



SR40 COAT Approval Concept

Report on COAT Approval Procedure

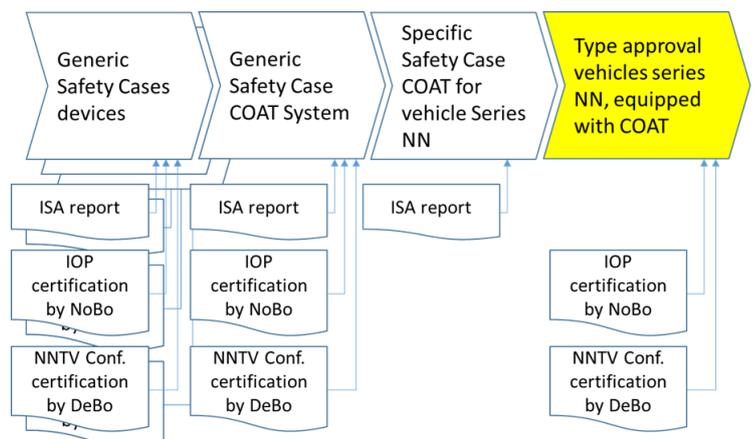
ECH-429.03-008
Version 1.0

Client:

SBB Informatik, Bern 65

Issued by:

ENOTRAC AG
Seefeldstrasse 8
CH-3600 Thun
Tel. +41 33 346 66 11
Fax +41 33 346 66 12
info@enotrac.com
www.enotrac.com



Released

2019-11-25

ECH-429.03-008.V1.0.Report_on_COAT_Approval_Procedure.docx

© ENOTRAC AG

Current version

Version	Date	Status	Prepared	Reviewed	Approved
1.0	2019-11-25	Released	D. Würzler	T. Vennemann	A. Bleiker

Previous version

Version	Date	Status	Prepared	Reviewed	Approved

Changes since the previous version

Intellectual property

This document was prepared by ENOTRAC AG on behalf of the client. The client receives the right of use for the document and the object depicted therein. ENOTRAC AG owns the copyrights. Reproduction, disclosure to third parties or exploitation of its contents beyond the intended use is prohibited without written consent.
© ENOTRAC AG

Bookmarks

Project title	ProjTitle1	SR40 COAT Approval Concept
	ProjTitle2	
Report title	DocTitle1	Report on COAT Approval Procedure
	DocTitle2	
	DocTitle3	
Report number	DocNumber	ECH-429.03-008
Client	ClientName	SBB Informatik, Bern 65
	ClientAddr	
Logos	EnoLogoHeader	
	ClientLogo1Header	
	ClientLogo2Header	
Contact	Contact	Dieter Würzler, Tel. +41 33 346 66 03
	Contact_Mail	dieter.wuerzler@enotrac.com

Content:

1	Summary	5
2	Introduction	6
2.1	Task	6
2.2	Objectives	6
2.3	Purpose of the document	6
2.4	Scope	7
2.5	Abbreviations and terms	7
3	Set of rules	9
4	System and Architecture	13
4.1	COAT system scope	13
4.2	System architecture	13
4.2.1	Generic System Architecture	13
4.2.2	Considered COAT architecture	15
5	Environment	16
5.1	Current situation	16
5.1.1	Demonstration of compliance process	16
5.1.2	Market, Technology	17
5.2	Outlook, Development	17
5.2.1	Rules and regulations, demonstration of compliance procedures	17
5.2.2	Market, Technology	19
6	Demonstration of Compliance	20
6.1	Hierarchy and logical sequence of the Generic Safety Cases for COAT	20
6.2	Generic Safety Case for each device / subsystem	21
6.3	Generic Safety Case for EVC	22
6.4	Generic demonstration of compliance for devices without safety responsibility	23
6.5	Generic Safety Case for the COAT System	24
6.6	Specific safety case for COAT on vehicle type NN	24
7	Independent Assessment	26
7.1	Independent safety assessment according to CENELEC	26
7.2	Assessment by experts in accordance with FOT directives	26
7.3	Examination and confirmation of interoperability	26
7.4	Concept proposal for independent assessments	28
8	Homologation	31
8.1	Fundamental principle	31
8.2	Type approval of the devices	31
8.3	Type approval of the COAT system	32
8.4	Type approval of vehicles	33

8.5	Type approval of the procedure	35
8.5.1	Categories of changes	35
9	Test infrastructure and test concept	37
9.1	Test laboratory of the system leader	37
9.2	Test vehicle and test track of the system leader	37
9.3	Minimal regression tests	38
10	Use Cases	39
10.1	First approval of the COAT devices and the COAT system	39
10.2	Functional extension of the COAT system	39
10.3	Functional changes	40
10.4	SW changes without changes to the interfaces	40
10.5	Bug fixes	40
11	Conclusions	42
11.1	Challenges	42
11.2	Potential	42
11.3	Recommendations	42
12	References	44
12.1	Basics	44
12.2	Laws, directives	44
12.3	Standards	45
12.4	Technical Specifications	45
12.5	Related documents, literature	46

1 SUMMARY

The task was to develop an approval procedure for COAT, with which the effort and throughput times for verification and approval, in particular for updates, can be drastically reduced compared to the procedures practiced today for ETCS onboard equipment. The results of this investigation are documented in this report.

In a first phase, the existing rules and regulations, which have to be followed for verification and approval, were analysed. In addition, proposals for a COAT system architecture, suitable for modular and flexible proof of safety, were developed. The two architecture variants are listed in the COAT system description [1]. The two variants of the COAT system architecture were examined with regard to the proof of safety and the approval procedure. The findings from the analysis of existing regulations and the COAT system architecture are documented in the COAT approval analysis report [2].

In order to achieve the objectives of an efficient proof of safety especially after changes, a modular architecture for COAT is proposed. The heart of COAT is a central computer (EVC) on which various applications such as Open ETCS, ATP, localization, train integrity, etc. run. This central computer is a commercially available platform, which enables applications up to SIL4 and supports software development with corresponding tools (development environment).

The central computer communicates via a CCS data bus with various peripheral devices which operate the interfaces between COAT and the outside (e.g. communication via GSM-R, reading of Eurobalises, reading of Euroloop, interface with the TCMS of the vehicle, man-machine interface with the locomotive driver) and which measure values such as speed, acceleration, position etc. with the associated sensors.

Communication between the peripheral devices and the EVC takes place via the CCS data bus, which is supplemented with the necessary protocols (Safety Layer) in order to enable safe data transmission, if required.

The safety cases have the same modular structure as the COAT architecture. The proof of safety is performed hierarchically over several levels: generic safety cases for each of the peripheral devices, generic safety cases for the EVC, generic safety case for the COAT system, which also includes the proof of safe data transmission. For the concrete application of the generic COAT system on a vehicle type, a specific safety case, based on the generic safety case, is required. This specific safety case demonstrates the implementation of the application conditions, the correct integration into the vehicle and the parameterisation of the specific application.

For the demonstration and certification of interoperability by a notified body, a structure of interoperability constituents (ICs) matching the system architecture and the safety demonstrations is proposed. Each COAT component for which a safety case, an ISA assessment report, an IOP certificate and a certificate of conformity with the NNTR is issued, also corresponds to a type approval object. In addition, a type approval shall be obtained for the process of the proof of safety after changes. This process regulates the re-validation of the proof of safety and the necessary regression tests for different categories of changes.

2 INTRODUCTION

2.1 Task

- Development of an approval procedure for COAT with drastically reduced effort and throughput times, compared to the procedures in place today for proof of safety and homologation of ETCS on-board equipment.
- Proposals for possible optimisation of the approval procedure by adapting the COAT system architecture and the applicable regulations.

2.2 Objectives

The objectives of the COAT approval procedure are as follows:

- Simplification of the proof of safety process through modularization of the safety cases and through standardized interfaces between the modules
- Reduction of effort and lead times for proof of safety and approval, especially for changes and updates.
- Reduction of elaborate track tests by using laboratory reference systems for the validation of individual modules.

2.3 Purpose of the document

This document contains the proposals for the proof of safety and approval process that have emerged from the analysis of the COAT system architectures and the applicable regulatory framework.

The document builds on the COAT system architectures of the system description [1] and the findings from the analysis report [2]

In order to improve the readability and comprehensibility of this document, reference is made to these two documents for the detailed information.

2.4 Scope

This report deals with the issues of the approval of COAT and vehicles equipped with COAT. The findings and recommendations relate to the COAT system and its architecture according to the system description [1]. The analysis, findings and proposals are based on the current rules and standards for the approval of ETCS equipment and interoperable vehicles in Switzerland.

2.5 Abbreviations and terms

Abbreviation, term	Explanation
AsBo	Assessment Body (Risk Assessment Body in the context of CSM-RA)
ATO	Automatic Train Operation
BTM	Balise Transmission Module
CCS	Control and Command System: train control, train protection and signalling
CENELEC	European standardisation body for electrical engineering
COAT	CCS onboard application platform for trackside related functions
COTS	Commercial off-the-shelf (components or products, can be HW or SW)
CSM-RA	Common Safety Method for Risk Assessment
DeBo	Designated Body
DMI	Driver Machine Interface
EMC	Electromagnetic Compatibility
ERA	European Union Agency for Railways
ETCS	European Train Control System
EVC	European Vital Computer; In the context of COAT, the abbreviation is used for the central computer platform, which also executes COAT applications in addition to the ETCS functionality.
FFFIS	Form Fit Function Interface Specification
FIS	Functional Interface Specification
FOT	Federal Office of Transport
FRMCS	Future Railway Mobile Communication System; replacement of the GSM-R
GoA2	Grade of Automation 2
GSM-R	Global System for Mobile Communication – Railways
HW	Hardware
IC	Interoperability constituent; In the context of COAT, the abbreviation is used for interoperability constituents ideally suited to the COAT system architecture. This definition of the IC differs from the basic interoperability constituents currently defined in the CCS TSI [28]. See also explanations in chapter 7.3 and recommendations in chapter 11.3.
IOP	Interoperability
ISA	Independent Safety Assessor (Independent Safety Assessor)
JRU	Juridical Recording Unit
LTM	Loop Transmission Module
NNTR	Notified National Technical Rules

Abbreviation, term	Explanation
NoBo	Notified Body
NSA	National Safety Authority.
OBU	Onboard Unit (ETCS equipment on the vehicle)
OCORA	Open CCS On-board Reference Architecture
RAMS	Reliability, Availability, Maintainability, Safety;
SDT	Safe Data Transmission
SIL	Safety Integrity Level
SRS	System Requirements Specification
SS	subset
STM	Specific Transmission Modules
SW	Software
TCMS	Train Control & Management System
TFFR	Tolerable Functional Failure Rate
TIMS	Train Integrity Monitoring System
TIU	Train Interface Unit
TSI	Technical specifications for interoperability

Tab. 1 Abbreviations and terms

3 SET OF RULES

In the analysis report [2] the existing comprehensive set of rules (laws, regulations, guidelines, standards) was examined for its relevance to the COAT approval procedure. The assessment of individual regulations and standards is documented in [2]. The following table briefly explains which regulations and standards must be observed for the demonstration of compliance and approval of COAT and which aspects are particularly relevant.

Regulation, standard	Ref.	Particularly relevant aspects
EBV 742.141.1: Ordinance on the Construction and Operation of Railways (Railway Ordinance); as of 15 May 2018	[5]	Legal basis of the guidelines to be followed. Requires the application of CSM [3] and [4] for significant changes.
EC 352/2009 CSM-RA: Regulation establishing a common safety method for the evaluation and assessment of risks	[3]	Method of risk analysis for significant changes. Need for independent assessment by a safety assessment body. This is discussed further in Chapter 7.
AB-EBV: Implementing Provisions for the Railway Ordinance, as of 1 July 2016	[6]	AB 38.1: Application of EN 50126 [17], [18], EN 50129 [19] and EN 50159 [22] for signalling systems with high safety relevance and safe communication.
Directive for the homologation of railway vehicles (Type approval / Authorisation to operate), V2.3a de, July 1, 2018	[7]	Regulates the approval process for interoperable (and non-interoperable) vehicles in Switzerland. This includes the type approval and the operating permit. Defines the content of the approval concept for vehicles and systems. Defines the structure and content of the safety case for the type approval and operating approval of vehicles. Defines criteria and procedures for modifications to vehicles and components, including SW.
RL UP-EB: Directive Independent Assessment Bodies for Railways, V2.0 dated 16 January 2017	[9]	According to Part A, Chapter 2, the Directive applies to following procedures: <ul style="list-style-type: none"> • Type approval of elements of vehicles • Type approval of vehicles • Operating permit for vehicles The Directive specifies which type of independent assessment is required for which subsystem and component (ISA, AsBo, NoBo, DeBo, SV).
RL TZL: Directive Type Approval of Railway Equipment Elements, V2.0_d dated 1 September 2014	[11]	The directive defines the procedure and tasks of the parties involved in the type approval. <ul style="list-style-type: none"> • For a type approval, the safety cases (e.g. according to EN 50129 [19]) and the conformity certificates (e.g. for IOP) as well as the necessary independent assessments (ISA, NoBo, DeBo) are required. • Proof of conformity with IOP can already be provided as part of the type approval.

