

SM ETCS CH

# Safety case concept to obtain ETCS homologation in Switzerland

(On-board and trackside equipment)

Version V 2.0

Date: 22.11.2014

	Created	QS reviewed	Approved
Date	22.11.14 <i>M. Kehrli</i>	The legally relevant version is the document in German language. The English version is only for information.	
Name	M. Kehrli		
Position / function	Safety Management SM ETCS CH		

## Document data sheet

Content	Structure of safety cases, requirements for their structure and content as well as the relationships of safety cases to each other, taking into account the IOP for ETCS vehicles and infrastructure facilities in Switzerland
Created by	M. Kehrli
Word processor	Microsoft Word 2010
File name	14_SF_ETCS_CH_RAMSiNa_Konzept_V202-en.doc
Status of the document	In processing / in review / <b><u>Approved</u></b>
Distribution list	Railway undertakings (RUs) Vehicle keepers (VKs) Infrastructure managers (IMs) Railway infrastructure undertakings (RIUs) FOT (in particular publication on FOT website)

## Proof of changes

Version	Date	Author	Notes of modifications
X1.00	08.11.2006	Markus Bolli	Opening of the document
X1.01	25.11.2006	Ulrich Hügli / Markus Blass	Reworking after review and division into two documents (2nd document as instructions for use)
X1.02	1.12.2006	Ulrich Hügli / Markus Blass	Corrections/supplements
X1.03	2.12.2006	Markus Bolli / Markus Blass	Corrections of diagrams/supplements
X1.04	07.12.2006	Hügli / Blass	Corrections
V1.10	15.12.2006	Markus Bolli	Revision in light of comments from the review
V1.11	5.9.08	Moor/Zürcher	Incorporation of findings after IBN from NBS and LBL, revision of Chapter "Maintaining the overall safety cases" and "Validation & requirements of validator", critical examination & corrections, review.
V 1.2	09.03.09	M. Kehrli	Revision in light of comments from the review of Version V1.11

V 1.3	08.05.09	M. Kehrli	Revision in light of additional comments, and approval
V 1.4	10.09.2012	M. Kehrli	Interim version
V 1.5	08.07.2013	M. Kehrli	Complete revision taking the following into account: <ul style="list-style-type: none"> <li>- BaRe2.2: RailNAO and RailO 2013</li> <li>- Corr A: Guideline for CCS Authorisation on Corridor A</li> <li>- UNIFE: Testing Strategy</li> <li>- Yet to be addressed revision comments</li> <li>- SM ETCS CH: Master Test concept</li> <li>- SA ETCS L2: SC concept TRK, APS CH</li> <li>- ETCS network: APS CH</li> <li>- ETCS L1LS</li> </ul>
X 2.0	18.7.14	M. Kehrli	Consideration of review comments and revision.
V 2.0	12.10.14	M. Kehrli	Approval of document
V 2.02	12.11.14	M. Kehrli	Minor changes from the QA review of V 2.0.

## Management summary

The present safety case concept provides an overview of the procedures to be followed in order to obtain type approval, authorisation of placing in service (APS) and network access in Switzerland. It also clarifies the roles and responsibilities of the FOT, railway companies and industry in these procedures.

The main section covers presentation of s safety case, which is necessary for ETCS homologation of vehicles or an APS of trackside equipment. In order to achieve safe operation, the safety case must be based on the technical and operational integration of the overall system. The safety case concept describes the structure of safety cases and specifies the requirements that must be met in terms of their structure and content. It also shows the relationships between the safety cases, taking into account the IOP for ETCS vehicles and ETCS lines in Switzerland.

The present version of the safety case concept has been supplemented with the necessary prerequisites to obtain a Swiss-wide ETCS APS for the on-board equipment. In particular, it satisfies corridor 1 requirements in keeping with [6].

## Table of contents

<b>1</b>	<b>Introduction</b>	<b>14</b>
1.1	Purpose of this document	14
1.2	Scope of application	14
1.3	Binding nature of this document	15
1.4	Document structure	15
<b>2</b>	<b>Explanation of roles in railway network</b>	<b>16</b>
2.1	General	16
2.2	Owner	16
2.3	Possessor	16
2.4	Applicant	16
2.5	Vehicle keeper (VK)	16
2.6	Vehicle Operator (VO)	17
2.7	Infrastructure Manager (IM)	17
2.8	Railway infrastructure undertaking (licenced)	17
<b>3</b>	<b>Explanation of the procedure</b>	<b>18</b>
3.1	Homologation	18
3.2	Network access	19
3.3	Other	20
3.4	Overview of homologation, APS and network access	22
<b>4</b>	<b>Structure of the safety cases for the integrated overall system</b>	<b>23</b>
4.1	General	23
4.2	IOP Notes (IX)	24
4.3	IOP Statement (VII)	25
4.4	IOP Certificate Overview (III)	27
4.5	Safety case for vehicle type and line (V)	29
4.6	Safety case for RBC (XII)	31
4.7	Safety case for ETCS L1LS technical components (XIII)	32
4.8	Safety case for technical integration of the signalling and automation system (VIII)	33
4.9	Safety case for technical and operational integration of signalling systems (IV)	34
4.10	Proof of compliance with operational phase requirements set forth in IM safety authorisation (SafeAuth-IM)	35
4.11	Safety case for OBU-EVC (X)	36
4.12	Safety case for integration of OBU in vehicle type (VI)	37
4.13	Safety case for technical and operational integration of vehicle types (II)	38
4.14	Proof of compliance with requirements in the operating phase for the purpose of obtaining a VO safety certificate.	40

4.15	Overall safety case for technical and operational integration of signalling systems and vehicles (I)	41
<b>5</b>	<b>Safety case structure</b>	<b>42</b>
<b>6</b>	<b>Overview table of safety case structure</b>	<b>43</b>
<b>7</b>	<b>Principles of certification</b>	<b>45</b>
7.1	The safety case for technical and operational integration of the entire system as the basis for issuance of an APS for on-board equipment	45
7.2	Difference between certificates and safety case	45
7.3	Validation requirements	45
7.4	Maintaining the safety cases for the integrated overall system	46
7.5	General requirements for the safety assessment	47
7.6	Occurrence of incidents	47
7.7	Tasks and responsibilities	47
<b>8</b>	<b>Annex A</b>	<b>50</b>
8.1	Contact details of railway infrastructure companies (RIUs)	50
8.2	Contact details of System Management ETCS Switzerland	50

## Figures

Figure 1: Document structure	15
Figure 2: Overview of homologation, APS and network access	22
Figure 3: Safety case structure	42

## Abbreviations, terms and definitions

APS	Authorisation of Placing in Service ( <i>Betriebsbewilligung BBW</i> )
BaRe	Railway reform
Ce	Certificate
CENELEC	European Committee for Electrotechnical Standardization
CH	Switzerland
CR	Change Request
CSM	Common Safety Methods
DAT	Design Authority Team
DeBo	Designated body ( <i>beauftragt benannte Stelle BBS</i> ) under [14]
ECM	Entity in Charge of Maintenance
eIXL	Electronic interlocking system
EN	European Standard
ETCS	European Train Control System
EVC	European Vital Computer
FOT	Federal Office of Transport (National Safety Authority in Switzerland)
I	Infrastructure Division (Division of Swiss Federal Railways)
I-AT-ZBF	Organisational unit within SBB's Infrastructure Division responsible for Train control systems
IM	Infrastructure Manager ( <i>Infrastrukturbetreiber, ISB</i> ); the company operating a railway line
IOP	Technical and/or operational interoperability
IP-RailO	Implementing Provisions to the Railways Ordinance
L2 CSR	ETCS Level 2, conventional speed range, $v < 160 \text{ km/h}$
L2 HSR	ETCS Level 2, higher speed range, $160 \text{ km/h} < v < 250 \text{ km/h}$

L1LS	ETCS Level 1 limited supervision
LCM	Lifecycle management
LEU	Lineside electronic unit
Ld	Locomotive driver
NNTR	Notified national technical rules
NoBo	Notified body under [14]
NTR	National technical rules
OBU	On Board Unit
OR	Operating Rules describing the safe handling of systems in operational use.
RailNAO	Rail Network Access Ordinance
RailO	Railways Ordinance
RBC	Radio Block Center
RIU	Railway infrastructure undertaking ( <i>Eisenbahninfrastrukturunternehmung, EIU or infrastrukturunternehmung, IU</i> )
RIXL	Relay interlocking system
RU	Railway Undertaking ( <i>Eisenbahnverkehrsunternehmung</i> ), the company operating a railway vehicle
S&A	Signalling and automation systems
Safe-Auth-IM	Safety authorisation ( <i>Sicherheitsgenehmigung, SiGe</i> ) issued by FOT to the Infrastructure Manager (IM)
SafeCert-VO	Safety certificate ( <i>Sicherheitsbescheinigung, SiBe</i> ) issued by FOT to the Vehicle Operator
SBB	Swiss Federal Railways SBB
SC	Safety case ( <i>Sicherheitsnachweis, SiNa</i> ), produced in accordance with [1] and [2].
SIOP	Safety-related verification or adequate verification of equivalent content (SBB term)
SM ETCS CH	ETCS System Management Switzerland



SPOC	Single Point of Contact
SRAC	Safety Related Application Condition
SRS	System Requirement Specification
TCCS	Train control and command system
Td	Train dispatcher
TET	Test Evaluation Team; body of subject matter experts who assess test cases and test results
TOR	Train operating regulations
TSI	Technical Specification of Interoperability
TVPS	Track vacancy proving system
UNISIG	Union Industry of Signalling
Vc	Vehicle
VK	Vehicle keeper

## Terms and definitions

Anomaly	Arises from 'findings' to which a product fault can be assigned after analysis
Applicant	Natural person or legal entity requesting network access for a vehicle.
Assessment	An opinion issued by an assessment body that meets requirements both in terms of expertise and independence.
Authorisation of Placing in Service	Decree with which the FOT confirms that the vehicle or the components have been adequately checked from both a technical and operational standpoint so that its deployment for a particular purpose under specific conditions of use is possible and that the vehicle is compliant with ETCS TSI requirements – if necessary. If type approval has been given, then the APS will also attest to conformity with the vehicle type.
Change Request	A modified or additional requirement (compared to the original state of requirements at the time the contract was signed).
DAT	Design Authority Team, decision-making body of the SM ETCS CH for questions regarding ETCS system design that need to be answered for application in Switzerland.

