

Traffic CS - Major Design Decisions

Author(s)	No	Subsection title	Author(s)
	1	Introduction	Golebniak, Udo <udo.golebniak@siemens.com>
	2	Traffic CS System Architecture	Kemkemer Martin <martin.kemkemer@sbb.ch>
	3	Authorisation and Supervision of Train Movements	BADOT Bertrand <bertrand.badot@alstomgroup.com>
	4	Reduction of Safety Functionality	Chadwick, Simon <simon.chadwick@siemens.com>
	5	Safe Train Extent based on Sensor Fusion	Chadwick, Simon <simon.chadwick@siemens.com>
	6	Management of Configuration Data	Kemkemer Martin <martin.kemkemer@sbb.ch>
Abstract	Traffic CS prepared this document of major design decisions to inform the sector about the strategic orientation in the Traffic CS Design. The present document provides justifications for the taken major design decisions as requested in the remit task SC2.4. The preliminary results of the Traffic CS top-down design including the content of the Traffic CS System concept form the input for the present document.		
Classification	EU-RAIL-internal		
Status	Approved / To be Decided		
Version	1.0		
Last Change Date	19.02.2025		

Copyright	Brussels: Europe's Rail Joint Undertaking, 2025 © Europe's Rail Joint Undertaking, 2025 This document is drafted by and belongs to EU Rail. EU Rail encourages the distribution and re-use of this document, the technical specifications and the information it contains. EU Rail holds several intellectual property rights, such as copyright and trade mark rights, which need to be considered when this document is used. EU Rail authorizes you to re-publish, re-use, copy and store this document without changing it, provided that you indicate its source and include the following mention [EU Rail trade mark, title of the document, year of publication, version of document, URL]. EU Rail makes no representation or warranty as to the accuracy or completeness of the information contained within these documents. EU Rail shall have no liability to any party as a result of the use of the information contained herein. EU Rail will have no liability whatsoever for any indirect or consequential loss or damage, and any such liability is expressly excluded. You may study, research, implement, adapt, improve and otherwise use the information, the content and the models in the this document for your own purposes. If you decide to publish or disclose any adapted, modified or improved version of this document, any amended implementation or derivative work, then you must indicate that you have modified this document, with a reference to the document name and the terms of use of this document. You may not use EU Rail's trade marks or name in any way that may state or suggest, directly or indirectly, that EU Rail is the author of your adaptations. EU Rail cannot be held responsible for your product, even if you have used this document and its content. It is your responsibility to verify the quality, completeness and the accuracy of the information you use, for your own purposes.
-----------	---

Table of Content

1	Introduction	5
1.1	Scope	5
1.2	Purpose	7
1.3	Glossary	8
1.4	Abbreviations	12
1.5	Reference Documents	13
2	Traffic CS System Architecture	14
2.1	Topic	14
2.2	Traffic CS Interpretation	14
2.3	Impact	15
2.4	Design Decision	16
2.4.1	Detailed Description	17
2.4.2	Comparison with today	19
2.4.3	Alternative Design Options	19

2.5	Rationale	19
2.6	Assumptions and Precondition	21
3	Authorisation and Supervision of Train Movements	22
3.1	Topic	22
3.2	Traffic CS Interpretation	22
3.3	Impact	22
3.4	Design Decisions	22
3.4.1	Detailed Description	23
3.4.2	Comparison with Today	24
3.4.3	Alternative Design Option	25
3.5	Rationale	25
3.6	Assumptions and Precondition	27
4	Reduction of Safety Functionality	28
4.1	Topic	28
4.2	Traffic CS Interpretation	28
4.3	Impact	28
4.4	Design Decisions	28
4.4.1	Detailed Description	29
4.4.2	Comparison with today	29
4.4.3	Alternative Design Options	30
4.5	Rationale	31
4.6	Assumptions and Preconditions	31
5	Safe Train Extent based on Sensor Fusion	33
5.1	Topic	33
5.2	Traffic CS Interpretation	33
5.3	Impact	33
5.4	Design Decisions	33
5.4.1	Detailed Description	34
5.4.2	Comparison with today	34
5.4.3	Alternative Design Options	35
5.5	Rationale	35
5.6	Assumptions and Preconditions	36
6	Management of Configuration Data	37
6.1	Topic	37
6.2	Traffic CS Interpretation	37
6.3	Impact	37
6.4	Design Decisions	37
6.4.1	Detail Description	38