Regulation, standard	Ref.	Particularly relevant aspects
EN 50126-1:2017: Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 1: Generic RAMS process	[17]	<p>Applicable to COAT for specification and demonstration of safety and reliability / availability / maintainability.</p> <p>The standard defines the principles of hierarchical systems over several levels and the principle of hierarchical proof of safety for such systems.</p> <p>Defines the principle of Basic Integrity and SIL. Is methodically aligned with the CSM-RA [3]</p>
EN 50129:2018: Railway applications - Telecommunications, signalling and data processing systems - Safety-related electronic systems for signalling	[19]	<p>Defines the development process for safety-relevant electronic and programmable components of signalling systems, from concept to proof of safety. Also valid for ETCS OBU.</p> <ul style="list-style-type: none"> • Contains the requirements that must be met and demonstrated for functions with a SIL. • Requirements for the development process for the targeted SIL • Requirements for allowable failure rates of random failures of safety-related functions (TFFR for the corresponding SIL) • ISA assessment is mandatory to demonstrate compliance with the standard. A positive report from the ISA is a prerequisite for approval.
EN 50128:2011: Railway applications - Telecommunications, signalling and data processing systems - Software for railway control and monitoring systems	[20]	<p>Defines the development process of safety-relevant software for signalling systems. According to the AB-EBV, ETCS OBU are part of the signalling installations.</p> <ul style="list-style-type: none"> • Contains, for the specified SIL of the software, the measures that must be implemented and proven in the development to avoid systematic errors. • Contains requirements for development tools (editors, compilers, test tools etc.) • ISA assessment is mandatory to demonstrate compliance with the standard. A positive report from the ISA is a prerequisite for approval.

Regulation, standard	Ref.	Particularly relevant aspects
EN 50657: 2017: Railway applications - Applications for railway vehicles - Software for railway vehicles	[21]	<p>The standard is derived from EN 50128 [20] and adapted to the requirements of SW for vehicles.</p> <p>For COAT, EN 50128 [20] is mostly applicable, because it is an application for signalling technology. This certainly applies to all applications on the EVC, but also to outsourced subsystems such as antenna or radio.</p> <p>EN 50657 [21] could also be applicable to subsystems that not only perform ETCS functions but are also used for other vehicle control functions. E.g. for the speed measurement, the JRU etc.</p>
EN 50159:2010: Railway applications - Telecommunications, signalling and data processing systems - Safety-related communication in transmission systems	[22]	<p>Safe data transmission via insecure networks between systems that fulfil safety functions according to EN 50129 [19]. Applies to all participants of the CCS bus with safe data transmission.</p> <p>The standard is a supplement to EN 50129 [19] regarding safe data transmission. Application of the standard requires application of EN 50126 [17], [18] and EN 50129 [19]. It cannot be considered and applied as a 'stand-alone' standard.</p>
EN 50155:2007: Railway applications - Electronic equipment for railway rolling stock	[23]	<p>Requirements for the design, component selection, manufacturing, documentation, type and routine testing of electronic devices and systems on rail vehicles. These requirements are intended to ensure and demonstrate the suitability of electronics for applications on rail vehicles.</p> <ul style="list-style-type: none"> • Compliance with the standard is required for all electronics on vehicles, including all COAT components and subsystems. In particular, the EVC must also meet this standard and pass the type tests (vibration tests, temperature, EMC, etc.).
EN 50121-3-2:2016/A1:2019: Railway applications - Electromagnetic compatibility - Part 3-2: Rolling stock - Equipment	[24]	<p>EMC standard that specifies limit values and measurement methods for equipment on railway vehicles, including COAT:</p> <ul style="list-style-type: none"> • Radiation of electromagnetic fields and generation of conducted interference, • Immunity of devices against electromagnetic fields and conducted interference (transient overvoltages etc.). <p>The type tests according to EN 50121-3-2 [24] are part of the type tests for electronic systems on vehicles according to EN 50155 [23].</p>

Regulation, standard	Ref.	Particularly relevant aspects
TSI CCS:2016: Technical specification for interoperability relating to the control-command and signalling subsystem	[26]	<p>Defines the essential requirements for the control-command and signalling (CCS) subsystem for both track-side and on-board equipment in order to ensure their interoperability in accordance with the relevant EU regulations. The requirements concern both functional and non-functional requirements.</p> <p>Basis for interoperability assessment by a NoBo.</p>
NNTR CCS: Notified national rules	[27]	<p>The NNTR contains country-specific requirements for on-board ETCS equipment. This may be an addition to an 'open point' in the TSI, a requirement due to a deviation of the CH rules from the corresponding requirements of the TSI or an additional requirement due to the CH rules without correspondence in the TSI.</p> <p>Additional requirements for the on-board ETCS are clearly formulated and have already been implemented several times. There are also requirements which do not apply to COAT as they relate to Class B train protection systems.</p>
System Leadership ETCS CH: Requirements for the Use of Vehicles on ETCS Lines	[14]	<p>The document [15] gives an overview of the procedures that must be followed to obtain a type approval, an operating permit and network access in Switzerland. It also clarifies the roles and responsibilities involved between BAV, railway companies and industry in these proceedings. The procedure described refers in particular to the vehicle level (proof of correct and safe integration of the equipment into the vehicle).</p>
ERTMS/ETCS subsets	[30] to [44]	<p>Define the interfaces between the different components of the on-board ETCS equipment and between the on-board equipment and the infrastructure.</p> <p>The scope of the individual subsets, their significance for COAT and the approval procedure are listed in the analytical report [2].</p>

Tab. 2 Rules and regulations

4 SYSTEM AND ARCHITECTURE

4.1 COAT system scope

COAT comprises the on-board CCS equipment required for ETCS approval in accordance with [14] in Switzerland. In addition, COAT also includes the on-board equipment required for future ATO operation with GoA2. Since COAT should be modular and functionally expandable, the system under consideration also includes functions that enable the exact localization of trains without axle counters or track circuits. Such functions are a prerequisite for future operation under ETCS L3.

The on-board antennas, transmitters and receivers required for ETCS, ATO and localisation are part of the considered system scope.

The trackside installations (such as loops, balises, antennas, transmitters and receivers, RBCs, signal boxes, etc.) are not part of the system scope under consideration. However, the proof of safe communication and interoperability of COAT equipment with track-side installations will be taken into account in the approval procedure.

4.2 System architecture

4.2.1 Generic System Architecture

The generic COAT architecture shown in Figure 1 is the result of the analysis of the applicable regulations and standards, considering the objective of modular verification and approval.

The architecture is characterized by the following features:

- Central computer using a commercially available SIL4-enabled platform (with the appropriate development environment for creating SILx application software). Applications such as ETCS L1 LS, ETCS L2, ATO etc. run on this computer platform. In this report the central computer is referred to as the EVC.
- Standardized data bus for COAT-internal communication with all peripheral devices belonging to the COAT system scope. Using the appropriate safety protocols, the data bus enables safe communication between EVC and the peripherals, and between the peripherals where safe communication is required.

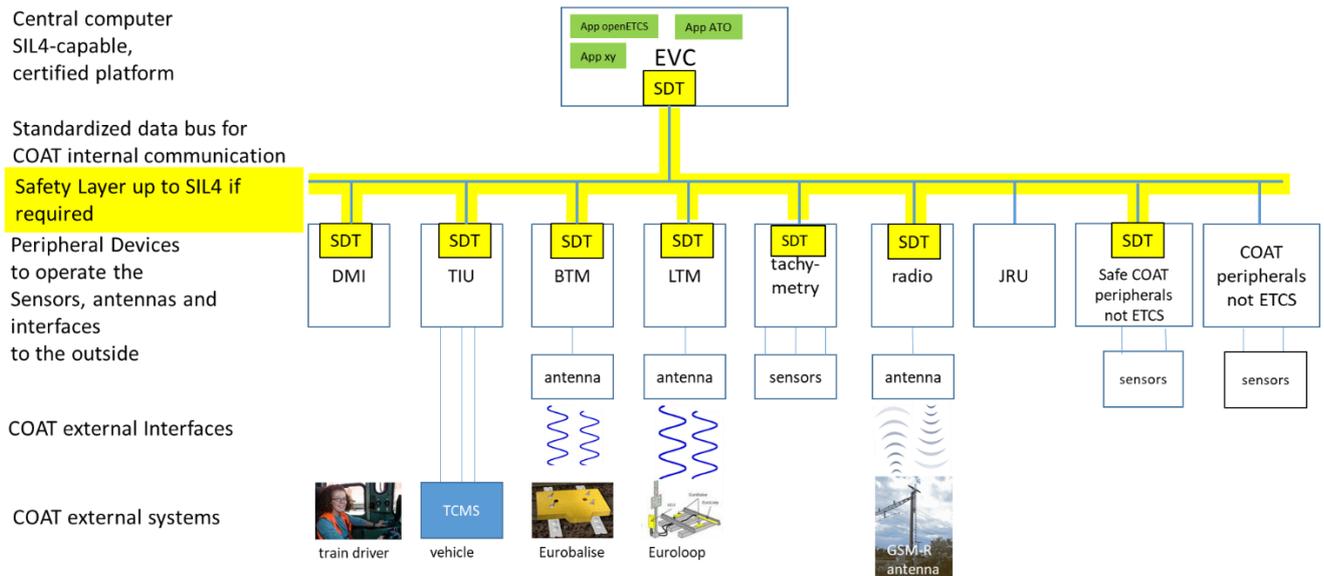


Figure 1 Generic COAT architecture, optimized for modular verification and approval

4.2.1.1 Reasons for this architecture

- Modular structure, which allows a modular verification process
- The complex external interfaces, which ensure interoperability, remain unchanged when COAT applications are modified or extended.
- The chances of finding a certified computer platform for the EVC are much greater if this platform only has to communicate with standardized bus systems.
- The architecture is suitable for setting up a reference system in the laboratory, in which the interfaces are emulated externally.
- The ETCS functionality and interoperability required by TSI CCS and the ERA sub-sets can be achieved overall with COAT.
- Simple possibilities to extend COAT with further functions (and the associated peripheral devices), e.g. for ETCS L3, ATO, train integrity (TIMS), etc.
- Simple replacement of individual devices for obsolescence, new technology (e.g. replacement of GSM-R by FRMCS), without affecting the other devices and the core functions.
- No safety verification is required for peripheral devices without safety functions, i.e. separation between safety-relevant and non-safety-relevant parts, but verification that there is no retroactive effect.

4.2.1.2 Risks of this architecture

- It may be difficult to find manufacturers for some of the peripherals, especially BTM and LTM, because these devices were previously integrated into the on-board units.
- Although the ETCS functionality and interoperability can be fulfilled with the overall COAT system, there could be difficulties in the conformity assessment by the NoBo, because the architecture partly differs from the architecture in ERA-Subset-026, and because not all subsets can be mapped 1:1 to the COAT architecture (example odometry).

- The integration of applications on the EVC that are not or not highly security relevant must be taken into account when evaluating the generic platform so that the platform supports the use of applications with different SIL (or without SIL).
- The greatest challenge is probably not the approval, but the specification of the requirements for all devices, interfaces and secure communication. The specification of this requirement is an indispensable prerequisite for procurement, verification and approval.

4.2.2 Considered COAT architecture

The approval procedure was examined for the COAT system architectures described in [1]. It was shown that the differences between the two variants I and E considered in [1] have no significant influence on the approval procedure. Therefore, the present report uses Variant I as the basis, where the sensors for velocity and position detection are directly connected to the CCS bus, while the evaluation takes place in the corresponding apps on the EVC. The COAT architecture shown in Figure 2 corresponds in its main features to the generic architecture considered optimal for modular approval according to section 4.2.1.