Finding	A deviation from the result expected to be found in (here mostly IOP) tests.
Generic	Describes the items that are identical or are present in identical form in each application
Homologation/ type approval	<p>Decree with which the National Safety Authority (in Switzerland, the Federal Office of Transport, FOT) confirms that the object of homologation has been tested to the extent that its use for a particular purpose under particular conditions is possible, and that interoperability – if required – is ensured. For vehicles, the type approval is generally issued at the same time as the authorisation of placing service for the first vehicle in a series.</p> <p>Type approval is intended for vehicles and components thereof (for scope see Appendix 1) that are used multiply in exactly the same way and in the same function (series). Type approval is intended to simplify and accelerate the FOT's testing for the authorisation of placing service procedure (Art. 7 Railways Ordinance).</p>
IM safety authorisation	Issued by the corresponding National Safety Authority (Federal Office of Transport in Switzerland), the IM safety authorisation or SafeAuth-IM ( <i>Sicherheitsgenehmigung, SiGe</i> ) acknowledges that the Infrastructure Manager fulfils the relevant safety requirements, in particular those concerning personnel (operations and maintenance) as well as internal organisation, for a defined line.
Incident	An occurrence whose cause has not yet been clarified
Infrastructure Manager	Any undertaking that operates a railway infrastructure in Switzerland
IOP issue	<p>Within the context of tests aimed at verifying the technical functional compatibility between vehicles and lines (IOP tests), an IOP issue is a discrepancy caused by flaws in the UNSIG specification.</p> <p>Note: product errors that should normally have been identified during product tests are often only detected during IOP tests. Such cases do not constitute IOP issues as such.</p>
Operational IOP tests	Tests based on the integrated technical system consisting of a line and vehicle and the corresponding operating rules (OR). All of these must be verified in order for a railway vehicle to be given ETCS Authorisation of Placing in Service in Switzerland (APS ETCS CH).
Odometry	The science of determining the location (direction/velocity) of a vehicle.
Overall system	Technical and operational interaction of vehicles and trackside equipment using ETCS.
Owner	Natural or legal person who has an object at their disposal, on a legal basis.
Possessor	Generally speaking: natural or legal person, who controls an object (actual physical control that the person has over the given object), regardless of the person's legal relationship to this object.

Railway infrastructure undertaking	A registered company to which a given portion of railway infrastructure has been assigned. In particular, an RIU is responsible for managing the life cycle of trackside systems.
Subset	Here a summary of CR according to UNISIG. Generally a thematic summary of requirements
Subsystem	On-board or trackside ETCS equipment.
System	Vehicle or trackside signalling system
System management ETCS	Body deployed by National Safety Authority (in Switzerland, the Federal Office of Transport, FOT) to ensure and enforce ETCS interoperability.
Validation	Testing to verify compliance with requirements observed in previous phases of the V model.
Vehicle Keeper (VK)	Natural or legal person who is responsible for the homologation, Authorisation of Placing in Service (APS) and functioning of a vehicle. The VK is generally an RU or a vehicle leasing company.
Vehicle Operator (VO)	A railway undertaking that operates a transport or infrastructure vehicle on the Swiss railway network
Vehicle type	Vehicle-side properties that are assigned not only to the individual instance (i.e. a given vehicle with vehicle number xy) but are identical in vehicles of the same construction.
VO safety certificate	The VO safety certificate or SafeCert-VO ( <i>Sicherheitsbescheinigung SiBe</i> ) acknowledges that the Vehicle Operator (network user) fulfils the relevant safety requirements, in particular those concerning staff and rolling stock deployed, as well as internal organisation, for a particular transport on a defined line.

## References

- [1] CENELEC: EN 50126, Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).
- [2] CENELEC: EN 50129, Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling.
- [3] ERA: COMMISSION DECISION of 25 January 2012 on the technical specification for interoperability relating to the control-command and signalling subsystems of the trans-European rail system (notified under document C(2012) 172) (2012/88/EU).
- [4] EU: COMMISSION REGULATION (EU) No. 1169/2010 of 10 December 2010 on a common safety method for assessing conformity with the requirements for obtaining a railway safety authorisation, 11 December 2010.
- [5] EU: COMMISSION REGULATION (EU) No. 445/2011 of 10 May 2011 on a system of certification of entities in charge of maintenance for freight wagons and amending Regulation (EC) No 653/2007.
- [6] Rail freight corridor 1 NSA working group: Guideline for CCS Authorisation on rail freight corridor 1, Version 1.0, 13/12/2013.
- [7] UNISIG: Framework Agreement European Lab, January 2014.
- [8] CH: 742.141.1 Ordinance of 23 November 1983 on the Construction and Operation of the Railways (Railways Ordinance, RailO) (status on 1 July 2013).
- [9] CH: 742.122 Rail Network Access Ordinance of 25 November 1998 (RailNAO) (status on 1 July 2013).
- [10] CH: 742.170 Federal Office of Transport Regulations of 1 November 2000 on the Issuance of Rail Service and Operational Regulations for Railways (RailRO) (status on 20 February 2001).
- [11] FOT: Guidelines set forth in Art. 6a, 7 and 8 of the Ordinance of 23 November 1983 on the Construction and Operation of the Railways (Railways Ordinance, RailO) (status on 1 July 2013).
- [12] FOT: Guidelines on type approval for elements of railway systems; modules, components and systems relating to civil engineering, railway tracks, electrical equipment and safety engineering, Version V 2.0, 1.9.2014.
- [13] Guidelines on homologation of railway vehicles (type approval/APS), Version V2.2, 1.1.2014.
- [14] FOT: Guidelines on independent railway testing authority (RL UP-EB). Use of independent railway testing authority for conformity and safety assessments in railway authorisation procedures, Version V 1.0, 1.7.13.
- [15] FOT: Guidelines on issuance of licences for network access, VO safety certificates (*Sicherheitsbescheinigung, SiBe*) and IM safety authorisations (*Sicherheitsgenehmigung, SiGe*), Version V 1.0, 1.7.13.
- [16] FOT: Guidelines on issuance of licences for network access and VO safety certificates (*Sicherheitsbescheinigung, SiBe*), Version 3.3.1, 01.09.2010.
- [17] SF/FOT: Prerequisites for the use of vehicles on ETCS lines, Annex 12.

- [18] SM ETCS CH: Master Test Concept for Issuance of an ETCS APS.
- [19] SM ETCS CH: Release Note for Baseline ETCS CH  
→ <http://www.bav.admin.ch/grundlagen/03708/03819/03821/index.html?lang=de>  
contact address SM ETCS CH: see Annex A.
- [20] SM ETCS CH: Requirements for validation of ETCS braking curves
- [21] SM ETCS CH: Handbook on Issuance of Safety case II, in progress.
- [22] SM ETCS CH: Safety Plan Safety Case V ETCS lines CH.

## Figures

Fig. 1 Document structure

Fig. 2 Overview of homologation, APS and network access

Fig. 3 Structure of safety case

# 1 Introduction

## 1.1 Purpose of this document

- 1.1.1.1 This document describes on a generic level the certificates, safety cases, safety assessments with their mutual dependencies and the involved processes to achieve access to ETCS equipped lines for ETCS equipped vehicles in Switzerland:
- 1.1.1.1.1 The structure of the individual parts of the safety case in their mutual dependency (document A is prerequisite for document B,
- 1.1.1.1.2 The structure of the individual parts of the safety case in terms of reusability of existing and to be created safety cases, based on the conclusions from subordinate safety cases,
- 1.1.1.1.3 Demonstrating processing sequences or parallels in the drawing up of safety cases, to enable a targeted and efficient formulation of the safety case for the integrated overall system,
- 1.1.1.1.4 Allocation of contents and responsibilities to the individual safety cases with regard to the roles 'Supplier', 'Applicant', 'Vehicle Keeper (VK)', 'Vehicle Operator (VO)', 'Railway Infrastructure Undertaking (RIU)' and 'Infrastructure Manager (IM)',
- 1.1.1.1.5 Allocation of contents and responsibilities to the individual safety cases with regard to systems vehicles and line, and to interoperability.

## 1.2 Scope of application

### 1.2.1 General

- 1.2.1.1 The present safety case concept applies to all ETCS signalling and automation systems, i.e. higher speed range (HSR, L2), conventional speed range (CSR, L2) and L1LS as well as ETCS-equipped vehicles travelling on ETCS-equipped lines.

### 1.2.2 ETCS L2 CSR/HSR

- 1.2.2.1 The present safety case concept applies to CSR and HSR speed ranges and is applicable to both.

### 1.2.3 ETCS L1LS

- 1.2.3.1 Aspects of ETCS L1LS affecting IOP documentation

IOP Notes (IX) → Listing of implemented CRs or SW version of the OBU

IOP Statement (VII) → L1LS must be taken into account in IOP test campaigns

IOP Certificates Overview (III) → certification that a sufficient number of tests have been carried out to confirm IOP,

and safety cases

Safety Case (XIII) for technical integration of signalling and automation system → safety case dealing with technical components such as balises, LEU, loop

Safety Case (VIII) for technical integration of signalling and automation system → Integration of L1LS-components in signalling and automation equipment, including design

Safety Case (IV) for technical and operational integration of signalling systems → operational and technical aspects of ETCS L1LS

Safety Case (V) for vehicle type and line → assessment of conducted network access tests.

- 1.2.3.2 Since ETCS L1LS is a background monitoring system, safety case (I) does not continue with L1LS.

1.2.3.3 With regards to on-board equipment, there are no other aspects to be considered than ensuring that functionality in the OBU is included and that the relevant network access tests have been carried out.

1.2.3.4 The transitions L1LS  $\leftrightarrow$  L2 must be taken into account for safety cases concerning ETCS L2.

## 1.2.4 Vehicles

1.2.4.1 The present safety case concept applies to all ETCS-equipped vehicles, regardless of whether these vehicles are also equipped with other train control systems.

## 1.3 Binding nature of this document

1.3.1.1 Strictly speaking, the present safety case concept serves as SM ETCS CH specifications and is linked to superordinate specifications through [17].