6.4.2 Comparison with today	38
6.4.3 Alternative Design Option	39
6.5 Rationale	39
6.6 Assumption and Preconditions	40

1 Introduction

1.1 Scope

This present document describes in more detail the key design decisions taken within the Traffic CS Domain of the ERJU System Pillar when writing the Traffic CS System Concept. [[Traffic CS System Concept](#)]. The System Concept is the leading document whereas this document provides more details on several key aspects.

The aim of this document is to lay out the principles to be applied for the on-going Traffic CS specification activities. It is possible that new findings in the course of the specification work will lead to future changes of design decisions. The document shall also serve as basis for consensus-building in the railway sector about the overall principles of the future standardised European CCS system.

The following table contains the major design decisions to be justified according to the tasks in the remit. The left column shows the original title from the remit. Due to the continuous clarification process partially those titles or terminology have been interpreted. Therefore the updated title/term is given in the second column, as it is used in the future Traffic CS design. Third column describes the interpretation of the respective design decision item by Traffic CS for justification in the present document. The details behind each interpretation are explained in the corresponding document section.

Topic title from remit	Subsection title	Interpretation by Traffic CS
Functional scopes of ETPS, PES and ATO-TS	2 Traffic CS System Architecture	Decisions about elements of the Traffic CS system architecture
Free placement of movement authorities (moving block)	3 Authorisation and Supervision of Train Movements	Decision to support a Train-Centric Authorisation of Movements and Train Movements "Anywhere to Anywhere".
Reduction of the SIL functionality	4. Reduction of Safety Functionality	Decision to separate functionality with high safety level from functionality with low safety level. Based on a lean and harmonised operational concept the number of functions allocated to the safety subsystem is reduced compared to current signalling.
Hybrid train detection and sensor fusion	5. Safe Train Extent based on Sensor Fusion	Decision to base Safe Train Extent on fusion of inputs from On-Board and Trackside.
Optimized ETCS version management	6 ETCS Version Management	This section will be added in a future version.
Efficient change of topology data	7 Management of Configuration Data	Decision to use external shared service(s) for provision of Infrastructure Data (e.g. containing topology data). These service(s) includes set up mechanism(s) allowing update of Infrastructure Data during runtime with minimised impact on operation.

The justification of each design decision (see section 2 to 7; except section 6) is done on the following sub-section structure in the present document.

Subsection	Title	Content
------------	-------	---------

Subsection	Title	Content
x.1	Topic	This section lists the specific design decision item, which is given in the remit task or proposed by other stakeholders for information of the sector. The stakeholders defined initially the SP requirements and CBO's to be achieved by the Traffic CS Specification and design work.
x.2	Traffic CS Interpretation	This section contains the detailed interpretation of the design decision item from Traffic CS Perspective. Due to ongoing clarification and specification work by Traffic CS the given remit items/titles partially have been adjusted to the current terminology. For this an explanation is given.
x.3	Impact	This section describes the technical / functional scope that is affected by the chosen solution for this remit item. The design decision may impact e.g. the logical allocation of functions between Traffic CS internal and external subsystems and the interface design.
x.4	Design Decisions	The section describes which design has been chosen by Traffic CS to cover the Topic. Note: All Design Decisions are defined as "Decision" work items: 
x.4.1	Detailed Description	The section comprises a detailed description of the design decision. Further it is explained how the issue is embedded in the overall Traffic CS System and entire SP design. This will be done e.g. on the base of an system architecture diagram.
x.4.2	Current Situation and alternative Design Options	Here is given a summary how the issue is managed in the legacy systems. Further alternative but not chosen design options are described briefly. - How does it look like in the legacy world? - Current situation - Alternative design options
x.5	Rationale	Why has this design been selected? Which and how Common Business Objectives (CBO's) are fulfilled by the design. What are the advantages. Note: • All rationales are defined as "Rational" work items:  • All rationales are linked to the corresponding Design Decision via an "relates to" link.
x.6	Assumptions and pre-conditions	Which assumptions have been taken in this context with regards to the design decisions. - What are necessary pre-conditions to implement this design decision? - What are consequences for other adjacent systems/interfaces and their functional scope caused by the design decision, e.g. in terms of their integration to an overall system?
x.7	Concerns from the sector	This section deals with major concerns of the sector in terms of the major design decisions. Such concerns will be derived, e.g.: - from earlier review comments on Traffic CS Deliverables - from dedicated questions of stakeholders In general, those concerns might be handled and answered on a FAQ Base (x.7.x - Headline as question)