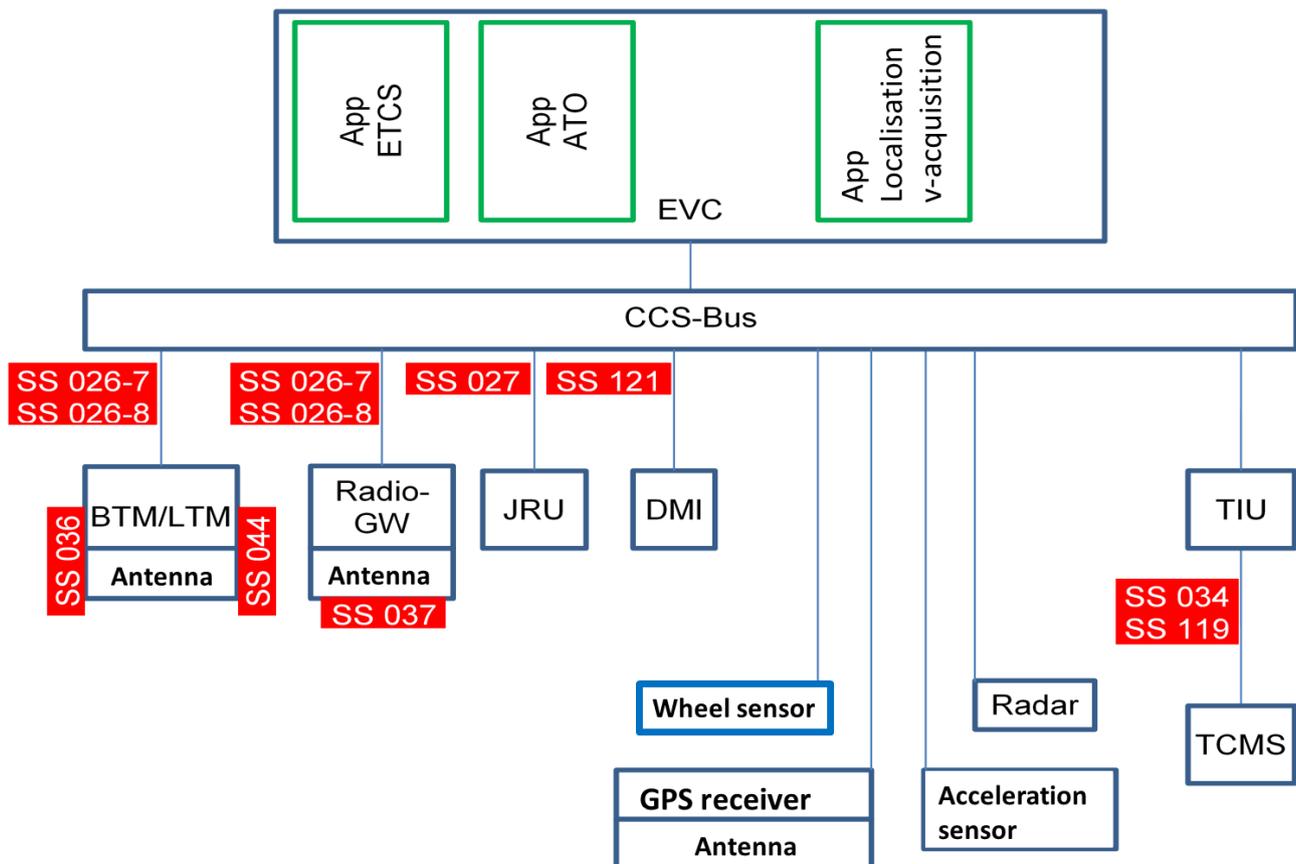


Figure 2 Considered COAT system architecture: Variant I

5 ENVIRONMENT

5.1 Current situation

5.1.1 Demonstration of compliance process

The procedure for obtaining an ETCS authorisation in Switzerland is set out in document [15]. This document deals with both the approval of infrastructure and rolling stock. The proof of safety for the entire system considers the interaction between vehicles and infrastructure. In addition to the technical aspects, this also includes the operational aspects.

The procedure is based on a hierarchical proof of safety structure. The document regulates the responsibilities of the parties involved (manufacturers, vehicle keepers, vehicle operators, infrastructure managers, licensed railway infrastructure companies) for the proofs at the various levels.

The structure of the demonstration of compliance is modular. Document [15] defines 13 different safety cases and proofs of interoperability and the relationships between them. The following safety cases are relevant for the scope of the COAT system:

No. X: Safety Case OBU-EVC, vehicle-independent, type-approved system

No. VI: Safety Case Integration of OBU in vehicle type

No. II: Safety Case for the vehicle type: prerequisite for the license to operate the vehicles of this type

The following evidence confirms interoperability and safe integration:

No. IX: IOP Notes of the OBU Supplier

No. VII: IOP Statement of the supplier of the track-side equipment supplier

No. III: IOP Overview of proof of safety and interoperability

No. I: Overall Safety Case for technically and operationally integrated signalling systems

On the infrastructure side, the procedure described in document [15] provides for modularity at the ETCS component level. For on-board equipment, the whole OBU, including EVC, is considered as one subsystem which is not further subdivided into components or modules in relation to the demonstration of compliance. However, the document does not exclude modularity within the subsystem. For the content and structure of the safety cases, document [15] refers to standard EN 50129 [19] which explicitly supports modular and hierarchical analyses.

For the type approval of components, the type approval and operating approval of vehicles, as well as for the independent assessment, document [15] is based on the FOT guidelines [11], [7] and [9] applicable in Switzerland.

5.1.2 Market, Technology

Up to now, the ETCS OBUs have mainly been supplied by the large manufacturers who, as members of the UNISIG working group, have jointly specified the ETCS system. Subsequently, each supplier has developed it and brought it onto the market. Even if individual components such as sensors, antennas, transmitters and receivers are purchased from suppliers, the system suppliers mentioned offer the entire vehicle equipment (OBU with EVC, antennas, etc.) as a complete system. The modularity of the system and the validation within the COAT system, which is the aim of COAT, can hardly be achieved with this situation, although the functional and technical requirements for the individual components and their interfaces are specified in the ETCS subsets. The investigation of these interfaces documented in the analysis report [2] shows that some of these specifications are not sufficient to modularize the OBU according to the proposed approach. The focus of the subsets is on the interoperability of the entire vehicle equipment with the infrastructure, not on the interchangeability of individual elements of the OBU, as is required for the implementation of COAT. This situation makes it more difficult for manufacturers outside UNISIG members to gain access to the market. Only for subsystems such as the DMI or the Juridical Recording Unit (JRU) is there a real opportunity for manufacturers other than OBU suppliers to market their products independently.

The central computer (EVC) is the heart of the ETCS vehicle equipment. In most cases these computers are proprietary systems of the big manufacturers mentioned above. Also the programming of these computers is done in most cases with specially developed tools, which are not freely available on the market. Thus, it is hardly possible to implement additional applications, e.g. for the ATO functions, on these computers.

Today, programmable controllers are available on the market which have been designed for safety-critical applications and have been assessed and certified in accordance with the relevant standards. These computer platforms also include the development tools required for programming and parameterizing the user software. Although the main market for such safety controllers is industrial equipment, there are also platforms on the market which meet the specific railway standards such as EN 50155 [23] and EN 50121 [24], but also the CENELEC RAMS standards for railway applications (EN 50126 [17], [18], EN 50128, [20] and EN 50129 [19]).

5.2 Outlook, Development

5.2.1 Rules and regulations, demonstration of compliance procedures

5.2.1.1 CENELEC Standards

The CENELEC-RAMS standards EN 5012x ([17], [18], [19], [[20], [21], [22]) have been fundamentally revised in recent years. The procedures for risk analyses in EN 50126 [17], [18] have been adapted to the process according to CSM-RA [3], [4]. SIL0 has been replaced by BI (Basic Integrity) and redefined especially for SW. This change has not yet been implemented in all standards, but is part of the ongoing revisions. It can be assumed that the requirements and procedures of the CENELEC-RAMS standards for the specification of safety requirements (in particular the SIL) and for the preparation and independent assessment of safety cases will remain stable in the coming years.

A CENELEC working group (WG 16) is preparing a standard draft on the subject of IT security. This standard will influence the implementation and verification of safe data transmission. The applicable

standard EN 50159 [22] focuses on the integrity of data transmission in terms of safety. Although certain security threats in open networks are also taken into account, the future standard will probably include further requirements for the defence against hacker attacks etc. Proof of safe data transmission for the safety layer of the CCS bus is likely to become more complex and demanding in the future.

5.2.1.2 TSI CCS

In principle, the version of the TSI CCS [26] according to the COMMISSION REGULATION (EU) 2016/919 of 27 May 2016 is still valid. A consolidated version is available in accordance with "Commission Implementing Regulation (EU) 2019/776 of 16 May 2019". In this edition, all changes concerning the 2016 edition have been incorporated.

Source: https://www.era.europa.eu/activities/technical-specifications-interoperability_en , heading "Control Command and Signaling TSI"

According to various sources, a new TSI is not expected until 2022. In this version, requirements for FRMCS (Future Railway Mobile Communication System; replacement of the GMS-R) are to be integrated. This also involves the entry into force of a new baseline (SRS 4.x.x).

Article 11 of Regulation (EU) 2016/919 2016/919 TSI CCS describes the procedure in connection with further development. A report is planned for June 2021, informing about the further development of ERTMS.

Article 11a provides relevant guidance for COAT authorisation:

- (2) Abolish the demonstration of technical compatibility between on-board units and different track-side ERTMS implementations.
- (3) Addresses the possibility of adapting trackside and on-board control, command and signalling system architectures, in particular to achieve a future-proof approach that facilitates the use of state-of-the-art technology and ensures backward compatibility.

5.2.1.3 Political environment

The development of Switzerland's relationship with the European Union can have a considerable influence on the approval procedure for COAT. Without a framework agreement with the EU, the existing bilateral agreements might not be adapted to the changed rules and responsibilities in the EU Member States. This could have an influence on the accreditation and recognition of notified bodies, the legal validity of the TSIs in Switzerland, the adoption and ratification of the 4th railway package, and thus also on the responsibilities of the FOT and the ERA for the approval of interoperable vehicles in international traffic.

According to the information provided by the FOT, the 4th railway package of the EU is to be adopted in two stages within the framework of the revisions of the Railway Ordinance [5]. It is intended to bring vehicle registration in Switzerland into line with procedures in the EU. This means that certain tasks and competences are transferred from the FOT to the ERA. It is not clear whether the FOT can make these adjustments without the consent of the Parliament and the Federal Council.

5.2.2 Market, Technology

Even the major manufacturers of railway equipment will hardly develop their own (proprietary) computer platforms, operating systems, data buses and software development tools in the future, but will rely instead on commercially available systems and concentrate on the development of application software. This applies particularly to platforms with safety functions (SIL1 to SIL4), the development and certification of which is very complex and time-consuming. For use as a COAT central computer (EVC), commercially available computer platforms with generic certifications up to SIL4-capability, together with the available software development tools, can be considered. As the market for industrial and automotive applications is much larger than for railway applications, the following two requirements severely restrict the market offering:

1. SIL certification must be carried out in accordance with the CENELEC railway standards [19] and [20]. Certification in accordance with the IEC 61508 industrial standard is not recognised for railway applications, although it can be regarded as technically equivalent. Subsequent certification in accordance with railway standards is possible, but is costly and often without added value in terms of safety.
2. Electronic equipment on railway vehicles must meet the requirements of standard EN 50155 [23] and the standards referenced therein, in particular EMC standard EN 50121-3-2 [24]. Conformity shall be demonstrated by type tests. This ensures that the electronic devices can withstand the harsh conditions of temperature, contamination, power supply, electromagnetic interference, vibrations and shocks during their service life of typically 20 years.

The lack of recognition of the equivalence of the SIL certification according to IEC 61508 can be regarded as an unnecessary measure to protect the railway market. The need to comply with the strict requirements of EN 50155 [23], in particular for the environmental tests, is technically justifiable because the environment on railway vehicles is indeed very demanding for electronics. However, for technologies that continue to develop rapidly, the underlying service life of 20 years would have to be critically questioned, because in reality such systems are rarely used for 20 years.

In contrast to the central computer (EVC), the peripheral devices connected to it via the CCS bus are in most cases very specifically designed for their function (e.g. speed measurement, acceleration measurement, reading balise telegrams, mobile radio transmitters and receivers, operation and display via a touch screen). Universal platforms are less suitable for these specific applications than for the EVC. For some of the functions, however, devices and sensors from other areas, e.g. from the aviation or automotive sector, could be used. For such equipment, the question of the set of rules to be applied arises again: railway standards vs. industrial standards or standards from the aviation or automotive industries. In order to keep market access as open as possible for manufacturers from other sectors, a standardized and widely used solution must be defined for the CCS data bus, because all peripheral devices must be able to communicate as safely as necessary via the CCS data bus.

6 DEMONSTRATION OF COMPLIANCE

6.1 Hierarchy and logical sequence of the Generic Safety Cases for COAT

The modularity and hierarchy of the safety cases is based on the COAT system architecture as described in Section 4.2. This means that a separate generic safety case in accordance with EN 50129 [19] is created for each device or subsystem. The integration of these devices and subsystems into the COAT system is covered by a generic safety case. This generic safety case must also include proof of safe communication between the devices via the CCS bus.

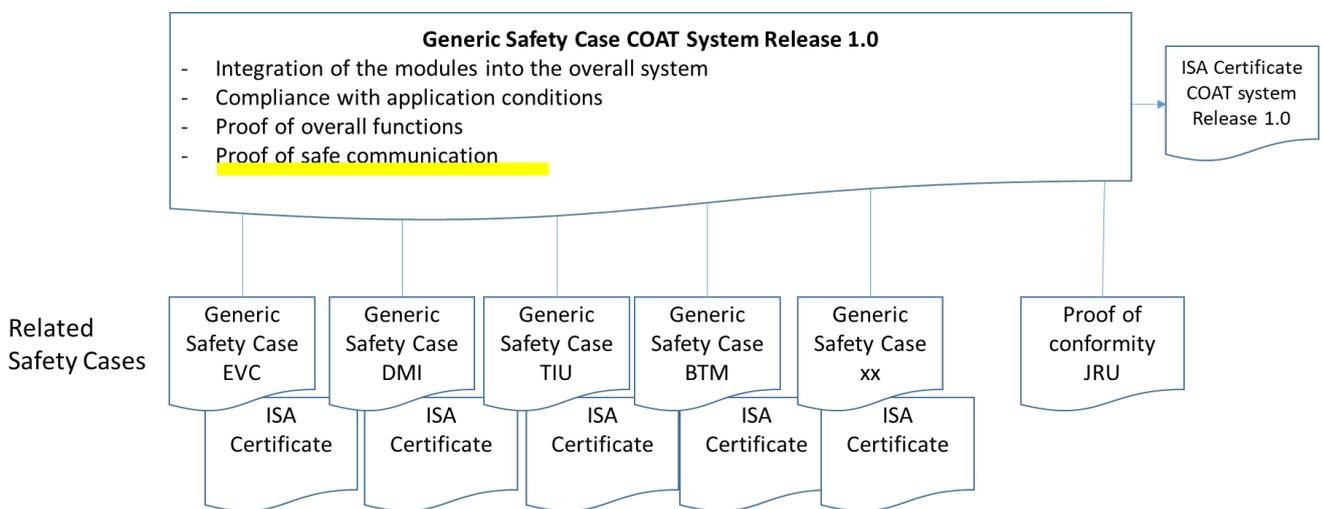


Figure 3 Hierarchy of Generic Safety Cases for the COAT System

The requirements are specified top down in accordance with the life cycle model of the CENELEC standards [17] and [19]. The safety cases, on the other hand, are created bottom-up. This does not preclude the parallel creation of safety cases, e.g. for the numerous peripheral devices on the same hierarchical level. Due to the dependencies (consideration of the exported application conditions, testing and proof of compatibility at the interfaces), however, the logical sequence according to the Figure 4 must be adhered to.

