Deliverable D4.1
Authorisation Strategy and Overall Safety Plan

Project acronym:	FP5-TRANS4M-R
Starting date:	2022-07-01
Duration (in months):	45
Call (part) identifier:	HORIZON-ER-JU-2022-01 (Topic: HORIZON-ER-JU-2022-FA5-01)
Grant agreement no:	101102009
Due date of deliverable:	Month 10 (M10)
Actual submission date:	2023-04-28
Responsible/Author:	Julian Brown (DBSYS) (authorisation and overall lead) Christopher Wörfel (DBSYS) (safety plan lead)
Dissemination level:	PU - Public
Deliverable Type:	R - Document, report
Status:	Submitted, Version 3.1 – V3.1

Reviewed: YES

Funded by the European Union

"Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Europe's Rail Joint Undertaking. Neither the European Union nor the granting authority can be held responsible for them."
"The project is supported by the Europe's Rail Joint Undertaking and its members."

Document History		
Revision	*Date*	*Description*
0.1	2023.02.03	*First draft*
0.2	2023.02.10	*First revision*
0.3	2023.02.14	*Further revision*
0.4	2023.04.26	*Revision incorporating input from the reviewers*
0.5	2023.04.27	*Final Version after the review submitted to Coordinator*
3.1	2024.01.26	*Revision after review process by EU-Rail JU*

Report Contributors		
Name	Beneficiary Short Name	Details of contribution
Nils Bruns	UIP	Pre-reviewer
Christian Bedau	Siemens	Pre-reviewer, Expert Locomotives
Marco Fasolini	Wabtec	Observer
Sneha Gosavi	Lindholmen	Observer
Steffen Jass	Knorr Bremse	Pre-reviewer
Fabio Lo Piccolo	SBB Cargo	Observer
Roman Mayer	UIP	Pre-reviewer
Philipp Oslislo	DB Systemtechnik	Observer
Thomas Erpenbeck	DB Systemtechnik	Co-Author (ch. 5.2.1)
Matthias Arnold	Voith	Co-Author (ch. 5.3)
Alejandro Buendia Martinez	RENFE	Observer
Alejandro Huergo	RENFE	Observer
M Pedegrini	ADIF	Observer
Markus Klohr	Alstom	Pre-reviewer
Szuecs Karoly Robert	ÖBB TS	Co-Author (ch. 3)
Stephan Hagenlocher	ÖBB Holding AG	Observer
Philipp Wagenknecht	Rail Cargo Group	Co-Author (ch. 3)
Steffen Jank	DB Systemtechnik	Co-Author (ch. 5.3)

Reviewers		
Name	Beneficiary Short Name	Details of contribution
Oliver Behrens	UIP	Content Quality Review
Gilles Peterhans	UIP	Content Quality Review
Johan Ahman	Dellner	Content Quality Review

Table of Contents

List of Tables

List of Figures

1 Executive Summary

The directive (EU) 2016/797 [EU2] states in Article 21, paragraph 12 that "*in the event of renewal or upgrading of existing vehicles which already have a vehicle authorization [...] a new vehicle authorization [...] shall be required if:*

(a) changes are made to the values of the parameters referred to in point (b) of paragraph 10 which are outside the range of acceptable parameters as defined in the TSIs;

(b) the overall safety level of the vehicle concerned may be adversely affected by the works envisaged; or

(c) it is required by the relevant TSIs."

With the objective of having the DAC with the related train-functions fitted into existing vehicles comes the necessity to assess how this impacts the vehicle authorisation taking into account Art. 21 (12) of the Directive 2016/797 mentioned above. As a re-authorisation of the existing fleet might prove to be impossible both in terms of time and costs, this document outlines the methods both to identify whether a new vehicle authorisation would be triggered and how to eventually demonstrate that this is not the case. The document provides a first generic evaluation of what the outcome of the assessment at the moment of the upgrade could be in practice. It is composed of:

1) The authorisation strategy dealing with the conditions (a) and (c) stated above
2) The safety plan dealing with the condition (b).

The authorisation strategy assesses whether the condition (a) is met by providing a preliminary analysis of the basic design characteristics as defined by the TSIs WAG and LOC&PAS. The result of this assessment shows that the upgrade of a vehicle with the DAC only is not expected to require a new vehicle authorisation. In case new and additional functions are part of the upgrade with the DAC, the document provides details on why a new vehicle authorisation might become necessary. In the authorisation strategy, the assessment if the condition (c) would be triggered is addressed by providing a preliminary TSI analysis. The conclusions are similar to what is providing above regarding the condition (a): in case of an upgrade with the DAC but without the related train-functions no new vehicle authorisation would be required. However, in case of upgrading a vehicle with the DAC and related train-functions which are part of the train control system (ETCS) a new vehicle authorisation might become necessary.

The authorisation strategy finally outlines the actions that should be followed when upgrading vehicles. Even if the upgrade does not trigger a new vehicle authorisation it may be necessary to get the changes made to the vehicles assessed against the TSI requirements or notified technical national rules by a Notified Body, a Designated Body and an Assessment Body. Additionally, the authorising entities will need to be notified about any change made to the

vehicles if a type exists for this vehicle and the entity managing the change is not the holder of the vehicle type authorisation. The idea behind streamlining this process would be to provide if possible generic records and reuse them for different vehicle upgrades. The safety plan has been developed in this sense and shall contribute to provide a generic assessment that the overall safety level will not be negatively affected when upgrading vehicles with the DAC and the related train-functions. As such the safety plan outlines the iterative process that will be used to ensure that the risks resulting from the upgrade of existing vehicles with the DAC and related functionalities are managed appropriately and will be used to prove that condition (b) is fulfilled.

Keywords: Authorization Strategy; Safety Plan; Generic Assessment; Interoperability

2 Abbreviations and Acronyms

Abbreviation / Acronym	Description
AsBo	Assessment Body
BDC	Basic design characteristic
CCS	Control-command and signalling subsystem
CSM	Common safety method
DAC	Digital Automated Coupler
DeBo	Designated Body
DIN	Deutsches Institut für Normung (German industrial standard)
EC	European Community
ECM	Entity in charge of maintenance
EMC	Electromagnetic compatibility
EN	European standard
ENE	Energy
ERA	European Union Agency for Railways
ERATV	European Register of Authorised Types of Vehicles
ETCS	European Train Control System
EU	European Union
HW	Hardware
ID	Identity
IC	Interoperability constituents
INF	Infrastructure
ISO	International Organization for Standardization
LOC&PAS	Locomotives and passenger rolling stock subsystem
NNTR	Notified national technical regulation
NOI	Rolling Stock, Noise
NoBo	Notified Body
OPE	Operation and traffic management
RA	Risk Assessment
RAP	Risk acceptance principles
TAF	Telematics applications for freight subsystem
TSI	Technical specification for interoperability
SAS	Safety assurance level
SMS	Safety management system
SAS	Software Safety assurance level

Abbreviation / Acronym	Description
SRAC	Safety-related application condition
WAG	Freight wagons

3 Background

The present document constitutes the Deliverable D4.1 “Authorisation strategy and overall safety plan” in the framework of the Flagship Project FP5- TRANS4M-R.

Content of WP D4.1:

The beneficiaries will determine details of the authorisation process (holder of the vehicle type authorisation, registration in ERATV, categorizing the change according to (EU) 2018/545 [EU3] Article 15(1)) with the aim to fit the DAC and its related functionalities into existing vehicles as a change without need for authorisation (Change not classified as triggering Art. 21(12)(a) of Directive (EU) 2016/797). Based on the input of WP2 and WP3 the beneficiaries will prepare a generic hazard record referred to (EU) 402/2013 [EU1] and define the risk acceptance criteria to assess and finally control the identified hazards. The hazard record and the risk acceptance criteria will be assessed and confirmed by an Assessment Body (AsBo) respectively a competent independent assessor.

4 Objective/Aim

The goal of the authorisation strategy and the safety plan is to implement the DAC with the related train-functions, its automation subsystems and components on freight wagons and locomotives. The preferred outcome is to replace the existing screw coupler and buffers on freight wagons and freight locomotives without the economic burden of re-evaluation and re-authorisation. In addition, care should be taken to avoid prolonged vehicle outages, due to the processes associated with a new authorisation, as this would result in the dramatical disruption of European Rail-freight operations. To simplify the approval, process a generic approach shall be adopted that is applicable to as many vehicles as is reasonably possible.

To achieve the preferred outcome, it is necessary that the changes to the vehicles can be classified either as

- Changes to an already authorised vehicle type (Art. 15 (EU) 2018/545 [EU3]
  - categorised as 15 (1) a) – c) in relation to the different migration levels ("DAC ready", DAC without activated electrical components or "full DAC") or as
- Changes to an already authorised vehicle (Art. 16 (EU) 2018/545 [EU3]) when
  - no conformity with an approved vehicle type or for which no vehicle type (ERATV) is available and/or
  - vehicles are administered by a change management entity that is not ≠ is the holder of the vehicle type approval

with no need for applying for a new type authorisation according to Art. 14 (EU) 2018/545 [EU3] or a new authorisation according to Art. 16 (EU) 2018/545 [EU3].

The scope of this strategy are freight wagons and freight locomotives that are technically compliant with the requirements of the adopted generic approach. Vehicles that are not covered by the system definition or require a more specific approach may need a new authorisation and are out-of-scope for this authorisation strategy.

5 Authorisation Strategy and Overall Safety Plan

5.1 Scope of the project

5.1.1 Scope of the change

The scope of the project is the deployment of the DAC with the related train-functions[1] into freight wagons and (freight) locomotives of the European railway system. In the form of an upgrade of existing vehicles and a standard for new vehicles. The emphasis of this document is the upgrade of existing vehicles as this poses the greater challenge in terms of the authorisation process. To reach this goal there will be changes to freight wagons and (freight) locomotives.

In the case of existing and new locomotives used in the transition period, a hybrid coupler shall be deployed for the existing vehicles as it must be compatible with the conventional screw coupler and buffers as well as the DAC. The upgrade includes the deployment of electrical and electronical equipment as well as hard and software updates to control the train related functions of the DAC. The new control unit on the locomotive will be used to control all the new couplers on the wagons and the loco and the related train functions. In the case of new locomotive types an integrated approach will be developed, the related train-functions will be integrated into the vehicle-software. Thus, a new release and a related variant-authorisation will be necessary in this case.

The changes to the freight wagons in relation to the deployment of the DAC in the current European rail freight system can be grouped in stages as defined below. These stages may be implemented individually with a fully authorised vehicle in between the individual stages or grouped into larger or even only one refit of the wagon. The following individual stages are possible parts of the current migration plan.

“DAC ready”:
At this stage the wagon has been pre-fitted with the DAC drawgear and spring package. Not installed at this stage is the coupler head. Cables, cable-conduits and a battery box may be installed (without function). At “DAC ready” status the side buffers remain in place and is still the conventional draw hook fitted instead of the automatic coupler head. In some cases, it might be necessary to alter or strengthen the wagons main frame structure at this stage to install the DAC draw gear/spring package correctly and insure it can withstand the forces introduced.

DAC with electrical components either not yet fitted or not in use:
In this stage, the side buffers are removed, and the screw coupler/draw hook is replaced with the DAC coupler head. The electrical equipment may also be pre-fitted. If this is the case, it is not put into operation yet and is left in an electrically dead state.

[1] the exact scope of functions and the train functions are currently still being defined

“Full DAC”:
Finally in this stage the electrical equipment is completely installed and activated. The wagon afterwards is fully operational powered and put into operation.

New additional functions enabled by DAC are installed:

According to the Grant Agreement it is planned to install at least some of the following new additional functions once the DAC is fully operational:

- train composition detection
- train length determination
- train integrity monitoring
- de-coupling control (from loco)
- automated brake test
- parking brake control (from loco)
- network based brake control (ep-brake)
- distributed power (multi traction)

These stages may be implemented individually or grouped into packages or even a single upgrade of the wagon. The hereby defined scope applies to both the following authorisation strategy and safety plan. In case of changes to the scope the following procedures shall be updated accordingly.

5.1.2 Project Stakeholders

The stakeholders and their staff involved in the deployment of the DAC with the related train-functions into freight wagons and (freight) locomotives are listed below.

