EUROPEAN UNION AGENCY FOR RAILWAYS

Making the railway system
work better for society.

Annex 10 to guide for the application of the CCS TSI

In accordance with Article 19(3) of Regulation (EU) 2016/796 of the European Parliament and of the Council of 11 May 2016

Guidance on the independent assessment of CCS ICs

Released by European Union Agency for Railways.

This document may serve as a clarification without however dictating in any manner compulsory procedures to be followed and without establishing any legally binding practice. The guide provides explanations on the provisions contained in the TSIs and should be helpful for understanding the approaches and rules described therein. However, it does not substitute to them.

The guide is publicly available, and when necessary regularly updated, to reflect progress with European standards and changes to the TSIs.

The reader should refer to the website of the European Union Agency for railways for information about its latest available edition.

The present document is a non-legally binding guidance of the European Union Agency for Railways. It is without prejudice to the decision-making processes foreseen by the applicable EU legislation. Furthermore, a binding interpretation of EU law is the sole competence of the Court of Justice of the European Union.

1 Introduction

1.1. Readers of the CCS TSI do not have all the same understanding of the TSI requirements, especially when reading parts of the specification outside the overall context. The following questions arise often, and lead to long discussions :

(a) **Question 1:** Does the CCS TSI limit the independent safety assessment to safety requirements of the CCS TSI (i.e. only the -S of RAMS), and therefore does it relax the assessor from the assessment of the applicant's demonstrations of fulfilment of the reliability, availability and maintainability (RAM) requirements of the TSI?

(b) **Question 2:** Does the CCS TSI leave freedom to the applicant, the manufacturer, or the NoBo (in the scope of the EC verification of conformity with requirements essential to safety), to select freely an independent safety assessor (ISA) for the independent safety assessment of Interoperability Constituents (ICs) instead of an AsBo?

1.2. The purpose of this part of the guideline for the application of the CCS TSI is answer to those questions, with a reference to the associated requirements of the CCS TSI as a justification.

1.3. It is importance to emphasise the following. The CCS TSI specification is a consistent set of inter-related requirements. It defines the mandatory process requirements the applicants shall apply for the design, implementation, manufacturing, installation, verification and validation (including safety acceptance), risk assessment and risk management, as well as for the independent assessment of both the CCS subsystems and their basic interoperability constituents. Thereby, unless explicitly written down in the CCS TSI, the following sections of the CCS TSI are interdependent with each other :

(a) section § 3.2.1 concerning the "**S**afety" requirements;
(b) sections § 3.2.2 and § 4.2.1 concerning the "**R**eliability and **A**vailability " requirements, and;
(c) section § 4.5 on "**M**aintenance" rules (referenced to also in section § 4.2.1.2.);

As explained below, they shall be applied to both the control-command and signalling "subsystems" and their basic "interoperability constituents or groups of interoperability constituents".

1.4. This implies that the reader shall not take out, and shall not interpret in isolation, any paragraph, or any section, outside the complete context of the CCS TSI. Otherwise, it is likely that partial readings of isolated parts of the CCS TSI result in the implementation of less restrictive processes, or less demanding requirements for the design, implementation, manufacturing, installation, verification and validation (including safety acceptance), risk assessment and risk management, and independent assessment of the CCS sub-systems, interoperability constituents or groups of interoperability constituents.

1.5. In addition to that, in order to enable the following for both CCS trackside and on-board sub-systems, as well as for the interoperability constituents, or groups of interoperability constituents :

(a) the mutual recognition of the applicant's demonstration of compliance with all applicable requirements of the CCS TSI;
(b) the safe integration of interoperability constituents, or groups of interoperability constituents, into the CCS trackside and/or on-board subsystems, without additional risk assessments and additional independent safety assessments;
(c) the safe integration of CCS trackside sub-system into the infrastructure structural and functional sub-systems;
(d) the safe integration of the CCS on-board sub-system into the rolling stock structural and functional sub-systems;

(e) the safe integration of CCS trackside and on-board sub-systems into the overall railway system, including thereby their integration into the SMS of the infrastructure manager and railway undertakings;

for the interoperability constituents (ICs), or groups of interoperability constituents, it is essential to apply the same processes, and same requirements, as for the CCS trackside and on-board sub-systems, to specify and demonstrate compliance with the applicable RAMS requirements.