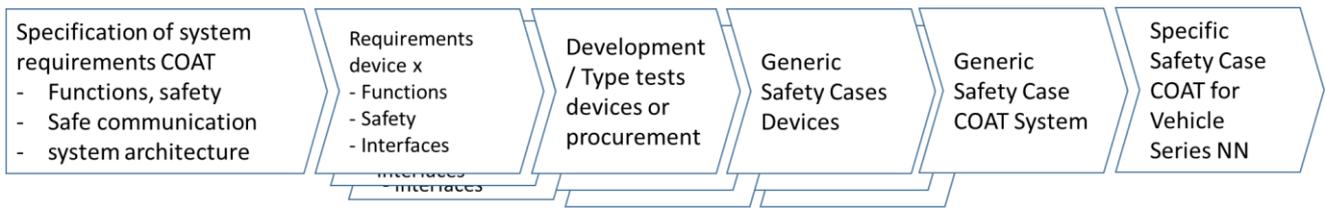


Figure 4 Logical sequence of the proof of safety procedure

6.2 Generic Safety Case for each device / subsystem

For each device or subsystem, a separate generic safety case in accordance with EN 50129 [19] is to be prepared. This includes the sensors and antennas belonging to the subsystem concerned. The scope of the generic safety case is illustrated by the example of the BTM in Figure 5. It comprises the interfaces to the CCS bus and the interface to the infrastructure, in this case to the Balise.

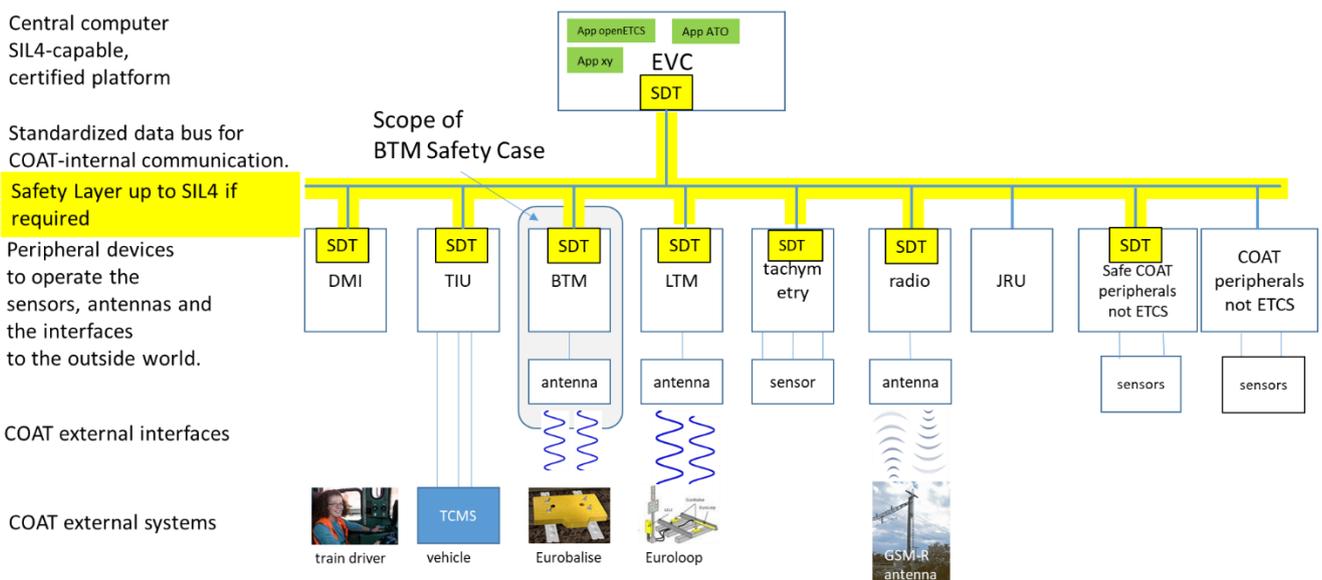


Figure 5 Scope of the generic safety case of a device using BTM as an example

The system requirements imposed on a constituent or subsystem include not only the functional and safety requirements but also the relevant requirements of the TSIs and ERTMS/ETCS subsets to ensure interoperability. Similarly, the requirements of the applicable standards, in particular EN 50155 [23] are part of the system requirement specification of the concerned subsystem or component. Depending on the software architecture, it could make sense that the applications of the peripheral device in question (running on the EVC to operate the peripheral device) are also part of the generic proof of safety for the peripheral device, and not just part of the proof of safety for the EVC.

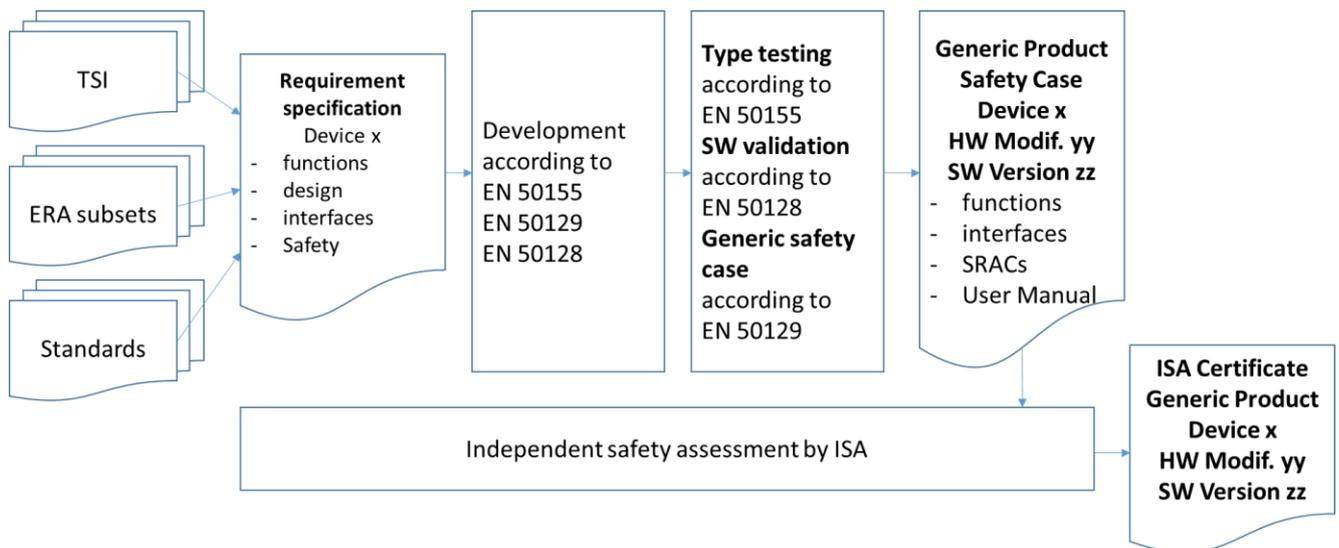


Figure 6 Generic Safety Case for each COAT device or subsystem

The validation in phase 9 of the life cycle must cover all system requirements, including the mentioned requirements from the TSIs, the ERTMS/ETCS subsets and the applicable standards. This also means that in the case of the BTM example, the correct recording of the balise telegrams must already be checked and verified within the framework of the demonstration of compliance for the BTM subsystem, not only within the framework of the examination of the entire COAT system. The extent to which tests in the laboratory are sufficient is the responsibility of the verifier, i.e. usually the manufacturer. However, it can make sense and be efficient to provide manufacturers with a pilot vehicle equipped with a COAT system (EVC, CCS bus) and a test track equipped with Eurobalises for a fee. At the level of devices and subsystems, it does not make sense to divide the demonstration of compliance process into proof of safety and proof of IOP, as practised at a higher system level in the proof of safety concept for ETCS approval in Switzerland [15].

6.3 Generic Safety Case for EVC

The generic safety case for the EVC is hierarchically on the same level as the generic safety cases for the other equipment and subsystems of COAT, even though the EVC plays a central role in the overall COAT system. The procedure for the proof of safety of the EVC is listed here separately as an example of a platform whose SIL capability has already been demonstrated by safety cases, assessment reports and certificates. This means that the generic safety case for the EVC refers to a hierarchically subordinate 'related safety case' of the generic platform. Compliance with the application conditions of the platform must be demonstrated in the EVC's generic safety case. This concerns in particular the correct use of the SW development tools. In addition, it must be checked whether all the evidence required for demonstration of compliance with the standards, in particular EN 50155 [23], is available. Any gaps and restrictions from the safety case or the associated ISA report must also be taken into account in the EVC safety case and, if necessary, passed on to the higher system level as application conditions.

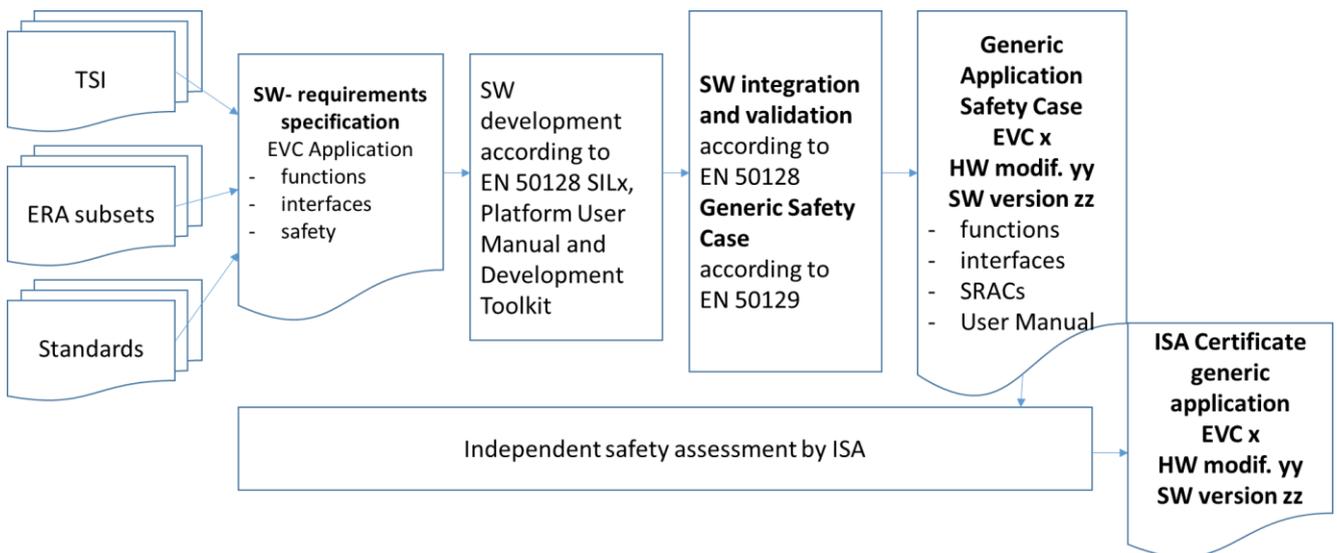


Figure 7 Generic Safety Case for EVC

6.4 Generic demonstration of compliance for devices without safety responsibility

Devices without safety responsibility, i.e. without functions with SIL requirements, can be part of the COAT system and communicate with the EVC via the CCS bus. For such peripheral devices, no safety case according to EN 50129 [19] is required. The software for these devices is not based on EN 50128 [20], but on EN 50657 [21], which applies to software on vehicles. Because no SIL requirements are placed on the software, the requirements of the standard for Basic Integrity apply to development and testing. An independent assessment by an ISA is required, neither for the devices nor for the software. Nevertheless, the manufacturer must be able to demonstrate compliance with the system requirements and thus also conformity with the standards, in particular EN 50155 [23]. This also applies to conformity with the interoperability criteria of the TSI and the ERTMS/ETCS subset, where applicable.