## 1.4 Document structure

1.4.1.1 The relationship between the present safety case concept, the master test concept in accordance with [18] and test specifications, e.g. the network access test, is shown in Fig. 1 below.

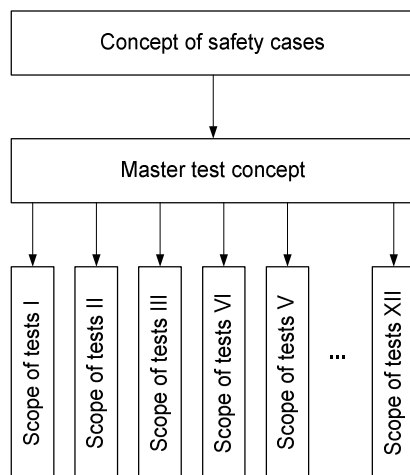


Figure 1: Document structure

## 2 Explanation of roles in railway network

### 2.1 General

- 2.1.1.1 The safety relevance of fitting vehicles with ETCS and their use, such as for international operation, make it necessary to clarify the roles of Owner, Possessor, Applicant, Vehicle Keeper (VK) and Vehicle Operator (VO).

### 2.2 Owner

- 2.2.1.1 An owner is a natural or legal person who has a vehicle or line at his or her disposal. This status is only of secondary importance when it comes to obtaining an APS for a railway vehicle or trackside subsystem.

### 2.3 Possessor

- 2.3.1.1 A possessor is a natural or legal person with actually physical control over a vehicle or trackside subsystem. This role is not suitable for obtaining an APS for a vehicle, since both the applicant as well as the Vehicle Keeper and Vehicle Operator may actually be the owner of the vehicle and therefore no clear tasks can be assigned.

### 2.4 Applicant

- 2.4.1.1 An applicant is a natural person or legal entity that applies for homologation of a railway vehicle.
- 2.4.1.2 Typically, on-board equipment suppliers are in the role of the Applicant, since new vehicles are procured on a turnkey basis, i.e. including APS. When equipping existing or end-of-life vehicles with ETCS train control equipment, the Vehicle Keeper (VK) is typically in the role of the Applicant.
- 2.4.1.3 With regard to homologation for vehicles, the Applicant is required to obtain the appropriate safety cases and safety assessments for each level.

### 2.5 Vehicle keeper (VK)

- 2.5.1.1 A Vehicle Keeper (VK) is in particular responsible for the homologation, APS and operating capability of a vehicle. This means that the VK is also responsible for ensuring that safety case II (incl. compliance with SRACs) and the corresponding safety assessment are up to date.
- 2.5.1.2 The VK is responsible for ensuring that its vehicles are in safe operating state. It also informs FOT when its vehicles have been inscribed in the register of rolling stock. The VK is responsible for the content of safety case II.
- 2.5.1.3 The VK is responsible for vehicle maintenance.
- 2.5.1.4 A VK may be an RU, a rolling stock leasing company or a vehicle supplier.



## 2.6 Vehicle Operator (VO)

- 2.6.1.1 A Vehicle Operator (VO) is a railway undertaking (RU), which is inscribed in the Swiss trade register within the meaning of Art. 8 of the Rail Network Access Ordinance and which operates a vehicle in Switzerland. Such RUs are referred to hereinafter as Vehicle Operators or VOs.
- 2.6.1.2 VOs are responsible for ensuring safe transport, in particular by managing vehicles, vehicle runs (location of vehicle, allocation of locomotive drivers, etc.), training locomotive drivers and adhering to operating rules (OR).
- 2.6.1.3 A VO may be a VK itself or operate vehicles of other VKs.
- 2.6.1.4 In order for an RU to run trains on the network of a foreign railway infrastructure undertaking (RIU) there must be an arrangement for access (between the RU and RIU), a licence for network access, and a SafeCert-VO (from the FOT to the RU). An APS of the on-board subsystem of the vehicle is a prerequisite for this.

## 2.7 Infrastructure Manager (IM)

- 2.7.1.1 An Infrastructure Manager (IM) is a railway infrastructure undertaking (RIU) that carries out its activities in Switzerland.
- 2.7.1.2 The IM is responsible for ensuring safe operation of a railway line.
- 2.7.1.3 If an IM manages a line on behalf of another RIU, this must be formalised in an operating agreement.
- 2.7.1.4 Line maintenance may be carried out by the IM but this does not always have to be the case.

## 2.8 Railway infrastructure undertaking (licenced)

- 2.8.1.1 The licenced railway infrastructure undertaking (RIU) is to be understood as complementary to the VK. It is responsible for lifecycle management and operation of equipment.
- 2.8.1.2 Equipment operation is understood to mean the aspects of construction, planning, design, installation and assembly, testing and commissioning of equipment as well as their monitoring over the entire life cycle. The handling of these aspects is a prerequisite for an APS to be issued and for the equipment to be put into operation (by the IM). The RIU may also be IM at the same time, but this does not always have to be the case.
- 2.8.1.3 The RIU is responsible for maintenance. The RIU may either perform maintenance directly or delegate this task to the IM or to a third party.

## 3 Explanation of the procedure

### 3.1 Homologation

#### 3.1.1 Type approval for on-board components

- 3.1.1.1 According to Art. 7 [8], type approval for vehicles and on-board components is a decree in which the FOT confirms to the vehicle supplier that the vehicle or the component have been adequately checked technically so that its deployment for a particular purpose under particular conditions is possible and that interoperability – if required – is ensured.

#### 3.1.2 APS for on-board equipment

- 3.1.2.1 Decree in which the FOT confirms to the VK that the vehicle or the component have been adequately checked technically so that its deployment for a particular purpose under particular conditions is possible and that interoperability – if required – is ensured. If type approval is given, then the APS also states compliance with the system to which the type approval refers.
- 3.1.2.2 Basically, the aim is to issue an APS that includes all ETCS applications in Switzerland. In other words, for a given vehicle type, the safety case and IOP certificates are to be produced not for specific lines, but rather for all aspects of Swiss-wide ETCS applications.
- 3.1.2.3 The APS shall clearly state which requirements (conditions) are included in the SafeCert-VO (*Sicherheitsbescheinigung, SiBe*) and must be implemented by the VO.
- 3.1.2.4 The APS is based on the safety case (I), (II) and (V) and their safety assessment. For new vehicles, aspects from the safety case (II) can be integrated into the safety case (VI) (aspects concerning maintenance and operation of the vehicle should only be passed on in the form of maintenance and operating manuals).

#### 3.1.3 Type approval for trackside components

- 3.1.3.1 According to Art. 7 [8], type approval for trackside components is a decree in which the FOT confirms to the trackside supplier that trackside equipment has been adequately checked technically so that its deployment for a particular purpose under particular conditions is possible and that interoperability – if required – is ensured. As a rule, for a type approval there is also a commercial interest to operate the type-approved system in different forms and within different applications.
- 3.1.3.1.1 An applicant, in particular a railway infrastructure undertaking, may apply for a type approval for aspects of equipment operation such as specifications for construction, planning, design work, installation and assembly, testing and commissioning of equipment.

#### 3.1.4 APS for trackside equipment

- 3.1.4.1 The Authorisation of Placing in Service of trackside equipment is a decree in which the FOT confirms to the railway infrastructure undertaking that trackside equipment has been adequately checked technically so that its deployment for a particular purpose under particular conditions is possible and that interoperability – if required – is ensured.

- 3.1.4.2 This instruction is based on the safety case (IV) and (I) as well as their safety assessments.

## 3.2 Network access

### 3.2.1 General

- 3.2.1.1 According to [9], an RU must undergo the procedures to obtain a licence for network access, a SafeCert-VO (*Sicherheitsbescheinigung, SiBe*) and an arrangement for access before vehicles can operate on a given line. Further helpful information can be found in [15] on page 12.

### 3.2.2 VO safety certificate (SafeCert-VO)

- 3.2.2.1 The SafeCert-VO (*Sicherheitsbescheinigung, SiBe*) under [9] and [15] is issued to the Vehicle Operator by the FOT.
- 3.2.2.2 The SafeCert-VO (*Sicherheitsbescheinigung, SiBe*) acknowledges that the RU fulfils the relevant safety requirements, in particular those concerning personnel and rolling stock deployed, as well as internal organisation, for a particular transport on a defined line.
- 3.2.2.3 This document certifies that
- 3.2.2.3.1 • only rolling stock suitable for the technical conditions of the line are deployed
  - 3.2.2.3.2 • only personnel who are adequately qualified for operations are deployed
  - 3.2.2.3.3 • the basic principles and rules for safe transport are adhered to.
- 3.2.2.4 The FOT must issue an APS for the vehicle to the VK before the SafeCert-VO (*Sicherheitsbescheinigung, SiBe*) may be issued to the RU. Railway vehicles will only be included in a SafeCert-VO when the FOT has issued the corresponding APS. The SafeCert-VO must indicate that compliance with the SRACs set forth in the APS have been verified.
- 3.2.2.5 According to [9], the SafeCert-VO (*Sicherheitsbescheinigung, SiBe*) is valid for no more than 5 years.

### 3.2.3 Licence for network access

- 3.2.3.1 The licence for network access according to [9] and [15] is a decree issued by the FOT to the railway undertaking.
- 3.2.3.2 With a licence for network access, the RU basically receives the right to claim network access. The authorisation shows that the RU meets the basic requirements for access to the network in terms of reliability, financial capacity and qualification of the personnel. The licence for network access is designed in such a way that the licences can be recognised between different countries in international traffic. The licence for network access remains valid for a maximum of 10 years; it can then be renewed upon request.

### 3.2.4 Arrangement for access

- 3.2.4.1 The arrangement for access under [9] and [15] is a private-law contract between the RIU and the RU. It is based on the RIU's Network Statement.

- 3.2.4.2 The arrangement for access regulates, in particular, operating aspects such as train paths (quality, price), operative interfaces, and channels of communication for the exchange of information.

