples are :</p> <p>(a) a financial consortium, or a regional public authority, which purchases a fleet of vehicles or trains from a manufacturer without consulting and involving the future railway undertaking(s), who will operate the vehicles, and the infrastructure manager on whose lines the vehicles will operate;</p> <p>(b) a regional public authority, or the Ministry, purchases the construction of a new, or the extension of an existing, (regional) railway line to a contractor without involving the infrastructure manager who will manage the traffic on the line.</p> <p>In order to manage properly these types of changes, and to improve the hazard identification and the proper preventive control of the associated risks, it is essential that the “procurement entity” also applies the top-down and system-based approach described in this paper. Right from the tender stage, and from the beginning of the project, the procurement entity should either involve the future operators (RUs) and the traffic manager (IM) in, or sub-contract to them, the proper management of the project. This gives the possibility to systematically identify early in the project the potential risks and to control the identified risks through technical improvements of the design instead of obliging the users to implement afterwards constraining operational and maintenance safety related application conditions for use.</p>
<p>2.5.9. In the absence of top-down system risk assessment and system risk management, some railway system hazards/risks might be non-identified and the associated system risk control measures missing. The proper risk assessments and risk managements of the constituting sub-systems cannot compensate the lack of proper risk identification and risk control at the level of the railway system.</p>

#### 2.5.10. **Independent safety assessment of safe integration**

At the level of the railway system, the system AsBo shall independently assess :

- (a) the overall organisation, management and coordination by the proposer of the development, risk assessment and risk management at the levels of both the railway system and the different contributing sub-systems;
- (b) the relevance and completeness of the risk assessment and risk management for the railway system as a whole;
- (c) the level of safety for the railway system as a whole;
- (d) the allocation by the proposer of the system functional, technical and safety requirements to the different contributing parts of the railway system, i.e. :
  - (1) the functions, requirements and hazards/risks to be managed directly by the proposer at the level of the railway system;
  - (2) the functions, requirements and hazards/risks allocated to every contributing sub-system and to be managed by the actor in charge of the development of the sub-system;

- (e) every concerned actor correctly understands the hazards/risks, functional, technical and safety requirements under their responsibility of control (i.e. proposer and all concerned actors);
- (f) the methods and resources deployed for demonstrating the compliance with the functional, technical and safety requirements :
  - (1) by the proposer for the system requirements that are not allocated to any contributing sub-system. This is the responsibility of the system AsBo;
  - (2) by every actor in charge of the development of a sub-system.

If every actor appoints a separate AsBo for assessing independently the sub-system under its responsibility, the system AsBo will cross accept the safety assessment report of the sub-system AsBo under the conditions of the Commission Implementing Regulation (EU) 402/2013. If there is no AsBo at the level of every sub-system, the proposer can ask the system AsBo to assess independently the risk assessment and risk management of every contributing part/sub-system;

- (3) by the proposer for the coordination and consolidation of the results imported from those sub-contractors, including the conclusions from the safety assessment reports of the respective AsBos of the contributing sub-systems. This includes the independent assessment of the following :
  - (i) the allocation of functional, technical and safety requirements to the contributing sub-systems (see bullet point (d)(2) above);
  - (ii) the demonstration of the appropriate risk control of every hazard/risk that is exported to the system by the risk assessment and risk management of the different sub-systems. This can be done by either complying with the exported safety related application conditions/ constraints (SRACs) or by defining other risk control measures that make the risk acceptable.

**Note :** *This set of activities corresponds to the part of the independent assessment of the safe integration to be carried out at the level of the railway system as a whole.*

## 2.6. Risk assessment, risk management and safe integration at the level of a sub-system (e.g. a structural sub-system or any modified part of the railway system)

- 2.6.1. As explained above, the safe integration, and its independent assessment by an AsBo, are not activities separate from the proposer's risk assessment and risk management activities.
- 2.6.2. As represented in Figure 3 above, at the level of either a sub-system or an element, component, constituent (*referenced here after as "sub-system under assessment"*) provided by a supplier, the risk assessment and risk management is a "bottom up process". As explained in section § 2.4.8. here above, the actor which initiates the change is responsible for coordinating the risk assessment, risk management and safe integration at the level of its sub-system. That actor plays the role of the proposer defined in the Commission Implementing Regulation (EU) 402/2013.