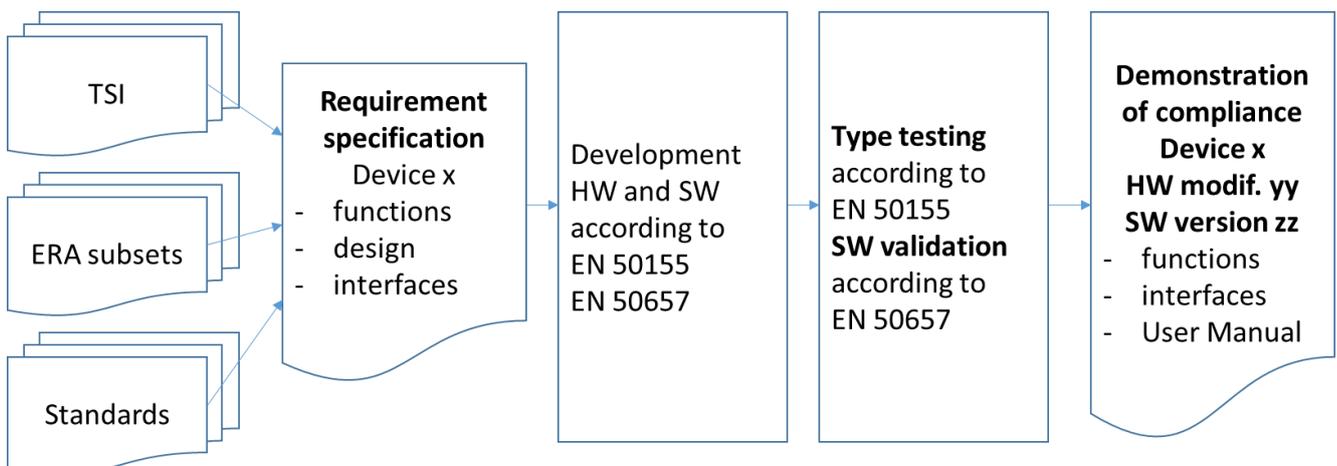


Figure 8 Generic demonstration of compliance for COAT devices without safety responsibility

6.5 Generic Safety Case for the COAT System

The generic safety case for the COAT system is based on the lower-level safety cases for devices and subsystems. The tests and verifications mainly concern the implementation of the application conditions inherited from the subordinate systems and the communication via the CCS bus. At this level, formal proof of safe communication must be provided in accordance with standard EN 50159 [22]. However, it is quite possible and to be expected that the integration of the safety layers by the individual bus participants has already taken place within the framework of the proof of safety of the subsystems and devices. Final proof of safe data transmission is only possible at this stage of the COAT system, however.

The generic safety case for the COAT system corresponds to the Safety Case X of the proof of safety concept for obtaining ETCS approval in Switzerland [15].

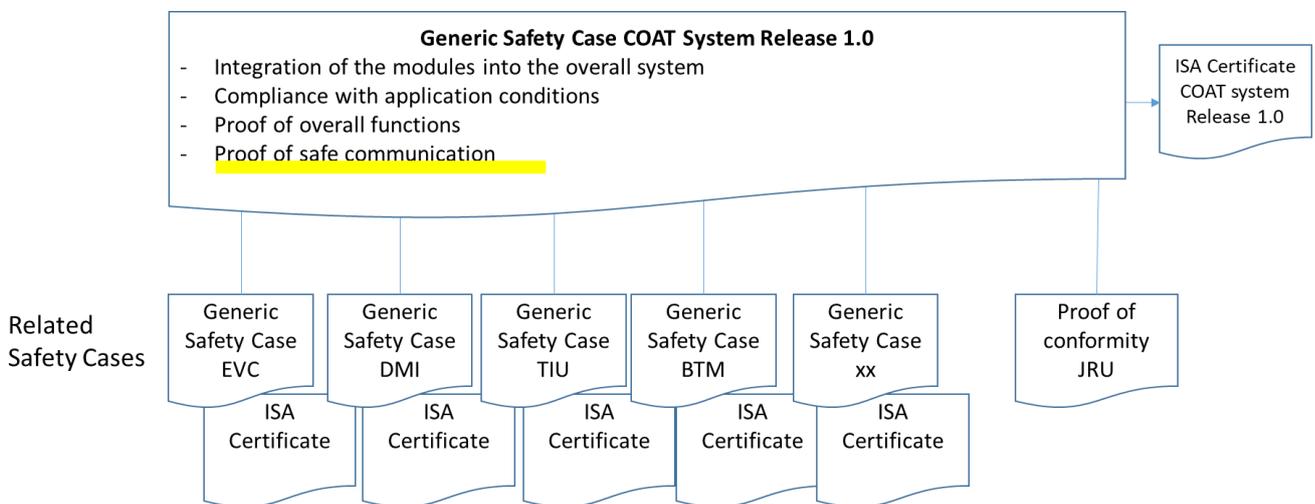


Figure 9 Generic Safety Case for the COAT system

Since the IOP requirements from the TSIs and ERTMS/ETCS subsets have also been incorporated into the system requirements for the overall COAT system at the beginning of the development lifecycle, compliance with these system requirements must also be verified and demonstrated as part of the validation and safety demonstration. In the demonstration of compliance concept [15] an IOP statement (Na VII) of the track side equipment supplier is required for this. In line with the objectives of ERTMS/ETCS, it should in the future be possible to provide this IOP proof with a pilot vehicle on a reference route for all track side equipment suppliers.

6.6 Specific safety case for COAT on vehicle type NN

As a prerequisite for the proof of safety and type approval or operating permit of a vehicle equipped with COAT, a specific safety case is required for the installation and parameterization of the generic system on a specific vehicle type. The specific safety case is based on the generic safety case for the COAT system. It must show that the application conditions (installation instructions for antennas, DMI, control elements, interfaces with the vehicle control system, etc.) are met. In addition, the overall function of the system and the interaction with the vehicle's functions (emergency brake, traction interlock, etc.) must be checked and verified.

The specific safety case for COAT on vehicle type NN corresponds to Safety Case VI according to [15].

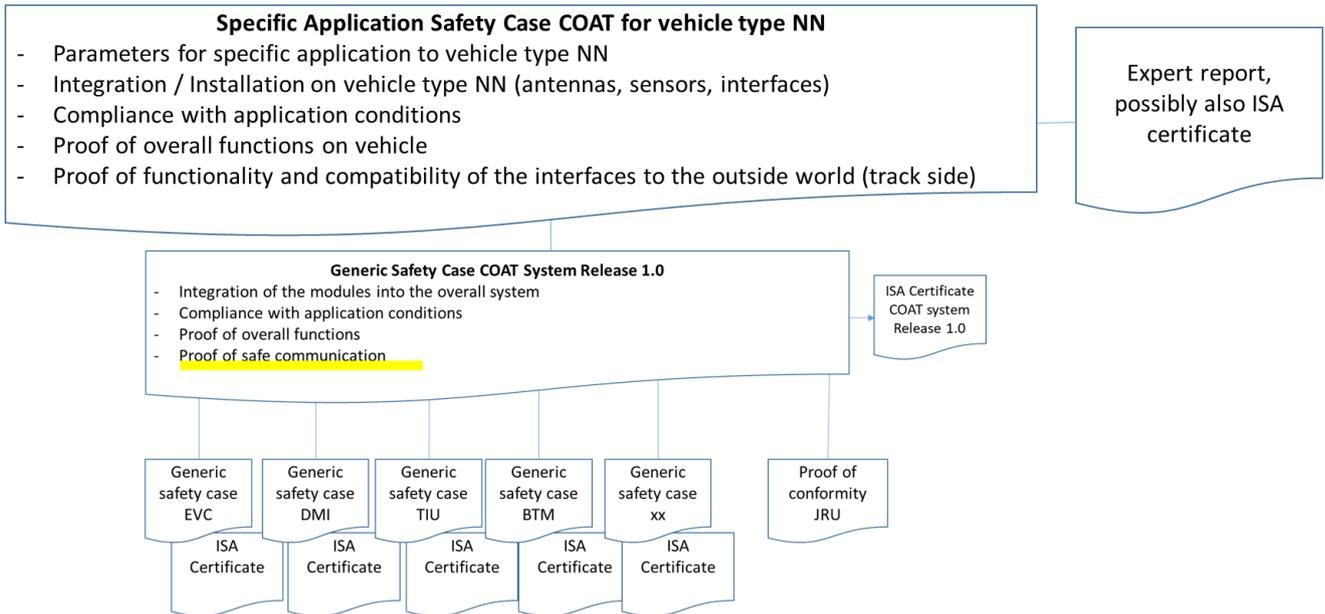


Figure 10 Specific Application Safety Case for COAT on vehicle type NN

7 INDEPENDENT ASSESSMENT

7.1 Independent safety assessment according to CENELEC

Independent assessment by an ISA is mandatory in the CENELEC RAMS standards EN 50128 [20] and EN 50129 [19] for systems and software with functions with SIL1..4. This means that an independent (positive) assessment by an ISA must be provided for all safety cases listed in chapter 6. The requirements for the assessor, the scope of the assessment and the contents of the assessment report are specified in the two standards [20] and [19] as well as in the superordinate standards EN 50126-1 [17] and -2 [18].

7.2 Assessment by experts in accordance with FOT directives

The directive for type approval [11] requires in certain cases the examination of the proof of safety by an expert. For the use and necessity of independent experts, the directive for type approval [11] refers to the directive for independent assessment bodies [9]. This directive specifies for each domain in which cases and for which components an independent assessment is required.

For the domain of **rolling stock**, reference is made to the directive for homologation of rolling stock [7]. It specifies in which cases which types of independent assessment must be carried out. For the type approval of interoperable rolling stock, a certificate of conformity with the TSIs by a Notified Body (NoBo) is required in any case. In addition, a certificate of conformity with the NNTR by a Designated Body is required. An assessment of the safety case by a risk assessment body (AsBo) is only required if the project has been classified as a significant change in the sense of the CSM [3] and the Railway Ordonnance [5].

For the **signalling** domain, the objects of an independent assessment are listed in a table. Proof of interoperability requires confirmation by a Notified Body. The application of CENELEC-RAMS standards EN 50126 [17], [18] is required for signalling systems and telematics applications, thus also for COAT. The proof of safety for systems and functions with high safety relevance (SIL3/4) must be carried out in accordance with EN 50129 [19]. This standard requires an independent safety assessment by an ISA.

7.3 Examination and confirmation of interoperability

The verification of interoperability according to the applicable TSI (TSI CCS [26] and TSI LOC&PAS [28]) shall be carried out by a Notified Body (NoBo). The safety demonstration concept for the ETCS approval in Switzerland [15] defines the required proofs of interoperability, but it does not require an independent assessment for them. The tasks of the NoBo in the hierarchically structured demonstration of compliance procedure are not explicitly defined. It can be assumed that vehicle approval requires examination and confirmation of conformity by a NoBo, as required by the FOT directive for homologation of rolling stock [7].

In order to enable a modular and hierarchical verification of the IOP by the NoBo for COAT, it is desirable to define the COAT modules, which have to fulfil interoperability requirements according to the TSI, as interoperability constituents (IC).¹ This would enable a NoBo to generically check and confirm IOP conformity for individual modules or subsystems, and not only within the framework of vehicle approval for a specific vehicle type. It is obvious that the examination and confirmation of IOP by a NoBo at vehicle type level would still be required, but the examinations carried out at the COAT module and COAT system level would significantly reduce and thus accelerate the examination at vehicle level. It should be noted that the proof of interoperability only covers the part and constituents of the COAT system which have to comply with interoperability requirements of TSI CCS [26] and TSI LOC&PAS [28], but not the peripherals and apps which fulfil additional COAT functions such as ATO. This is shown schematically in Figure 11 and Figure 12 with COAT peripherals outside the scope of the IC, some of them with safety relevance, others without.

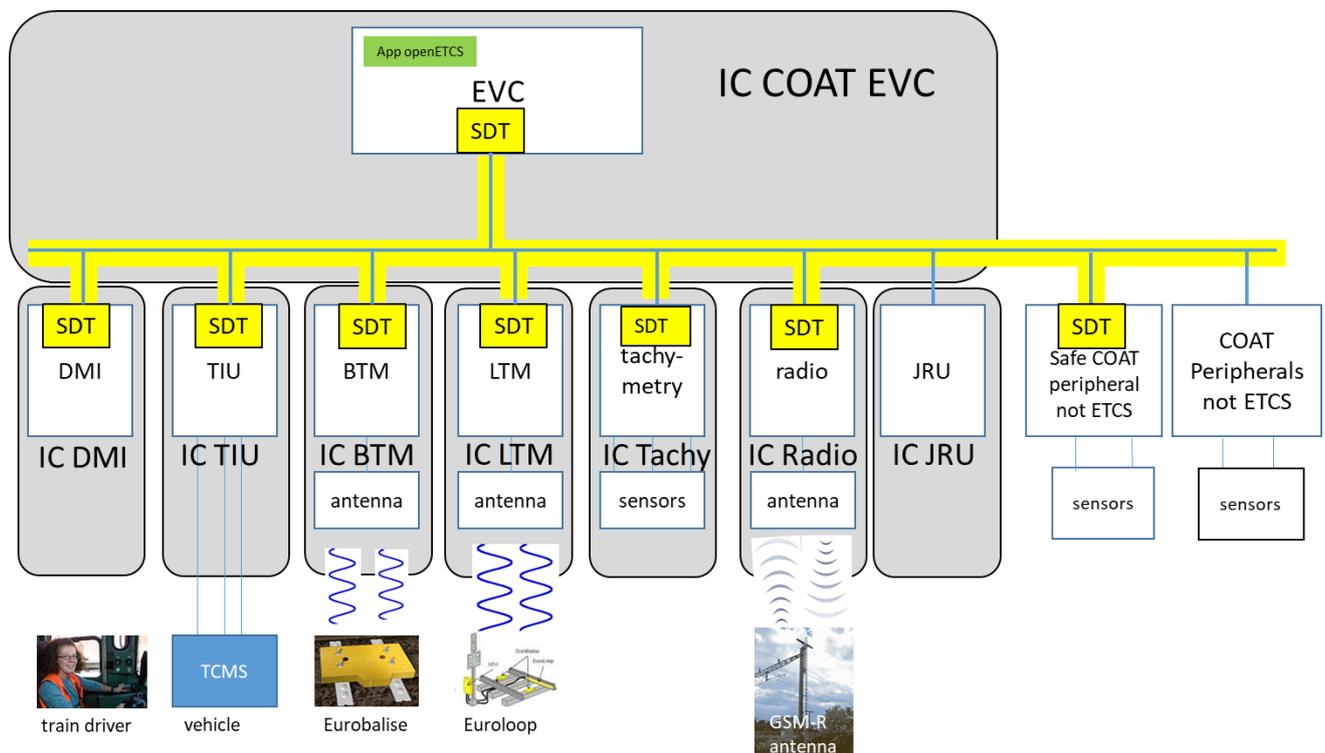


Figure 11 COAT components as interoperability constituents IC

¹ The term IC is not used here in accordance with the definition of the basic interoperability constituents in the currently valid CCS TSI, but it is a proposal that in the future ICs should be structured differently so that the NoBo could simultaneously check the IOP aspects for each component. Whether a (formally valid) certification by NoBo will already be possible at COAT component level depends on future developments of the CCS TSI. See also chapter 5.2.1.2 and recommendations in chapter 11.3.