The reader can find further guidance on safe integration in the "Agency clarification note on safe integration [Ref. ERA1209-063]" on the Agency website.

1.6. To help the reader with the understanding of this document, it is worth reminding beforehand the relevant requirements of the CCS TSI (Regulation 2019/776).

2 Reminder of the legal requirements in the CCS TSI

2.1 Safety

2.1.1 Section § 3.2.1. on safety requirements of the CCS TSI explicitly specifies the following :

Note : *in the CCS TSI only the main sections are numbered. In this guide, for an easier reference to the different requirements of section § 3.2.1 of the TSI, the sub-sections of section § 3.2.1 are numbered in the chronological order as follows.*

3.2.1.1	*…*
3.2.1.2	*To ensure that the measures taken to achieve safety do not jeopardise interoperability,* ***the requirements of the basic parameter defined in point 4.2.1*** *(Control-Command and Signalling reliability, availability and safety characteristics relevant to interoperability)* ***shall be respected****.*
3.2.1.3	*For the ETCS Class A system the safety objective is apportioned between the Control-Command and Signalling On-board and Trackside Subsystems. The detailed requirements are specified in the basic parameter defined in point 4.2.1 (Control-Command and Signalling reliability, availability and safety characteristics relevant to interoperability). This* ***safety requirement shall be met together with the availability requirements as defined in Point 3.2.2*** *(Reliability and Availability)*
3.2.1.4	*For the ETCS Class A system:* *(a) the changes made by railway undertakings and infrastructure managers shall be managed in compliance with the processes and procedures of their safety management system;* *(b) the changes made by other actors (e.g. manufacturers or other suppliers) shall be managed according to the risk management process set out in Annex I to the Commission Implementing Regulation (EU) No 402/2013 , as referred to in Article 6(1)(a) of Directive (EU) 2016/798 of the European Parliament and of the Council.*
3.2.1.5	*Additionally the correct* ***application of the risk management process as set out in Annex I of Regulation (EU) No 402/2013****, as well as the appropriateness of the results from this application, shall be* ***independently assessed by a CSM assessment body according to Article 6 of that Regulation****. The CSM Assessment Body shall be accredited or recognised according to the requirements in Annex II of Regulation (EU) No 402/2013 in the fields of 'Control-command and signalling' and 'System safe integration' as listed in item 5 'classification' of ERADIS database entry for Assessment Bodies.*
3.2.1.6	*The application of the specifications as referred to in* ***Annex A, Table A 3 is an appropriate means to fully comply to the risk management process as set out in Annex I of the Commission Implementing Regulation (EU) No***

	402/2013 *for design, implementation, production, installation and validation (incl. Safety acceptance) of* ***interoperability constituents and subsystems****. When different specifications from the ones referred to in Annex A, Table 3 are applied, at least equivalence shall be demonstrated with the specifications in Annex A, Table 3.*
3.2.1.7	***Whenever the specifications*** *as referred to* ***in Annex A, Table A 3 are used*** *as an appropriate means to fully comply to the risk management process as set out in Annex I of the Commission Implementing Regulation (EU) No 402/2013, in order to avoid unnecessary duplication of independent assessment work,* ***the independent safety assessment activities that are required by the specifications referred to in Annex A, Table A 3 shall be carried out by an Assessment Body*** *accredited or recognized as specified in the section above instead of a CENELEC independent safety assessor.*

2.2 Reliability and Availability

2.2.1 In the CCS TSI, only the main sections are numbered. In this guide, for an easier reference to the different requirements of a TSI section, this guide numbers also the different sub-sections in the chronological order, as presented below.