The sub-system risk assessment and risk management shall be based on a clear and complete sub-system definition (see explanations above and in particular section § 2.1.2.), the architectural break down structure of the sub-system and the environmental, operational and maintenance requirements specified at the level of the whole railway system (see Figure 1 above). In order to give the assurance that the sub-system under assessment fulfils safely all functional, technical and safety requirement objectives specified at the level of the whole railway system, the risk assessment and risk management of the sub-system under assessment must demonstrate that :

- (a) the risks arising from the design and the implementation of the sub-system under assessment are systematically identified, managed and controlled correctly to an acceptable level [the risks arising from the use and maintenance of the sub-system are covered in point (b) below]. This means that :
- (1) the safety requirements apportioned to the sub-system under assessment by the risk management at the level of the railway system are correctly captured and fulfilled;
  - (2) the hazards, and associated risks, imported through the interfaces shared with the other sub-systems or other involved actors, and which are to be controlled by the sub-system under assessment, are received from the relevant actors/sub-systems, correctly assessed and managed to an acceptable level (either by implementing the imported safety requirement(s) or risk control measure(s), or by identifying more appropriate ones);
  - (3) the proposer acknowledges the correct reception of those hazards, and associated risks, from the other sub-systems or other actors shared across the interfaces. And the proposer agrees to control and manage them at the level of the sub-system under assessment;
  - (4) all reasonably foreseeable hazards, and associated risks, that may arise from the design choices and the implementation of the sub-system under assessment are systematically identified and acceptable risk control measures (i.e. safety requirements) are defined. This includes the identification of hazards, and proper control of associated risks, required for the safe integration of all components or parts in the functional and technical architecture of the sub-system under assessment;
  - (5) the sub-system under assessment as a whole is then safely designed and implemented to fulfil all the safety requirements above (i.e. both those identified by the risk assessment and those imported from the system level or through the interfaces shared with the other sub-systems);
  - (6) the human and organisational elements are adequately considered and managed as part of the sub-system safe integration;

**Note :** *The correct consideration, assessment and demonstration of fulfilment of all those safety requirements, especially those resulting from the architecture of the sub-system (see bullet point (a)(4) above), correspond to the part of the safe integration to be done at the level of the sub-system under assessment;*

- (b) the risks arising from the operation and maintenance of the sub-system under assessment are systematically identified and managed. This means that :
- (1) the sub-system boundaries, interfaces and dependencies with the rest of the railway system are exhaustively addressed. The hazards and risks associated to the functions and the information shared across the interfaces with the other sub-systems or other involved actors are systematically identified<sup>(14)</sup> and managed jointly with those actors/sub-systems;
  - (2) the hazards, and associated risks, shared across the interfaces with the other sub-systems or other involved actors that cannot be controlled at the level of the sub-system under assessment are transferred to the relevant actors in charge of implementing the identified safety requirement(s) [or risk control measure(s)];
  - (3) the actors to whom the shared hazards/risks, and associated safety requirements [or risk control measure(s)] are transferred acknowledge the reception of the information and agree to control the associated risks<sup>(15)</sup>;

<sup>(14)</sup> The “Interface Hazard Analysis (IHA)” and “Hazard and Operability Analysis (HAZOP)” are the methodologies commonly used for identifying and managing the risks at the interfaces in the railway field.

<sup>(15)</sup> In the scope of a vehicle authorisation, as the customer/user might not be known yet this requirement cannot be verified. It is thus important to fulfil the requirement in (b)(4) of section § 2.6.2.



- (4) the safety related application conditions/constraints (exported SRACs, also called in some literature “exported constraints”) necessary for the safe integration of the sub-system under assessment into its physical, functional, environmental, operational and maintenance context, as well as the associated hazards/risks, are clearly identified and communicated to the relevant user(s)/maintainer(s);
- (5) the interactions between human, technological and organisational factors are adequately considered and managed in the design, implementation and use of the sub-system.