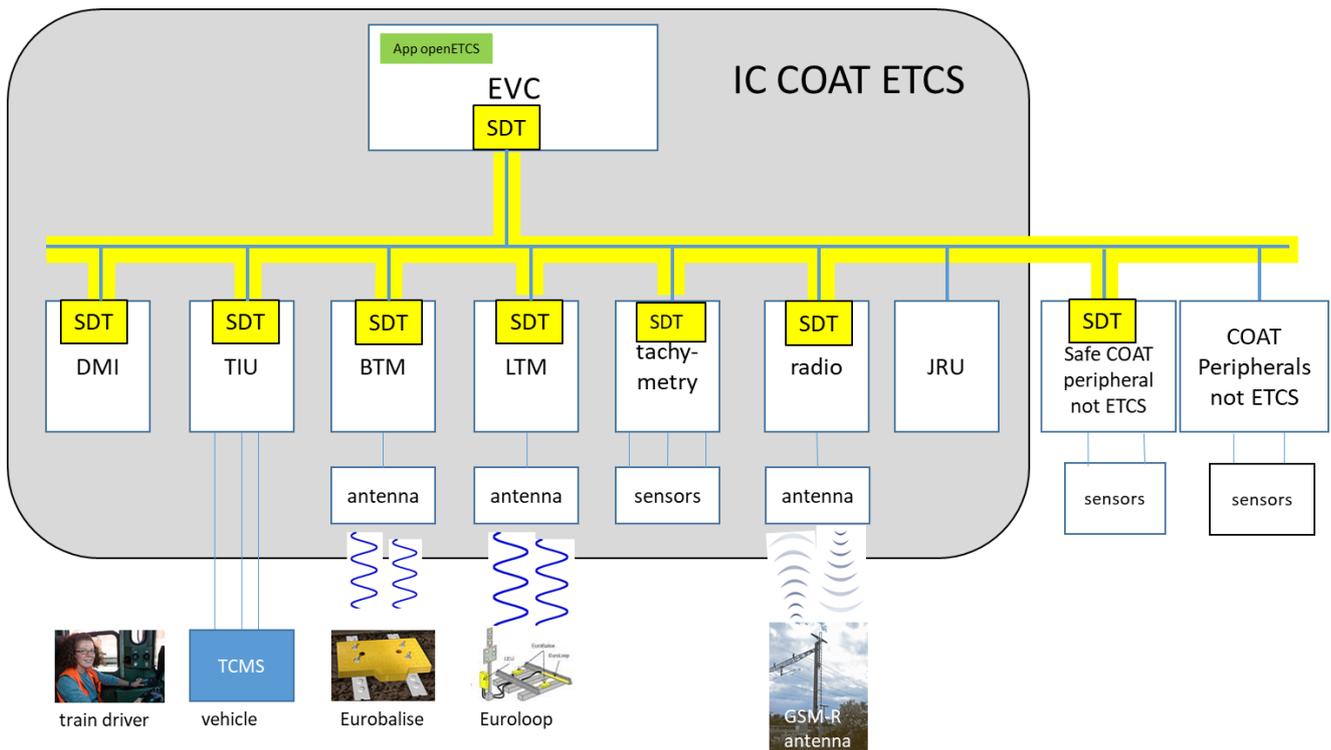


Figure 12 COAT ETCS system as interoperability constituent

The entire COAT system, which guarantees the ETCS functionality, can also be defined as IC and its conformity can be checked and evaluated generically, analogous to the proof of safety of the COAT system according to CENELEC, which also includes all safety-relevant functions that go beyond the ETCS functionality, e.g. ATO.

7.4 Concept proposal for independent assessments

The proposed approach to independent assessments aims at meeting the requirements of the TSIs, CENELEC standards and the FOT on the one hand, but also at achieving the objectives of COAT for modular, flexible and efficient certification on the other hand. In order to avoid duplication of assessments of the same aspects by different assessment bodies, it is necessary that each entity in charge of assessment is competent and, if necessary, accredited for several aspects of the assessment of a component or subsystem. However, it is not necessary that the same entity is assessing all the components and subsystems listed.

Although the project to develop and approve COAT can be regarded as a significant change (to the previous concept of the ETCS Onboard Unit, as it is highly safety-relevant, innovative and complex), an additional assessment by a risk assessment body (AsBo) based on EBV [5] 8a, paragraph 4 is not considered reasonable, as all aspects are already sufficiently covered by the other independent assessments.

Object of the assessment	What is checked?	Certificates to be issued	Required skills and accreditations
COAT EVC	<ul style="list-style-type: none"> - Generic Safety Case according to EN 50129 incl. safe data transmission (SDT) according to EN 50159 - Conformity with EN 50155 - IOP for IC COAT EVC - Conformity with NNTR 	<ul style="list-style-type: none"> - ISA Report / Certificate for the Safety Case according to EN 50129 with SDT - IOP certificate for IC COAT EVC - Certificate of conformity with NNTR - Recommendation for type approval by expert 	<ul style="list-style-type: none"> - ISA for CENELEC - NoBo - DeBo - Expert for type approval
COAT peripheral component with ETCS function	<ul style="list-style-type: none"> - Generic safety case according to EN 50129 incl. SDT according to EN 50159 - Conformity with EN 50155 - IOP for IC COAT component - Conformity with NNTR 	<ul style="list-style-type: none"> - ISA Report / Certificate for the Safety Case according to EN 50129 with SDT - IOP certificate for IC COAT component - Certificate of conformity with NNTR - Recommendation for type approval by expert 	<ul style="list-style-type: none"> - ISA for CENELEC - NoBo - DeBo - Expert for type approval
COAT peripheral component without ETCS function, but with safety relevance	<ul style="list-style-type: none"> - Generic safety case according to EN 50129 incl. SDT according to EN 50159 - Conformity with EN 50155 	<ul style="list-style-type: none"> - ISA Report / Certificate for Safety Case according to EN 50129 with SDT - Recommendation for type approval by expert 	<ul style="list-style-type: none"> - ISA for CENELEC - Expert for type approval
COAT peripheral component without ETCS function, without safety relevance			<p>No independent assessment. Declaration of conformity with EN 50155 by manufacturer</p>
COAT system	<ul style="list-style-type: none"> - Generic safety case according to EN 50129 incl. SDT according to EN 50159 - Conformity with EN 50155 - IOP for IC COAT ETCS - Conformity with NNTR 	<ul style="list-style-type: none"> - ISA Report / Certificate for Safety Case according to EN 50129 with SDT - IOP certificate for IC COAT ETCS - Certificate of conformity with NNTR - Recommendation for type approval by expert 	<ul style="list-style-type: none"> - ISA for CENELEC - NoBo - DeBo - Expert for type approval

Object of the assessment	What is checked?	Certificates to be issued	Required skills and accreditations
Vehicle type NN with COAT system	<ul style="list-style-type: none"> - Specific safety case for COAT according to EN 50129 - IOP for vehicles with COAT - Conformity with NNTR for vehicle with COAT 	<ul style="list-style-type: none"> - ISA Report / Certificate for Specific Safety Case for COAT according to EN 50129 - IOP certificate for vehicles with COAT - Certificate of conformity with NNTR for vehicle with COAT 	<ul style="list-style-type: none"> - ISA for CENELEC² - NoBo - DeBo

Table 3 Proposed approach for independent assessment

² Due to the FOT's feedback, no further independent examination by an AsBo is planned in addition to the ISA.

8 HOMOLOGATION

8.1 Fundamental principle

Type approvals by the FOT are sought for COAT subsystems and components, as well as for the generic COAT system. Prerequisites for the type approval of an object:

- Safety case according to CENELEC
- Assessment report by the ISA (confirmation of the safety case)
- Certificate of interoperability by the NoBo, if it is an IC
- Certificate of conformity with the NNTR by the DeBo, if it is an IC
- Recommendation for type approval by the expert

The recommendation of type approval by the expert in the form of an expert report should be a mere formality, especially in the case of type approval items, which are also defined as IC, because the assessments by ISA, NoBo and DeBo should cover conformity with the entire set of applicable rules and regulations.

In the case of COAT components that are neither IC nor safety-relevant, a separate expert opinion may be necessary and useful in order to check and confirm conformity with the applicable standards, such as EN 50155, and the Swiss regulations (EBV [5], AB-EBV [6]). However, the directive [11] only applies to the type-approval of safety related elements of railway installations. It is not foreseeable at this stage of the COAT project whether any components that are relevant neither for interoperability nor for safety could be part of COAT at all.

8.2 Type approval of the devices

The type approval objects are all elements that are also defined as IC. In addition, peripheral devices which do not have to fulfil interoperability criteria are also subject to type approval, especially if they are relevant to safety. In order to achieve the desired modularity and flexibility for approval, the type approval objects must be congruent with the IC and the safety cases and have the same hierarchy.

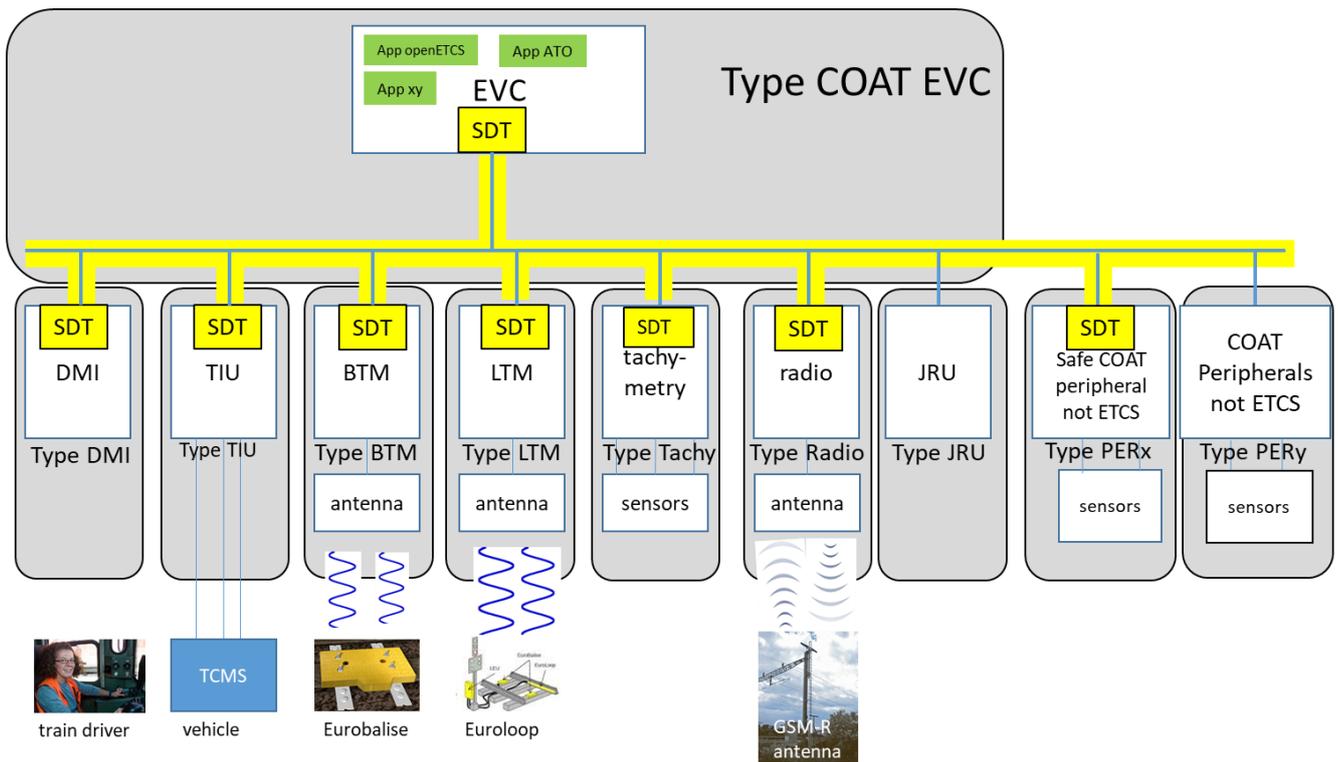


Figure 13 Type approval items: COAT components

8.3 Type approval of the COAT system

Type approval should also be sought for the generic COAT system. As with the safety case and the IC, this will be a generic maximum configuration. Specific applications of COAT, i.e. for a specific type of vehicle, will only consist of a subset of the devices and applications. In addition, it is to be expected that several (equivalent) type-approved devices from different manufacturers will be available for individual peripheral devices. The type approval for the COAT system must specify which type-approved devices can be used.