### **3.2.5 IM safety authorisation (SafeAuth-IM)**

- 3.2.5.1 The SafeAuth-IM (*Sicherheitsgenehmigung, SiGe*) is issued by the FOT to the Infrastructure Manager (IM).
- 3.2.5.2 The SafeAuth-IM is recognition that the IM fulfils the relevant safety requirements, in particular those concerning staff and trackside equipment deployed, and those concerning internal organisation, to ensure safe operation of the infrastructure facilities.
- 3.2.5.3 This document certifies that
- 3.2.5.3.1 • only systems that are suitable for the technical conditions are deployed
  - 3.2.5.3.2 • only staff who are adequately qualified for operations are deployed
- 3.2.5.4 Before the SafeAuth-IM (*Sicherheitsgenehmigung, SiGe*) can be obtained, an APS must be issued to the IM either by the FOT itself or by the RIU (i.e. FOT delegates issuance of the APS). Trackside equipment will only be included in a SafeAuth-IM when the FOT has issued the corresponding APS. The SafeAuth-IM must indicate that compliance with the requirements and conditions set forth in the APS have been verified.
- 3.2.5.5 According to [9], the SafeAuth-IM is valid for three to five timetable periods.

## **3.3 Other**

### **3.3.1 Lease agreement**

- 3.3.1.1 The lease agreement is a private-law contract between the VK and the RU.
- 3.3.1.2 In particular, it regulates operational aspects such as operative interfaces, applicable regulations, communication channels for the mutual exchange of information.

### **3.3.2 Operating agreement**

- 3.3.2.1 The operating agreement is a private-law contract between the RIU and the IM.
- 3.3.2.2 In particular, it regulates operational aspects such as management of operations, operative interfaces, applicable regulations, communication channels for the mutual exchange of information.
- 3.3.2.3 This applies to both standard cases and exceptional situations (fault and emergency management)

### **3.3.3 Register of rolling stock**

- 3.3.3.1 According to [8] Art. 5i<sup>36</sup>, VK must provide the vehicle data declared mandatory in no. 1 of the Annex to the Commission Decision 2011/107/EU<sup>37</sup> in the register of rolling stock within the meaning of Article 17a of the Railways Act (RailA).

### **3.3.4 Register of infrastructure**

- 3.3.4.1 According to [8] Art. 15f, RIUs must provide the information required for network access in the register of infrastructure.

### 3.3.5 Remarks

- 3.3.5.1 Homologation procedures are not addressed further in this document, as they are fully covered by [12] and [13].
- 3.3.5.2 The network access procedure is covered in [16] and is also not addressed in this document.
- 3.3.5.3 In particular, the presentation of safety case to obtain an APS of ETCS-equipped trackside and on-board subsystems is dealt with in the following. The APS is a prerequisite for issuance of the SafeCert-VO (*Sicherheitsbescheinigung, SiBe*) or SafeAuth-IM (*Sicherheitsgenehmigung, SiGe*).

### 3.4 Overview of homologation, APS and network access

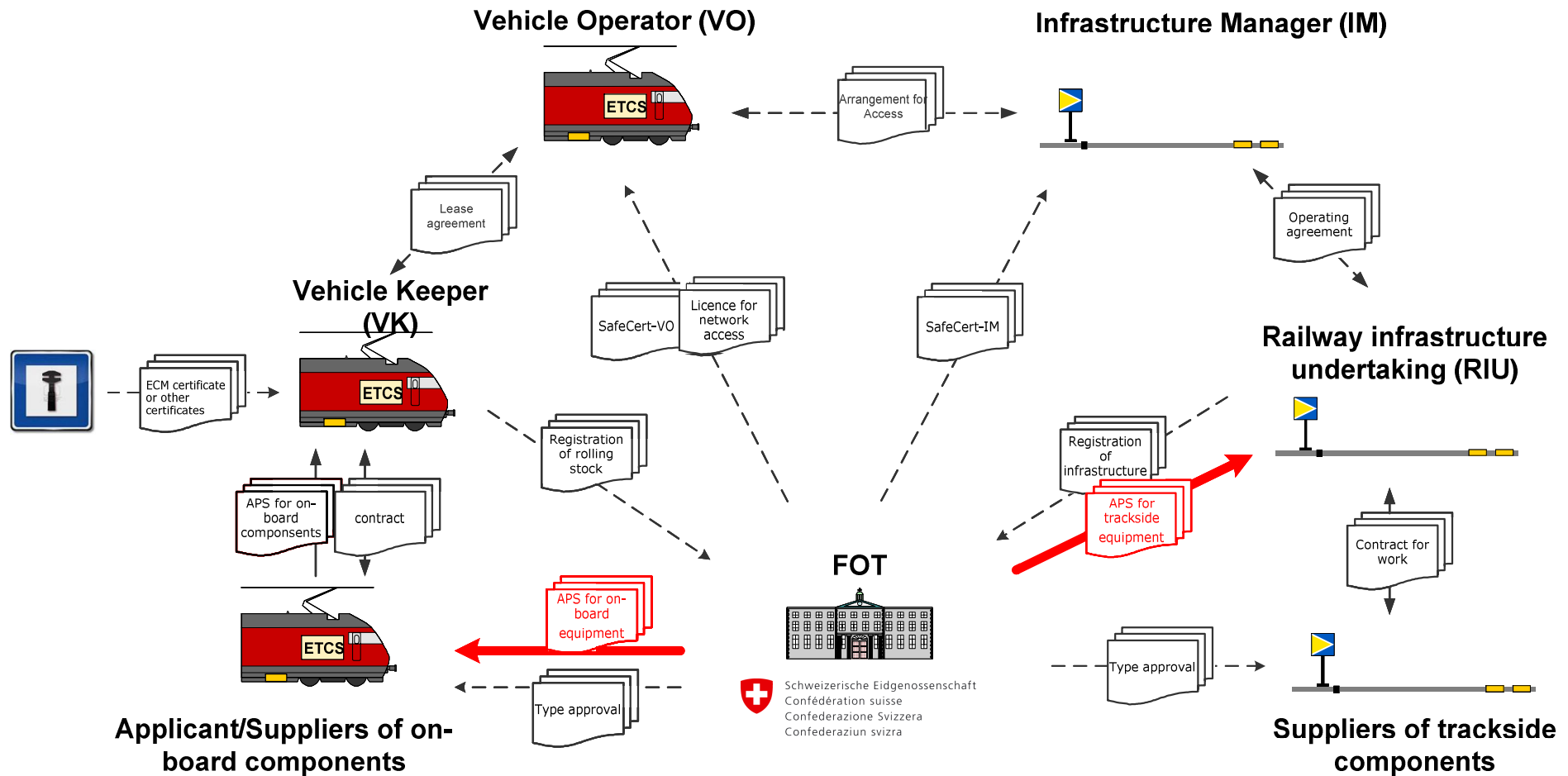


Figure 2: Overview of homologation, APS and network access

## **4 Structure of the safety cases for the integrated overall system**

### **4.1 General**

- 4.1.1.1 Since the structure of the safety case for the integrated overall system builds on conclusions from subordinate safety cases, the generic safety cases that lie lower in the safety case hierarchy will be considered first.
- 4.1.1.2 The parts of the safety case that a supplier must provide as part of a delivery contract are described only insofar as they concern interoperability considerations towards certification.
- 4.1.1.3 The following considerations refer to Figure 3 and the associated Table according to Chapter 6.

## **4.2 IOP Notes (IX)**

### **4.2.1 Overview**

- 4.2.1.1 IOP Notes (IX) provide an overview of the status of the software version and the CR implementations on the part of OBU.

### **4.2.2 Content**

- 4.2.2.1 The IOP Notes (IX) include the following in particular:
  - 4.2.2.1.1 Information about the implemented Technical Specification of Interoperability (TSI) baseline and its version, the NNTR as well as a list of CRs implemented in the OBU.
  - 4.2.2.1.2 Reference of standard documents for the DMI
  - 4.2.2.1.3 The version of Subset 91 'Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2'
  - 4.2.2.1.4 Any deviations from the specifications as well as confirmation that these deviations do not result in any impairment to trackside equipment or the vehicle.
- 4.2.2.2 With the IOP Notes, the OBU supplier confirms compliance with the TSI-relevant System Requirement Specification (SRS) as well as with the SM's specifications [19] for technical interoperability on all Swiss ETCS implementations (L1LS, L2 CSR, L2 HSR).
- 4.2.2.3 The IOP Notes (IX) constitute generic certification on the part of the OBU supplier that the ETCS status, the implementation of subsets and versions, and the parameterisation correspond to the values specified by the SM.
- 4.2.2.4 Operational aspects of railway operations are only taken into account in generic technical interoperability insofar as they form the basis for the selection of implemented functionalities in consultation with suppliers.
- 4.2.2.5 The IOP Notes may be drafted with the OBU Release Note.

### **4.2.3 Requirements passed on to the IOP Statement (VII)**

- 4.2.3.1 Compared to the IOP Statement (VII), the IOP Notes (IX) cover areas that cannot be proven by fulfilment of technical requirements (country-specific characteristics) in the product's technical specifications (additional requirements, restrictions, etc.).
- 4.2.3.2 Compared to the IOP Statement (VII), the IOP Notes (IX) also cover any deviations from the specifications and include confirmation that these additional implementations do not result in any impairments to trackside equipment or the vehicle.
- 4.2.3.3 Once the supplier of trackside equipment has completed IOP laboratory tests, the IOP Notes (IX) will be updated and a closing statement will be added to the final remarks of the IOP Statement (VII). Thus, the IOP Statement (VII) should contain a common view shared by the RBC/L1LS supplier and the OBU supplier.

### **4.2.4 Responsibility**

- 4.2.4.1 The OBU supplier is responsible for the IOP Notes (IX). Cooperation between individual UNISIG companies is addressed in [7].



## 4.3 IOP Statement (VII)

### 4.3.1 Overview

4.3.1.1 The IOP Statement (VII) is a summary of the IOP testing activities.

### 4.3.2 Content

4.3.2.1 The IOP Statement (VII) is a summary of the IOP testing activities and includes the following:

4.3.2.1.1 List of interoperable SW versions of OBUs and RBCs considered in the IOP testing activities as well as L1LS implementations.