- Manufacturers of freight wagons
- Keepers of freight wagons
- Manufacturers of Interoperability-Constituents
- Manufacturers of locomotives
- Keepers of locomotives
- Suppliers of subsystems
- Railway Undertakings
- Operating personnel
- Notified Bodies
- Authorising entities (ERA and NSA)
- Assessment Bodies
- Entity in charge of maintenance

All here listed stakeholders are affected by the authorisation strategy and the safety plan described in this document.

5.2 Authorisation strategy

5.2.1 Legal and Normative Framework of the Authorisation Strategy

The applicable legal framework of the vehicle authorisation procedure is contained in the Directive (EU) 2016/797 [EU2], the TSIs and the Implementing Regulation (EU) 2018/545 [EU3]. For the deployment of the DAC with the related train-functions into already authorized vehicle types and already existing freight wagons and (freight) locomotives the Regulation (EU) 2018/545 [EU3] sets out a categorisation of the changes in Article 15(1):

> *(a) a change that does not introduce a deviation from the technical files accompanying the EC declarations for verification for the subsystems. In this case there is no need for verification by a conformity assessment body, and the initial EC declarations of verification for the subsystems and the vehicle type authorisation remain valid and unchanged;*
>
> *(b) a change that introduces a deviation from the technical files accompanying the EC declarations for verification for the subsystems which may require new checks and therefore require verification according to the applicable conformity assessment modules but which do not have any impact on the basic design characteristics of the vehicle type and do not require a new authorisation according to the criteria set out in Article 21(12) of Directive (EU) 2016/797;*
>
> *(c) a change in the basic design characteristics of the vehicle type that does not require a new authorisation according to the criteria set out in Article 21(12) of Directive (EU) 2016/797;*
>
> *(d) a change that requires a new authorisation according to the criteria set out in Article 21(12) of Directive (EU) 2016/797.*

For the strategy it is important to differentiate between the scope of deploying the DAC with the related train-functions as a change to an existing **vehicle type** or to a number or series of existing **vehicles**. Figure 1 shows the process in principle.

The DAC components themselves are planned to be defined and authorised as Interoperability Constituents (ICs) in the amended TSIs, as defined in the Interoperability Directive 2016/797. These ICs shall be fully qualified and come with an EC Declaration of Verification of conformity and/or suitability for use provided by the manufacturers. To facilitate the migration, two DAC ICs may be defined: one IC used in the “DAC ready” stage, which covers only some parts of the future DAC, while the coupling functionality will still be provided by means of a screw coupling. Then, a second IC used in the “full DAC” stage, which includes the DAC full coupler, including the DAC ready part and electric/data communication functionalities. The formal description of these ICs needs to be clarified and defined in the amended TSIs, together with the conditions for a freight wagon and a locomotive to receive a DAC, and guidance for maintenance and operation.

Case 1: Entity managing the change = holder of type authorisation

When deploying the DAC and assessing the impact of the change at the level of an existing vehicle type, article 15 "Changes to an already authorised vehicle **type**" of (EU) 545/2018 provides criteria in (1) a) – c) for the holder of the type authorisation to implement changes. New tests and thus a review according to the relevant conformity assessment modules and Revision/adaptation of the EC declarations of verification of the Subsystems as well as the technical documentation may be required as well as a registration of a new version of the existing vehicle type in ERATV, but no application for a new type authorisation is required.

Case 2: Entity managing the change ≠ holder of type authorisation or no vehicle type is present in ERATV

For entity managing the change`s who are not holder of the type authorisation, the current legal framework doesn't provide the possibility to apply Art. 15 and the related categories but only if they would apply for a vehicle type approval first.

To follow the strategy and reaching the above-mentioned preferred outcome (no need for a new authorisation) such entity managing the changes should follow the procedure of Art. 16 relating to the "Changes to an already authorised vehicle" and not to an existing vehicle type.

Art. 16(4) (EU) 545/2018 describes the procedure that is to be followed when the entity managing the change is not the holder of the vehicle type authorisation:

If the entity managing changes categorised in accordance with Article 15(1)(b) and (c) to an already authorised vehicle is not the vehicle type authorisation holder it shall:

> *(a) assess the deviations from the technical files accompanying the EC declarations for verification for the subsystems;*
>
> *(b) establish that none of the criteria set out in Article 21(12) of Directive (EU) 2016/797 are met;*
>
> *(c) update the technical files accompanying the EC declarations for verification for the subsystems;*
>
> *(d) notify the changes to the authorising entity. This may apply to a vehicle or a number of identical vehicles.*
>
> *The authorising entity may issue, within 4 months, a reasoned decision requesting an application for authorisation in case of a wrong categorisation or insufficiently substantiated information.*

The criteria triggering a re-authorisation in art. 21(12) of Directive (EU) 2016/797 [EU2] are:

> *(a) changes are made to the values of the parameters referred to in point (b) of paragraph*

10 which are outside the range of acceptable parameters as defined in the TSIs;

(b) the overall safety level of the vehicle concerned may be adversely affected by the works envisaged;

(c) it is required by the relevant TSIs.

In addition, the conformity assessment procedure must be followed, which is described in the Commission Decision (2010/713/EU). In order to properly complete the process according to the Commission Implementing Regulation (EU) 2019/250, the mandatory form "EC declaration of verification" must be complied with.

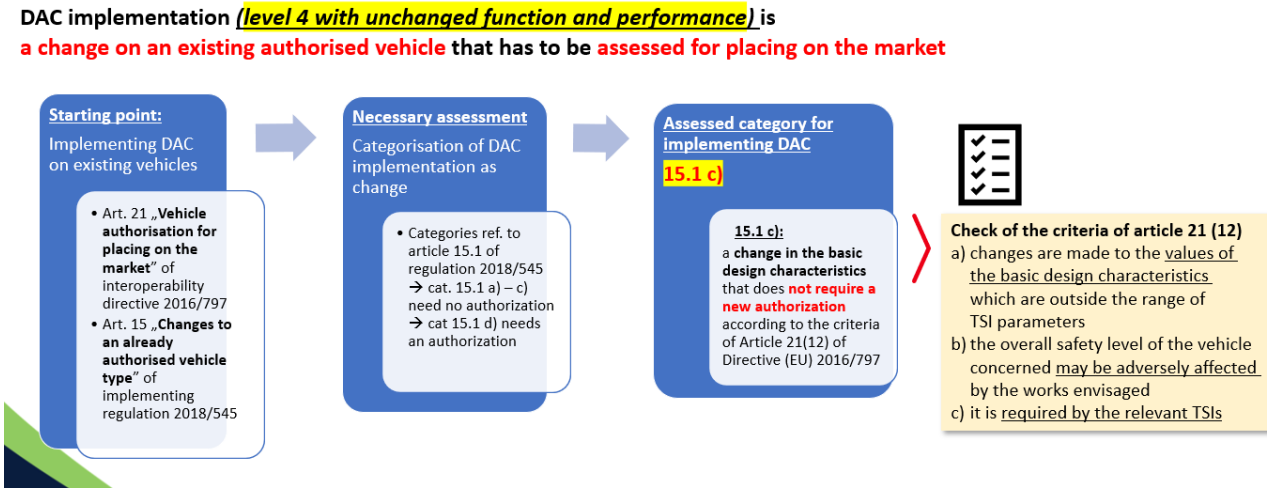

Figure 1 Categorisation of DAC implementation due to the legal frame

5.2.2 Categorization of the Change to Authorised Vehicles

Art. 15(1) of Commission Implementing Regulation (EU) 2018/545 [EU3] defines four categories to categorise the changes to authorised vehicles that cannot be classified and managed in the framework of maintenance. Following the upgrade of a vehicle with the DAC, criteria (a) can be ruled out as there will be inevitably a deviation from the original vehicle documentation.

If the other two criteria given in Art. 21(12) of Directive (EU) 2016/797 [EU2] are assumed not to be fulfilled, the difference between the categories (b), (c) and (d) of Article 15 (1) [EU3] can be condensed down to the question whether a Basic Design Characteristic (BDC) of the vehicle is affected and whether it is affected in such a way that it triggers the need for a new vehicle authorisation. The BDCs and the extent to which they can be changed without the need for a new vehicle authorisation are defined in table 17a of the Commission Regulation (EU) 1302/2014 (TSI LOC&PAS) [EU6] if the vehicle concerned is a locomotive or table 11a of the Commission Regulation (EU) 321/2013 (TSI WAG) [EU4] if the vehicle in question is a freight wagon.

5.2.2.1 Upgrade of Wagons

As described in chapter 5.1 the deployment of the DAC with the related train-functions may take place in four individual stages. Thus, the changes to the vehicles may need to be assessed and authorised for each stage separately. In the following chapter the changes for each stage will be categorized separately according to Art. 15 (1) of the Commission Implementing Regulation (EU) 2018/545 [EU3]. If the individual stages described are grouped together in one approval process, then the criteria linked to the "highest category" will apply.

5.2.2.1.1 DAC-ready

The following Basic Design Characteristics taken from Table 11a of the TSI WAG could become affected at this stage of the upgrade:

Basic design characteristic (BDC)	Change to BDC that is classified as category (c)	Change to BDC that is classified as category (d)	Criteria to stay within Category b) Art. 15(1) (EU) 2018/545 [EU3]
Reference profile	N/A	Change of reference profile the vehicle is conform to	reference profile is not affected by the new components
Permissible payload for different line categories	Change of any of the vertical loading characteristics resulting in a change of the line category(ies) the wagon is compatible with	N/A	increase in mass lies within the defined boundaries
Stopping distance	Change of stopping distance of more than ± 10 %	N/A	depends on change of mass
Maximum deceleration for the load condition 'design mass under normal payload' at the maximum design speed	Change of more than ± 10 % on the maximum average brake deceleration	N/A	depends on change of mass
Thermal capacity expressed in terms of Speed Gradient Brake distance	N/A	New reference case declared	depends on change of mass

Table 1 BDC DAC "Ready"

All of the above listed BDCs could become affected at the "DAC ready" stage of the upgrade as additional components are installed on the wagon. This will lead to a slight increase of the wagons tare weight that could affect the permissible payload or the braking characteristics. If it can be demonstrated that the increase in mass lies within the defined boundaries mentioned in the table above and that the reference profile is not affected by the new components, then the change made to the wagons can be **classified as category (b)** according to Art. 15 (1) of the Commission Implementing Regulation (EU) 2018/545 [EU3].

5.2.2.1.2 DAC with electrical components either not yet fitted or not in use

The following Basic Design Characteristics taken from Table 11a of the TSI WAG could become affected at this stage of the upgrade:

Basic design characteristic (BDC)	Change to BDC that is classified as category (c)	Change to BDC that is classified as category (d)	Criteria to stay within Category c) Art. 15(1) (EU) 2018/545 [EU3]
Type of end coupling	Change of end coupler type	N/A	
Reference profile	N/A	Change of reference profile the vehicle is conform to	reference profile is not compromised
Minimum vertical convex curve radius capability	Change in minimum vertical convex curve radius capability the unit is compatible with of more than 10 %	N/A	minimum vertical curve radius capabilities are not compromised
Minimum vertical concave curve radius capability	Change in minimum vertical concave curve radius capability the unit is compatible with of more than 10 %	N/A	minimum vertical curve radius capabilities as well as the reference profile are not compromised
Permissible payload for different line categories	Change of any of the vertical loading characteristics resulting in a change of the line category(ies) the wagon is compatible with	N/A	change of mass lies within the defined boundaries
Stopping distance	Change of stopping distance of more than ± 10 %	N/A	depends on change of mass, brake function must not be affected
Maximum deceleration for the load condition 'design mass under normal payload' at the maximum design speed	Change of more than ± 10 % on the maximum average brake deceleration	N/A	depends on change of mass, brake function must not be affected
Thermal capacity expressed in terms of Speed Gradient Brake distance	N/A	New reference case declared	depends on change of mass

Basic design characteristic (BDC)	Change to BDC that is classified as category (c)	Change to BDC that is classified as category (d)	Criteria to stay within Category c) Art. 15(1) (EU) 2018/545 [EU3]
Temperature range	Change of temperature range (T1, T2, T3)	N/A	environmental conditions of the vehicle remain unchanged
Snow, ice and hail conditions	Change of the selected range 'snow, ice and hail' (nominal or severer)	N/A	environmental conditions with which the wagon is compatible remain unchanged

Table 2 BDC DAC without electrical components

At this stage of the DAC upgrade some components will be added and some will be removed from the wagon. This could lead to a change in the wagons tare weight and thus the same BDCs could be affected as was the case with the previous "DAC ready" stage. Again, it must be demonstrated that the change of mass lies within the defined boundaries. It must also be shown that the minimum vertical curve radius capabilities as well as the reference profile are not compromised by the use of the new coupler and that the environmental conditions with which the wagon is compatible remain unchanged. Crucially at this stage the couple type will change from the screw coupler to that of the DAC. Thus, the BDC "Type of end coupling" will be affected. This means that the change made to the wagon at this stage of the upgrade can be **classified as category (c)** according to Art. 15 (1) of the Commission Implementing Regulation (EU) 2018/545 [EU3].

