Start-up activities for Advanced Signalling and Automation Systems

Compendium Safety & Interoperability

Target system & related processes
WHY THIS COMPENDIUM?

Not all experts involved in Shift2Rail projects have the same level of information about the legal framework and established processes in the CCS domain (they may also lack a clear view on the strategic vision which is addressed in the S2R Master Plan and MAAP)

That is needed to converge research activities towards the next evolution of the digital railway system in Europe

This compendium provides guidance by basic information and strategic targets thus helping to overcome silo-approaches and integrating into a coherent future railway target system of IP2
TABLE OF CONTENTS

1. OVERVIEW
   › Key concepts for managing the shared railway system

2. CHANGE MANAGEMENT
   › How to introduce innovation into the shared system

3. DESIGN AND PRODUCTION
   › of vehicles, network projects, subsystems and components

4. CCS SPECIFICITIES

ABBREVIATIONS
Chapter 1

Overview: Key concepts for managing the shared railway system
Roles and responsibilities
If it moves, it is a Railway Undertaking (RU) responsibility.

If it is fixed, it is an Infrastructure Manager (IM) responsibility.

The National Safety Authority (NSA) supervises the IMs and RUs.
Each RU and IM has a Safety Management System (SMS). It must ensure that its part of the system is operated in a safe manner.

For all the sub-systems they operate, the RUs and IMs must ensure that they always meet the essential requirements for:

- Safety
- Environmental protection
- Technical Compatibility
- Reliability and Availability
- Health
- Access (for people of reduced mobility)

conforms to the rules:

- CSM on SMS
- TSIs
- National rules

Other actors (e.g. manufacturers, keepers, maintainers, loaders, etc) contribute to the safety of the system but the primary responsibility rests with the **RU or IM**. The **SMS** of RU or IM must ensure the efforts of these suppliers deliver the above. Entities in charge of maintenance (ECM) of Freight Wagons are certified.
ROLES AND RESPONSIBILITIES – REGULATORY FRAMEWORK
AUTHORISATION OF VEHICLES AND NETWORK PROJECTS

The Triangle of Transparency

Rule setter
EC + Member States

Authorising Entity
ERA or National Safety Authority

Assessment Body
NoBo
DeBo
CSM AsBo

Source: European Union Agency for Railways
WHAT IS INTEROPERABILITY?

Objectives from the Interoperability Directive

› to define an optimal level of technical harmonisation;
› to make it possible to facilitate, improve and develop rail transport services within the Union and with third countries;
› to contribute to the completion of the single European railway area and
go to contribute to the progressive achievement of the internal market.
MANAGING A SHARED SYSTEM

It follows that where it is necessary for all actors to “do the same thing“, for meeting:
- the objectives of the directive
- the essential requirements for the system as a whole
- the essential requirements for their part of the system

Then the things that everybody “must do the same” must be laid down in rules
- the TSIs for the target system specifications and
- national rules for legacy system specifications

For all other elements of system specification the actors may choose their own method of meeting the essential requirements
- below the red line in slide 10
Human and organisational components need to be integrated in all the requirements (both mandatory and voluntary).

* Some parts of standards can become law. For details see chart 32 „How standard parts become law“
Chapter 1

Overview: Key concepts for managing the shared railway systems

SAFETY
Risk-based safety regulation
More safety assurance
Higher safety maturity
Commitment and capability to do Safety

Safe Operations
SMS Enhancement
Safety Culture
STRONG REGULATORY SAFETY CULTURE

Source: European Union Agency for Railways
SAFETY STRUCTURES

- Permissioning scheme for equipment
- Permissioning scheme for safety management systems
- Maintenance scheme for rolling stock (incl. ECMs)
- Independent Supervision (NSAs)
- Independent Accident Investigation (NIBs)
- Independent Assessment Bodies (CSM Risk Assessment)
- Defined responsibilities in law (cannot subcontract responsibility)
- Where there is a need for a Common Approach – “Common Safety Methods”
- Monitoring at a European Level (Commission & Agency) including CSIs and CSTs (NRVs)
THE RISE OF SAFETY MANAGEMENT SYSTEMS