1.2 Purpose

The major design decisions described in the present document are the result of the top-down system design process (SEMP V3.0) applied by Traffic CS. The design itself is based on the:

- CBOs defined by the stakeholders of the sector
- System requirements as listed in the Traffic CS System concept
- The first results on the evaluation of the harmonized ETCS Level 2 operation concept (without signals; except shunting signals if needed).

The following figure depicts the allocation of design decisions to the Traffic CS architectural elements.

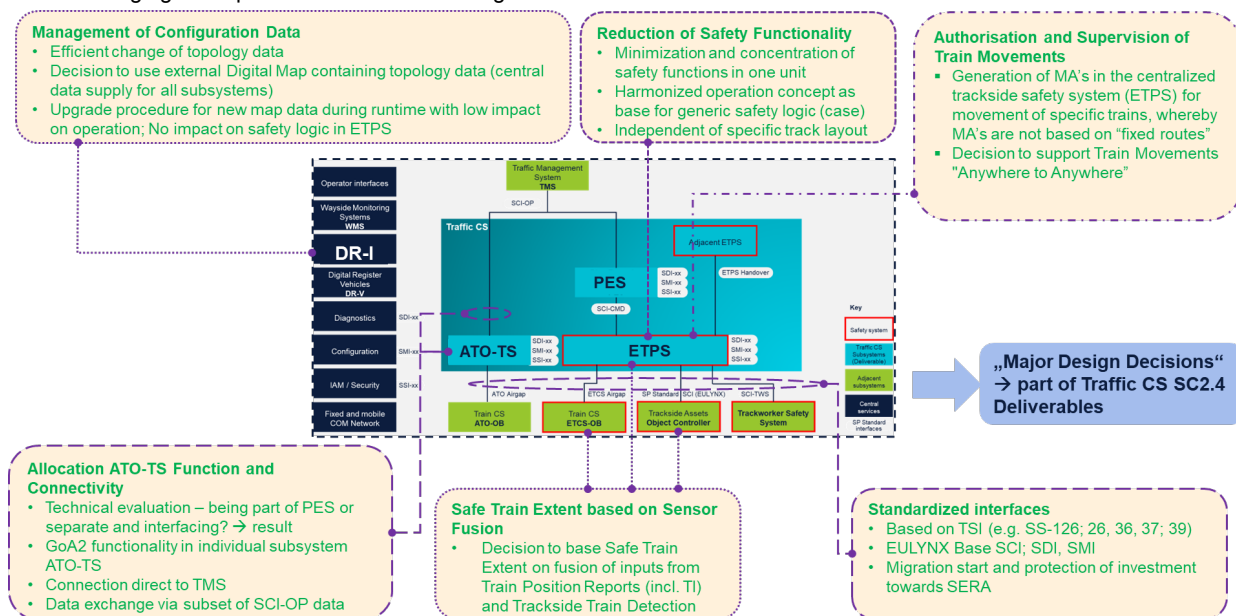


Figure 2 - Allocation of design decisions to the Traffic CS Architecture - 12/2024

NOTE: The design decisions in the present document do not include:

- the ATO GoA3/4 Functional scope, which will be part of a later design stage
- the issue of Enhanced Backward Compatibility (EBC)
 - NOTE: EBC is considered as subject of an ERTMS analysis in terms of: "there might be an intention that higher ETCS system versions (SV's) of trackside can interact with higher and also with lower ETCS system versions of onboards simultaneously". The current backwards compatibility ensures only that onboards with higher ETCS SV can run on trackside operated with lower ETCS SV's.
- migration scenarios, which are prepared in the ongoing SC2.4 Design phase.