5.2.2.1.3 DAC is fully operational

Assuming no additional equipment is installed or removed the following Basic Design Characteristics taken from Table 11a of the TSI WAG could become affected at this stage of the upgrade:

Basic design characteristic (BDC)	Change to BDC that is classified as category (c)	Change to BDC that is classified as category (d)	Criteria to stay within Category b) Art. 15(1) (EU) 2018/545 [EU3]
Compatibility with train detection systems	N/A	Change of declared compatibility with one or more of the three train detection systems: • Track circuits • Axle counters • Loop equipment	full compatibility with related entity managing the change requirements

Table 3 BDC Full- DAC

If it can be demonstrated that the change doesn't impact the compatibility with train detection systems by powering the electrical equipment and there will be no new BDCs defined in future versions of the TSI WAG like for example "DAC Level", then the change made to the wagons can be **classified as category (b)** according to Art. 15 (1) of the Commission Implementing Regulation (EU) 2018/545 [EU3].

5.2.2.1.4 New additional functions enabled by DAC are installed

As was the case with the other stages of the DAC upgrade the categorisation according to Art. 15 (1) of the Commission Implementing Regulation (EU) 2018/545 [EU3] will depend on the affected BDCs listed in Table 11a of the version of the TSI WAG. Additionally, to the BDCs listed for the other stages, the following BDCs appear especially noteworthy with the view on the introduction of future related train functions:

Basic design characteristic (BDC)	Change to BDC that is classified as category (c)	Change to BDC that is classified as category (d)
Axle bearing condition monitoring	N/A	Fitting/Removal of on-board detection system
Parking brake	Parking brake function installed/removed	N/A
Wheel slide protection (WSP)	N/A	Fitting/removal of WSP function

Table 4 BDC DAC Additional functions

In respect to the TSI CCS there should be no obligation to re-authorise the vehicle if the new components are certified as ICs, according to chapter 6.3.3. (2) of TSI CCS. If this is not the case the interface between the TSI WAG and TSI CCS shall be checked regarding the need for re-authorisation of the vehicles in question.

5.2.2.2 Upgrade of Locomotives

The strategy for upgrade of the locomotives differs from that of the wagons in that preferably all locomotives where this is possible shall be fitted with a so-called hybrid coupler that is compatible to the old screw coupler and the new DAC. The upgrade of the hybrid coupler to locomotives will be more complex and thus challenging than the upgrading freight wagons with the DAC and the related train functions. The reasons for this are:

- More mass will be introduced to the vehicles as the hybrid coupler will be heavier and the side buffers will remain in place. Locomotives rarely have a payload that could be reduced to compensate for this. The main frame, bogies and especially the wheelsets of existing locomotives are often already close to their permissible load limits.
- The TSI LOC&PAS poses more requirements than the TSI WAG that will be affected by the upgrade. For example, in many cases it will be difficult to show compliance to the requirements defined for passive safety.

- The electrical end electronical parts of the DAC should be integrated into the existing locos. It shall be shown that this will have no adverse effects on the safety.

The following Basic Design Characteristics taken from Table 17a of the TSI LOC&PAS could be affected by the upgrade of locomotive with the hybrid coupler:

Basic design characteristic (BDC)	Change to BDC that is classified as category (c)	Change to BDC that is classified as category (d)
Type of end coupling	Change of end coupler type	N/A
Design mass in working order	Change in any of the corresponding basic design characteristics resulting in a change of the line category(ies) the vehicle is compatible with	N/A
Design mass under normal payload		
Design mass under exceptional payload		
Static axle load in working order		
Static axle load under nominal payload		
Static axle load under exceptional payload		
Total vehicle mass (for each vehicle of the unit)	Change in any of the corresponding basic design characteristics resulting in a change of the line category(ies) the vehicle is compatible with	Change of more than ± 10 %
Mass per wheel	characteristics resulting in a change of the line category(ies) the vehicle is compatible with or Change of more than ± 10 %	N/A
Reference profile	N/A	Change of reference profile the vehicle is conform to
Minimum vertical convex curve radius capability	Change in minimum vertical convex curve radius capability the unit is compatible with of more than 10 %	N/A

Basic design characteristic (BDC)	Change to BDC that is classified as category (c)	Change to BDC that is classified as category (d)
Minimum vertical concave curve radius capability	Change in minimum vertical concave curve radius capability the unit is compatible with of more than 10 %	N/A
Minimum horizontal curve radius capability	Increase of minimum horizontal curve radius of more than 5m	N/A
Compatibility with train detection systems	N/A	Change of declared compatibility with one or more of the three train detection systems: • Track circuits • Axle counters • Loop equipment
Emergency braking: Stopping distance and deceleration profile for each load condition per design maximum speed.	Change of stopping distance of more than ± 10 %	N/A
Service braking: Stopping distance and deceleration profile for the load condition 'design mass under nominal payload' at the design maximum speed.	Change of stopping distance of more than ± 10 %	N/A
Thermal capacity in terms of maximum line gradient, associated length and operating speed	Change of maximum gradient, associated length or operating speed operating speed for which the brake system is designed in relation with brake thermal energy capacity	Change of maximum brake thermal energy >= 10 %
Temperature range	Change of temperature range (T1, T2, T3)	N/A
Snow, ice and hail conditions	Change of the selected range 'snow, ice and hail' (nominal or severer)	N/A

Table 5 BDC DAC locomotive

The only BDC that will be inevitably affected is "Type of end coupling". Thus, the upgrade of a

locomotive with a hybrid coupler must at least be **classified as category (c)** according to Art. 15 (1) of the Commission Implementing Regulation (EU) 2018/545 [EU3].

5.2.3 Preliminary TSI Analysis

To be able to confirm that the criteria (c) listed in Art. 21(12) of Directive (EU) 2016/797 [EU2] is not triggered, it is necessary to check which TSI requirements of both the TSI WAG and TSI LOC & PAS could be affected by the change to the vehicle. At this stage this preliminary analysis aims at verifying that this criteria (c) is not triggered.

The following table lists the TSI WAG chapters that may be affected by the DAC upgrade:

Title of chapter- TSI WAG	Chapter
End coupling	4.2.2.1.1
Strength of unit	4.2.2.2
Integrity of the unit	4.2.2.3
Gauging	4.2.3.1
Compatibility with load carrying capacity of lines	4.2.3.2
Compatibility with train detection systems	4.2.3.3
Safety against derailment running on twisted track	4.2.3.5.1
Running dynamic behaviour	4.2.3.5.2
Safety requirements	4.2.4.2
Functional and technical requirements	4.2.4.3
In-service brake	4.2.4.3.2.1
Parking brake	4.2.4.3.2.2
Thermal capacity	4.2.4.3.3
Environmental conditions	4.2.5
Fire safety	4.2.6.1
Protection against electric hazard	4.2.6.2

Table 6 TSI- analysis; TSI WAG

The TSI LOC&PAS chapters that may be affected by the upgrade of the DAC are listed in the following table:

Title of chapter- TSI LOC&PAS	Chapter
End coupling	4.2.2.2.3
IC automatic centre buffer coupler	5.3.1
IC manual end coupling	5.3.2
Rescue coupling	4.2.2.2.4
Staff access for coupling and uncoupling	4.2.2.2.5
Strength of vehicle structure	4.2.2.4

Title of chapter- TSI LOC&PAS	Chapter
Passive safety	4.2.2.5
Fixing of devices to carbody structure	4.2.2.7
Load conditions and weighted mass	4.2.2.10
Gauging	4.2.3.1
Wheel load	4.2.3.2.2
Rolling Stock characteristics for compatibility with train detection systems	4.2.3.3.1
Safety against derailment running on twisted track	4.2.3.4.1
Running dynamic behaviour requirements	4.2.3.4.2 a)
Limit values for running safety	4.2.3.4.2.1
Track loading limit values	4.2.3.4.2.2
Structural design of bogie frame	4.2.3.5.1
Minimum curve radius	4.2.3.6
Functional requirements	4.2.4.2.1
Safety requirements	4.2.4.2.2
Type of brake system	4.2.4.3
Emergency braking	4.2.4.4.1
Service braking	4.2.4.4.2
Direct braking command	4.2.4.4.3
General requirements	4.2.4.5.1
Emergency braking	4.2.4.5.2
Service braking	4.2.4.5.3
Parking braking command	4.2.4.4.5
Temperature	4.2.6.1.1
Snow, ice and hail	4.2.6.1.2
Lamp controls (tbd, if rear coupler is used to indicate train end)	4.2.7.1.4
Power Supply General	4.2.8.2.1
Electrical protection of the train	4.2.8.2.10
Interior layout	4.2.9.1.4
Driver's desk- Ergonomics	4.2.9.1.6
Driver display unit and screens	4.2.9.3.3
Controls and indicators	4.2.9.3.4
Labelling	4.2.9.3.5
Radio remote control function by staff for shunting operation	4.2.9.3.6
Onboard tools and portable equipment	4.2.9.4
Radio remote control function by staff for shunting operation	4.2.9.3.6
Measures to prevent fire	4.2.10.2

Title of chapter- TSI LOC&PAS	Chapter
Special requirements for stabling of trains	4.2.11.6
Documentation for operation and maintenance, General	4.2.12.1
General documentation	4.2.12.2
Documentation related to maintenance	4.2.12.3
The maintenance design justification file	4.2.12.3.1
The Maintenance description file	4.2.12.3.2
Operating documentation	4.2.12.4
Rescue related descriptions	4.2.12.5

Table 7 TSI- analysis; TSI LOC&PAS

In none of the TSI chapters listed in the two tables above is there a statement that would trigger the criteria (c) given in Article 21(12) of Directive (EU) 2016/797 [EU2].

5.2.4 NNTR Analysis

Currently there are no NNTRs that apply to freight wagons equipped with screw couplers. There are however several NNTRs and national regulations that would apply to a fully fitted DAC-wagon in most of the relevant countries. These NNTRs can be grouped into the following main categories:

- EMC-requirements
- Automatic coupling / rescue coupling requirements
- Systems requiring monitoring
- Requirements concerning operational procedures
- Worker's safety
- Special environmental conditions

Under Deliverable D4.2 (M13), we have planned to analyse these national requirements in more details with the aim of incorporating them into the relevant TSIs. This is necessary as it would be highly unpractical to employ a DeBo for each country the wagon is to travel through and would endanger the current single authorisation of freight wagons and the given international interoperability. Therefore, it shall be assumed for this authorisation strategy that an assessment of national requirements by a DeBo will not be necessary.

5.2.5 Approach

The goal of the authorisation strategy is to demonstrate under which conditions the deployment of the DAC with the related train functions can be implemented as a change to existing vehicles which doesn't trigger one of the criteria listed under Art. 21 (12) of regulation (EU) 2016/797 [EU2].

As explained in chapter 4 the conditions which trigger a new authorisation only apply to Art. 21(12) b) "change affects the overall safety level" and have to be checked in detail. There will

be a generic risk assessment which shall provide evidence that the overall safety level is not negatively affected by the change (deploying the DAC with the related train functions).

Existing vehicles for which the criteria and parameters determining the scope of the generic risk assessment apply, the deployment of the DAC with the related train functions can be assessed by this approach. These criteria and parameters will be used to draft a checklist which the entity managing the change can use to demonstrate that fitting the DAC with the related train functions in an existing vehicle doesn't require a new authorisation.

The entity managing the change will have in any case to update the vehicle documentation and document the assessment of the change in case it's as well the holder of the vehicle type authorisation. When the entity managing the change is not the holder of the vehicle type authorisation- or there is no vehicle type authorisation for the vehicle – the ECM has to notify the change to the authorising entity (ERA). The authorisation strategy which the ECM should choose to follow is "no need for new authorisation" as mentioned in the chapter 5.2.1.