› 6th July 1988 – Piper Alpha oil production platform explosion

› 167 lost, only 62 survivors

› Lord Cullen’s recommendations (106) move away from prescription to safety cases as a more effective system
The SMS must:

- be documented in all relevant parts
- describe the distribution of responsibilities within the organisation of IM or RU
- show how control by the management on different levels is secured
- show how staff and their representatives on all levels are involved
- show how continuous improvement of the safety management system is ensured

All these requirements shall be included in the SMS
The requirement of the SMS shall be fulfilled through:

› safety policy and corporate safety targets
› compliance with standards or other prescriptive conditions
› change management
› risk management
› operational and front-line staff competence management
› communication and info exchange, document management
› emergency management
› reporting of unexpected outcomes
› internal auditing of the SMS

All these elements shall be defined in the organisation of the company and shall be DOCUMENTED
SAFETY MANAGEMENT SYSTEMS

› Check whether SMS is sufficient to allow operation to begin (Certification: CSM for Conformity Assessment (*) / CSM on SMS requirements (EU) 2018/762 – maximum validity 5 years)

› Supervision of the functioning of the SMS by National Safety Authorities during operation (CSM Supervision)

› Railway Undertakings checking for themselves that their systems are functioning correctly during operation (CSM Monitoring)

(*) The CSM for Conformity Assessment will be definitively repealed in 2025
COMMON APPROACH TO RISK ASSESSMENT

- Basically CSM is an iterative process made of 3 steps:
  (a) Identification of hazards, associated safety measures and resulting safety requirements
  (b) Risk analysis and risk evaluation based on exiting risk acceptance principles
  (c) Demonstration of the system compliance with the identified safety requirements

- Additional requirements for mutual recognition:
  (a) Hazard Management
  (b) Independent Assessment (Assessment Body)

Source: European Union Agency for Railways
THE 3 RISK ACCEPTANCE PRINCIPLES

1. Codes of Practice (CoP)
   - Implicit Risk Acceptance Criteria (RAC)
     - Comparison with criteria

2. Reference System
   - Explicit RAC
     - Comparison with criteria

3. Risk Estimation
   - Safety criteria?
     - Frequency
     - Severity
     - Risk
       - Comparison with Design Targets
         - prevent catastrophic consequences
           - catastrophic 10E-9
           - critical 10E-7

Apply one or more risk acceptance principles (RAP)
The objective is prevention of accidents and possible improvement of railway safety.

The investigation body shall investigate serious accidents and might investigate in addition also those accidents and incidents which under slightly different conditions might have let to serious accidents.

The investigation body shall, at its discretion, decide whether or not to investigate such an accident or incident. In its decision it shall take into account:

(a) the seriousness of the accident or incident
(b) whether it forms part of a series of accidents or incidents relevant to the system as a whole;
(c) its impact on railway safety and
(d) requests from IM, RU and NSA
INTEROPERABILITY DIRECTIVE VS SAFETY DIRECTIVE

› The **Interoperability Directive** covers all things the actors **must do the same** to make the shared system work

› The **Safety Directive** contains the requirements to ensure that the actors **manage their part of the shared system safely**

› Sometimes the Interoperability Directive “imports” concepts from the Safety Directive (e.g. the use of the CSM RA for requirements capture for vehicle type design)
Overview: Key concepts for managing the shared railway system

VEHICLE AUTHORISATION
WHAT IS VEHICLE AUTHORISATION?

Why is it required?