2.2.2 Section § 3.2.2 of the CCS TSI on "reliability and availability" explicitly specifies the following requirements :

3.2.2.1.	*…*
3.2.2.2.	*The level of risk caused by age and wear of constituents used within the subsystem shall be monitored. The requirements for* ***maintenance stated in point 4.5 shall be respected****.*

2.2.3 Section § 4.2.1.2 of the CCS TSI on "reliability and availability" requirements explicitly specifies the following :

4.2.1.2.1.	*This point refers to the occurrence of failure modes not causing safety hazards but creating degraded situations,* ***the management of which could decrease the overall safety of the system****.*
4.2.1.2.2.	*…*
4.2.1.2.3.	*To ensure that the relevant infrastructure managers and railway undertaking are given all the* ***information*** *they need* ***to define appropriate procedures for managing degraded situations****, the technical file accompanying the EC declaration of verification for an on-board or trackside CCS subsystem shall contain the calculated availability/reliability values related to failure modes having an impact on the capability of the CCS subsystem to supervise the safe movement of one or more vehicles or to establish radio voice communication between traffic control and the train drivers.*
4.2.1.2.4.	*…*
4.2.1.2.5.	*To allow the infrastructure managers and railway undertakings to* ***monitor, during the life of the subsystems****, the level of risk and the respect of the reliability/availability values used for the definition of procedures to* ***manage degraded situations****, the requirements for* ***maintenance stated in point 4.5*** *(Maintenance rules) shall be respected.*

2.3 Maintenance rules (Maintainability)

2.3.1 In the CCS TSI, only the main sections are numbered. In this guide, for an easier reference to the different requirements of a TSI section, this guide numbers also the different sub-sections in the chronological order, as presented below.

2.3.2 Section § 4.5 of the CCS TSI on "maintainability rules" explicitly specifies the following requirements related to the maintainability of the ETCS Class A sub-systems and ICs :

4.5.	*The **maintenance rules** of the subsystems covered by this TSI shall **ensure that** the values quoted in **the basic parameters** indicated in Chapter 4 **are maintained within the required limits throughout the lifetime of the subsystems**. However, during preventative or corrective maintenance, the subsystem may not be able to respect the values quoted in the basic parameters; the maintenance rules shall ensure that safety is not prejudiced during these activities.*
4.5.	*The entity in charge of the Control-Command and Signalling Subsystems shall set up maintenance rules to achieve the above objectives. To assist with the preparation of these rules, the following requirements shall be respected.*
4.5.1.	***Responsibility of the manufacturer of equipment***
	The manufacturer of equipment incorporated in the subsystem shall specify:
	(1) all maintenance requirements and procedures (including health monitoring, diagnosis of events, test methods and tools and also the required professional competence) necessary for achieving essential requirements and values quoted in the mandatory requirements of this TSI throughout the equipment life-cycle (transport and storage before installation, normal operation, failures, repair work, checking and maintenance, decommissioning, etc.). For equipment error corrections see point 6.5;
	(2) the health and safety risks that may affect the public and the maintenance staff;
	(3) the conditions for first line maintenance, i.e. the definition of Line Replaceable Units (LRUs), the definition of approved compatible versions of hardware and software, the procedures for replacing failed LRUs, the conditions for storing LRUs and for repairing failed LRUs;
	(4) the checks to be carried out if equipment is subject to exceptional stress (e.g. adverse environmental conditions or abnormal shocks);
	(5) the checks to be carried out when maintaining equipment other than Control-Command and Signalling equipment and which influences the Control-Command and Signalling Subsystems (e.g. changing the wheel diameter).
4.5.2.	***Responsibility of the applicant for subsystem verification***
	The applicant shall :
	*(1) **ensure that the maintenance requirements as described in point 4.5.1** (Responsibility of the Manufacturer of Equipment) **are defined** for all components within the scope of this TSI **regardless of whether or not they are interoperability constituents**;*
	*(2) complete the above requirements **taking into account the risks arising from interactions between different components of the subsystem and interfaces to other subsystems**.*

3 Links between the Safety (S), Reliability (R), Availability (A) and Maintainability (M) (RAMS) requirements in the CCS TSI

3.1 The CCS TSI specifies the safety, reliability, availability and maintainability (RAMS) requirements in separate sections. However, a careful reading of each section clearly shows some relation between those four sets of performance requirements. For a proper specification, and demonstration of their achievement, it is important to understand those requirements.