4.3.2.1.2 Statement of compliance with technical SRACs between OBUs and RBCs.

4.3.2.2 It is a written certificate from the trackside supplier.

4.3.2.3 It differs from generic technical interoperability (i.e. no regard given to specific implementation) in that the investigations have been carried out in an 'application-specific' environment. This means that the laboratory tests (and possibly also tests on site) were carried out in an integrated state, with as many of the involved components and corresponding subsystems as possible in a 'final' state, i.e. one that corresponds to a future reality. The IOP Statement (VII) states:

4.3.2.3.1 how the test cases were constructed (requirements)

4.3.2.3.2 how the test cases were performed (test scenarios)

4.3.2.3.3 what the test results were (test protocols)

4.3.2.3.4 how the findings (discrepancy, anomaly, IOP Issue, CRs) have been handled

4.3.2.3.5 and it gives an evaluation of the individual test results, and an overall evaluation.

4.3.2.4 The IOP-statement (VII) certifies that there is sufficient technical interoperability of the OBU with trackside subsystems (RBC or L1LS) based on theoretical considerations, laboratory experiments, and practical experience on the line that includes operational as well as basic findings from signalling technology and testing methodology.

4.3.2.5 The certificate says nothing about the implementation of TSI and SRS in the components used, and thus nothing about the safety of these components either.

4.3.2.6 The form of presentation may be chosen freely. The IOP Statement also contains the RBC supplier's certificate or the L1LS equipment certificate, which shows the state of the ETCS, the implementation of subsets and versions, and the parameterisation of the values prescribed by ETCS System Management, as indicated in the IOP Notes (IX).

### 4.3.3 Requirements incorporated from (IX)

4.3.3.1 See 4.2.3.

### 4.3.4 Requirements passed on to (X), (XII) and (III)

4.3.4.1 Requirements for safety case (X) (OBU), safety case (XII) (RBC) and safety case (XIII) (L1LS) in terms of faults found that need to be processed.

4.3.4.2 Listing of all discrepancies that have been revealed by the IOP tests. This list is passed on to the IOP Certificate Overview (III).

### 4.3.5 Omitting the IOP Statement (VII)

- 4.3.5.1 At the discretion of the RIU, the IOP Statement (VII) can be omitted for a system that has already been introduced if the IOP Statement does not have to be modified as the result of an impact analysis. The justification for this omission must be given in safety case (III).

#### **4.3.6 Responsibility**

- 4.3.6.1 The supplier of trackside equipment supplier is responsible for the IOP Statement (VII). Cooperation between the individual UNISIG companies is addressed in [7].

## 4.4 IOP Certificate Overview (III)

### 4.4.1 Overview

- 4.4.1.1 The 'IOP Certificate Overview' (III) provides a summary of all homologations of OBU / RBC or OBU / L1LS combinations for which an IOP must be shown.

### 4.4.2 Content

- 4.4.2.1 In particular, the 'IOP Certificate Overview (III)' contains the following
- 4.4.2.1.1 A summary assessment of the technical IOP activities under VII,
  - 4.4.2.1.2 the listing of the interoperable OBU/RBC or L1LS combinations and
  - 4.4.2.1.3 Lists possible unresolved points from VII and evaluates their safety relevance.
- 4.4.2.2 describes procedures for the handling of IOP findings, quality management and influences on operational and organisational interoperability.
- 4.4.2.3 The structure of the 'IOP Certificate Overview (III)' is based on Standard EN 50129, but it remains a certificate without final treatment of safety-related topics.
- 4.4.2.4 All IOP discrepancies are documented. The 'IOP Certificate Overview (III)' shows where and how further treatment is envisaged. Particular weight is given to possible safety-related discrepancies that would lead to further requirements being posed. Assessment of whether an IOP discrepancy is relevant to safety is made by evaluating the OBU, RBC or L1LS components. Accordingly, the safety-related points from certificate (III) are exported to safety case (V); or IOP Certificate Overview (III) lists the safety-related points that have been exported to safety cases (X), (XII) or (XIII).
- 4.4.2.5 The following independent topics are explained further below:
- 4.4.2.5.1 'Reporting of anomalies': how faults (discrepancies) were discovered, how triage was carried out (OBU supplier, TRK supplier, RIU, SM (System design ETCS CH)), how anomalies were evaluated and treated (DAT/TET), and the consequences for the projects.
  - 4.4.2.5.2 'Technical and operational conditions', resulting from error handling, ...
    - ... in terms of the topics that were not implemented (not relevant and/or not implemented by UNISIG and/or not yet determined)
    - ... in terms of the topics that should be entered into the subsystems at a later date.
- 4.4.2.6 The details of the implementation of anomalies in the associated IOP lists are not final, and are subject to correction. Decisions on processing the anomalies are the responsibility of the trackside and vehicle suppliers, or RIU and VK, and must thus be given in their certificates.

### 4.4.3 Requirements incorporated from (VII)

- 4.4.3.1 See 4.3.4.
- 4.4.3.2 If the IOP Statement (VII) is omitted, the results according to 4.2.3 must be included.

### 4.4.4 Requirements passed on to (V)

- 4.4.4.1 The IOP Certificate Overview (III) shows:
- 4.4.4.1.1 Discrepancies that require particular, non-technical error handling, where not handled by safety cases (XII) and (X) according to Fig. 3. In general this error handling leads to additional operating rules, rules and regulations.

#### **4.4.5 Responsibility**

4.4.5.1 System Management ETCS CH is responsible for the IOP Certificate Overview.

## **4.5 Safety case for vehicle type and line (V)**

### **4.5.1 Overview**

- 4.5.1.1 The safety case for vehicle type and line (V) certifies the safe interaction between the vehicle type and track-side implementations.
- 4.5.1.2 General specifications for the content of the safety case (V) are given in [22]. Here only a rough overview is provided.

### **4.5.2 Content**

- 4.5.2.1 The 'Safety case for vehicle type and line (V)' for each line should be understood as a summary of statements on all the safety- or availability-relevant elements resulting from the interplay of vehicle and line that should also be considered as new topics for the 'Safety case for technical and operational integration of vehicle type(s) (II)' or the 'Safety case for technical and operational integration of signalling systems (IV)', and which result from:
  - 4.5.2.1.1 the review of all existing trackside risk analyses and the measures derived therefrom with relevance to the vehicle types in question,
  - 4.5.2.1.2 the review of all existing vehicle-side risk analyses and the measures derived therefrom with relevance to the line in question,
  - 4.5.2.1.3 the review of all existing trackside faults and the measures derived therefrom with relevance to the vehicle types in question,
  - 4.5.2.1.4 the review of all existing vehicle-side faults and the measures derived therefrom with relevance to the line in question,
  - 4.5.2.1.5 the SRACs of the line exported to the vehicle, if they have not been incorporated as requirements of OBU design, or as network access requirements,
  - 4.5.2.1.6 the SRACs of the vehicle to the line, if they have not been incorporated as requirements of the design of trackside safety systems,
  - 4.5.2.1.7 the operational rules or otherwise derived regulations for operation (L2 and L1LS) and, if necessary, maintenance of vehicles, if they have not been incorporated as requirements into the layout of the OBU, and
  - 4.5.2.1.8 the operational rules or otherwise derived regulations for operation and, if necessary, maintenance of the line, if they have not been incorporated as requirements of the RBC design.
- 4.5.2.2 The safety case V certifies that operational, organisational interoperability has been sufficiently tested for the vehicle types, through theoretical considerations, and if necessary tests in the laboratory and on site.

### **4.5.3 Need for new network access tests**

- 4.5.3.1 Under certain circumstances, certification may result in the need for further network access tests, which must be specified in more detail in the safety case (V).
- 4.5.3.2 The licensed RIU is responsible for deciding whether new network access tests are needed. This decision is based on available impact analyses and consideration of possible effects on the availability and safety of railway operations.

### **4.5.4 Requirements incorporated from (II), (III) and (IV)**

- 4.5.4.1 See 4.4.4, 4.9.4, and 4.13.4.

**4.5.5 Requirements passed on to (I)**

- 4.5.5.1 Notes to (I) on special features of the safety case for a particular vehicle type or the specific line.

**4.5.6 Responsibility**

- 4.5.6.1 The RIU prepares safety case (V) at the request of the VK.

## **4.6 Safety case for RBC (XII)**

### **4.6.1 Overview**

4.6.1.1 The Safety Case for RBC (XII) attests to the technical safety of the RBC.

### **4.6.2 Content**

4.6.2.1 The safety case for RBC (XII) attests to the technical safety of the generic RBC product.

4.6.2.2 The present document makes no further statements on the content, as this is prescribed by [2].

### **4.6.3 Requirements incorporated from (VII)**

4.6.3.1 See 4.3.4.

### **4.6.4 Requirements passed on to (VIII)**

4.6.4.1 SRACs exported to neighbouring systems, such as IXLs, other RBC's, and TCCS, are passed on to the corresponding safety cases.

4.6.4.2 In addition, any SRACs concerning integration in the trackside subsystem is exported to safety case (VIII).

### **4.6.5 Responsibility**

4.6.5.1 The RBC supplier is responsible for the safety case.

## **4.7 Safety case for ETCS L1LS technical components (XIII)**

### **4.7.1 Overview**

- 4.7.1.1 The 'Safety case for ETCS L1LS technical components' certifies the technical safety of components required for ETCS L1LS.

### **4.7.2 Content**

- 4.7.2.1 The Safety case for ETCS L1LS components certifies technical safety of generic balise and LEU products.
- 4.7.2.2 This document does not make any further statements on the content than those found in [2].

### **4.7.3 Requirements incorporated from (VII)**

- 4.7.3.1 See 4.3.4.

### **4.7.4 Requirements passed on to (VIII)**

- 4.7.4.1 SRACs to neighbouring systems such as signal boxes in particular are passed on to the corresponding safety cases of these systems.
- 4.7.4.2 In addition, any SRACs relating to integration into the trackside subsystem are passed on to safety case (VIII).

### **4.7.5 Responsibility**

- 4.7.5.1 The supplier of ETCS L1LS components is responsible for safety case (XIII).



## **4.8 Safety case for technical integration of the signalling and automation system (VIII)**

### **4.8.1 Overview**

- 4.8.1.1 Safety case for technical integration of the signalling and automation system (VIII) certifies that signalling systems have been safely integrated and that the design work has been properly carried out.