› Public interest
› Special check at a safety relevant event (new or upgraded vehicle design)
› To ensure compatibility of networks and vehicles managed by different entities
› IMs and RUs can not always be relied upon spontaneously to deliver full interoperability
› For interoperability, it is necessary to deliver technical compatibility: “The technical characteristics of the infra and fixed installations must be compatible with each other and with those of the trains to be used on the system”.
› Legal certainty for applicants
› Equality of treatment for manufacturers in all Member States

Source: European Union Agency for Railways
WHAT IS VEHICLE AUTHORISATION?

Vehicle Type Authorisation is:

› Legal act issued by an authorising entity based on reasonable assurance that the applicant and the actors supporting the applicant have fulfilled their responsibilities (full definition in Art. 2 (16) of Regulation 2018/545)

Its Purpose is:

› To ensure conformity with the essential requirements of the applicable legislation

› To enable individual vehicles manufactured according to the design type to be placed on the market based on an applicant’s declaration of conformity to the type

Source: European Union Agency for Railways
WHAT IS VEHICLE AUTHORISATION?

The Authorising Entity

SHOULD:
- satisfy itself of the efficacy of the process
- satisfy itself of consistency, completeness and plausibility of the documentation

SHOULD NOT:
- repeat or duplicate work carried out by other checking bodies
- use the authorisation process to check or evaluate the competence of checking bodies

Source: European Union Agency for Railways
WHAT IS VEHICLE AUTHORISATION?

Is vehicle authorisation time limited?
To give applicants legal certainty a vehicle type authorisation/Vehicle authorisation for placing on the market is generally not time limited.

When a vehicle/vehicle type authorisation may be rendered invalid?
Only under two cases:
›  Rules change (TSIs and/or NTRs) – Renewed authorisation required
›  Subsequent discovery that the essential requirements were not met at authorisation (defective design or manufacture) – Amendment – Suspension or Revocation of authorisation

Not to be used in case of failure to meet the essential requirements due to actions or inactions of RUs or ECMs in the operation of their SMS (e.g. poor maintenance)

Source: European Union Agency for Railways
First individual Vehicle authorised To Place on Market

Subsequent Vehicles Authorised to Place on the Market The basis of conformity To Type

RU contemplates running a service on a route

RU uses vehicle type characteristics (ERATV - RINF) to establish vehicle route compatibility

RU uses vehicle type characteristics to define train characteristics

Return of experience Feedback from maintenance checks Feedback from incident reporting

Vehicles of this type maintained by ECM as part of RUs SMS according to maintenance instructions for vehicle type

Trains operated by RU using SMS over compatible routes according to limits and conditions of use for type

RU checks compatibility of proposed train composition with the route by comparing train characteristics with RINF And OPE TSI (Network statement),

RU acquires track access for trains

RU uses vehicle type characteristics to define train characteristics

SMS of RU Use of vehicles Supervision by NSAs

Applicants Responsibility Vehicle design and construction

First individual Vehicle manufactured

Vehicle Type Authorised (incl Maint instructions and L&COU)

Applicant Produces a new or updated design and associated maintenance instructions and limits and conditions of use
COMPATIBILITY OF TRAINS WITH ROUTES

Technical parameters of routes and rolling stock derive from various TSIs, e.g. TSI CCS, INF, RST, SRT, PRM, Noise - and also still from National Technical Rules.

ERATV:
EU register of authorised type of vehicles

RINF:
Register of Infrastructure

Technical parameters of rolling stock

compatibility of rolling stock with route

Technical parameters of
- route A
- route B
- route C
- route D
Chapter 2

Change Management: How to introduce innovation into the shared system
Interoperability Directive

Annex III: Essential Requirements

"1.1.4. The design of fixed installations and rolling stock and the choice of the materials used must be aimed at limiting the generation, propagation and effects of fire and smoke in the event of a fire."