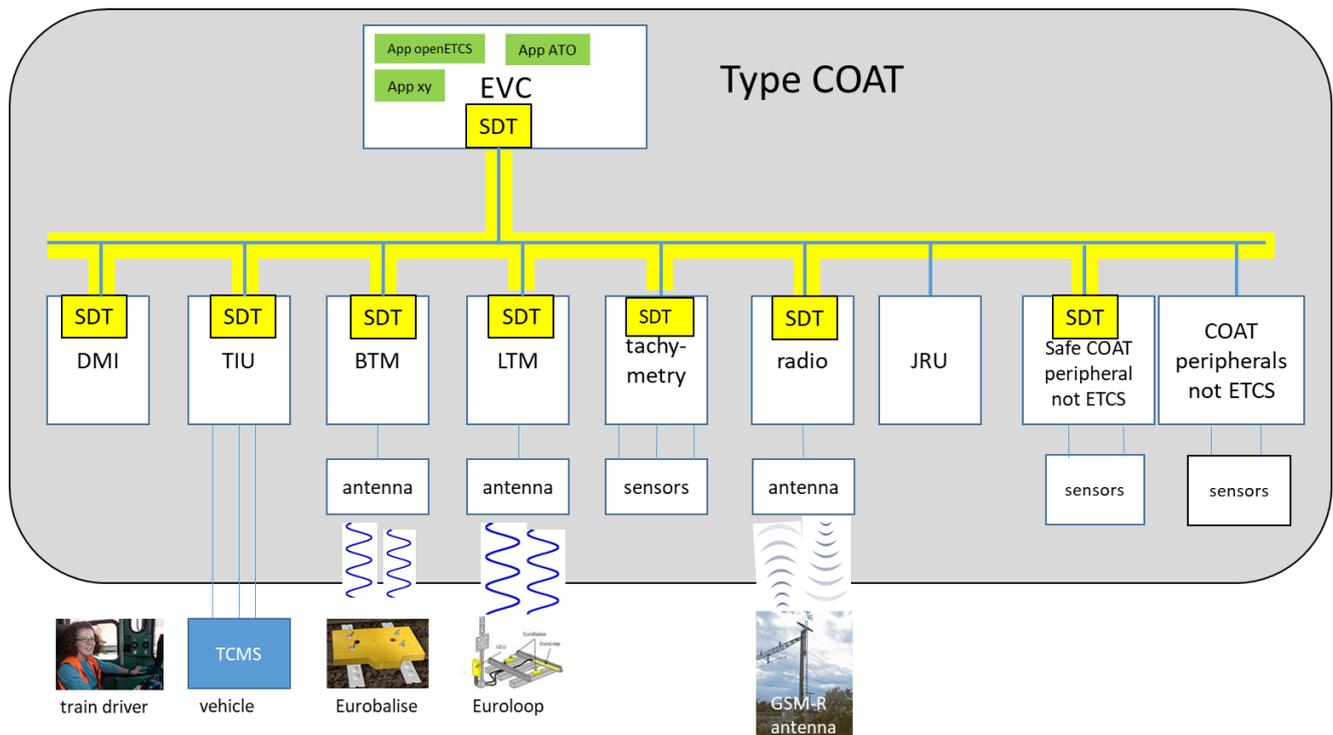


Figure 14 Type approval item: COAT System

8.4 Type approval of vehicles

The type-approval of interoperable rolling stock is governed by the Railway Vehicle Approval Directive [7]. For the COAT system, a specific safety case in accordance with CENELEC is required with the assessment report by the ISA. The specific safety demonstration applies to the specific configuration and parameterisation of COAT for the specific vehicle series. The specific safety case is based on the generic safety case for the COAT system, which in turn is based on the lower-level safety cases for the COAT devices.

The interoperability of the entire vehicle with integrated COAT, configured and parameterised for the specific vehicle type, must be certified by the NoBo. The conformity of the entire vehicle with the NNTR must also be confirmed by the DeBo.

A type approval of the specific configuration of the generic COAT system for a particular vehicle type makes no sense, because this configuration of COAT can only be used for this vehicle series. The reuse of the system within the vehicle series is ensured by the type approval of the vehicle, usually obtained with the first vehicle.

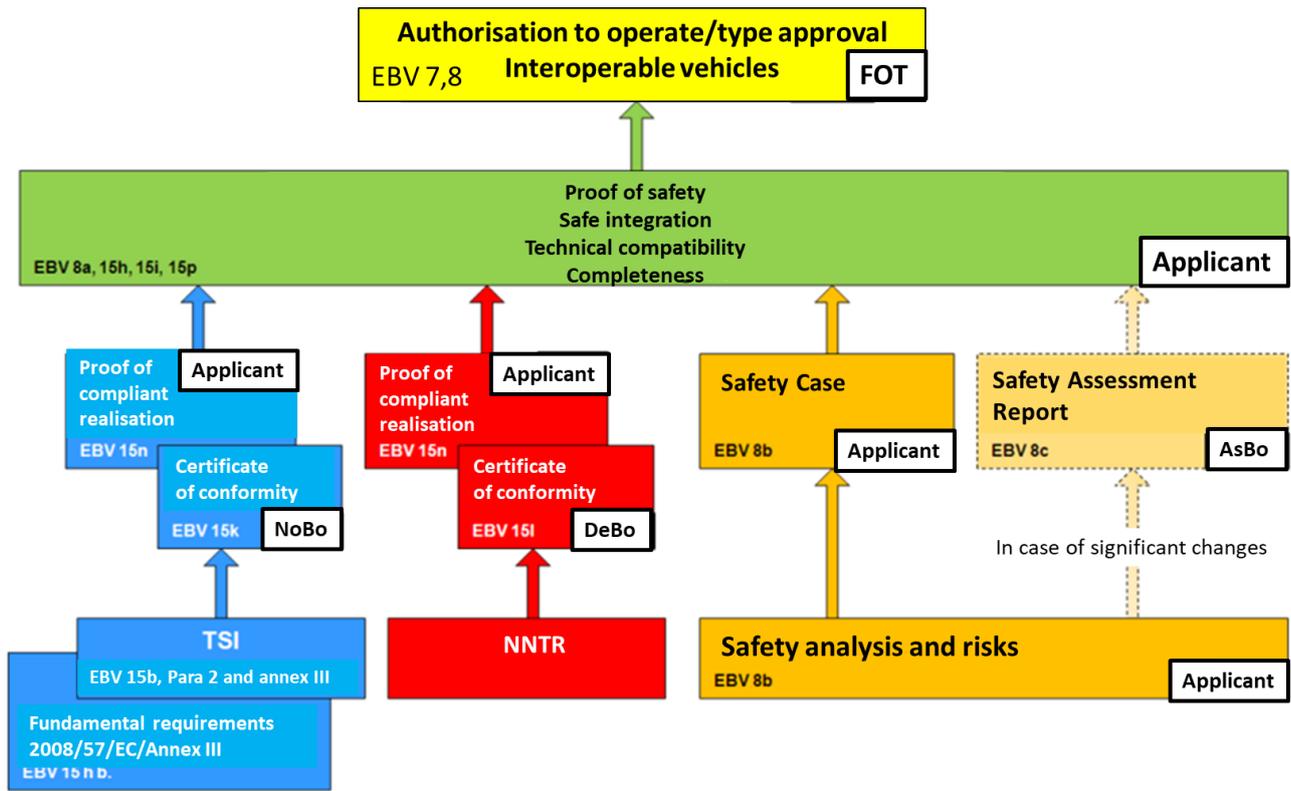


Figure 15 Evidence required for the type approval of interoperable vehicles according to [7]

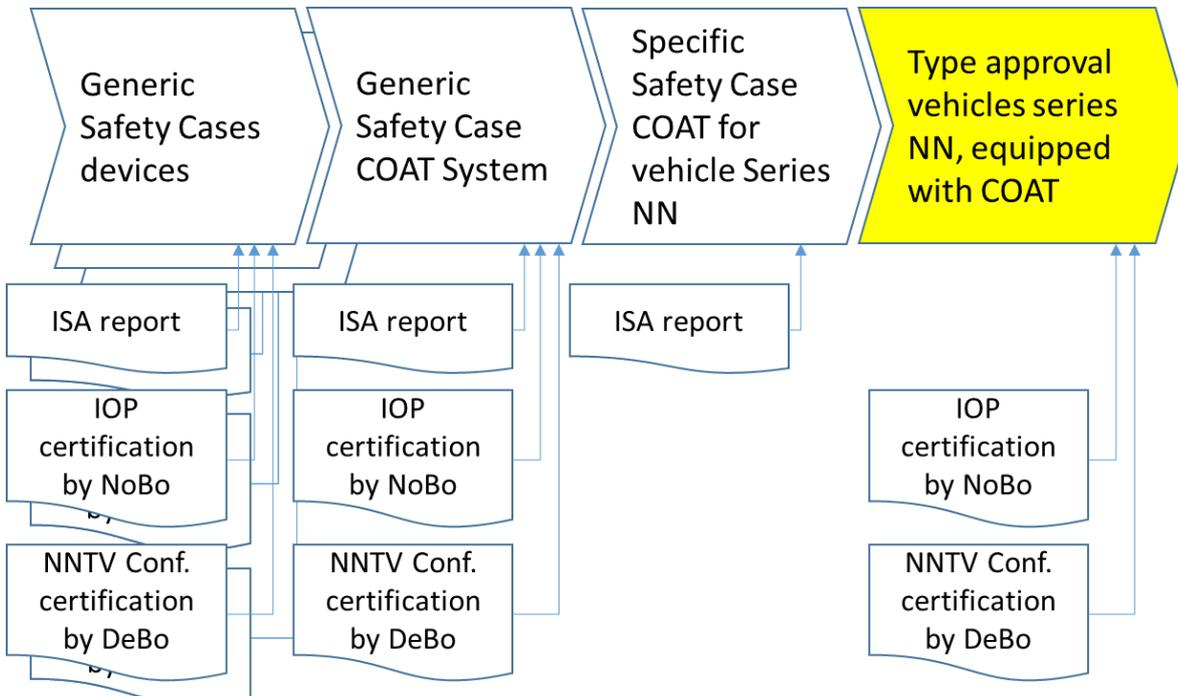


Figure 16 Evidence and assessment reports / certificates from the COAT point of view

8.5 Type approval of the procedure

The Directive on the type-approval of elements of railway installations [11] also provides for the possibility of type-approval of procedures. This possibility should be used in particular for the approval procedure following changes to COAT components and to the whole COAT system. The purpose of this procedure is to regulate the following aspects:

- Assessment of the changes: Responsibility, criteria, categories
- Procedure for re-validating the evidence for the different categories of changes
- Definition of minimum mandatory regression tests for each change category and for each type approval object
- Definition of the test environment:
 - o Tests which can be carried out in the laboratory environment
 - o Tests to be carried out on the vehicle and on the track
- Required documentation of changes for the various categories, e.g:
 - o revision of the relevant specifications and supporting documents, or
 - o Addendum to the documents concerned, but without revision of the documents themselves.
- Inclusion and role of the independent assessment bodies for the different categories of changes
- Documentation of the expert opinions and certificates of the independent assessment bodies depending on the change category, e.g. :
 - o revision of assessment reports and certificates, or
 - o Supplementing existing assessment reports and certificates with supplements (declarations of validity).

8.5.1 Categories of changes

The Directive on the type-approval of elements of railway installations [11] provides for two categories of amendments in the field of signalling:

1. Functional changes
2. Change of the technical implementation (HW / SW)

These two categories of changes could be supplemented by a category in which no changes are made to the object itself, but only to the associated documents. Such changes are particularly necessary when, in the course of operation, it becomes apparent that additions to the application conditions are necessary, or when test specifications need to be clarified. Since these documents are also part of the

demonstration of compliance and safety, a formal update of the documents and proofs is required, even without any changes to the hardware or software.

9 TEST INFRASTRUCTURE AND TEST CONCEPT

9.1 Test laboratory of the system leader

For the testing and initial approval of COAT components and the COAT system, but above all for the approval after changes, the approval of components from other manufacturers and the correction of errors, the establishment of a test laboratory in which the real COAT hardware and software can be tested is of great use. In the test laboratory, the communication between the various participants via the CCS data bus can also be tested under real conditions, without the need for installation on a vehicle and test runs on the track.

The environment, the track-side systems and parts of the peripheral devices, e.g. the vehicle, the balises, loops, the stationary GSM-R receivers and transmitters, the sensors for speed measurement etc. must be simulated by appropriate hardware and software for the laboratory setup. The test laboratory shall include the complete (maximum) system scope of COAT. For the tests of individual devices, the respective device of the laboratory setup is replaced by the test object (equipment under test). The laboratory with the COAT system (minus the test object) forms the test environment for such laboratory tests.