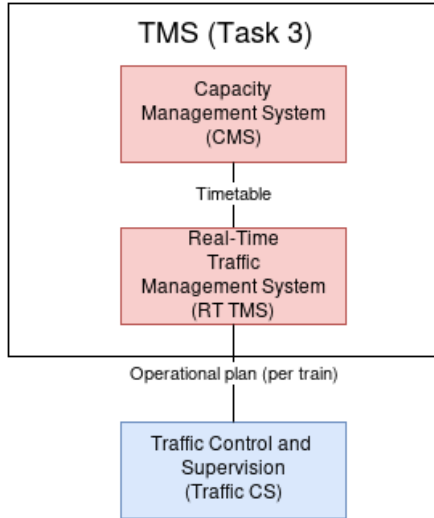
Please be aware, beside here described major design decisions there is also a larger number of minor design decisions which are covered in the System Concept as well (see [Traffic CS System Concept](#)).

1.3 Glossary

Term	Definition
Application Configuration Data	The Application configuration refers to use case-specific data for the Consuming Systems for a specific application. These can be detailed as SPT2TS-127776 - Infrastructure data i.e., Track edges, Track geometry, Track properties, Segment Profiles, etc. and SPT2TS-127777 - Vehicle data i.e., Braking and Traction efforts, Rolling coefficients, etc.
Area of Control	The Area of Control is the topologically limited extent and the infrastructural Trackside Assets in this geographical extent. The term is used here for defining the technical and operational responsibility of a Trackside Subsystem.
CCS System	The control command and signalling (CCS) system covers signalling, train control, positioning equipment and telecommunications.
Configuration Data	The (CCS/TMS) Configuration Data refers to a conglomerate of different configuration data required for CCS/TMS systems. These can be broadly classified as SPT2TS-127773 - Application Configuration Data and SPT2TS-127774 - System Configuration Data . CCS/TMS Configuration Data is provided via the configuration interface to the CCS/TMS Systems. The configuration data is assumed static within a version and changes occur only when there is a version change or increase, opposite to dynamic data, which may change within a configuration version of the system.
Digital Register - Infrastructure	The Digital Register Infrastructure (DR-I) is a database managing and providing static infrastructure data as central service. The data exchange between Traffic CS and this database is based on the EULYNX Standard Maintenance Interface SMI-xx via the subsystem Configuration (MDM).
ERTMS/ATO Trackside	ERTMS/ATO Trackside (ATO-TS) is the ERTMS/ATO trackside subsystem. ERTMS/ATO provides a set of non-safety functions related to speed control, accurate stopping, door opening and closing, and other functions traditionally assigned to a driver, while the safety of operation is still ensured by ETCS with regards to the speed and distance limits and also by other safe systems.
European Railway Traffic Management System	European Railway Traffic Management System (ERTMS) is a single European signalling and speed control system that ensures interoperability of the national railway systems, reducing the purchasing and maintenance costs of the signalling systems as well as increasing the speed of trains, the capacity of infrastructure and the level of safety in rail transport. (ERA definition)
European Trackside Protection System	The Trackside Protection System is the core system of Traffic CS, implementing the safety critical functions. The Trackside Protection System controls all Trackside Assets Control and Supervision (TACS) connected to ETPS, for example points, level crossings, and manages Movement Permissions for trains, whilst maintaining the safety of the railway.
FOULING POINT	The place where a vehicle standing on a converging line would come into contact with a vehicle on the other line.
Fixed Virtual Block	A Fixed Virtual Block is a Fixed Block where the limits are virtual and do not necessarily correspond to train detection boundaries.
Infrastructure data	Infrastructure Data is a detailed digital representation of the railway network that contains all infrastructure related information necessary for planning and performing railway operations, such as infrastructure characteristics, location and details of Field Elements, etc. The Infrastructure Data is static and remains unchanged until intended infrastructure updates occur.
Interlocking	Interlocking is a set of signaling devices which physically materializes, in the area of action of a switch post (junction, crossing of tracks, etc.) through mechanical, and / or electrical solutions. It allows train movement if the safety conditions have been met regarding train maneuver and signal control devices.
Legacy system	A legacy system is a system built without using SERA system specifications. It can use Class A or Class B train protection, e.g. interlocking with national light signals or interlocking with national ETCS L2 implementation without SERA operational rules.