For the situation in which the entity managing the change is the holder of the vehicle type authorisation and the change is managed as a change to a vehicle type for a series of existing vehicles, this entity managing the change shall create a new vehicle type version (article 15 (3) of (EU) 2018/545 [EU3]). In this case there is a vehicle type version which means that all vehicles of that vehicle type can be upgraded or modified to this version in conformity; there is no need for notification for all single vehicles as foreseen in article 16 (4) of (EU) 2018/545 [EU3].

In both cases (entity managing the change is holder of the vehicle type authorisation and it is not) the EC declarations of verification of the subsystems as well as the technical documentation has to be updated. This is also the case for the safety assessment report and the requirements capture. These updated documents should be added to the technical file of the vehicle type or to the single vehicles if there is no type authorisation and to be submitted by notification to the authorising entity.
However, in order to fulfil criteria for the majority of vehicles, the following references shall be included in the updated documents to validate and provide evidence that the legal requirements are met:

1. <u>Generic Risk Assessment</u>

The risk assessment shall cover all the risks identified at IC level, with the upgrade of the freight wagon with a DAC and the related train functions at all stages ("DAC-ready" to "DAC fully operational"), as well as all foreseeable exported risk[2].

Provide a well a generic risk assessment covering the upgrade of the targeted fleet, based on

[2] All foreseeable risks to be overtaken by other systems/actors

- A description of the upgrade (functional requirements or concrete technical requirements and the corresponding assessment methodology), and the impacted interfaces.
- Targeted fleet, including exempted railway vehicles.
- A reference to the risk assessment set out in point 14.2
- Consequence of the changes in the light of the risk assessment: version or type/variant.
- version or type/variant.

The risk assessment is intended to evaluate the potential degradation from the pre-existing safety level as required in Art. 21(12)(b) of the Interoperability Directive.

2. **Overarching safety reports** on the overall safety level and on the requirements capture and an **overarching EU Certificate** for the change "DAC implementation"

The entity managing the change uses this reports and certificates for documentation and notification by declaring that these reports and certificate apply to the change "DAC deployment"

3. **Overarching Certificate for the EC Verification of Subsystems**

The entity managing the change can upgrade the vehicles based on this overarching certificate for the EC verification of subsystems. Due to the need of certifying the DAC deployment as a change foreseen for several designs the certificate should refer to module SH1 of the decision EU 2010/713.

The generic risk assessment, the overarching safety reports and certificates have a defined scope of requirements and design which is the content of their assessment. To apply these documents for a concrete vehicle upgrade it is necessary that the vehicle is conform to all these requirements. Otherwise, a separate assessment must be provided as an individual and specific assessment for a single vehicle or a vehicle type.

4. **Checklist for entities managing the change**

The requirements defining the scope of the generic risk assessment and the overarching documents will be summarised and published as a checklist for the entity managing the change. Thus, it shall be easily understandable for each such entities which requirements have to be fulfilled. They can then better understand what needs to be checked and demonstrated to fulfil the requirements set out in the Regulation (EU) 2018/545 [EU3] when performing the particular change in the case of a DAC-upgrade without the need for a new authorisation.

In certain cases, the design of the concerned vehicles (locomotives and wagons) might need to be modified to accommodate the DAC in such a way that it cannot be covered by the generic risk assessment or the TSI requirements. These modified vehicle or vehicle types will require a new authorisation.

5. Proposal for Updating the TSIs

Risks which are identified both at IC level and at vehicle level should be preferably controlled via concrete requirements in the amended TSI WAG and TSI LOC&PAS.
In the case of wagons for the transport of dangerous goods, high-level safety targets should be included in RID and detailed requirements should be added to the TSI WAG.

To realistically achieve the overall goal, it may be necessary to include exceptions i.e., generic exceptions in aspects of the certification process. This is required as although the newly introduced components are all standardised the vehicles are not in a standardised authorisation status. Thus, the current necessity to assess the changes made to the vehicles by a NoBo/ DeBo/ AsBo could result in a potentially overwhelming task. Those derogations shall be included in the TSIs and allow above all to reduce the time necessary for NoBos to perform their assessment. This could be achieved for example by providing derogations to the type examinations or by providing options for simplifying the demonstration of conformity.

5.3 Overall Safety Plan

5.3.1 Aim of the Safety Plan

Purpose of the safety plan is to define the activities necessary for conducting the risk management process according to implementing regulation (EU) 402/2013 [EU1], hereinafter also referred as CSM-RA. The risk management process shall ensure that risks introduced are managed in compliance with this Regulation.

In accordance with Annex I, chapter 1.1.6 of the CSM-RA the safety plan describes the organisation and the experts appointed to carry out the risk assessment process, the different actors' tasks, and their risk management activities to manage hazards and the associated safety measures.

The processes for risk management, including the activities with the required input and output documents, are recorded in the safety plan. It thus describes all safety management activities at the level of the overall project in conformity with Annex I, Chapter 1.1.1. of the CSM-RA and specifies the requirements for the documentation.

In case of the project **"Full digital freight train operation"** the risk management process shall cover the affected factors listed hereunder:

☐ Overall safety level of the rolling stock concerned is compromised according to Interoperability Directive 2016/797/EU [EU2] Art 21 (12) b).

☒ Requirements Capture according to implementing regulation 2018/545/EU [EU3] Article 13 is necessary.

☒ Requirements based on the Technical Specifications Interoperability demand a risk management process.

☐ Measures to mitigate the consequences of nonconformities in accordance with Implementing Regulation (EU) 2018/545 [EU3] Article 27 are required.

The safety plan is valid for the vehicles which are within the scope of the project as defined under 5.1.

5.3.2 System Interface

The safety plan for the **"Full digital freight train operation"** describes the procedure of safety case management for the integration of the Digital Automatic Coupling and the related train functions into the European rail system. The following figure shows the system interfaces that shall be considered in this context.

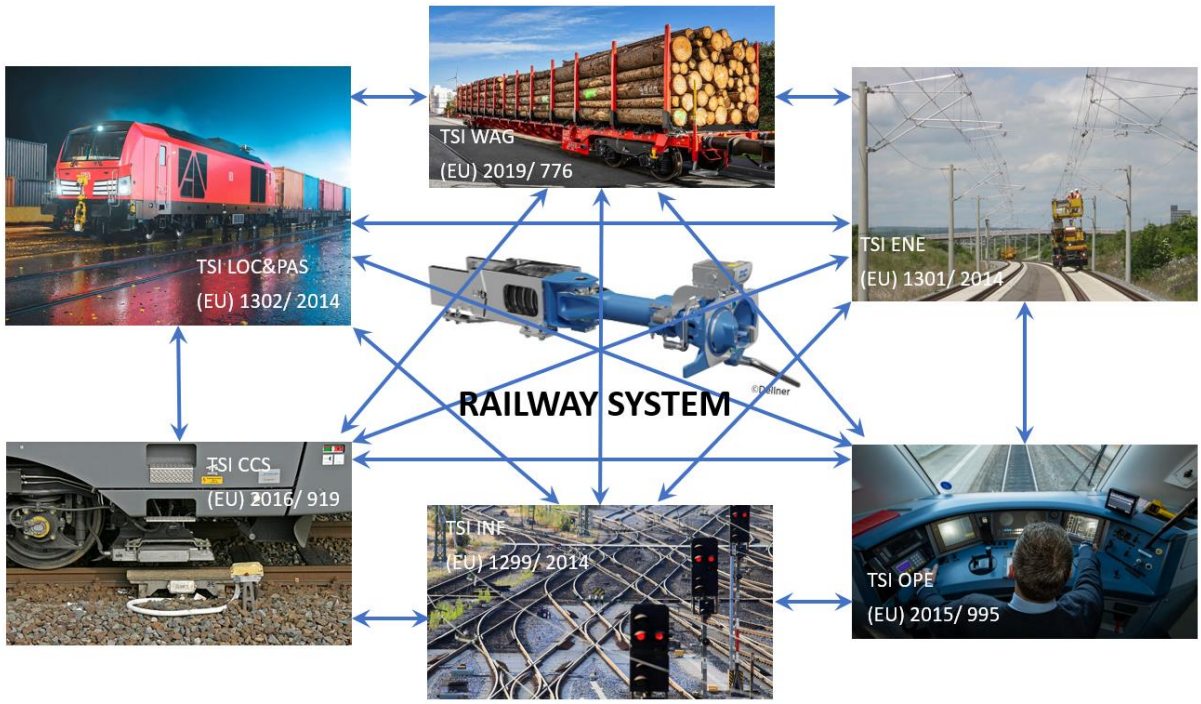

Figure 2 System interfaces, railway system

Affected?	ID	Title of Technical specification of Interoperability
☒	**TSI WAG**	Commission Regulation (EU) No 321/2013 of 13 March 2013 concerning the technical specification for interoperability relating to the subsystem rolling stock — freight wagons of the rail system in the European Union and repealing Decision 2006/861/EC [EU4]
☒	**TSI ENE**	Commission Regulation (EU) No 1301/2014 of 18 November 2014 on the technical specifications for interoperability relating to the energy subsystem of the rail system in the Union [EU5]
☒	**TSI LOC& PAS**	Commission Regulation (EU) No 1302/2014 of 18 November 2014 concerning a technical specification for interoperability relating to the rolling stock — locomotives and passenger rolling stock subsystem of the rail system in the European Union [EU6]

Affected?	ID	Title of Technical specification of Interoperability
☒	**TSI OPE**	Commission Regulation (EU) 2015/995 of 8 June 2015 amending Decision 2012/757/EU concerning the technical specification for interoperability relating to the operation and traffic management subsystem of the rail system in the European Union [EU7]
☒	**TSI NOI**	Commission Regulation (EU) No 1304/2014 of 26 November 2014 on the technical specification for interoperability relating to the subsystem rolling stock — noise amending Decision 2008/232/EC and repealing Decision 2011/229/EU [EU8]
☒	**TSI TAF**	Commission Regulation (EU) No 1305/2014 of 11 December 2014 on the technical specification for interoperability relating to the telematics applications for freight subsystem of the rail system in the European Union and repealing the Regulation (EC) No 62/2006 [EU9]
☒	**TSI CCS**	Commission Regulation (EU) 2016/919 of 27 May 2016 on the technical specification for interoperability relating to the control-command and signalling subsystems of the rail system in the European Union [EU10]
☒	**TSI INF**	Commission Regulation (EU) No 1299/2014 of 18 November 2014 on the technical specifications for interoperability relating to the 'infrastructure' subsystem of the rail system in the European Union [EU11]

Table 8 Affected TSI

5.3.3 Legal and Normative Framework of the Safety Plan

To create a Single European Railway Area (SERA), the European institutions have published the Railway Safety Directives 2016/798/EU [EU12] and Interoperability Directive (EU) 2016/797 [EU2] for technical harmonisation of the railway as well as requirements on the railway safety. These directives have been implemented into national law in the Member States.

The Interoperability Directive 2016/797/EU, in addition to the technical requirements for safety in Art. 21, formulates requirements for authorisations for placing a product on the market. Paragraph (9) of the article refers to the adoption of an implementing regulation by the Commission to fulfil the requirements of the authorisation. This has been implemented with the introduction of the implementing regulation (EU) 2018/545 [EU3], which thus provides a basis for the safety demonstration described in this document.

Another basis for the safety case management is the implementing regulation (EU) 402/2013 [EU1]. A suitable method to demonstrate compliance to the requirements of the CSM-RA is the European standard EN 50 126-1 [ST1]. The safety case management described in this project is based on the most recently named European standard.

5.3.4 Requirements Capture

The following figure shows the relationship between the requirements according to Art. 13 of Directive (EU) 2018/545 [EU3], the CSM-RA and the European standard EN 50 126-1 [ST1] in regard of the Requirements Capture. This is described in detail in the clarification note

ERA1209/146 [EU4].