3.2 <u>Reading the CCS TSI from the perspective of the Safety (S) requirements :</u>

(a) section § 3.2.1 of the CCS TSI requires the applicant to identify the applicable safety, and to demonstrate their achievement, in compliance with either :

(1) **option 1 :** the risk management process in Annex I of Regulation 402/2013, or;
(2) **option 2 :** the specifications referred to in Annex A, Table A 3 of the CCS TSI (i.e. CENELEC standards), usable as an appropriate means to comply with the risk management process in Annex I of Regulation 402/2013;

(b) "*to ensure that the measures taken to achieve safety do not jeopardise interoperability, …*", sub-sections § 3.2.1.2 and § 3.2.1.3 require then that "*… the requirements of the basic parameter defined in point 4.2.1 (Control-Command and Signalling **Reliability, Availability** and **Safety** characteristics relevant to interoperability) shall be respected*" also.

Those two sub-sections explicitly require the applicant to ensure that the compliance with the safety requirements of the CCS TSI does not compromise the compliance with the reliability and availability requirements, and vice versa;

(c) reading then the requirements in point 4.2.1 on the Reliability and Availability :

(1) point 4.2.1.1 defines again the **Safety** requirements to be fulfilled in terms of tolerable hazard rate (THR) for random failures, for the on-board ETCS and for the trackside ETCS;

(2) point 4.2.1.2 relates to **Availability** and **Reliability**, and thus to the occurrence of "*failure modes not causing safety hazards but creating degraded situations, the management of which could decrease the overall safety of the …*" ETCS system, and which therefore shall also be managed;

(3) point 4.2.1.3 requires that "*the relevant infrastructure managers and railway undertaking are given all the information they need to define appropriate procedures for managing …*" those degraded situations in terms of technical, operational and organisational (i.e. including human and organisational factors – HOF) measures;

(4) point 4.2.1.5 requires that "*to allow the infrastructure managers and railway undertakings to monitor, during the life of the subsystems, the level of risk and the respect of the reliability/availability values used for the definition of procedures to manage degraded situations, the requirements for maintenance stated in point 4.5 (**Maintenance** rules) shall be respected.*". See section § 3.3 below.

(d) sub-section § 3.2.1.3 explicitly requires that "*for the ETCS Class A system the safety objective … safety requirement shall be met together with the availability requirements as defined in Point 3.2.2 (**<u>Reliability and Availability</u>**).*

(e) sub-section § 3.2.2.2. requires that "*the level of risk caused by age and wear of constituents used within the subsystem shall be monitored. The **requirements for maintenance stated in point 4.5** shall be respected.*"

The reading of the sections on the Safety (S) requirements of the CCS TSI, and of the respective references to the Reliability (R), Availability (A), and Maintainability (M) requirements, clearly shows that the CCS TSI closely links those four sets of requirements (RAMS) to each other.

3.3 Reading the CCS TSI from the perspective of the Reliability (R), Availability (A) and Maintainability (M) requirements :

Point 4.5 of the CCS TSI defines the **Maintenance** rules for the CCS sub-systems. Compliance with those maintenance rules is also required through the requirements on safety in point § 3.2.2.2, and through the requirements on reliability and availability in point § 4.2.1.5 of the CCS TSI. Point 4.5 requires the following :

(a) "*the **maintenance rules** of the subsystems covered by this TSI shall **ensure that** the values quoted in **the basic parameters** …*" related to **Reliability**, **Availability** and **Safety** "*… indicated in Chapter 4 **are maintained within the required limits throughout the lifetime of the subsystems***";

(b) "*the entity in charge of the Control-Command and Signalling Subsystems shall set up maintenance rules to achieve …*" the Reliability, Availability and Safety requirements of the CCS TSI;

(c) Those two bullet points result in the following requirements in the CCS TSI :

(1) by virtue of point 4.5.1 (see text reminded in section § 2.3 above), the manufacturer of the ETCS equipment is responsible for :