Term	Definition
MOVEMENT AUTHORITY	Permission for a train to run to a specific location within the constraints of the infrastructure.
Movement Permission	Movement Permissions (MPs) are stored within the trackside safety system. A Movement Permission is an extent of track reserved within the trackside safety system for a particular Train Object to move. A Movement Permission includes all conditions under which the movement of the Train Object can be performed safely. A Movement Permission always refers to exactly one Train Object. A Movement Permission is distinct from a Movement Authority, which is sent from the trackside safety system to the ETCS On-Board.
Moving Block	Moving block is a concept where Movement Authorities can end at any location on the track. The Safe Train Extent of each train moves with that train based on its reported position and train integrity status and is not constrained to fixed block locations.
Operating State	The Operating State is the logical real-time representation of the actual state of the physical railway system in the Area of Control (e.g. information about the currently operating Train Units, the occupation of tracks, or the settings of Field Elements). The knowledge about the Operating State enables TMS to keep itself current with the operational situation in the Area of Control and to recognise deviations from an Operational Plan during execution. Further, it allows for identifying upcoming or existing conflicts between Operational Plans and developing appropriate countermeasures.
Operational Data	Operational Data refers to real-time information generated from daily operations and activities related to the functioning of railway systems, reflecting the current status of operations (e.g. locked position of a switch). Operational data is exchanged between CCS/TMS systems via Standard Communication Interfaces (SCI-xx). <i>Note: while Operational Data can be related to infrastructure or vehicle configuration data, it is clearly separated from SPT2TS-127779 - Configuration Data.</i>
Operational Plan	The Operational Plan is the result of the planning process performed by TMS. An Operational Plan will be issued by the TMS for any operationally relevant activity. This comprises all movements of Physical Train Units incl. shunting operations (Operational Movement), restrictions due to e.g., infrastructure maintenance and construction works, and warning measures during restrictions.
Parameter Data	Parameter Data define the system configuration data required for national and supplier-specific operative environments. A notable example of such data are ETCS national values. ETCS national values may be required for migration purposes and shall be replaced by SERA standardised values in the target system.
Plan Execution System	The Plan Execution System is a subsystem of Traffic CS which is responsible for: - processing the Operational Plans provided by the TMS, which are based on the Operating State of the railway within the Area of Control and - providing the Operating State within the Area of Control received from Trackside Protection System towards the TMS.
Radio Block Centre	Radio Block Centre is a computer-based system that elaborates messages to be sent to the train on basis of information received from external trackside systems and on basis of information exchanged with the on-board subsystems. The main objective of these messages is to provide movement authorities to allow the safe movement of trains on the Railway infrastructure area under the responsibility of the RBC. The interoperability requirements for the RBC are mainly related to the data exchange between the RBC and the on-board subsystem. (subset26-2)
Safe Train Extent	The Safe Train Extent represents the extent of the track that may be occupied by a connected train. It is calculated from train-side information (Confirmed Rear End and Max Safe Front End derived from the ETCS Position Report) and track-side information (track vacancy proving sections like track circuits or axle counters), taking into account the most recent information available from these train- and track-side information sources. Remarks: - The Safe Train Extent for a train will be updated when new information becomes available. - For a moving train, it is likely that the train will move outside the Safe Train Extent between update