TSIs specify requirements to ensure the 4 objectives of the Directive

TSI LOCPAS, ch. 3.1: Elements of the rolling stock subsystem corresponding to the essential requirements

<table>
<thead>
<tr>
<th>Ref. Point</th>
<th>Element of the rolling stock sub-system</th>
<th>Safety</th>
<th>Reliability-Availability</th>
<th>Health</th>
<th>Environmental protection</th>
<th>Technical compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.10.2</td>
<td>Fire safety – Measures to prevent fire</td>
<td>1.1.4</td>
<td>1.3.2</td>
<td>1.4.2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Harmonised™ EU standards specify one way that the essential requirements may be met in accordance with the TSIs
AGILE V-CYCLE FOR EACH STAGE:
FROM INNOVATION TO STANDARD PRODUCT

- Innovation → Prototype
- Prototype → “Technical Specification”
- Serial Production → State of the art
- State of the art → Standard
- Standard → “normal” authorisation

Authorisation?
Non-conformities to regulation

REX: Return of Experience
What should a TSI cover?

- TSIs must specify **The Optimal Level of Harmonisation**

- If a common specification is necessary for:
  - Network-Vehicle Compatibility
  - Market opening
  - Avoiding Member States creating their own rules for the essential requirements

Then it should be within a TSI

**BUT** only if a railway specific specification is necessary
**RESEARCH & INNOVATION, STANDARDS, REGULATION**

**Research & Innovation (S2R + EC (MOVE + RI))**

- **SERA research & innovation needs leading to standards developments for the future system and contributing to defining target systems in regulatory requirements reviewing project activities and results**

- **Technical Regulation (EC)**
  - Technical Specifications for Interoperability
  - ERA Technical document
  - Common Safety Methods
  - Implementing Acts and others

- **Recommendation for Regulation**

- **ERA Requests for standards**
  - To be part of regulation
  - To confer presumption of conformity with regulation

- **Standards**
  - CEN/CENELEC/ETSI and others
S2R R&I RESULTS AND PROCESS
LEADING TO STANDARDS/REGULATION

Shift2Rail internal process

- S2R R&I results
  - S2R CCA WA 3.2
    - Develop Maintain
  - S2R Rolling Innovation Plan
  - S2R
    - Assisting the S2R projects/TDs:
      - Overview of standardisation activities, ongoing and planned
      - Monitoring of progress
      - Assistance in the timely development of appropriate standards
      - Close cooperation with relevant partners and organisations
    - Bring its input into the regulatory framework and standardization plan

Stakeholders e.g. ERRAC

RASCOP Platform (chaired by EC)

European Commission

Advisory task proposing guidelines for R&D leading to technical standards for interoperability and safety, after stakeholders consultation

Detailed Guidance in specific cases

Standardisation request after stakeholder consultation

Others, SSO

CEN/CLC/ETSI

JPC-R

ISO / IEC / ITU

ERA

Feed into RASCOP Platform (chaired by EC)

S2R R&I to reg/stds formal process
Chapter 3

Design and production of vehicles, network projects, subsystems and components
Also operational/human aspects need to be taken into account. This will highly influence the setting of requirements (steps 1 to 4) and should be checked and adequately tested in step 8 (integration).
It is important to define what is in and what is out of the system in scope. Clear and unambiguous terminology shall be used, preferably as defined in international standards. The EU legal framework for the railway system and its sub-systems shall be understood and applied. Standards should be coherent and may support efficient application of legal requirements, though remaining voluntary as standards typically are.
THE RAILWAY SYSTEM

Rolling Stock

Environ-
ment

Technology

People

Operation

Telematics

Maintenance

CCS

Energy

Infrastructure

Process
Legal framework based on the Railway Safety Directive are the Common Safety Methods on Risk Acceptance (CSM-RA) with 3 Risk Acceptance Principles (RAP). For RAP 1, standards are the most common Codes of Practice (CoP). For RAP 3, two quantitative design targets (DT) are available. A generic function structure and system structure can support the risk assessment and also the allocation of technical requirements.
RISK ASSESSMENT: FUNCTION OR SYSTEM