### **4.8.2 Content**

- 4.8.2.1 This safety case is based on the subordinate safety cases that were complied with for the following points:
    - 4.8.2.1.1 Absence of reaction of individual products
    - 4.8.2.1.2 Correct integration of individual interfaces
    - 4.8.2.1.3 Compliance of balise telegrams with the specification, position, labelling
    - 4.8.2.1.4 Correctness of system design work and design rules
    - 4.8.2.1.5 Compliance with SRACs of the individual products
    - 4.8.2.1.6 Correctness of operating and maintenance manual.
  - 4.8.2.2 This safety case is based on the subordinate safety cases of trackside systems such as in particular the RBC, signal boxes, train control and command system (TCCS), balises, and L1LS components. It certifies the safety of the integrated technical system.
  - 4.8.2.3 The present document makes no further statements on the content, as this is prescribed by [2].
- ### **4.8.3 Requirements incorporated from (XII) and (XIII)**
- 4.8.3.1 SRACs exported from subordinate safety cases, in particular those concerning the RBC, IXL and TCCS, balises and L1LS components are treated on a technical level.
- ### **4.8.4 Requirements passed on to (IV)**
- 4.8.4.1 SRACs that need to be processed operationally, and which cannot be processed technically, are exported to the higher-level operational safety case.
  - 4.8.4.2 However, it should be noted that the SRACs relating to undeveloped products or technical errors may only be passed on temporarily and in consultation with the RIU.
- ### **4.8.5 Responsibility**
- 4.8.5.1 The corresponding integrator is responsible for the safety case for the technical integration of the signalling and automation system (VIII).

## **4.9 Safety case for technical and operational integration of signalling systems (IV)**

### **4.9.1 Overview**

- 4.9.1.1 The 'safety case for technical and operational integration of signalling systems (IV)' makes statements on all safety-related points of trackside safety systems.

### **4.9.2 Content**

- 4.9.2.1 Safety case IV is concerned with the following:

4.9.2.1.1 Compliance with SRACs

4.9.2.1.2 Implementation of operations concept

- 4.9.2.2 This safety case makes a final statement on the safety-relevant aspects of the technically and operationally integrated safety systems.

4.9.2.3 This safety case deals with signalling systems and certifies that the original safety requirements have been met. Interoperability of the signalling and automation system mainly depends on the RBC type or on L1LS implementation.

4.9.2.4 The present document makes no further statements on the content, as this is prescribed by [2].

4.9.2.5 Requirements that only concern ORs, from safety case (IV) to VOs are included in the network access requirements, in Swiss TORs or in implementing provisions to Swiss TORs.

### **4.9.3 Requirements incorporated from (VIII)**

- 4.9.3.1 See 4.8.4

### **4.9.4 Requirements passed on to (I) and (V)**

- 4.9.4.1 The requirements passed on here are derived from:

4.9.4.1.1 the trackside risk analyses and the measures derived therefrom with relevance to the vehicle types in question,

4.9.4.1.2 the trackside faults and the measures derived therefrom with relevance to the vehicle types in question, and

4.9.4.1.3 the trackside SRACs, if they have not been incorporated as requirements for OBU design, or as network access requirements.

### **4.9.5 Requirements passed on to operational evidence for Safe-Auth-IM**

- 4.9.5.1 The requirements passed on are in particular:

4.9.5.1.1 Proof of compliance with operating regulations governing operating rules

4.9.5.1.2 Proof of training of operations personnel

4.9.5.1.3 Proof of compliance with maintenance regulations

4.9.5.1.4 Proof of training of maintenance personnel.

### **4.9.6 Responsibility**

- 4.9.6.1 The railway infrastructure undertaking is responsible for the safety case for technical and operational integration of signalling systems (IV).

## **4.10 Proof of compliance with operational phase requirements set forth in IM safety authorisation (SafeAuth-IM)**

4.10.1.1 The Infrastructure Manager must provide the following documents in particular

- Proof of compliance with operating regulations governing operating rules
- Proof of training of operations personnel
- Proof of compliance with maintenance regulations
- Proof of training of maintenance personnel.

depending on the SafeCert-VO request.

4.10.1.2 This is already covered by the existing specifications given in [9] and [15].

## **4.11 Safety case for OBU-EVC (X)**

### **4.11.1 Overview**

4.11.1.1 The safety case for OBU-EVC (X) attests to the technical safety of the OBU.

### **4.11.2 Content**

4.11.2.1 The safety case for OBU-EVC attests to the technical safety of the OBU and compliance with the technical requirements of the generic product.

4.11.2.2 The present document makes no further statements on the content, as this is prescribed by [2].

### **4.11.3 Requirements incorporated from (VII)**

4.11.3.1 See 4.3.4.

### **4.11.4 Requirements passed on to (VI)**

4.11.4.1 SRACs for neighbouring systems such as vehicle bus system and DMI are exported to safety case (VI).

4.11.4.2 In addition, any SRACs concerning integration into the on-board subsystem, vehicle operation and maintenance are passed on to safety case (VI).

### **4.11.5 Responsibility**

4.11.5.1 The OBU supplier is responsible for the safety case for OBU-EVC (X).

## **4.12 Safety case for integration of OBU in vehicle type (VI)**

### **4.12.1 Overview**

- 4.12.1.1 The safety case for OBU - vehicle integration (VI) provides evidence of the safe integration of the OBU in the corresponding vehicle type as well as the correctness of the paramterisation.

### **4.12.2 Content**

- 4.12.2.1 Safety case VI covers the following in particular:
  - 4.12.2.1.1 Vehicle integration, incl. DMI, braking system, vehicle buses, antennas, etc.
  - 4.12.2.1.2 Correctness of maintenance manual
  - 4.12.2.1.3 Correctness of operating manual
- 4.12.2.2 The vehicle-side safety case for integration of OBU in vehicle type (VI) is based on the subordinate safety cases for on-board components, in particular safety case (X) and provides evidence of the safety of the OBU in the vehicle.
- 4.12.2.3 Braking curve validation is also located at the level of the Safety case for integration of OBU in vehicle type (VI).
- 4.12.2.4 The present document makes no further statements on the content, as this is prescribed by [2].

### **4.12.3 Requirements incorporated from (X)**

- 4.12.3.1 SRACs on technical integration, which have been exported from the subordinate safety cases, in particular safety case (X), are treated on a technical level.

### **4.12.4 Passing on of requirements in operating and maintenance manuals**

- 4.12.4.1 Operational application conditions can only be passed on as instructions in operating and maintenance manuals.
  - 4.12.4.1.1 Certain trains (e.g. motor train units) are only authorised in certain formations. If the use in special train formations (e.g. multiple traction, composition with additional or fewer wagons) is envisaged, in particular together with vehicles without ETCS equipment, the requirements to be taken into account in the SafeCert-VO must be clearly indicated.
- 4.12.4.2 Technical aspects of trackside systems or equipment must be clarified at the technical level among suppliers within the framework of IOP certification.

### **4.12.5 Responsibility**

- 4.12.5.1 The vehicle integrator is responsible for the safety case for integration of OBU in vehicle type (VI).

## 4.13 Safety case for technical and operational integration of vehicle types (II)

### 4.13.1 Overview

- 4.13.1.1 Safety case II provides evidence that safe operation of the vehicle is possible. Technical aspects are of secondary importance.

### 4.13.2 Content

- 4.13.2.1 General information about the content of safety case (II) is provided in [21]. Here, only a rough overview is provided.
- 4.13.2.2 Safety case (II) makes statements on all safety-related points of the subsystems necessary for operation, and their components.
  - 4.13.2.2.1 **Concerning operational integration of the vehicle**  
(particularly with regard to the entering of train data, train category, axle load, brakes and braking characteristics of the vehicle, including failure behaviour)
  - 4.13.2.2.2 **Concerning the operating instructions, meaning the requirements for vehicle operation**  
(particularly with regard to the procedure followed when braking properties cannot be maintained)
  - 4.13.2.2.3 **Concerning regulations on the use of vehicles, including possible restrictions**  
(particularly with regard to carrying along vehicles with multiple-unit control (mode, fault), towed, vehicle in non-leading (NL) mode in the middle or at the rear of the train, carrying of vehicles when ETCS is not working, pushing and intermediate locomotives, locomotive trains, minimum towing capacity)
  - 4.13.2.2.4 **Concerning conditions of application**  
(for instance, the area of application of the vehicle, restrictions (e.g. CH only), use of tilt system, speed restrictions) and
  - 4.13.2.2.5 **Concerning certification of processes to ensure proper maintenance.**
- 4.13.2.3 This safety case is concerned with the vehicle and deals with the fulfilment of the safety requirements. It considers the interplay with the line only insofar as the subsystem ETCS is based on the trackside conditions (e.g. the network access requirements) in the form of vehicle requirements and specifications.
- 4.13.2.4 Further, it considers the interplay with the line only insofar as there are vehicle-side conditions for the trackside subsystem in the form of SRACs. These may have already been addressed and evaluated within (II); if not, this must be done in (V).
- 4.13.2.5 Additional rules for drawing up this safety case are provided in [1] and [2].
- 4.13.2.6 Responsibility for drawing up the 'safety cases for vehicles (II)' lies with the VK.
- 4.13.2.7 The VK makes the necessary arrangements with the VO concerning the following points in particular:
  - 4.13.2.7.1 Fault reporting channels, incident reporting channels, in particular backup of data collected by train recording unit (TRU)
  - 4.13.2.7.2 Training of locomotive drivers (responsibility of RU) so that they are able to operate the vehicle
  - 4.13.2.7.3 Compliance with operating manual
  - 4.13.2.7.4 Any minor maintenance

### 4.13.3 Requirements incorporated from (VI)

- 4.13.3.1 The inbound requirements here are:
  - 4.13.3.1.1 the SRACs from safety case (VI), and, for existing vehicles,
  - 4.13.3.1.2 the network access requirements of the line.

#### **4.13.4 Requirements passed on to (I) and (V)**

4.13.4.1 The requirements passed on to (V) are derived from:

- 4.13.4.1.1 the vehicle-side risk analyses and measures derived therefrom with relevance to the lines in question,
- 4.13.4.1.2 the vehicle-side faults and measures derived therefrom with relevance to the lines in question,
- 4.13.4.1.3 the SRACs of the vehicles, if they have not been incorporated as requirements for RBC design,
- 4.13.4.1.4 the operating rules or derived operating rules and possibly the maintenance rules for the line, if they have not been incorporated as requirements for RBC design.