Term	Definition
Single European Railway Area	Defining the fundamental design principles and process for adopting a functional architecture for rail as a system, with a focus on CCS, CMS and TMS supporting the implementation of the SERA (Single European Railway Area)
Subsystem - Maintenance and Data Management	The Subsystem - Maintenance and Data Management performs the services required for the operation of the EULYNX System. Service functions may be provided also to the adjacent systems.
System Configuration Data	The System Configuration data refers to the static data set required to configure systems with primary information before being put into operation. These data are elaborated as  SPT2TS-127829 - Parameter Data
TEMPORARY SPEED RESTRICTION	A planned speed restriction imposed for temporary conditions such as track maintenance.
Trackside Asset	Trackside Assets are elements on or near the track which are used to monitor (using sensors) and/or control (using actuators) the movement of vehicles through the railway network to provide a safe route through the railway network. They can be switchable or non-switchable and are controlled by the actors Trackside Asset Control and Supervision.
Trackside Assets Control and Supervision	The Trackside Assets Control and Supervision (Trackside Assets CS) with its subsystems (aka Object Controller) controls and supervises the Trackside Assets. 
Trackside Train Detection	The proof of the presence or absence of trains on a defined section of line 
Traffic Control and Supervision	Traffic Control and Supervision is the CSS Trackside System in charge of the control and supervision of the Railways Traffic. It includes ETCS Trackside and ATO Trackside.

Term	Definition
Traffic Management System	According to  SPT2TRAFFIC-3312 - CMS TMS System Concept the Traffic Management System (TMS) plans and controls the train runs to be performed. Internally the TMS is split in two parts:  <pre> graph TD subgraph TMS_Task3 [TMS Task 3] CMS[Capacity Management System CMS] RTTMS[Real-Time Traffic Management System RT TMS] CMS -- Timetable --> RTTMS end RTTMS -- "Operational plan (per train)" --> TCS[Traffic Control and Supervision Traffic CS] </pre> <i>Figure 1 - TMS Scope in System Pillar Architecture</i> • Capacity Management System (CMS) The CMS plans the timetable (train runs / routes / timings). • Real-Time Traffic Management System (RT TMS) The RT TMS controls the production (execution) of the timetable. It provides for every train run an Operational Plan to Traffic CS. RT TMS reacts to deviations (e.g. delays) and defines measures like re-routing or re-periodisation and updates the Operational Plans accordingly.
Train Control and Supervision	The Train Control and Supervision (Train CS) contains all CCS/TMS onboard functions, especially for ATO, ATP, radio, localisation, map services, train integrity and train length information, as well as advisory information systems used by the driver for operational reasons.
Train Object	Train Object is the object needed by the Traffic CS to manage the connected trains currently performing their mission. Note: This Train Object could nevertheless correspond to a train not (yet) localised by Traffic CS. If the train is localised by Traffic CS, the Safe Train Extent is the extent of the Train Object.
Usage Restriction Area	A Usage Restriction Area (URA) limits or constraints operation on a part within the Area of Control. URAs can be created according to an Operational Plan (e.g. for enabling construction works) or in response to an incident (e.g. as a mitigation measure). There are various limitations possible for a URA, e.g. speed restriction, full track closure or deactivate automatic operation.
Vehicle data	Vehicle Data is a detailed definition of the static train/vehicle characteristics i.e., Braking and Traction efforts, rolling coefficients, of the train, wagons, locomotives used for railway operations. 
Wayside Monitoring System	Wayside Monitoring Systems are used for diagnostic and maintenance purposes as well as for hazard identification. In this context WMS Systems are applied for monitoring of rolling stock (vehicles) and/or the wayside infrastructure. Some examples include (not exhaustive): - Acoustic Bearing Defect Detectors - Avalanche detection - Hot axle box detection.

1.4 Abbreviations

Abbreviation	Definition
ATO	Automatic Train Operation
ATO-TS	ERTMS/ATO Trackside
AoC	Area of Control
CBO	Common Business Objective
CCS	Control-Command and Signalling
CMS	Capacity Management system
CS	Control and Supervision
CTC	Centralized traffic control
DR-I	Digital Register - Infrastructure
ERTMS	European Railway Traffic Management System
ETCS	European Train Control System
ETPS	European Trackside Protection System
FVB	Fixed Virtual Block
IM	Infrastructure Manager
IXL	Interlocking
MA	MOVEMENT AUTHORITY
MB	Moving Block
MDM	Subsystem - Maintenance and Data Management
MP	Movement Permission
OB	On-Board
PES	Plan Execution System
RBC	Radio Block Centre
RT	Real Time
RU	Railway Undertaking
SERA	Single European Railway Area
SIL	Safety Integrity Level
SP	System Pillar
SPRA	System Pillar Reference Architecture
STE	Safe Train Extent
TA	Trackside Asset
TMS	Traffic Management System
TSR	TEMPORARY SPEED RESTRICTION
TTD	Trackside Train Detection
Traffic CS	Traffic Control and Supervision
URA	Usage Restriction Area
WMS	Wayside Monitoring System