(i) the identification of risks shared across the interfaces of the ETCS equipment with other equipment, or sub-systems, including human operators, that can arise during the operation and maintenance of the ETCS equipment in its physical, functional, environmental, operational, and maintenance context;

(ii) the identification of associated safety related application conditions (SRACs) necessary for the safe integration of the ETCS equipment (Class A sub-systems or interoperability constituents) into its physical, functional, environmental, operational, and maintenance context;

(iii) "*the checks to be carried out when maintaining equipment other than CCS equipment and which influences the CCS sub-systems (e.g. changing the wheel diameter)*" (requirement in point 4.5.1(5));

(2) point 4.5.2 explicitly requires the applicant for the sub-system verification to be responsible for ensuring that :

(i) "*… the maintenance requirements as described in point 4.5.1 …*", (under the responsibility of the manufacturer of the ETCS equipment) "*… are defined for all components within the scope of this TSI **regardless of whether or not they are interoperability constituents***";

(ii) "*… the above requirements …*" are complete (i.e. SRACs necessary for the safe integration of the ETCS equipment into its physical, functional, environmental, operational, and maintenance context) "*… taking into account the risks arising from interactions between different components of the subsystem and interfaces to other subsystems*" (i.e. the risks shared across the interfaces).

The reading of the sections on the Maintainability (M) requirements of the CCS TSI, and of the respective references to the sections on the Reliability (R), Availability (A), and Safety (S) requirements, also clearly shows that the CCS TSI closely links those four sets of requirements (RAMS) to each other.

4 CENELEC requirements for the specification and demonstration of RAMS

4.1 The CENELEC 50126-1 standard is dedicated to railway applications for the "*Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*". It defines a "*Generic RAMS Process*".

4.2 This chapter does not claim to summarise in a few lines, or in a few paragraphs, more than 100 pages of a detailed and consistent set of requirements for the specification and management of RAMS. The aim is to refer to equivalent relations between the R-A-M-S elements of the CENELEC standard as those specified in the CCS TSI (refer to the analysis in chapter 3 above).

4.3 A careful reading of the following sections of the CENELEC 50126-1 standard permits to arrive at the same conclusions as the ones raised in chapter 3 above :

(a) section § 5.5 describes the elements of railway RAMS and the interaction between the four RAMS elements (reliability, availability, maintainability and safety), in the context of railway systems. The following can be read in section § 5.5 of CENELEC 50126-1 :

(1) CENELEC explicitly states that those four "*… **RAMS elements are interlinked in the sense that a weakness in any of them or mismanagement of conflicts between their requirements can prevent achievement of a …**"* **reliable system**. "*For example, a safety target can be achieved by ensuring the system enters a safe state (e.g. all trains stopped) in the event of a particular failure. The defined safe state can depend on operational/maintenance context (e.g. a train at standstill at platform rather than in tunnel). If there are circumstances where this safe state has a significant adverse impact on reliability/availability then a different and optimised solution might be needed in order to achieve the RAM targets without compromising safety.*"

(2) "*Attainment of in-service availability targets will be achieved by optimising reliability & maintainability whilst considering the influence of maintaining safety. The related requirements can be met and controlled by a combination of design and implementation measures and through the ongoing, long term maintenance and operational activities, all according to the system environment.*"

(3) "*Failures in a system operating within the …*" limits " *… of an application and environment will have an impact on the system's reliability, availability and safety, with the level of impact being determined by the system functionality and design. The environment and the operational rules can also influence these effects.*"

(b) section § 5.6 describes the factors influencing railway RAMS. The following can be read in sub-clause § 5.6.1 of CENELEC 50126-1 :

(1) the sub-clause "*…defines a process to support the identification of factors which influence the RAMS performance of railway systems, with particular consideration given to the influence of human factors*";

(2) "*The RAMS performance of a railway system is influenced in three ways, that can interact* "

(i) by sources of failure introduced internally within the system at any phase of the system life cycle;
(ii) by sources of failure imposed on the system during operation; and
(iii) by sources of failure imposed on the system during maintenance activities.