**Note:** *This corresponds to the part of the safe integration to be done by the user/maintainer of the sub-system under assessment.*

- 2.6.3. The actors receiving those safety requirements and associated hazards/risks shared across the interfaces with the system under assessment are then responsible to demonstrate the appropriate control of those shared hazards/risks that fall under their area of responsibility. They can either comply with the exported safety requirements or define other ones that make the risk acceptable. The same applies to the exported safety related application conditions/constraints (SRACs).
- 2.6.4. The AsBo of the sub-system under assessment is responsible for independently assessing the correctness and fitness for purpose of the risk assessment and risk management processes, and the suitability of the results from the application of those processes, in achieving the objectives above, i.e. in assessing that :
  - (a) the proposer demonstrates that the sub-system under assessment is safely designed and implemented and can fulfil safely the intended functional, technical and safety requirement objectives of its system definition;
  - (b) the sub-system under assessment can be used and maintained safely in its physical, functional, environmental, operational and maintenance context, in both the nominal and degraded modes of operation, if the exported hazards/risks are controlled to an acceptable level.
- 2.6.5. The AsBo accredited in the area of a structural (e.g. Rolling Stock) or functional (e.g. traffic operation and management) sub-system has the necessary technical knowledge and capability to assess independently that :
  - (a) the proposer demonstrates the safe integration of the different parts and components within the architecture of the sub-system under assessment, as described in the note at the end of section § 2.6.2.(a) above;
  - (b) the proposer identifies and communicates to the right actors the safety related application conditions/constraints (exported SRACs) necessary for the safe integration of the sub-system under assessment into its working physical, functional, environmental, operational and maintenance context (see section § 2.6.4.(b) above). These safety related application conditions/constraints (exported SRACs) are needed to carry out the safe integration referenced in the note at the end of section § 2.6.2.(b) above.

**Note:** *This set of activities corresponds to the part of the independent assessment of the safe integration to be carried out at the level of the sub-system under assessment.*

## 2.7. Conclusion

- 2.7.1. Safe integration of a change to the railway system is implicitly an integral part of a comprehensive and consistent risk assessment and risk management process. If carried out systematically as described in the sections above, there are no additional checks or demonstrations to do.

- 2.7.2. Indeed, a comprehensive and consistent risk assessment and risk management, which fully address the safe integration, implies the implementation of a system based and top-down approach as represented in Figure 3. This means that it is not only important to assess the impacts of a change locally at the level of the sub-system but it is also essential to assess the change in its physical, functional, environmental, operational, and maintenance context. The risk assessment must thus go beyond the boundaries of the change/sub-system in order to identify and assess 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 elements, components, constituents, structural or functional 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.
- 2.7.3. The implementation of a system based and top-down approach (see Figure 3) has to provide the demonstration that :
- (a) At the level of the railway system, the infrastructure manager and the railway undertakings :
    - (1) carry out a “top-down” risk assessment and risk management, “... *where appropriate* ...”, in cooperation<sup>(16)</sup> “... *with each other*”, involving all other railway actors who have a potential impact on the safe operation of the railway system;
    - (2) allocate to every contributing actor and sub-system the functional, technical and safety requirements, and the associated hazards/risks, that are to be fulfilled and managed by the actor in charge of the development of the sub-system.For more details on the full set of activities to complete, refer to section § 2.5. here above.
  - (b) At the level of every impacted/contributing sub-system, the actor in charge of its development :
    - (1) carries out a “bottom-up” risk assessment and risk management, where appropriate, in cooperation with the other actors in charge of the development of the other sub-systems, in order to identify and manage jointly the hazards and related safety measures that need to be handled at the interfaces shared between their respective sub-systems;
    - (2) demonstrates that the sub-system under assessment is safely designed and implemented and fulfils safely the intended functional, technical and safety requirements allocated to it.For more details on the full set of activities to complete, refer to section § 2.6. here above.
- 2.7.4. In the absence of such a top-down analysis, some railway system hazards/risks might remain non-identified and therefore uncontrolled. The proper and bottom-up risk assessments and risk managements for the constituting sub-systems cannot always compensate the lack of proper top-down risk assessment and risk management at the level of the railway system.