4.13.4.2 Notes on the certification of the specific vehicle are passed on to (I).

#### **4.13.5 Requirements passed on to operational evidence for SafeCert-VO**

4.13.5.1 The requirements passed on are in particular:

- 4.13.5.1.1 Proof of compliance with the operating regulations governing operating rules
- 4.13.5.1.2 Proof of training of operations personnel

#### **4.13.6 Special cases**

4.13.6.1 Deployment of the vehicle in special train formations:

- 4.13.6.1.1 Some trains (e.g. motor train units) are permitted only in particular formations. If deployment is planned in special train formations (e.g. multiple traction, composition with additional or fewer wagons etc.), in particular if together with vehicles that do not have ETCS equipment, the requirements to be observed in the SafeCert-VO must be clearly indicated.

#### **4.13.7 Responsibility**

4.13.7.1 The VK is responsible for safety case (II).

#### **4.14 Proof of compliance with requirements in the operating phase for the purpose of obtaining a VO safety certificate.**

- 4.14.1.1 The VO/RU must provide proof of compliance with the operating regulations governing operational processes, training of locomotive personnel, etc., in accordance with the request for a SafeCert-VO.
- 4.14.1.2 This is already covered by the existing specifications under [9] and [15].



## 4.15 Overall safety case for technical and operational integration of signalling systems and vehicles (I)

### 4.15.1 Overview

- 4.15.1.1 The overall safety case for technical and operational integration of signalling systems and vehicles (I) ultimately certifies the safety of ETCS implementation.

### 4.15.2 Content

- 4.15.2.1 The higher-level overall safety case contains the considerations of the individual vehicle types, makes a **final safety evaluation of the line and all vehicles**, and refers to existing documents and safety cases from preliminary processes. These represent the considerations according to Figure 3:
  - 4.15.2.1.1 safety case for vehicles (II) and associated independent safety assessment on the ETCS equipment including its implementation.
  - 4.15.2.1.2 safety case for the trackside signalling systems (IV) and associated independent safety assessment.
  - 4.15.2.1.3 certificate of operational, line-related interoperability (V).
  - 4.15.2.1.4 certificate of the technical interoperability (III), (VII) and (IX), if not already described sufficiently in the relevant safety cases for on-board or trackside systems.
  - 4.15.2.1.5 certificate of fulfilment of any conditions resulting from the independent safety assessments for safety cases (II), (IV) and (V).
- 4.15.2.2 Any deviations from the actually performed safety case procedure from the procedure described in this concept should be noted in safety case I.

### 4.15.3 Requirements incorporated from (II), (IV) and (V)

- 4.15.3.1 See 4.5.5, 4.9.4. and 4.13.4.

### 4.15.4 Responsibility

- 4.15.4.1 The RIU is responsible for safety case (I).

## 5 Safety case structure

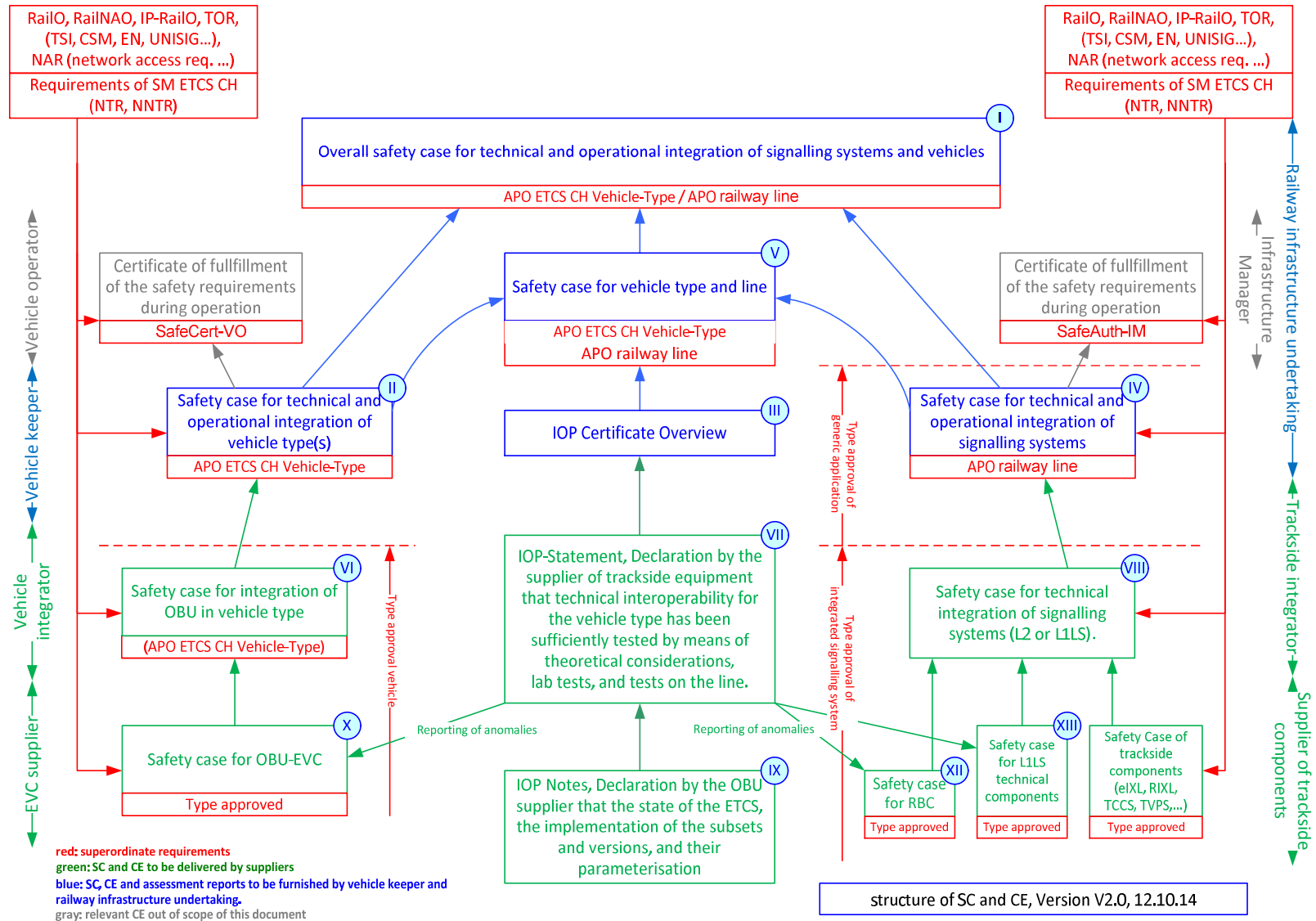


Figure 3: Safety case structure

## 6 Overview table of safety case structure

No.	Title	Content	Responsibilities	Requesting party	Validation	Review
(I)	Overall safety case for technical and operational integration of signalling systems and vehicles (I)	Higher-level document certifying that the various vehicle types can run sufficiently safely on line with equipment delivered by ETCS suppliers. This means that the required documents (safety case, independent safety assessment, validation reports, etc.) of the preliminary processes vehicle type, line, and their interaction, are complete and correct.	RIU	Applicant commissions this task to RIU	No validation at this level; taken over from preliminary processes	Yes
(II)	Safety case for technical and operational integration of vehicle type(s) (II)	Safety case for the on-board ETCS equipment including technical and operational integration. This document covers in particular regulations, instructions and operational conditions. Safety case (II) must specifically list the relevant points that must be included in the RU safety certificates.	Applicant or VK	No external mandate given	Validation in view of higher-level requirements from operator's viewpoint, and ensuring compliance with all SRACs	Yes
(III)	IOP Certificate Overview (III)	Certificate that combination of OBU and RBC or L1LS functions within the boundaries tested. The certificate shows the origin and performance of the IOP test cases and certifies error handling. The certificate summarises the findings of the IOP Statement (VII).	SM ETCS CH	No external mandate given	No	No, since it is not a safety case
(IV)	Safety case for technical and operational integration of signalling systems (IV)	Integral operational and technical safety case according to EN50126/50129 for trackside equipment. This document covers in particular regulations, instructions and operational conditions.	RIU	No external mandate given	Yes	Yes
(V)	Safety case for vehicle type and line (V)	Safety case for the safety requirements made from line to vehicle and vice versa. It also includes evaluation and certification of measures implemented as a result of this. It also contains the certificate for the network access tests prescribed by the IM according to [18].	RIU	Applicant commissions this task to RIU	Validation in view of higher-level requirements from operator's viewpoint, and ensuring compliance with all SRACs	Yes
(VI)	Safety case for integration of OBU in vehicle type (VI)	Safety case for the integration of ETCS equipment in the vehicle, the associated parameterisation and documentation. The prescribed safety objectives must be met for this.	Vehicle integrator	No external mandate given	Yes	Yes
(VII)	IOP Statement	Declaration by the supplier of trackside equipment that technical interoperability for the vehicle type has been sufficiently tested by means of theoretical considerations, laboratory experiments, and on the line.	RBC supplier	OBU supplier commissions this task to RBC supplier	No Individual test cases are validated.	No, since it is not a safety case

No.	Title	Content	Responsibilities	Requesting party	Validation	Review
(VIII)	Safety case for technical integration of signalling and automation system (VIII)	Safety case for technical integration of signalling systems (L2 or L1LS).	Trackside integrator(s)	No external mandate given	Yes	Yes
(IX)	IOP Notes (IX)	Declaration by the OBU supplier that the state of the ETCS, the implementation of the subsets and versions, and their parameterisation, correspond to the values prescribed by SM ETCS CH and the RIU.	OBU supplier	No external mandate given	No	No, since it is not a safety case
(X)	Safety case for OBU-EVC (X)	Certificate from the OBU supplier that the OBU fulfils the general requirements (standards) and specific requirements (specifications), and performs as planned. This safety case is drawn up according to FOT rules to obtain generic type approval.	OBU supplier	No external mandate given	Yes	Yes
(XII)	Safety case for RBC (XII)	Safety case for the RBC technical system drawn up according to [2].	RBC supplier	No external mandate given	Yes	Yes
(XIII)	<b>Fehler! Kein gültiges Resultat für Tabelle.</b>	Safety case for the ETCS L1LS technical components drawn up according to [2].	ETCS L1LS supplier	No external mandate given	Yes	Yes