(3) "*To create …*" reliable "*… systems, factors which could influence the RAMS of the system need to be identified, their effect assessed and the cause of these effects managed throughout the life cycle of the system, by the application of appropriate controls to optimise system performance.*"

4.4 Section § 6 of CENELEC 50126-1 standard specifies the general requirements for the management of railway RAMS. It defines the approach to be followed for "*… planning*, *managing, controlling and monitoring all aspects of a system …*" under assessment, "*… including RAMS, as the system … progresses through the life cycle phases. The focus of the RAMS process is to* ***reduce the incidence of failures and/or the consequences throughout the life cycle, and thus minimise the residual risk resulting from these errors***."

4.5 Table 1 in section § 6.2 of CENELEC 50126-1 standard summarises the relationships between the RAMS tasks to be considered throughout the lifecycle of the system under assessment. It also summarises the links between the four RAMS elements. In particular, the following can be read :

(a) Phase 3 of the CENELEC V life-cycle on "risk analysis and evaluation" :

(1) RAM tasks :

(i) update **RAM plan;**

(2) Safety tasks :

(i) perform risk analysis;
(ii) establish hazard log;
(iii) update safety plan;
(iv) **establish independent safety assessment plan**;

The establishment of the independent safety assessment plan has to take into account on how the RAM and Safety requirements are managed for the system under assessment.

(b) Phase 4 of the CENELEC V life-cycle on "specification of system requirements" :

(1) RAM tasks :

(i) establish RAM requirements specification;
(ii) update the RAM plan;
(iii) establish validation plan for RAM requirements;

(2) Safety tasks :

(i) establish safety requirements specification;
(ii) establish safety-related application conditions;
(iii) update hazard log;
(iv) update the safety plan;
(v) establish validation plan for safety requirements;

The safety related application conditions (SRACs) are a result of both the Safety and RAM assessments.

4.6 Based on the explanations in sections § 4.3, § 4.4 and § 4.5, concerning the CENELEC 50126-1 standard requirements, it is unnecessary to look for additional evidence of the close links in that standard between :

(a) the specification and demonstration of safety (S) requirements;
(b) the specification and demonstration of the other three elements of RAM requirements.

4.7 The CENELEC 50126-1 standard acknowledges that :

(a) the four elements of RAMS are interlinked;
(b) a weakness in any of them, or a mismanagement of conflicts between their requirements, can prevent the achievement of a reliable system.

The CENELEC 50126-1 standard defines equivalent requirements to those of the CCS TSI for the specification and demonstration of RAMS.

5 Shall independent assessment be limited to safety requirements, or on the contrary shall it cover the entire scope of RAMS requirements?

5.1 Based on the arguments developed in chapter 3, regardless of whether the CCS TSI is considered from the perspective of compliance with the **Safety (S)** requirements, or from the perspective of compliance with the **Reliability (R)**, **Availability (A)** or **Maintainability (M)** requirements, those four RAMS elements are closely linked, complementary and impact each other. Compliance with one element has the potential to prevent the achievement another RAMS element.

As pointed out in chapter 4, similar conclusions can be withdrawn also from the reading of the CENELEC 50126-1 standard.

5.2 Thereby, in order to be able to provide an expert judgement on the achievement of the applicable safety requirements, the independent assessment shall not be limited to SAFETY. As explained in section § 6.6(b) below, the AsBo independent assessment shall cover all four elements of RAMS. However, the AsBo shall focus the independent assessment to the applicant's specification and demonstration of safety, and parts of the RAM requirements that are likely to impact adversely the achievement of the safety requirements.

6 Is the AsBo responsible for the independent safety assessment of ICs, or can an ISA carry out the work?

6.1 Sub-section § 3.2.1.4 of the CCS TSI (see text reminded in section § 2.1 above) specifies the processes applicable for the management of changes of the CCS sub-systems in function of the categories of railway stakeholders. In particular, bullet (b) in sub-section § 3.2.1.4 of the CCS TSI explicitly requires the manufacturers and suppliers to manage all changes of the ETCS Class A system "*… according to the risk management process set out in Annex I …*" of Regulation 402/2013.