---

<sup>(16)</sup> *Explicit obligations in Article 4 of the Safety Directive (EU) 2016/798.*

### 3. Legal background

3.1. The European railway legislation explicitly requires the safe integration of structural sub-systems within the railway system. See the references in the sections below.

#### 3.2. Interoperability Directive 2008/57/EC

Article 15(1) on the “procedure for placing in service” (structural sub-systems)

“... Member States shall take all appropriate steps to ensure that“ the structural “... sub-systems may be placed in service only if they are designed, constructed and installed in such a way as to meet the essential requirements ... when integrated into the rail system. In particular, they shall check:

- the technical compatibility of these subsystems with the system into which they are being integrated,
- the safe integration of these subsystems in accordance with Articles 4(3) and 6(3) of Directive 2004/49/EC.”

#### 3.3. Interoperability Directive (EU) 2016/797

Article 18(4) on the “authorisation for the placing in service of fixed installations”

“The applicant shall submit a request for authorisation of the placing in service of fixed installations to the national safety authority. The application shall be accompanied by a file which includes documentary evidence of:

(...)

- (c) the safe integration of the subsystems, established on the basis of the relevant TSIs, national rules, and the common safety methods (‘CSMs’) set out in Article 6 of Directive (EU) 2016/798;

(...)”

Article 21(3) on the “vehicle authorisation for placing on the market”

“The application for a vehicle authorisation for placing on the market shall be accompanied by a file concerning the vehicle or vehicle type and including documentary evidence of:

(...)

- (c) the safe integration of the subsystems referred to in point (a) within the vehicle, established on the basis of the relevant TSIs, and where applicable, national rules, and the CSMs referred to in Article 6 of Directive (EU) 2016/798;

(...)”

Point 1. “general requirements” in Annex III on the “essential requirements”

“1.5. Technical compatibility

The technical characteristics of the infrastructure and fixed installations must be compatible with each other and with those of the trains to be used on the rail system. This requirement includes the safe integration of the vehicle's subsystem with the infrastructure”.

...

Point 2.4. on the “technical file accompanying the ‘EC’ declaration of verification” in Annex IV on the “‘EC’ Verification Procedure for Subsystems”

“(…)

(e) *when verification of safe integration is required pursuant to in point (c) of Article 18(4) and in point (c) of Article 21(3), the relevant technical file shall include the **assessors’ report(s) on the CSMs on risk assessment** referred to in Article 6(3) of Directive 2004/49/EC”.*

### 3.4. Commission Implementing Regulation (EU) 402/2013

Point 1.2.7 in Annex I

*“... , the proposer is responsible for ensuring that the risk management covers the system itself and its integration into the railway system as a whole.”*

Point 5.2. in Annex I

*“The documentation produced by the proposer under point 5.1 shall at least include:*

*(…)*

*(d) all assumptions relevant for system integration, operation or maintenance, which were made during system definition, design and risk assessment.”*

### 3.5. Commission Implementing Regulation (EU) 2018/545

Article 2. Definitions

*“(12) ‘safe integration’ means the fulfilment of the essential requirement on safety as specified in Annex III of Directive (EU) 2016/797 when combining parts into its integral whole, such as a vehicle or a subsystem as well as between the vehicle and the network, with regards to the technical compatibility”.*

Article 13. Requirements capture

*“2. The requirements capture performed by the applicant shall in particular cover the following requirements:*

- (a) essential requirements for subsystems referred to in Article 3 and specified in Annex III to Directive (EU) 2016/797;*
- (b) technical compatibility of the subsystems within the vehicle;*
- (c) safe integration of the subsystems within the vehicle; and*
- (d) technical compatibility of the vehicle with the network in the area of use.*

*3. The risk management process set out in Annex I to Commission Implementing Regulation (EU) No 402/2013 shall be used by the applicant as the methodology for requirements capture as regards the essential requirements ‘safety’ related to the vehicle and subsystems as well as safe integration between subsystems for aspects not covered by the TSIs and the national rules.”*