Functions
- Manage route
- Manage speed
- Separate trains

Systems
- CCS
- Telecom
- Power
Here the risk analysis according to RAP no. 3 is embedded in more detail in the system design process. The system must meet the essential requirements (safety, technical compatibility, environmental protection, health, access for PRMs, reliability and availability).
SAFETY AND IT-SECURITY

RAM and Safety

System Definition

System

Hazards

Vulnerability

Risk Analysis

Safety

Reliability

Availability

Maintainability

Security Level (SL)

(IEC 62443)

IT-Security

Threats

Foundational Requirements

FR1

FR2

FR3

FR4

FR5

FR6

FR7

International Standards

EN 50126
EN 50129
EN 50128
EN 50657
EN 50159

CLC WG A16
IEC 27000 ff
IEC 62443 ff

Tolerable Hazard Rate

THR

Tender Targets

Design Targets (DT)

by legal framework

Results in SIL

on system level

Final breakdown of independent safety functions and TFFR / SIL allocation per function

Towards

System Requirements

System Architecture & Design
LIFE-CYCLE OF A TECHNICAL PRODUCT

For coherent specification of system requirements formal methods should be applied and systems engineering processes performed.
LIFE-CYCLE OF A TECHNICAL PRODUCT

Architectures are key to achieve an unambiguous understanding before starting the system design process.
LIFE-CYCLE OF A TECHNICAL PRODUCT

Concept

System Definition and Application conditions

Risk Analysis and Evaluation

Specification of System Requirements

Architecture & Apportionment of system requirements

Design and Implementation

Manufacture

Integration

System validation

System Acceptance

Decommissioning

Acceptance Test

System Test

Integration Test

Component Test

Testing of conformity of requirements with various technical design solutions in various different scenarios can take place on different levels. There is clear expectation to gain confidence and ensure reproducibility, and to reduce cost. Authorisation process roles and responsibilities are described.
Aim: Failure detection and error reduction to enable a safe and reliable system (the railway system as a whole)

- **Failure**: Deviation of the system from its expected result
- **Error**: Human action producing an incorrect result
- **Fault / defect**: The cause of an error or failure

**Lab or on-site tests?**
- Time and effort
- Reproducibility
- Worst-case scenarios
- Number of units
- Environmental conditions
- Individual system boundaries
- Pass/fail criteria
Operation starts after authorisation and integrating the new technology into the system. Lessons learnt from operation may trigger change of authorisation criteria, standards, further requirements or maintenance processes. Operational procedures and rules become increasingly harmonised on EU-level with implementing interoperable technology.

**STEP 10 – System Acceptance**
- NoBo Certification of Interoperability Constituents
- Vehicle Type or Infrastructure Subsystem Authorised
- Customer requirements are met (including “requirements capture”)
- RU integrated in its SMS
  - Operations (includes route compatibility check)
  - Maintenance
  - Update to Safety Certificate/Authorisation (where necessary)
Chapter 4

CCS specificities
EUROPEAN COMMISSION (DG MOVE)
• Legislate (Interoperability/Safety Directives; CCS TSI)
• Follow-up ERTMS deployment - Member States (EU 2017/6)
  • Financing ERTMS deployment (CEF-INEA/EIB)
  • Lead ERTMS Memorandum of Understanding (MoU)

European Union Agency for Railways (ERA)
• System Authority for the ERTMS specifications (Annex A of CCS TSI)

(Manages) ERTMS Change Control Management (CCM)

Representative Bodies
appoint experts, consultation, support MoU

Contributes to specifying Research

Shift2Rail Joint Undertaking (S2R JU)
• Manages all EU funded Rail R&I
• Focused R&I on CCS incl. ERTMS/ETCS

SHIFT2RAIL PROGRAMME
Dedicated work on ERTMS « Game Changers »
(ATO, Moving Block, Satellite positioning, Next Gen Comm.)