By virtue of sub-section § 3.2.1.6 (see text reminded in section § 2.1 above), that requirement applies to both the ETCS Class A on-board and trackside subsystems, **as well as to their basic interoperability constituents**. That means that sub-section § 3.2.1.4(b) does not relax explicitly any requirement of Regulation 402/2013 for the design, implementation, manufacturing, installation, verification and validation (including safety acceptance), risk assessment and risk management, and independent assessment of the interoperability constituents of the ETCS Class A system.

6.2 Consequently, as explained in chapter 3, the reader shall not read sections § 4 and § 4.2.1, and chapters 5 and 6, of the CCS TSI in isolation to interpret them as a derogation to the mandatory requirements of section § 3.2.1 of the CCS TSI. They specify detailed requirements complementary to the ones in section § 3.2.1. In particular, concerning the interoperability constituents, those other sections do not modify which conformity assessment body is to be in charge of the independent assessment of the correct application of the risk management process set out in Annex I of Regulation 402/2013 and of the appropriateness of the associated results.

6.3 Regardless whether the considered change is a modification of the ETCS Class A on-board and trackside subsystems, or of their basic interoperability constituents, the risk assessment of the change shall be managed in compliance with either :

(a) **option 1 :** the risk management process in Annex I of Regulation 402/2013, or;
(b) **option 2 :** the specifications referred to in Annex A, Table A 3 of the CCS TSI (i.e. CENELEC standards), usable as an appropriate means to comply with the risk management process in Annex I of Regulation 402/2013.

In addition to that, according to the requirements in sub-sections § 3.2.1.5 (related to option 1) and 3.2.1.7 (related to option 2) of the CCS TSI (see text reminded in section § 2.1 above), the

independent safety assessment activities shall be carried out in both cases by a CSM assessment body (AsBo) accredited or recognised in accordance with the requirements in Annex II of Regulation (EU) No 402/2013. Therefore, the CCS TSI does not allow the independent safety assessment activities to be performed by a CENELEC independent safety assessor (ISA).

6.4 Thereby, considering also the following :

(a) the CENELEC standards referred to in Annex A, Table A 3 of the CCS TSI define the requirements for the specification and demonstration of the achievement of the RAMS (reliability, availability, maintainability and safety) requirements;
(b) CENELEC 50126-1:2017 and 50126-2:2017 standards requires the independent assessment of the specification and demonstration of the achievement of the RAMS requirements;
(c) sub-section § 3.2.1.7 of the CCS TSI (see text reminded in section § 2.1 above) explicitly requests that "*… the independent safety assessment activities that are required by the specifications referred to in Annex A, Table A 3 …*" of the CCS TSI "*… **shall be carried out by an assessment body** accredited or recognised … instead of a CENELEC independent safety assessor*";
(d) based on the arguments in chapter 5, the independent assessment shall not be limited to SAFETY but it shall cover all four elements of RAMS,

the independent assessment of the correct specification and demonstration of the achievement of the RAMS (reliability, availability, maintainability and safety) requirements must be carried out also by the CSM assessment body (AsBo).

6.5 The compliance with the CCS TSI requires therefore the CSM AsBo to independently assess not only the safety, but also the reliability, availability and maintainability, requirements of the ETCS Class A on-board and trackside subsystems, as well as of their basic interoperability constituents, defined in sections § 4.2.1 and § 4.5.1 of the CCS TSI.