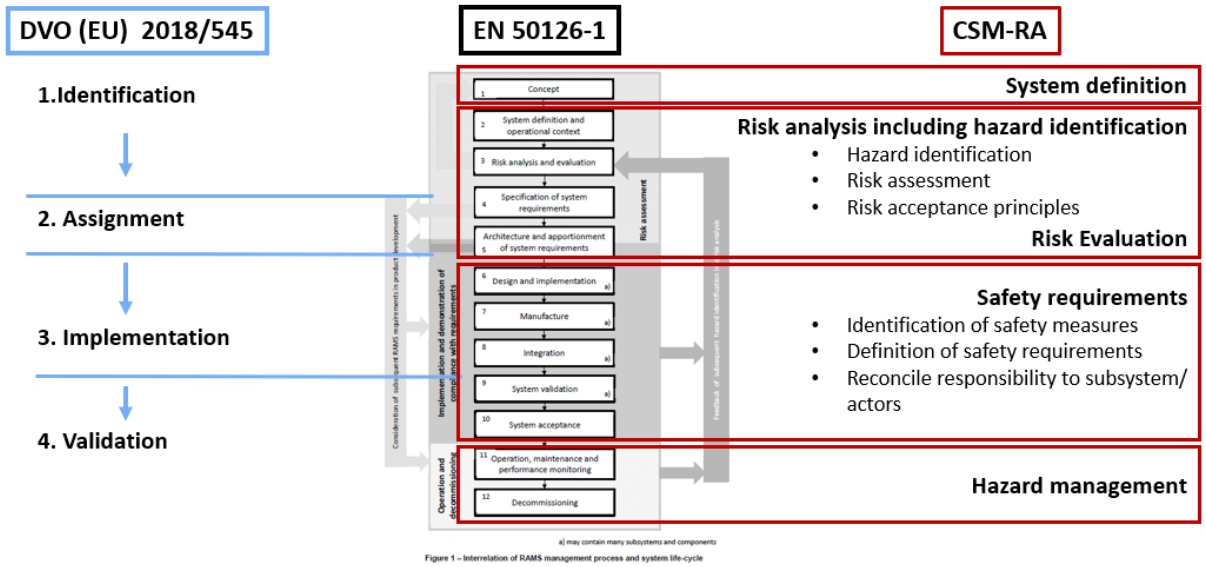

Figure 3 Relationship (EU) 2018/545 [EU3], CSM-RA an EN 50 126-2 [ST1]

For the "Requirements Capture" the following sources will be used.

- Basic requirements according to Directive (EU) 2016/797 [EU2]
- Requirements according to the Technical Specifications Interoperability (TSI)
- Requirements according to Notified National Technical Rules (NNTR) listed in the Reference Document Database (RDD)
- Requirements according to other European directives and regulations
- Requirements according to the regulations of the railway company of member states

For the project **"Full digital freight train operation",** freight wagons and locomotives shall be fitted with a digital automatic centre buffer coupler (DAC) and related train functions. In principle, upgrading freight wagons is formally dealt with in the TSI WAG. In the current version not all aspects of the change are covered. For example, the compatibility of the change with electromagnetic requirements or coupling criteria with automatic couplers or activation of emergency braking in case of train separation are missing. The aspects which are not dealt with by the TSI WAG and further deviating regulations have been identified in accordance with Art. 13(3) and Art. 28 of the Commission implementing regulation 2018/545/EU. These aspects are evaluated within the risk management procedure and the fulfilment of the identified safety requirements are described here. In the case of locomotives, the TSI LOC&PAS is mandatory. Should there be any aspect not dealt with in the TSI LOC&PAS, the procedure will be the same as used on the TSI WAG for freight wagons described above.

Since the project is a European project for the creation of a common European digital freight rail transport system, the NNTRs are also analysed as requirements. It is recommended to

transfer the topics identified by the NNTR analysis as rules in the corresponding regulations, in particular the NNTR as specific cases into a new version of the TSI WAG.

The requirements formulated in Art. 13(1) of the Commission implementing regulation 2018/545/EU are listed in the following table. The responsibilities as regards their implementation for the project **"Full digital freight train operation"** have been assigned in the same table.

(EU) 2018/545 [EU3] Article 13(1) In accordance with the overall objective of managing and mitigating identified risks to an acceptable level, the applicant shall, before submitting an application, undertake a requirement capture process which shall ensure that all the necessary requirements covering the design of the vehicle for its life cycle have been:			
Legal text	**Responsible**	**Participating**	**Implementation in the project by:**
(a) **identified** properly	Proposer	Approval manager Safety manager Project manager	▪ Risk management with ○ Analysis of TSI-Requirements ○ Analysis of NNTR-Requirements ○ Analysis of requirements of the European directives and regulations ▪ Analysis of regulations of the railway company of member states ▪ System definition according to migration strategy ▪ Hazard identification and classification
(b) **assigned** to functions or subsystems or are addressed through conditions for use or other restrictions; and	Proposer	Safety manager Project manager Technical experts	▪ Hazard tree ▪ Hazard log
c) **implemented** and	Proposer	Safety manager Project manager Technical experts Principal contractor	▪ Development and redesign process of the railway company of the member state ▪ Supplier management of the railway company of the member state

(EU) 2018/545 [EU3] Article 13(1) In accordance with the overall objective of managing and mitigating identified risks to an acceptable level, the applicant shall, before submitting an application, undertake a requirement capture process which shall ensure that all the necessary requirements covering the design of the vehicle for its life cycle have been:			
Legal text	**Responsible**	**Participating**	**Implementation in the project by:**
c) **validated**.	Proposer	Project manager Principal contractor	▪ Safety case management ▪ Acceptance process of a railway vehicle of the railway company of the member state

Table 9 Requirements Art. 13(1) 2018/545/EU

Paragraphs 2 and 3 of Art. 13 of Regulation (EU) 2018/545 [EU2] define the requirements to be met by the applicant for the subsystem under consideration when introducing a change. The process for recording the requirements defined here is carried out in three steps.

In the first step, the safety requirements for the subsystem under consideration are determined in relation to the essential requirements of safety in accordance with the Interoperability Directive (EU) 2016/797 [EU2] Annex III. In a second step, further requirements on the subsystem are determined and covered by the TSI and NNTR analysis as part of the preparation of the approval concept. In a third step of the process, the results from the two previous steps are reconciled in an allocation matrix.

(EU) 2018/545 [EU3] Article 13 (2) The requirements capture performed by the applicant shall in particular cover the following requirements:			
Legal text	**Step 1**	**Step 3**	**Step 3**
a) essential requirements for subsystems referred to in Article 3 and specified in Annex III to Directive (EU) 2016/797;	▪ System definition according to migration strategy ▪ Hazard identification ▪ Determination of risk acceptance principle → Safety requirements	▪ TSI- Analysis ▪ NNTR-Analysis → Approval concept	→ Allocation matrix Tabel 3
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.			

Table 10 Requirements Art. 13(2) (EU) 2018/545 [EU2]

Title	Hazard ID	RAP	2016/797/EU, Annex III	Regulation	Required proof → Responsible
Mass	BB1	COP	Safety 1.1.3	**TSI LOC&PAS 4.2.2.10** → EN 15663	Validation Mass balance → Technical expert mass

Table 11 Allocation matrix, Requirements Art.13(2) (EU) 2018/545 [EU2] (example)

(EU) 2018/545 [EU2] Article 13 (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.

Legal text	Step 1	Step 3	Step 3
-	▪ System definition according to migration strategy ▪ Hazard identification ▪ Determination of risk acceptance principle → Safety requirements	▪ Analysis of requirements of the European directives and regulations → Requirements of the European directives and regulations	→ Allocation matrix Table 5 and 6

Table 12 Requirements Art. 13(3) (EU) 2018/545 [EU2]

Directive/ Regulation	Essential requirements 2016/797/EU Interoperability of the rail system Annex III					
	Safety	Technical compatibility	Reliability and availability	Health	Environmental protection	Accessibility
2011/65/EU	-	-	-	X	X	-

Table 13 Allocation matrix I, Requirements Art. 13(3) (EU) 2018/545 [EU2] (example)

Directive / Regulation	Technical Implementation	Implementation in the project by:	Responsible	Independent evaluation	Hazard- ID
2011/65/EU	EN IEC 63000	Proof of conformity	Principal contractor Supplier	---	---

Table 14 Allocation matrix II, Requirements Art. 13(3) (EU) 2018/545 [EU2] (example)

5.3.5 Actors and Relationship between the Actors

A project-specific team shall be set up to carry out the safety case management in accordance with Commission Implementing Regulation (EU) 402/2013 [EU1].

Demonstrating that a specific person is suitable or qualified is the responsibility of the department responsible for the person in accordance with Annex I, 1.1.2 and 1.1.6 of the Commission Implementing Regulation (EU) 402/2013 [EU1]. The project manager is responsible for appointing a person with appropriate expertise from the responsible department. The responsibility for the professional qualification of the selected experts lies with the respective head of the department, who confirms the professional suitability of the persons in writing.

This chapter describes

- Role of the proposer
- The tasks of the different actors and their risk management activities.
- The organisation and the experts appointed to carry out the risk assessment process.

For the experts of the expert team, verifier, validator and safety manager, documents shall be provided, which provide evidence on the respective education, training and professional experience. These documents are made available to the assessment body for checking the competence of the persons involved. Likewise, the competence of experts and assessors to be involved in the future must be demonstrated to the assessment body.

5.3.5.1 Actors

5.3.5.1.1 Proposer

The responsibility for the implementation of the risk management process according to CSM-RA is a result of the infrastructure managers and railway undertakings responsibility for the safe operation of the rail system and the control of risks associated with it as defined in Art. 4 (1) (d) and (d)(i) (EU) 2016/798.

In the CSM-RA, this responsibility is assigned to the role of the proposer as 'the company or organisation in charge of implementing the change'.

In the case of the implementation of the DAC, the 'proposer' can be one of the following (Art.3 (11) (EU)2013/402):

- an entity in charge of maintenance which implements measures in accordance with Article 14a (3) of Directive 2004/49/EC; (new: Art.14 (2) of directive (EU) 2016/798)
- contracting entity or a manufacturer which invites a notified body to apply the 'EC' verification procedure in accordance with Article 18(1) of Directive 2008/57/EC (new: Art. 15(1) (EU) 2916/797) or a designated body according to Article 17(3) of that Directive (new: Art. 13(1) (EU) 2916/797);
  (e.g., the manufacturer of an 'interoperability constituent'.)

The proposer shall be responsible

- for applying the CSM-RA, including the assessment of the significance of the change, and for conducting the risk management process set out in Annex I CSM-RA and for documenting the risk assessment in the hazard record.
- for involving experts and other stakeholders in the risk assessment
- for coordinating the collaboration between the different actors involved, according to their respective tasks in order to manage the hazards and their associated safety measures.
- for ensuring that risks introduced by suppliers and service providers, including their subcontractors, are also managed in compliance with Annex I CSM-RA. To this end, the proposer may enforce through contractual arrangements that suppliers and service providers, including their subcontractors, participate in the risk management process set out in Annex I CSM-RA.

Based on the results of the application of the CSM-RA and on the safety assessment report provided by the assessment body, the proposer shall, according to Art. 16 CSM-RA, produce a written declaration that all identified hazards and associated risks are controlled at an acceptable level.

The proposer can delegate the right to carry out the risk assessment to a safety manager. The safety manager endorses then the responsibility of the proposer for the duration of the project.

5.3.5.1.2 Safety Manager

The safety manager designated by the proposer is responsible for the risk management procedure as defined in Annex I of the Commission Implementing Regulation 402/213/EU. He is authorised to act for and on behalf of the proposer during the project and reports to the proposer.

The safety manager carries out and documents the risk management procedure and participates by providing the necessary evidence that the safety requirements are fulfilled.

Within the scope of his activities, the safety manager has the right to escalate an issue if he feels a safety requirement will not be fulfilled despite the risk control measure proposed within the project. The escalation levels are described in the project manual.

Safety responsibility is transferred back to the proposer after completion of the safety assessment report by the assessment body. The safety manager is responsible for the project-related, technical communication with the assessment body.

5.3.5.1.3 Verifier and Validator

In addition to the functions described in the CSM-RA, the proposer is supported in the project by the roles of an independent verifier and validator (based on preferred organisational structure according to EN 50 126-1 [ST1].

The verifier examines and assesses, based on evidence, that the results (process, documentation, software or application) of the respective steps of the risk management process meet the requirements for completeness, correctness and consistency.

The validator checks and investigates the fulfilment of safety requirements and safe integration of components and related functions into the vehicle. The independence of the persons within the organisation must be ensured. The independence of the validator from the proposer must be ensured from a technical and organisational point of view. In addition, neither validator nor verifier take on design or implementation tasks.