Carry out research
Propose “enhancements” for next CCS TSI (ERTMS/ETCS)

Railway Stakeholders

Requirements
Feedback from operations
Maintenance of specifications ("error corrections")

Provides input on (new) enhancements to be included in CCS TSI
SCOPE OF TSI CCS*

* CCS on board/trackside subsystems = “All the on-board/trackside equipment required to ensure safety and to command and control movements of trains authorised to travel on the network”
SCOPE OF TSI OPE

*will be derived from operational procedures and individual requirements for RU/IM safe operation
## ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATO</td>
<td>Automatic Train Operation</td>
</tr>
<tr>
<td>CEF</td>
<td>Connecting Europe Facility</td>
</tr>
<tr>
<td>CEN</td>
<td>European Committee for Standardization</td>
</tr>
<tr>
<td>CENELEC</td>
<td>European Committee for Electrotechnical Standardization</td>
</tr>
<tr>
<td>CER</td>
<td>Community of European Railway</td>
</tr>
<tr>
<td>CCS</td>
<td>Control Command and Signalling</td>
</tr>
<tr>
<td>CSM</td>
<td>Common Safety Method</td>
</tr>
<tr>
<td>DeBo</td>
<td>Designated Body</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECM</td>
<td>Entity in Charge of Maintenance</td>
</tr>
<tr>
<td>EIM</td>
<td>European Rail Infrastructure Managers</td>
</tr>
<tr>
<td>EN</td>
<td>European Norm</td>
</tr>
<tr>
<td>ERA</td>
<td>European Union Agency for Railways</td>
</tr>
<tr>
<td>ERATV</td>
<td>European Register of Authorised Types of Vehicles</td>
</tr>
<tr>
<td>ERTMS</td>
<td>European Rail Traffic Management Systems</td>
</tr>
<tr>
<td>ETCS</td>
<td>European Train Control System</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>EUG</td>
<td>ERTMS Users Group</td>
</tr>
<tr>
<td>IM</td>
<td>Infrastructure Manager</td>
</tr>
<tr>
<td>INEA</td>
<td>Innovation and Network Executive Agency</td>
</tr>
<tr>
<td>ISO</td>
<td>International standard organisation</td>
</tr>
<tr>
<td>IP2</td>
<td>(Shift2Rail) Innovation Programme 2</td>
</tr>
<tr>
<td>LOC&amp;PAS (TSI)</td>
<td>Locomotive and Passenger</td>
</tr>
<tr>
<td>MAAP</td>
<td>Shift2Rail Multi Annual Action Plan</td>
</tr>
<tr>
<td>MoU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>NSA</td>
<td>National Safety Authority</td>
</tr>
<tr>
<td>NTR</td>
<td>National Technical Rules</td>
</tr>
<tr>
<td>NRV</td>
<td>National Reference Values</td>
</tr>
<tr>
<td>NoBo</td>
<td>Notified Body</td>
</tr>
<tr>
<td>RAC</td>
<td>Risk Acceptance Criteria</td>
</tr>
<tr>
<td>RAM</td>
<td>Reliability, Availability, Maintainability</td>
</tr>
<tr>
<td>RINF</td>
<td>Register of Infrastructure</td>
</tr>
<tr>
<td>RU</td>
<td>Railway Undertaking</td>
</tr>
<tr>
<td>S2R JU</td>
<td>Shift2Rail Joint Undertaking</td>
</tr>
<tr>
<td>SMS</td>
<td>Safety Management System</td>
</tr>
<tr>
<td>TR</td>
<td>Technical Report</td>
</tr>
<tr>
<td>TSI</td>
<td>Technical Specifications for Interoperability</td>
</tr>
<tr>
<td>TS</td>
<td>Technical Specification</td>
</tr>
<tr>
<td>UIC</td>
<td>Union Internationale des Chemins de Fer</td>
</tr>
<tr>
<td>UNIFE</td>
<td>Union des Industries Ferroviaires Européennes</td>
</tr>
</tbody>
</table>