In order to avoid dependencies on individual manufacturers, the test laboratory would have to be set up and operated by the system leader. However, the laboratory may be made available to manufacturers for testing their products against appropriate compensation.

9.2 Test vehicle and test track of the system leader

Even a very complete and realistic test laboratory cannot cover all aspects of real operation. It therefore makes sense to equip a test vehicle with a complete (maximum) COAT system analogous to the test laboratory. This system shall be configured and parameterised for the test vehicle. In particular, with this test vehicle the complex interfaces of COAT with the infrastructure and the vehicle can be tested under real conditions, i.e. the data transmission from the balises and loops, the communication via GSM-R (or a future system), the interfaces with TCMS and the brake system, the interface with the driver.

Such tests shall be able to be carried out on a real line equipped with ETCS for L1, L2 and the transition between these systems. Instead of a test track to be specially equipped for this purpose, it should be possible to run on selected track sections of existing, already equipped lines. However, for test runs with the COAT test vehicle on commercial routes, the operating permit issued by the FOT must also be taken into account, because the test vehicle loses the operating permit when a component or app is replaced by the test object. This procedure should also be governed by the procedure under 8.5 or by a separate directive.

For the same reasons as for the test laboratory, the test vehicle would have to be equipped and operated by the system operator. The routes used can be operated under the responsibility of the Infrastructure Manager.

9.3 Minimal regression tests

One of the objectives of COAT is to reduce the amount of tests on the vehicle and on the track as much as possible, especially after modifications. Even with the planned modular structure, it will be necessary to confirm the correct functioning and interoperability after modifications with tests in the laboratory, on the vehicle and on the track. This also applies to functions and components that are not affected by the change, at least not intentionally.

In order to minimise the scope of tests, in particular on the vehicle and on the track, without compromising safety and functionality, minimum (mandatory) regression tests should be planned and specified for each COAT component (HW and SW) and for each level of integration up to the vehicle level. The need for individual test cases can be pre-defined for the different change categories based on generic impact analysis. The minimum regression tests to be performed are a subset of the tests specified and performed for initial approval and the corresponding safety and IOP evidence.

The additional tests required must be defined for each change based on the specific impact analysis, and these tests are also a subset of the tests performed at the time of initial approval, provided that the associated requirement specification (and therefore the test specification) did not need to be changed.

10 USE CASES

10.1 First approval of the COAT devices and the COAT system

For the specification, development and initial approval of COAT devices and the COAT system, the development life cycle in accordance with CENELEC EN 50126-1 [17] and EN 50129 [19] must be followed. Phases 4 (specification of system requirements) and 5 (architecture and apportionment of system requirements) are decisive for the concurrent development of the various devices and applications. The demonstration of compliance is carried out as described in chapter 6.

10.2 Functional extension of the COAT system

An extension of the COAT system with additional functions such as train integrity (TIMS) can be achieved by

- additional peripheral devices connected to the CCS bus and / or
- additional information obtained from the existing peripheral devices which has not yet been transmitted via the bus interface and / or
- additional applications to be developed and implemented on the EVC.

This means for the demonstration of compliance:

- Safety cases according to EN 50129 [19] for the new peripheral devices
- ISA assessment report for the safety cases of the new peripheral devices
- Update of the safety cases for modified peripheral devices
- Update of ISA reports for modified peripherals
- IOP and NNTR examination of the new peripheral devices by NoBo / DeBo if the extension is due to changes in the TSI (e.g. ETCS L3)
- Update of IOP and NNTR certificates for modified peripherals for which IOP and NNTR certificates were issued at the time of initial approval
- Update of the Generic Safety case for the COAT System
- Update of the ISA report for the updated safety case of the COAT system
- Update of the specific safety cases for COAT for the vehicle types concerned
- Update of the assessment report for the updated specific safety cases for COAT for the vehicle types concerned
- Update of the Safety Case for the vehicle types concerned

- Update of the IOP certificate by the NoBo for the vehicle types concerned
- Update of the NNTR certificate by the DeBo for the vehicle types concerned

10.3 Functional changes

Formally, the generic safety case of the device and the associated ISA certificate lose their validity because they refer to the precise configuration of hardware and software. This does not apply to parameters whose change is already planned in the generic safety case.

As a result, all higher-level safety cases and their associated ISA certificates formally lose their validity because they refer to the exact versions of the associated (related) safety cases.

The generic safety cases on the same level, i.e. the other devices, remain valid as long as nothing changes at the interface and as long as their software does not need to be changed.

10.4 SW changes without changes to the interfaces

SW changes that affect only the local software of a peripheral device require an update of the generic safety case of that device because the generic safety case is valid for the exact configuration of the hardware and software of that device.

As long as this SW change does not require any changes to the device interface, updating the higher-level safety cases is of a purely formal nature. It can be done e.g. by an 'Addendum'.

For the generic safety case of the device with modified SW, it must be demonstrated that the modification functions as expected, and that it has been implemented without retroactive effects, i.e. that the other functions of the device and the proofs are still valid.

- Tests on a reference system in the laboratory to confirm compatibility at the interface
- Minimal regression tests up to the integration on the vehicle
- Update of the assessment report of the modified device
- Formal validation of the assessment reports of the higher-level safety cases by the ISA

In general, such SW changes have no intended impact on interoperability and NNTR compliance. Any unintended influences on interoperability or conformity with the NNTR must be detected by the minimal regression tests.

10.5 Bug fixes

Error corrections are necessary if it becomes apparent in operation that systems or components do not behave as specified or as expected (even if the expected behaviour was not explicitly specified).

Errors that have already been made in the specifications require the correction of the specifications and their implementation. This may even require extensions of the functionality according to section 10.2 and thus require a very time-consuming re-validation and approval.

Minor errors can often be corrected in individual software components without requiring changes to the interfaces. In addition to the actual error correction, it is also necessary in this case to formally update the relevant safety cases (including those at higher hierarchical levels). In addition to the tests of the modified components, the minimum regression tests according to the type-approved procedure for the corresponding modification category are required for the verification of freedom from retroactivity.

11 CONCLUSIONS

11.1 Challenges

- Definition of the standard for the CCS data bus.
- Specification of requirements for all devices, interfaces and safe communication.
- Find manufacturers for complex peripherals, especially for BTM and LTM.
- NoBo conformity assessment because the proposed COAT architecture differs from the architecture in ERA-Subset-026, and because not all subsets can be mapped 1:1 to the COAT architecture.

11.2 Potential

- The modular structure of COAT has a great potential for reducing costs and lead times, especially in the case of changes and extensions in the operation and maintenance phase of the life cycle.
- The modular structure ensures that changes to individual modules have no impact on other modules as long as the interfaces remain unchanged.
- The initial approval is only insignificantly or not at all penalized by the modular structure of the system and the approval concept, since existing, very complex interfaces to the outside world (track side) are hardly changed.

11.3 Recommendations

- Striving for congruent structures for
 - the safety cases according to EN 50129,
 - the interoperability constituents IC,
 - the type approval objects
- The participation of the FOT and the system leader for ETCS in international committees and projects is intended to influence the further development of the TSI in order to enable modular examination of the interoperability components in accordance with the COAT system

architecture. ERA is already making efforts towards a new, future-oriented system architecture (see Chapter 5.2.1.2).

- Assignment of independent assessment bodies which are able, in terms of their capabilities and the necessary accreditations, of assessing and certifying an object with respect to
 - independent assessment as ISA according to CENELEC,
 - examination of interoperability as a notified body (NoBo),
 - examination of conformity with NNTR, and
 - expert opinion for type approval
- Type approval of the procedure for the validation of demonstration of compliance after modifications, graduated for different categories of modifications.
- Laboratory set-up by the COAT/ETCS system leader in order to be able to carry out tests for initial approval and after modifications independently from the manufacturers and to minimise the scope of tests on the vehicle and on the track.
- Equipment of a pilot vehicle for IOP tests of the COAT system and individual components on suitable sections of railway line.
- Clear specification of interfaces. Based on these interface specifications seek dialogue with potential suppliers for the critical subsystems.

12 REFERENCES

12.1 Basics

- [1] ECH-429.03-003: System Description COAT, Version 1.0
- [2] ECH-429.03-004: Analysis report COAT approval, version 1.0

12.2 Laws, directives

- [3] EC 352/2009 CSM-RA: Regulation establishing a common safety method for the evaluation and assessment of risks
- [4] EU 2015/1136: Implementing Regulation amending the Implementing Regulation on the common safety method for risk evaluation and assessment
- [5] EBV 742.141.1: Ordinance on the Construction and Operation of Railways (Railway Ordinance); as of 15 May 2018
- [6] AB-EBV: Implementing Provisions for the Railway Ordinance, as of 1 July 2016
- [7] Directive for the homologation of railway vehicles (Type approval / Authorisation to operate), V2.3a de, July 1, 2018
- [8] RL NZB: Richtlinie zum Erlangen Netzzugangsbewilligung und Sicherheitsbescheinigung sowie Sicherheitsenehmigung (Directive for Obtaining Network Access Permits and Safety Certificates as well as Safety Permits), 1 January 2018
- [9] RL UP-EB: Directive Independent Assessment Bodies for Railways, V2.0 dated 16 January 2017
- [10] RL Nachweisführung SA: Directive for the homologation of signalling systems, version 3.0, 23.10.2015
- [11] RL TZL: Directive Type Approval of Railway Equipment Elements, V2.0_d dated 1 September 2014
- [12] Guideline for CCS Authorisation on Rail Freight Corridors
- [13] RL IOP: IOP requirements for complementary network lines, V1.1 of 1 May 2016
- [14] System Leadership ETCS CH: Requirements for the Use of Vehicles on ETCS Lines, V2.4.2 dated 12.06.2019
- [15] System Leadership ETCS CH: Proof of Safety concept for obtaining approval in Switzerland, version 2.0 of 22.11.14

- [16] System Leadership ETCS CH: Master test concept for obtaining an ETCS operating licence, Version 1.5 of 17.05.2016

12.3 Standards

- [17] EN 50126-1:2017: Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 1: Generic RAMS process
- [18] EN 50126-2:2017: Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 2: System-related safety methodology
- [19] EN 50129:2018: Railway applications - Telecommunications, signalling and data processing systems - Safety-related electronic systems for signalling
- [20] EN 50128:2011: Railway applications - Telecommunications, signalling and data processing systems - Software for railway control and monitoring systems
- [21] EN 50657: 2017: Railway applications - Applications for railway vehicles - Software for railway vehicles
- [22] EN 50159:2010: Railway applications - Telecommunications, signalling and data processing systems - Safety-related communication in transmission systems
- [23] EN 50155:2007: Railway applications - Electronic equipment for railway rolling stock
- [24] EN 50121-3-2:2016/A1:2019: Railway applications - Electromagnetic compatibility - Part 3-2: Rolling stock - Equipment
- [25] EN 50125-1:2014: Railway applications - Environmental conditions for equipment - Part 1: Equipment on rolling stock

12.4 Technical Specifications

- [26] TSI CCS:2016: Technical specification for interoperability relating to the control-command and signalling subsystem
- [27] NNTR CCS: Notified national rules; valid since July 2016
- [28] TSI LOC & PAS:2019: Technical Specification for Interoperability for the subsystem 'rolling stock - locomotives and passenger coaches' (2019)
- [29] NNTR LOC & PAS: Notified National Technical Rules; valid from June 2015 and July 2016 respectively.
- [30] ERTMS/ETCS Subset-026-7: System Requirements Specification, Chapter 7, ERTMS/ETCS language, Version 3.6.0

- [31] ERTMS/ETCS Subset-026-8: System Requirements Specification, Chapter 8, Messages, Version 3.6.0
- [32] ERTMS/ETCS Subset-027: FIS Juridical Recording, Version 3.3.0
- [33] ERTMS/ETCS Subset-034: FIS Train Interface, Version 3.2.0
- [34] ERTMS/ETCS Subset-035: FFSIS Specific Transmission Module, Version 3.2.0
- [35] ERTMS/ETCS Subset-036: FFFIS for Eurobalise, Version 3.1.0
- [36] ERTMS/ETCS Subset-037: FIS EuroRadio, Version 3.2.0
- [37] ERTMS/ETCS Subset-044: FFFIS for Euroloop, Version 2.4.0
- [38] ERTMS/ETCS Subset-056: STM FFFIS Safe Time Layer, Version 3.0.0
- [39] ERTMS/ETCS Subset-057: STM FFFIS Safe Link Layer, Version 3.1.0
- [40] ERTMS/ETCS Subset-058: FFFIS STM Application Layer, Version 3.2.0
- [41] ERTMS/ETCS Subset-121: FFFIS DMI-EVC Interface, Version 0.3.0
- [42] ERTMS Users Group: EEIG 97E2675B: FFFIS Odometer, Version 5, 31.7.1998
- [43] ERTMS/ETCS UNIT, ERA/ERTMS/033281: Interfaces between Control-Command and Signalling trackside and other subsystems, 3.0
- [44] ERTMS/ETCS Subset-119: FFFIS Train Interface, Version 0.1.13

12.5 Related documents, literature

- [45] European Railway Agency – Feasibility Study Odometry and DMI Interface V 1.6 07/06/2013
- [46] Safety Plan - smartrail 4.0, draft version 1, 27.8.2019
- [47] Type approval application according to Art. 18x EBG / Art. 7 EBV for the specification of the AWG "Trackside Asset Drive Control", Version 1, 27.8.2019.