5.3.5.1.4 Approval Manager

During the project, the approval manager acts as a contact person for vehicle keepers, railway undertakings and manufacturers of rolling stock with the aim of obtaining approval from the competent authorising entity. A positive outcome of the project shall be strengthened through the development of an authorisation strategy, the definition of the assessment basis through a TSI/NNTR analysis, the operation of registers and the coordination of the conformity assessment with the competent bodies. In doing so, the project interests are represented to various stakeholders, such as assessment bodies, national safety authorities and authorising

entity.

5.3.5.1.5 Project Manager

The project manager is responsible for the planning, control, and implementation of the project in accordance with deadlines, quality, and costs. According to the requirements of the safety management, he or she provides the resources of the technical experts for the processing of the safety topics. The responsibility for the technical qualification of the selected experts lies with the respective head of the technical department, who confirms the technical competences of the persons in writing. Several project managers from different divisions can be integrated into the project. In this case, the leading project manager is the project manager of the principal contractor.

5.3.5.1.6 Technical Experts

The technical experts conduct and prepare the technical individual verifications and participate in the risk management process. They are bound by the safety manager's instructions in all safety-relevant aspects and are appointed by the project manager in consultation with the heads of the specialist departments based on their specialist knowledge. The technical experts provide the technical input for the documents to be prepared within the framework of the risk management procedure.

5.3.5.1.7 General Contractor

The rolling stock is converted by the general contractor. Documents required for the conversion, such as design documents, are made available to him by the technical experts for production. The general contractor is represented in the project by its project manager.

After the conversion has been carried out, it is documented by the general contractor. The conversion is carried out in accordance with the quality management system and specific quality-assured processes of the general contractor.

5.3.5.1.8 Suppliers

Suppliers of functionally safety-relevant systems or services participate in the conversion of the vehicles on behalf of the principal contractor and are thus part of the safety demonstration process in accordance with CSM-RA Art. 5. The verification on the part of the suppliers is integrated into the overall documentation of the project.

The suppliers must maintain a safety and quality management system to meet the requirements of CSM-RA Annex I, Chapter 1.1.2. and Article 6, Chapter 2, b).

5.3.5.1.9 Conformity Assessment Body

The conformity body is defined as a body issuing declarations of conformity according to Directive 2016/797/EU Article 2(42). It shall comply with the requirements relating to its legal form, impartiality and employees set out in Articles 30 to 32 of the Directive. A conformity assessment body is designated by a member state and may be a notified body, a designated

body or both.

5.3.5.1.9.1 Notified Body

A notified body is a conformity assessment body authorised to assess the conformity or suitability for use of the constituents in relation to the TSIs concerned in accordance with Chapter VI of Directive 2016/797/EU Chapter 2. The notified body shall draw up a dossier in accordance with Article 15 (4) of Directive 2016/797/EU.

5.3.5.1.9.2 Designated Body

A designated body is a conformity assessment body which is authorised to assess the conformity or suitability for use of the constituents in terms of Chapter VI of Directive 2016/797/EU Chapter 3 about the National Notified Technical Regulations concerned. The designated body shall issue a test certificate in this respect.

5.3.5.1.10 Assessment Body

An assessment body is, according to CSM-RA Annex II, an independent, competent external or internal natural person, organisation, or body. It is recognised in accordance with Article 9 of the notified directive and carries out an independent assessment in accordance with CSM-RA Article 6 about the safety case. As a result of the assessment, it shall prepare a safety assessment report in accordance with implementing regulation (EU) 402/2013 [EU1], Article 15.

The documents relevant to the safety assessment shall be agreed with the delegated body in a list of documents. The safety assessment shall be carried out by the assessment body in accordance with Annex III of the Implementing Regulation (EU) 402/2013 [EU1] based on an agreed chart of depreciation.

The result of the safety assessment shall be documented in a safety assessment report in accordance with Article 15 and Annex III of the CSM-RA and the suitability and IT application of the risk management procedure set out in Annex I of the CSM-RA shall be confirmed.

5.3.5.2 Relationship between the Actors

Chapter 1.2 of Annex I of the Commission Implementing Regulation (EU) 402/2013 [EU1] applies to safety case management. The first point of contact for these topics is the safety manager, who is also responsible for compliance with the interfaces focus area described in this chapter. The safety manager therefore has an interface to all actors of the safety case management in the further course of this chapter, with the aim of managing common risks on the interfaces focus areas. The individual interfaces focus areas on the project are described below.

5.3.5.2.1 Relationship to the Proposer

All documents created within the framework of the safety case management shall be handed over to the proposer at the end of the project. The handover is to be confirmed by him in

writing. This also applies to the hazard record, which must be continued under the responsibility of the proposer after handover.

The proposer is informed by the safety manager about necessary measures or SRACs, e.g., for operation and maintenance. The proposer assesses these and forwards them to the body responsible for compliance. If the SRACs can be implemented by the entity responsible for compliance, the proposer confirms the acceptance of the requirements in writing to the safety manager. If the justification is not sufficient, a requirement shall be formulated by the safety manager.

5.3.5.2.2 Relationship to the Risk Management

Risk management ensures that the risk management process is implemented correctly and is primarily carried out by the safety manager. The safety manager works closely with the the project team. Furthermore, the project safety manager maintains communication with the safety managers of the suppliers and the general contractor.

The risk management, in coordination with the project manager and proposer, takes over the communication to the assessment body.

5.3.5.2.3 Relationship to the Authorisation Management

The facts to be verified are coordinated with the applicant and the entity managing the change. With the involvement of the safety manager, the applicant or the entity managing the change carries out a TSI/NNTR relevance analysis, which brings together all aspects of verification about TSI and NNTR. The documentation of the risk assessment process needs to be countersigned by the applicant or the entity managing the change responsible for the project.

5.3.5.2.4 Relationship to the General Contractor

The conversion of the rolling stock is carried out according to the defined procedures of the general contractor. Design documents for the conversion are provided by the technical experts. After transit of the conversion, the general contractor documents that the conversions have been carried out in accordance with the design documents.

In accordance with the authorisation strategy, an EC inspection of the quality system is carried out for the implementation of the conversion.

5.3.5.2.5 Relationship to the Technical Experts

The technical experts provide the documentation required for the verification and provide technical support for the safety verification. The documents required for the preparation of the records, including documentation from suppliers, are provided by the principal contractor.

The documentation of the risk assessment procedure and the technical safety report are co-signed by the responsible technical experts. The technical experts prepare the electrical and

mechanical design documents in the project, according to which the principal contractor implements the conversion work. The technical experts are also used as vehicle testers, if necessary, and test selected and commissioned functions, which are defined in a test specification, on one of the converted vehicles. The project team decides on a suitable test vehicle.

5.3.5.2.6 Relationship to the Suppliers

The supplier of functionally safety-relevant systems receives a requirement specification from the project manager, which includes the safety requirement to be fulfilled.

The engineering including the safety verification of the supplier is the responsibility of the supplier. Proof of compliance with the safety requirement is provided by the supplier in a suitable manner.

5.3.5.3 Project Team

The table below shows a proposal for the composition of a project team for safety case management.

Actor	**Propose for actor**
Proposer	ECM or person of manufacturer of the freight wagon, locomotive or component
Safety manager	ECM or person of manufacturer of the freight wagon, locomotive or component with experience of safety case management
Project manager	ECM or person of manufacturer of the freight wagon, locomotive or component
Applicant/entity managing the change	ECM or person of manufacturer of the freight wagon, locomotive or component
Technical expert Mass	ECM or person of manufacturer of the freight wagon, locomotive or component with experience in mass management of rail vehicles
Technical expert entity managing the change	ECM or person of manufacturer of the freight wagon, locomotive or component with experience in entity managing the change of rail vehicles
Technical expert, Strength	ECM or person of manufacturer of the freight wagon, locomotive or component with experience in strength of rail vehicles
Verifier	Independent safety expert chosen by the proposer
Validator	Independent safety expert chosen by the proposer
Assessment Body	Chosen AsBo according to NANDO

Actor	Propose for actor
Notified Body	Chosen NoBo according to NANDO/ ERADIS
Designated Body	Chosen NoBo according to RDD
Principal Contractor	ECM of the freight wagon or locomotives or manufacturer of the freight wagon or locomotives
Manufacturers/Suppliers	---
further experts / reviewers	---

5.3.6 Generic Risk Management Process

In the following table there are shown the planned steps of the risk management process as well as the responsible actor of the step according to CSM and the chapter of the explanatory of the step in this document.

Designation	Responsible	Chapter
Risk management process		
Planning of the risk management process	Proposer supported by safety manager	
Project environment and stakeholders		5.1
Definition of the tasks, the different actors and their risk management activities	Proposer, expert team	5.3.5
Evidence of the application of appropriate quality assurance measures	Proposer, expert team	5.3.6.1
Preparation of safety plan (incl. definition of methods and instruments for risk assessment)	Proposer, expert team	5.3.6.2
Risk assessment process		
System Definition	Proposer, expert team	5.3.6.3.1
Risk Analysis including hazard identification	Proposer, expert team	5.3.6.3.2
Hazard identification	Proposer, expert team	5.3.6.3.2.1
Risk assessment	Proposer, expert team	5.3.6.3.2.2
Risk acceptance principles	Proposer, expert team	5.3.6.3.2.3
Risk Evaluation	Proposer, expert team	5.3.6.3.2.4
Definition of safety requirements		

Designation	Responsible	Chapter
Identification of safety measures	Proposer, expert team	5.3.6.5
Definition of safety requirements	Proposer, expert team	5.3.6.5
Acceptance of safety requirements	Proposer, expert team	5.3.6.6.8
Hazard management	Proposer supported by safety manager	5.3.8.3
Demonstration of compliance with safety requirements	responsible actors under the supervision of the proposer, validator	
Evidence from the application of the risk management process		
Documentation of the risk management process	Proposer supported by safety manager	
Independent evaluation of the risk management process		
Safety assessment report	Independent assessment body	5.3.6.7.2
Written statement of the proposer	Proposer	5.3.6.7.3

Table 15 Steps of risk management process

5.3.6.1 Evidence of the Application of Appropriate Quality Assurance Measures

Effective safety and quality management must be established in a company for the entire life cycle of a system/subsystem after deploying a change or upgrading the system/subsystem. Monitoring and control processes must be implemented in order to be able to detect and specifically eliminate sources of error. Only in this way can the required goals for safety and quality be achieved and continuously increased. The close relationship between safety and quality is evident in the fact that safety and availability goals are monitored and met through the same tools and control methods. These include:

- Fulfilment of reliability and maintainability requirements
- Ongoing monitoring of maintenance work and the operational environment

The risk management procedure is directly concerned only with safety and not primarily with quality. The methods listed have the objective of underpinning the specifications of the CSM-RA.
The risk management process includes appropriate quality assurance measures and is carried out by qualified personnel. The methods for monitoring and controlling quality are described separately as part of quality management.

Compliance with this requirement is ensured via the following evidence:
The proposer has a quality management system based on EN ISO 9001 [ST2], which covers all the necessary processes for a risk management processes.

5.3.6.2 Determination of Methods and Tools for Risk Assessment

Risk assessments are an important building block for identifying and recording hazards, their causes and effects on rail operations, and for determining the safety requirements of systems and processes. The risk management regulations or the SMS do not specify more detailed requirements for the practical design and format of the hazard record.

The methods and instruments used there correspond to and complement the provisions of the CSM-RA.

5.3.6.3 Risk Assessment Process

The risk assessment process includes the following steps:

- System Definition
  - Preparation of the system definition
  - Preliminary coordination of system definition with experts
- Risk Analysis including hazard identification
  - Hazard identification
  - Risk assessment
- Selection of risk acceptance principles
- Risk Evaluation
  - Verification of appropriate application of risk acceptance principles
  - Verification of uniform application of risk acceptance principles
- Definition of safety requirements
  - Determination of possible safety measures
  - Define safety requirements
  - Decision, who will be in charge of fulfilling the safety requirements
- Hazard management
  - Establish and maintain hazard records

All hazards identified in the risk assessment process and the corresponding safety measures along with system assumptions are documented in hazard logs by the proposer until the safety assessment report is submitted and are continuously reconciled and updated with the risk assessment process.

The hazard record shall include all hazards, together with all related safety measures and system assumptions identified during the risk assessment process. It shall contain a clear reference to the origin of the hazards and to the selected risk acceptance principles and clearly

identify the actor(s) in charge of controlling each hazard. It is updated whenever an already identified hazard changes or a new hazard is identified.