Table 1: Overview of safety cases

## 7 Principles of certification

### 7.1 The safety case for technical and operational integration of the entire system as the basis for issuance of an APS for on-board equipment

- 7.1.1.1 Generally speaking, an APS for on-board equipment is issued to an applicant and an APS for trackside equipment is issued to a licenced RIU.
- 7.1.1.2 The APS for on-board equipment not only requires a safety case for the overall integrated system, but also full documentation concerning the vehicle and implementation of all regulatory measures that enable the VK or VO to use the systems safely and efficiently at all user levels. Following implementation of the railway reform 2.2 in federal legislation (RailO, RailNAO), an RIU must also be an RU if vehicles are to travel on the line.
- 7.1.1.3 The safety case for the integrated overall system is one of the basics for obtaining an APS for on-board equipment. An APS is not issued for a specific line. Instead, an ETCS CH APS is issued on the basis of safety cases (I), (II), (IV) and (V). Aspects concerning ETCS L1LS are included according to 1.2.3.
- 7.1.1.4 The present concept enables the clear allocation of responsibilities and identification of the various participants involved in the preparation of the safety case. It explains the information required of them in superordinate certificates so as to ensure parallel execution of assigned tasks and an understanding of processing sequences to be carried out.
- 7.1.1.5 In order to ensure the joint, safe operation of systems and subsystems, the safety case for the integrated overall system also considers all peripheral requirements such as technical documentation, manuals, implementation regulations, maintenance instructions, conditions, operational instructions, training documents and training concepts as well as their implementation and corresponding validation reports at the appropriate level.
- 7.1.1.6 The safety case for the integrated overall system always falls under the scope and responsibility of the RIU.

### 7.2 Difference between certificates and safety case

- 7.2.1.1 The content structure of the safety case must meet the requirements set forth in [2]. In contrast, there are no binding guidelines on the issuance of certificates in terms of content structure, validation and safety assessment.

### 7.3 Validation requirements

#### 7.3.1 Purpose of validation

- 7.3.1.1 Validation shall ensure that all conditions of use have been properly and completely fulfilled so that safe operation of the railway is possible.

### **7.3.2 Choice of validator**

- 7.3.2.1 For the choice of the validator, the specification regarding independence from [2] must be taken into account.

### **7.3.3 Criteria for recognition of validators**

- 7.3.3.1 A validator shall satisfy at least the following criteria:

- 7.3.3.1.1 Proven knowledge of the Swiss train operating regulations (TOR)
- 7.3.3.1.2 Good knowledge of Swiss railway regulations
- 7.3.3.1.3 Practical experience in the Swiss railway sector
- 7.3.3.1.4 Experience with certification of railway signalling systems
- 7.3.3.1.5 Technical expertise in implementation of trackside equipment.

## **7.4 Maintaining the safety cases for the integrated overall system**

### **7.4.1 Requirements for issuance of a safety case**

- 7.4.1.1 Safety cases must be produced in accordance with [2].
- 7.4.1.2 In particular, the older version of the safety case to be revised (particularly outstanding issues), the safety assessment associated with the older version of the safety case, the SRACs and outstanding issues of subordinate safety cases and safety assessment shall be taken into account.

### **7.4.2 Reasons for modifying a safety case**

- 7.4.2.1 Reasons for modifying a safety case include in particular technical modifications such as new functionalities, new parameterisation data, changes in the SRACs and their fulfilment as well as new applications.
- 7.4.2.2 Each modification of a subordinate safety case leads to an upgrade of the higher-level safety case, at least in terms of its referencing.
- 7.4.2.3 It may be necessary to update a safety case if network access is granted to new vehicle types, if there are new findings, if faults have been identified, or if a change of use is planned.

### **7.4.3 Duty to inform the National Safety Authority (FOT, in Switzerland)**

- 7.4.3.1 According to [13], the FOT must be notified of any modifications to vehicles. The FOT decides whether to issue the APS.

## **7.5 General requirements for the safety assessment**

### **7.5.1 Purpose of the safety assessment**

- 7.5.1.1 The safety assessment ensures that all necessary steps according to [1] have been fully performed to the required standard of quality.
- 7.5.1.2 Process of analysis to evaluate whether the designers have produced a product that fulfils the specific requirements, and whether the product is suitable for its intended purpose.

### **7.5.2 Need for a safety assessment**

- 7.5.2.1 According to [1], a safety assessment as illustrated in Fig. 3 is always necessary.
- 7.5.2.2 A new safety assessment of a safety cases is required in particular when the risk situation or the risk assessment has changed (on the basis of new or revised risk analysis) or when new SRACs have been exported to the corresponding safety case.
- 7.5.2.3 If a new safety assessment does not seem necessary, then the producer of the safety case must indicate the reasons for this. The ISA will either confirm that the existing safety assessment is still valid or will issue a new safety assessment.

### **7.5.3 Selection of the ISA, requirements for approval of the ISA**

- 7.5.3.1 The ISA must provide evidence of his or her qualifications to the FOT.
- 7.5.3.2 The ISA must provide evidence of his or her qualifications in order to carry out the activity according to [14].

## **7.6 Occurrence of incidents**

### **7.6.1 Information channels**

- 7.6.1.1 Any incidents arising during operation of lines or vehicles must be reported immediately to the RIUs or VKs concerned as well as to FOT, SM ETCS CH (e-mail address in 8.2) and corresponding suppliers.

### **7.6.2 Impact analysis**

- 7.6.2.1 SM ETCS CH shall instruct RIUs to carry out an impact analysis or implement any required measures.

## **7.7 Tasks and responsibilities**

### **7.7.1 General**

- 7.7.1.1 The tasks and responsibilities listed here are by no means exhaustive.

### **7.7.2 Tasks and responsibilities RBC or L1LS suppliers**

- 7.7.2.1 RBC or L1LS suppliers are responsible for drafting the IOP Statement (VII) certifying that deployed systems are interoperable. At the request of OBU suppliers, they also carry out the necessary analyses and IOP test and draft IOP Statement (VII).

7.7.2.2 RBC or L1LS suppliers are in particular responsible for drafting and updating their safety cases (XII and XIII) and corresponding safety assessment as well as the IOP Statement (VII). They must also immediately notify the users of their equipment as well as SM ETCS CH and FOT of any newly identified hazards.

### **7.7.3 Tasks and responsibilities of OBU suppliers**

7.7.3.1 The OBU suppliers are responsible submitting a request to RBC or L1LS suppliers to carry out the necessary analyses and IOP test as well as to draft the IOP Statement (VII). In addition, they indicate the status of the OBU in the IOP Notes (IX).

7.7.3.2 OBU suppliers are in particular responsible for drafting and updating their safety case (X) and corresponding safety assessment as well as the IOP Notes (IX). They must also immediately notify the users of their equipment as well as SM ETCS CH and FOT of any newly identified hazards.

### **7.7.4 Tasks and responsibilities of trackside equipment integrators**

7.7.4.1 Trackside equipment integrators are in particular responsible for drafting and updating their safety case (VIII) and corresponding safety assessment. They must also immediately notify the users of their equipment as well as SM ETCS CH and FOT of any newly identified hazards.

### **7.7.5 Tasks and responsibilities of on-board equipment integrators**

7.7.5.1 On-board equipment integrators are in particular responsible for drafting and updating their safety case (VI) and corresponding safety assessment. They must also immediately notify the users of their equipment as well as SM ETCS CH and FOT of any newly identified hazards.

### **7.7.6 Tasks and responsibilities of railway infrastructure undertakings**

7.7.6.1 Railway infrastructure undertakings are responsible for submitting any necessary requests to suppliers for the IOP Statement (VII) concerning future combinations of ETCS versions as well as IOP Notes (IX) from the VK if modifications to RBC or L1LS are needed.

7.7.6.2 Railway infrastructure undertakings are in particular responsible for drafting and updating their safety case (IV, V und I) and corresponding safety assessment. They must also immediately notify the operators of their infrastructure as well as SM ETCS CH and FOT of any newly identified hazards.

### **7.7.7 Tasks and responsibilities of the Vehicle Keeper**

7.7.7.1 VKs are responsible for submitting any necessary requests to OBU suppliers for IOP notes (IX) concerning future combinations of ETCS versions as well as IOP statement (VII) from the RBC or L1LS suppliers if modifications to on-board equipment are needed.

7.7.7.2 VKs are in particular responsible for drafting and updating their safety case (II) and corresponding safety assessment. The Vehicle Operator, SM ETCS CH and FOT must immediately be notified of newly identified hazards.



**7.7.8 Tasks and responsibilities of the Vehicle Operator**

7.7.8.1 VOs have no IOP-related tasks.

7.7.8.2 Vehicle operators are responsible for immediately notifying the IMs and RIUs concerned as well as SM ETCS CH and FOT in the event of identified hazards in relation to their vehicles.

**7.7.9 Tasks and responsibilities of infrastructure managers**

7.7.9.1 IMs have no IOP-related tasks.

7.7.9.2 IMs are responsible for immediately notifying the RUs and RIUs concerned as well as SM ETCS CH and FOT in the event of identified hazards in relation to their trackside equipment.

**7.7.10 Tasks and responsibilities of SM ETCS CH**

7.7.10.1 The SM ETCS CH is in particular responsible for the ETCS configurations (SW versions) used and for the drafting of safety case III.

7.7.10.2 The SM ETCS CH is also responsible for making the necessary arrangements to clarify identified hazards and notifying the RIU and VK concerned as well as FOT.

## **8 Annex A**

### **8.1 Contact details of railway infrastructure companies (RIUs)**

#### **8.1.1 SPOC**

SBB Infrastructure Division I-AT-ZBF

Hilfikerstrasse 3

3000 Bern 65

E-mail: [xizbpam@sbb.ch](mailto:xizbpam@sbb.ch)

### **8.2 Contact details of System Management ETCS Switzerland**

#### **8.2.1 System Management ETCS Switzerland**

SBB Infrastructure Division I-AT-ZBF

Hilfikerstrasse 3

3000 Bern 65

E-mail: [sf.etcs@sbb.ch](mailto:sf.etcs@sbb.ch)