6.6 Responsibilities with respect to the specification and demonstration of RAMS :

In order to ensure that the four RAMS elements are properly considered, and there are no unidentified and uncontrolled risks that could impact adversely the achievement of the applicable safety requirements :

(a) the applicant is responsible for :

(1) the proper specification and demonstration of all four elements of RAMS, including the justifications concerning the RAM requirements that do not impact the safety requirements;
(2) the establishment of documented evidence of the proper management of RAMS requirements;

(b) the AsBo is responsible for :

(1) the independent safety assessment of the compliance of the applicant's RAMS activities with the relevant requirements of the CCS TSI;
(2) the independent safety assessment of the correct separation by the applicant of requirements into safety related ones and non safety-related ones (i.e. RAM requirements), based on evidence and justifications provided by the applicant;
(3) focussing the independent safety assessment to the applicant's specification and demonstration of safety, and parts of the RAM requirements that are likely to impact adversely the achievement of the safety requirements;
(4) build the expert judgement on the conformity of the ETCS Class A on-board and trackside subsystems, basic "interoperability constituent" or "group of interoperability constituents" with the applicable requirements of the CCS TSI, including the suitability of the results from the applicant's risk assessment.

7 Can a railway actor request an AsBo to sub-contract a part of independent safety assessment to another conformity assessment body (e.g. to an ISA)?

7.1 Based on the arguments presented in chapter 6, as well as from the requirements in Regulation 402/2013, from the legal point of view :

(a) The applicant must not sub-contract to a CENELEC independent safety assessor (ISA) the independent assessment of the RAM, or of RAMS requirements, neither for the ETCS Class A on-board and trackside subsystems, nor for their basic interoperability constituents, and then;
(b) the applicant must not oblige the AsBo to provide its experts judgement on the conformity of an ETCS Class A subsystem or IC with the requirements of the CCS TSI based on an ISA report.

The use of external experts and sub-contractors by an AsBo is also strictly regulated in sections § 6.1 and 6.3 of the ISO/IEC 17020:2012 standard referenced to in Regulation 402/2013.

By virtue of section § 6.3.3 of the ISO/IEC 17020:2012 standard, "*whenever subcontractors carry out work that forms part of an …*" AsBo independent assessment, "*… the responsibility for any determination of conformity of the inspected item …*" (i.e. an ETCS Class A subsystem or IC) "*… with the requirements shall remain with …*" the AsBo. Thereby, not respecting the bullet point (b) in section § 7.1 above would oblige the AsBo to take the responsibility for the ISA work whereas the AsBo does not have any control means over the ISA working methodology and conclusions, nor on which ISA to select, how to verify its competence and how to monitor the ISA performance.

7.2 Although the roles and working methods of the AsBo are similar to the ones of the CENELEC ISA referred to in CENELEC 50128, 50657:2017 and 50129 standards, there is a fundamental difference between the two bodies :

(a) the AsBo is obliged to be accredited or recognised, and to demonstrate the compliance with all the requirements and criteria, including competence in well-defined areas, as set up in Annex II, Regulation 402/2013, whereas;
(b) the CENELEC 50129:2018, 50128:2011 and 50657:2017 standards setup **competence** (see Table B.8 of CENELEC 50128:2011 and 50657:2017) and **independence** requirements for the ISA (see e.g. Figure 2 and section § 5.1.2 of CENELEC 50128:2011 and 50657:2017). However, those standards do neither require the ISA to demonstrate its independence and competence nor oblige the ISA to be accredited or recognised by an acknowledged entity vs. neither those CENELEC requirements, nor the ISO/IEC 17020 standard and Regulation 402/2013 requirements. The ISA accreditation or recognition is exceptional in the EU. It is imposed by the national legislation of a few EU Member States (e.g. Germany).

Because of those fundamental differences, the independent assessment report of a CENELEC non-accredited/non-recognised ISA does not provide the same level of trust and confidence as the independent assessment report of a CSM AsBo accredited/recognised in compliance with Regulation 402/2013. Thereby, an ISA report cannot be mutually recognised by another conformity assessment body without additional checks.

8 Conclusion

8.1 From the explanations and references in the sections above, it can be concluded that :

(a) the AsBo independent assessment shall not be limited to safety but shall cover all four elements of RAMS;
(b) the independent assessment of the compliance of ETCS Class A subsystems and interoperability constituents falls fully under the responsibility of a CSM AsBo.

8.2 The CCS TSI and Regulation 402/2013 do not permit the independent assessment activities to be carried out by a CENELEC ISA for any part of the ETCS Class A subsystem, including interoperability constituents or groups of interoperability constituents.