At the same time, the proposer coordinates for each interface relevant to the system under assessment and without prejudice to specifications of interfaces defined in relevant TSIs, that the concerned actors cooperate with each other to identify and manage jointly the hazards and related safety measures that need to be handled at the interfaces. The management of shared risks at the interfaces shall be coordinated by the proposer.

When agreement cannot be reached between two or more actors it is the responsibility of the proposer to find a solution. Independently from the definition of the system under assessment, the proposer is responsible for ensuring that the risk management covers the system itself and its integration into the railway system as a whole.

5.3.6.3.1 System Definition

The risk management process starts from a definition of the system under assessment and addresses at least the following issues:

a. System objective (intended purpose).
b. System functions and elements, where relevant (including human, technical and operational elements).
c. System boundary including other interacting systems.
d. Physical (interacting systems) and functional (functional input and output) interfaces.
e. System environment (for example energy and thermal flow, shocks, vibrations, electromagnetic interference, operational use).
f. Existing safety measures and, after the necessary relevant iterations, definition of the safety requirements identified by the risk assessment process.
g. Assumptions that determine the limits for the risk assessment.

5.3.6.3.2 Risk Analysis including Hazard Identification

5.3.6.3.2.1 Hazard Identification

Responsible:
WP4 - Equipment Authorisation Procedures, Train Authorisation Strategy and Procedures
Subtask 4.3 Identification and assignment of requirements and harmonization of safety architecture

How:

Based on operational procedures, understanding the functions applicable to a freight train (from planning to train preparation, train inauguration, train run, shunting to train termination) and communication modes (normal and degraded mode), the stages of operations of a freight train will be modelled.

5.3.6.3.2.2 Risk Assessment

To focus the risk assessment efforts upon the most important risks, the hazards are classified according to the estimated risk arising from them. Subsequently, the identified hazards and risks are evaluated, and a safety classification will be performed for each function considered to derive a SIL. The safety classification will be made by means of safety parameters. Based on expert judgement, hazards associated with a broadly acceptable risk need not be analysed further but shall be registered in the hazard record. Their classification shall be justified in order to allow independent assessment by an assessment body.

As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional safety measure (e.g., when SIL = 0). The expert judgement takes into account that the contribution of all the broadly acceptable risks does not exceed a defined proportion of the overall risk.

5.3.6.3.3 Risk Acceptance Principles

Responsible:
WP4 - Equipment Authorisation Procedures, Train Authorisation Strategy and Procedures
Subtask 4.3 Identification and assignment of requirements and harmonization of safety architecture

How:
Based on the hazard identification from the previous step, the risk acceptance principle and criteria are assigned to the identified hazards. Furthermore, the safety requirements with their respective degree of severity are defined in this step, as well as the allocation of the safety responsibility to the respective actors concerned.

The risk acceptability of the system under assessment is evaluated by using one or more of the following risk acceptance principles:

- the application of codes of practice
- a comparison with similar systems
- an explicit risk estimation

Risk acceptance principles are divided into implicit and explicit procedures. Implicit risk acceptance is demonstrated by applying a set of rules or proving a reference system. Implicit proofs are called implicit because the acceptance criterion is not known to be a sharp boundary. In explicit risk assessment, the proof of risk acceptance is performed against a sharply defined acceptance boundary ('harmonised quantitative design targets '). Depending

on the acceptance principle selected, special attention should be paid to:

5.3.6.3.3.1 Use of Codes of Practice

In case: It is shown that the hazards several or all hazards are appropriately covered by the application of relevant codes of practice. The codes of practice shall satisfy at least the following requirements:

a. They must be widely recognised in the railway domain. If this is not the case, the codes of practice will have to be justified and be acceptable to the assessment body.

b. They must be relevant for the control of the considered hazards in the system under assessment. Successful application of a code of practice for similar cases to manage changes and control effectively the identified hazards of a system in the sense of this Regulation is sufficient for it to be considered as relevant.

c. Upon request, they must be available to assessment bodies for them to either assess or, where relevant, mutually recognize, in accordance with Art. 15(5) of [EU1], the suitability of both the application of the risk management process and of its results.

Where compliance with TSIs is required by Directive (EU) 2016/797 [EU2] and the relevant TSI does not impose the risk management process according to [EU1], the TSIs may be considered as codes of practice for controlling hazards, provided above requirement (b) is fulfilled.
Similarly, NNTRs may be considered as codes of practice when requirement (b) is fulfilled. If one or more hazards are controlled by codes of practice fulfilling the above requirements, then the risks associated with these hazards shall be considered acceptable. This means that:

- these risks need not be analysed further.

5.3.6.3.3.2 Use of a Reference System

In case: If it is shown that the hazard is adequately covered by a similar system that could be taken as a reference system. A reference system shall satisfy at least the following requirements:

a. it has already been proven in-use to have an acceptable safety level and would therefore still qualify for approval in the Member State where the change is to be introduced.

b. it has similar functions and interfaces as the system under assessment.

c. it is used under similar operational conditions as the system under assessment.

d. it is used under similar environmental conditions as the system under assessment

If a reference system fulfils the requirements listed above, then for the system under assessment the risks associated with the hazards covered by the reference system shall be considered as acceptable.

5.3.6.3.3.3 Explicit Risk Assessment and Evaluation

In case: If the hazards are not covered by one of the two risk acceptance principles laid down in points 2.3 and 2.4, the demonstration of risk acceptability shall be performed by explicit risk estimation and evaluation.

Risks resulting from these hazards shall be estimated either quantitatively or qualitatively, or when necessary both quantitatively and qualitatively, taking existing safety measures into account completion of the risk analysis.

The proposer is not obliged to perform additional explicit risk estimation for risks that are already considered acceptable by the use of codes of practice or reference systems.

The acceptability of the estimated risks shall be evaluated using risk acceptance criteria either derived from or based on requirements contained in Union legislation or in NNTRs. Depending on the risk acceptance criteria, the acceptability of the risk may be evaluated either individually for each associated hazard or the combination of all hazards considered in the explicit risk estimation.

If the risk associated with one hazard or a combination of several hazards is considered acceptable, the identified safety measures are registered in the hazard record. Where hazards arise as a result of failures of functions of a technical system, the following harmonized design targets shall apply to those failures:

- Criterion: a) where a failure has a credible potential to lead directly to a catastrophic accident (an accident in which a large number of people are usually harmed and several people are killed) ('directly' means that the failure of the function has the potential to lead (=may lead) to the type of accident without the need for additional failures to occur), the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be highly improbable (occurrence of a failure with a failure rate less than or equal to 10-9 per hour of operation) that a failure of the function will occur.
- Criterion: b) where a failure has a credible potential to lead directly ('directly' means that the failure of the function has the potential to lead (=may lead) to the type of accident without the need for additional failures to occur)) to a critical accident (accident in which usually a very small number of people are harmed and at least one person is killed;), the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be improbable (occurrence of a failure with a failure rate of 10-7 or less per operating hour).

the harmonized design targets set out above shall be used for the design e.g., of electrical, electronic and programmable systems. They shall be the most demanding design targets that can be required for mutual recognition. They shall neither be used as overall quantitative targets for the whole railway system of a Member State nor for the design of purely mechanical technical systems.

The risk associated with the failures of functions of technical systems referred to in point 2.5.5 shall be considered as acceptable if the following requirements are also fulfilled

a. Compliance with the applicable harmonized design targets has been demonstrated.

b. The associated systematic failures and systematic faults are controlled in accordance with safety and quality processes commensurate with the harmonized design target applicable to the technical system under assessment and defined in commonly acknowledged relevant standards.

The determination of the selected risk acceptance principle or verification procedure has to be documented in the function list of the vehicle.

5.3.6.4 Risk Evaluation

The proposer demonstrates in the risk evaluation that the selected risk acceptance principle is adequately applied. The proposer also checks that the selected risk acceptance principles are used consistently.

5.3.6.5 Identification of Safety Requirements

The application of risk acceptance principles shall identify possible safety measures that make the risk(s) of the system (or of the changes to the system) under assessment acceptable.

Based on the selected risk acceptance principles, the resulting safety requirements that the system to be evaluated must fulfil are determined from the identified hazards, risks and the documented function list. Put together they form the hazard protocol which is developed into a safety requirement specification.

Where the risk acceptance principle is based on codes of practice, the use of the codes of practice shall be registered in the hazard record as safety requirements for the relevant hazards.

Where a comparison with similar systems has been chosen as the risk acceptance principle, the safety requirement requires a demonstration by comparison that the hazards are adequately covered by a similar system that can be used as a reference system.

Criteria:

- the safety requirements for the hazards covered by the reference system may be derived from the safety analyses or from an evaluation of safety records of the reference system.
- these safety requirements are registered in the hazard record as safety requirements for the relevant hazard.

Where explicit risk assessment and evaluation has been selected for a hazard as a risk acceptance principle,

- The application conditions for the safe integration of the technical system under assessment into the railway system shall be identified and registered in the hazard record.
- these application conditions shall be transferred to the actor responsible for the demonstration of the safe integration.

5.3.6.6 Definition of Safety Requirements

Among these safety measures, those selected to control the risk(s) shall become the safety requirements to be fulfilled by the system. Safety requirements for suppliers and the entity managing the change.

Responsible:
WP4 - Equipment Authorisation Procedures, Train Authorisation Strategy and Procedures
Subtask 4.3 Identification and assignment of requirements and harmonization of safety architecture

How:
Based on the result of task 4.1 the proposer shall undertake a risk assessment as referred to Commission Implementing Regulation (EU) 402/2013 from which new or modified requirements might arise for the validation of subsystems to ensure a safe integration of the DAC with the related train functions into the vehicles and still guarantee safe operations of the vehicles concerned.

5.3.6.6.1 Safety Architecture and Allocation of Safety Responsibilities

To determine possible safety measures the safety responsibility can be distributed among all involved elements of the system architecture. Thus, limiting the risk to an acceptable level at different system levels by deriving associated safety measures.

For this purpose, **hazard trees may be created** allowing the distribution of the safety responsibilities to the subsystems based on the previously identified SIL

Hazard trees are used to split up and share safety responsibilities. The goal of splitting up the system safety requirements is to break down the safety objectives identified at the overall system level to lower levels, i.e., sub-functions and interfaces, and possibly to different stakeholders (e.g., subcontractors).

5.3.6.6.2 Derivation of the Safety Requirements

The requirements for the relevant elements of the system architecture and subsystems are derived from the hazard trees and fully diagrammed. The safety requirements are assigned to subsystems and/or components. Risk acceptance criteria and, if applicable, the required verification and acceptance processes and procedures for validation are assigned to the safety requirements.

For each identified element of the system architecture with a safety requirement level >0, the fulfilment of the measures against failures shall be demonstrated under all specified operating conditions and environmental influences. It shall also be demonstrated that any implemented fail safe mechanisms function properly.

5.3.6.6.3 Requirement for Elements of System Architecture containing Software

If the elements of the system architecture contain software, a verification is performed in accordance with EN 50657 depending on the respective requirements for the Software Safety Assurance Level (SSAS).

5.3.6.6.4 Requirements for Non-Interference

For all elements of the system architecture that contain software with software security assurance level (SSAS) = 0 and where there is a connection to software with a higher SSAS proof of non-interference shall be provided.

5.3.6.6.5 Requirement for Elements of System Architecture containing Hardware

For elements of the system architecture that contain hardware, the safety relevant specifications shall be appropriate.

5.3.6.6.6 Requirement for Elements of the System Architecture exposed to External Influences

If an element of the system architecture is open to external influences; these influences are described and evaluated with respect to the assigned safety responsibilities. This also concerns the continuation of the correct function under influences such as aging and special operating conditions.

5.3.6.6.7 Requirement for Activities by Persons involved in Operations

If an element of the system architecture includes activities by operating personnel or other persons involved in operation, the process of informing the relevant operator shall be documented. The inclusion of the relevant processes into the Safety Management System (SMS) shall be shown. In addition, safety-relevant conditions of use can be handed out in an operator manual and/or other safety-relevant documents in connection with the intended operation of the system.

5.3.6.6.8 Acceptance of Safety Requirements

Based on the results of the last steps of the risk assessment procedure, it will be up to the actor responsible for the individual safety requirements to indicate whether the requirement can be fulfilled as described. If the requirement can be fulfilled as described, the requirement shall be included in the checklist for the Entity Managing the Change. Such safety requirements should be included in the TSI. If the safety requirement is deemed as fulfilled and integrated into the TSI, the TSI- analysis provided herein should be adapted accordingly.

If the responsible actor indicates a safety requirement as being out of reach (impossible to be fulfilled), this requirement should be revised iteratively. The starting point for the iterative

revision must be decided within the project management.

Without prejudice to civil liabilities in accordance with the legal requirements of the Member States, the risk assessment process shall fall within the responsibility of the proposer. The proposer shall decide, with agreement of the actors concerned, who will be responsible for 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.

If, in order to fulfil a safety requirement, an actor identifies the need to implement a risk control measure which doesn't fall under his remit, the concerned actor shall, after agreement with the responsible actor, transfer the management of the related hazard to the latter.

5.3.6.6.9 Completion of Identification and Definition of Safety Requirements

The identification and definition of safety requirements is completed when all safety requirements for the system and the respective persons responsible for fulfilment have been defined and documented in the hazard records.

The proposer shall ensure that risks arising from its suppliers and service providers, including their subcontractors, are also managed in accordance with the CSM-RA. To this end, the proposer may enforce through contractual arrangements that suppliers and service providers, including their subcontractors, participate in the risk management process set out in Annex I CSM-RA. Suppliers shall demonstrate compliance of their products with the safety requirements.

5.3.6.7 Independent Evaluation of the Risk Management Process

5.3.6.7.1 Review of the Documentation of the Risk Management Process

The approach chosen for demonstrating compliance with the safety requirements, as well as the demonstration itself, shall be subject to independent assessment by an assessment body.

5.3.6.7.2 Safety Assessment Report

The assessment body shall record its conclusions in a safety assessment report. The safety assessment report is prepared by an assessment body in accordance with the CSM-RA.

5.3.6.7.3 Written Declaration by the Proposer

The assessment body sends its safety assessment report to the proposer for review and own assessment. Based on the application of the risk management process as well as its results

and the submitted safety assessment report, the proposer shall prepare a written declaration confirming that all identified hazards are maintained at an acceptable level.

5.3.7 Project Risk Assessment Process

The figure below provides a visual description of the risk assessment process which will be applied in this project and is based on the description in the chapter 5.3.6 of this document.

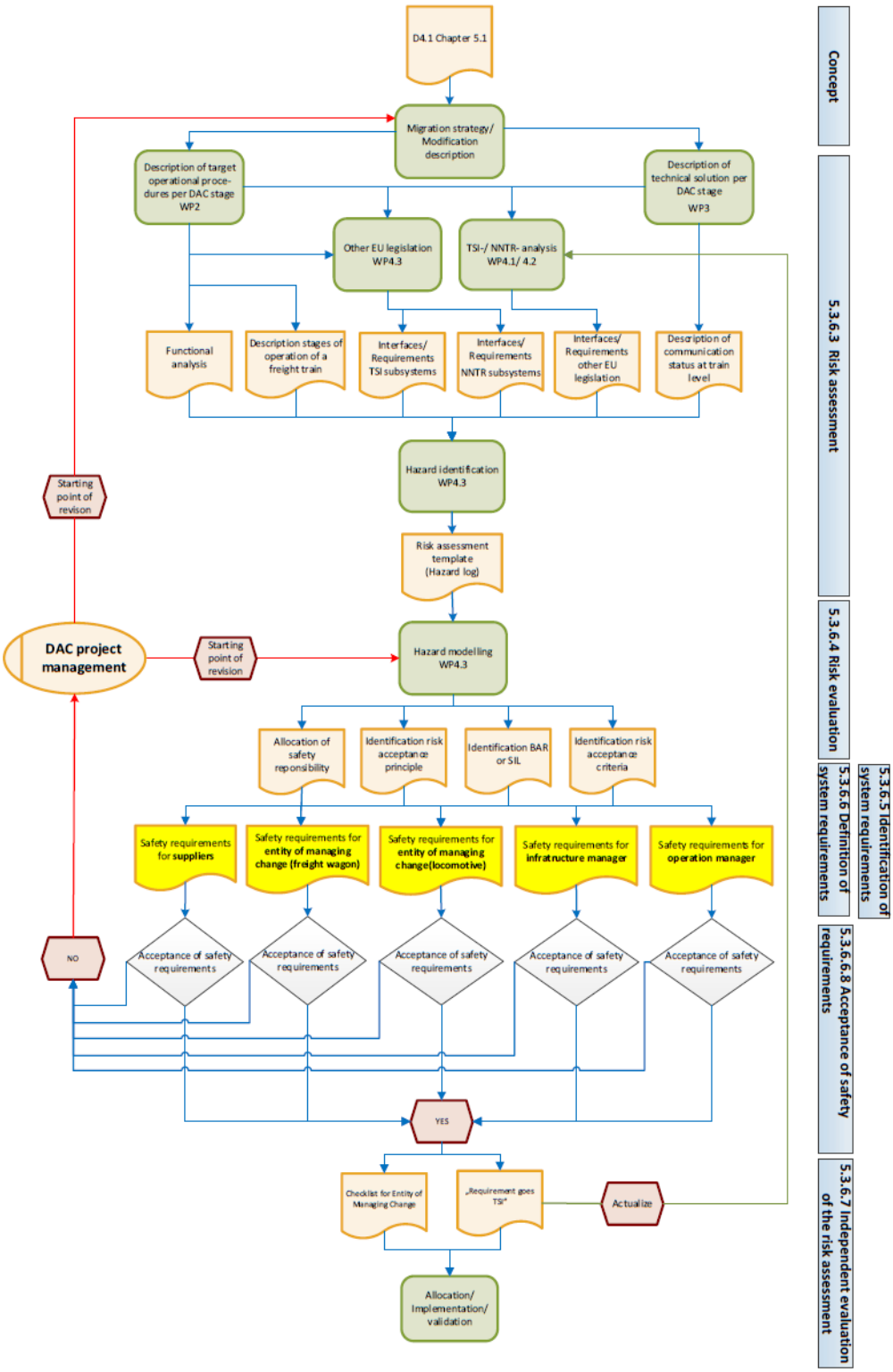

Figure 4 Project Risk Assessment Process

5.3.8 Documentation

The documentation to be provided as outcome of the risk management process is described in the chapters 5.3.8.1 – 5.3.8.5 hereunder.

5.3.8.1 Description of the Changes

Based on the stages defined in this document and the migration strategy, a description of all the changes which might be deployed at the level of the existing vehicles will be prepared. Maintenance tasks shall be clearly identified, as they are not part of the risk management procedure and are therefore under the responsibility of the proposer. The description of the changes will be used as the basis for system definition, hazard identification, hazard classification and requirements capture. All the information will be brought together in the "change analysis".

5.3.8.2 Documentation of the Risk Assessment

Considering the safety plan and based on the description of the changes, the documentation of the risk assessment procedure will be drafted by the safety manager. The drafting process for the risk assessment procedure is explained in the chapter 5.3.7 " Project risk assessment process" and includes as an outcome the system definition, the list of the safety requirements, the hazard records and the related risk acceptance principle as well as the provision of the required technical specifications.

5.3.8.3 Hazard Records

The hazard records in accordance with Art. 3 (16) of the Commission Implementing Regulation (EU) 402/2013 [EU1] lists the safety measures and safety assumptions defined to control the risks associated with the hazards and identified in the risk assessment procedure as a table for each vehicle version. Furthermore, the actors responsible for the technical verification are named and any necessary transfers of responsibilities are recorded.

5.3.8.4 Technical Verifications

The technical verifications are prepared by the respective technical experts, checked, and approved by the project manager. They are referenced in full or in excerpts in the documents of the chapters described above and describe the control of the risks associated with the hazards l based on the project-specific changes to an existing vehicle or vehicle type.

5.3.8.5 Safety- related Application Condition

The safety-related measures resulting from the risk assessment procedure, and which cannot be implemented in the vehicle subsystem, are transferred to other subsystems in the form of Safety-related application conditions, or SRACs. Typically, SRACs are handed over to operations and maintenance subsystems. In rare cases, individual SRACs can also be transferred to the infrastructure subsystem. SRACs can result both from safety requirements considered in the risk management process and coming from documents handed over by the supplier (manuals), or as a safety measure defined during the evaluation process. SRAC's must

be maintained by the Safety Manager within the so-called Technical Safety Report and will be appropriately assessed, and compliance confirmed by the proposer prior to finalising the generic risk assessment.

6 Conclusion

The upgrading of existing freight wagons with DAC and the related train functions will bring many advantages compared to the current coupling system which is the standard in Europe. However, the associated new hazards and risks must be identified and covered by appropriate safety measures before an upgrading can start. This means that an exhaustive set of requirements followed by a detailed and consistent test campaign ensuring a very high reliability and safety standards of the DAC with the related train functions at interoperability constituent level must be conducted.

Then, the **safe integration of the DAC into a vehicle** requires also extensive risk management and testing to avoid any safety and reliability concerns after upgrade.

The authorisation strategy and safety plan are part of an iterative process. This means that if there are some changes to the current FDFTO project's constraints like for example at the level of the migration strategy, of target operational procedures, related train functions etc. the authorisation strategy and safety plan shall be adapted accordingly.

It may be possible to deploy the DAC without the need for a new authorisation up to the stage "DAC is fully operational" (without the related train functions). For some of the additional train related functions listed in 5.1 will have the potential to trigger a new vehicle authorisation. This is especially true for those functions that will become part of the future train control system (ETCS).

If the proposed safety plan is implemented correctly by WP 4.3, then it can be used as evidence that the overall safety level will not be adversely affected according to Art. 21(12) b) Directive (EU) 2016/797 [EU2].

The TSIs shall be amended in any case with the new requirements concerning the DAC and the related train functions, especially those that are currently covered by national regulations or not yet included in the concerned subsystem. It may be necessary to include exemptions in the TSIs regarding the DAC upgrade to make the overall goal of introducing the DAC in the whole rail-freight sector feasible.

7 References

7.1 EU Directives and Regulations

Reference	Title	Date
[EU1]	Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009	30 April 2013
[EU2]	Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (recast)	11 May 2016
[EU3]	Commission Implementing Regulation (EU) 2018/545 of 4 April 2018 establishing practical arrangements for the railway vehicle authorisation and railway vehicle type authorisation process pursuant to Directive (EU) 2016/797 of the European Parliament and of the Council	4 April 2018
[EU4]	Commission Regulation (EU) No 321/2013 of 13 March 2013 concerning the technical specification for interoperability relating to the subsystem 'rolling stock — freight wagons' of the rail system in the European Union and repealing Decision 2006/861/EC	13 March 2013
[EU5]	Commission Regulation (EU) No 1301/2014 of 18 November 2014 on the technical specifications for interoperability relating to the 'energy' subsystem of the rail system in the Union	18 November 2014
[EU6]	Commission Regulation (EU) No 1302/2014 of 18 November 2014 concerning a technical specification for interoperability relating to the 'rolling stock — locomotives and passenger rolling stock' subsystem of the rail system in the European Union	18 November 2014
[EU7]	Commission Regulation (EU) 2015/995 of 8 June 2015 amending Decision 2012/757/EU concerning the technical specification for interoperability relating to the 'operation and traffic management' subsystem of the rail system in the European Union	8 June 2015
[EU8]	Commission Regulation (EU) No 1304/2014 of 26 November 2014 on the technical specification for interoperability relating to the subsystem 'rolling stock — noise' amending Decision 2008/232/EC and repealing Decision 2011/229/EU	26 November 2014
[EU9]	Commission Regulation (EU) No 1305/2014 of 11 December 2014 on the technical specification for interoperability relating to the telematics applications for freight subsystem of the rail system in the European Union and repealing the Regulation (EC) No 62/2006	11 December 2014
[EU10]	Commission Regulation (EU) 2016/919 of 27 May 2016 on the technical specification for interoperability relating to the 'control-command and signalling' subsystems of the rail system in the European Union	27 May 2016

Reference	Title	Date
[EU11]	Commission Regulation (EU) No 1299/2014 of 18 November 2014 on the technical specifications for interoperability relating to the 'infrastructure' subsystem of the rail system in the European Union	18 November 2014
[EU12]	Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety	11 May 2016

7.2 Standards

Reference	Title	Date
[ST1]	EN 50 126-1; Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process;	10-2018
[ST2]	EN ISO 9001; Quality management systems - Requirements	11-2015
[ST3]	EN 15 663; Railway applications - Vehicle reference masses	03-2019
[ST4]	EN IEC 63 000; Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances	05-2019