1.5 Reference Documents

Following are listed main reference documents for this Major Design Decisions document:

No	Title	Link / Document index
1	Traffic CS System Concept	 Traffic CS System Concept
2	GRANULARITY CONCEPTS AND PRINCIPLES	 ARC-D2.3 Granularity Concepts and Principles
3	SEMP Systems Engineering Management Plan V3.0	 SEMP Systems Engineering Management Plan
4	Common Business Objectives	 Common Business Objectives
5		
6		

2 Traffic CS System Architecture

2.1 Topic

This section addresses an item from the SC2.4 Remit: “Functional scope of ETPS and PES and ATO-TS”.

This design criterion is a key requirement of the rail sector aligned by the stakeholders in the Common Business Objectives (CBO).

The following main objectives, defined by the sector in the CBO's, are to be fulfilled by the System Pillar Reference Architecture (SPRA) and specifically the Traffic CS system Architecture.

- **Establish Standardisation:** Establish a standardised reference system architecture for the TMS/CCS target system for rail operations with ETCS Level 2, enabling the implementation of a harmonised railway operation processes (CONUSE: [List of Operational Capabilities](#), work in progress) and employment processes (CONEMP: [Traffic CS Requirements for CONEMP](#)). This architecture gives the blueprint for TMS/CCS products to be manufactured by Industry partners and commissioned by Infrastructure Managers and Railway Undertakings across Europe. The standardised target system, along with the harmonised CONUSE and CONEMP, aims to reduce the technical and procedural diversity and complexity of today's systems and processes, providing a business case for Infrastructure Managers, Railway Undertakings, and Industry partners. The primary goal is to accelerate and expand the rollout of ETCS Level 2 throughout Europe, thereby establishing a Single European Railway Area (SERA).
- **Support Modularity:** The creation of a modular system architecture enables the adaptation of the TMS/CCS target system to national needs while decoupling the life-cycles of the subsystems involved, thus facilitating the updatability, interchangeability, and maintenance. Infrastructure Managers and Railway Undertakings possess the flexibility to define an application based on standard subsystems with a standardised behaviour while retaining some configuration options (e.g. On-Sight speed limit).
- **Optimize Safety Approvals:** Optimizing of safety approvals will facilitate the rollout of ETCS Level 2 across Europe and improve the updatability of systems.
- **Support of Migration Strategies:** The TMS/CCS target system will be specified in a way that different national migration strategies and rollout plans - which are strongly varying across the European Railways (IM's and RU's) in terms of technology, schedules etc. - are supported.

The System Pillar Reference Architecture (SPRA) is a reference specification of the TMS/CCS target system which has to be aligned by the sector stakeholders (Infrastructure Managers, Railway Undertakings, Suppliers). It is designed to improve the efficiency, safety, and interoperability of railway operations across Europe, ultimately supporting the goals of the Single European Railway Area (SERA).

2.2 Traffic CS Interpretation

Traffic CS is as a modular and standardised system that integrates various subsystems, including the Plan Execution System (PES), the European Trackside Protection System (ETPS) and ATO Trackside (ATO-TS). The architecture of Traffic CS is designed to provide flexibility and scalability, enabling the system to adapt to different operational contexts and requirements. By allowing a set of harmonised operational rules, the Traffic CS system architecture aims to streamline processes, reduce complexity, and improve the overall efficiency. Finally, the Traffic CS system architecture is intended to enhance safety approval efforts and reduce life-cycle costs for the TMS/CCS target system.

2.3 Impact

The design of the target Traffic CS system architecture is expected to have a positive impact on the railway operations processes (CONUSE) and the employment processes (CONEMP), the latter including various aspects such as system configuration, system integration, testing and validation, training, deployment, sustaining, and track adaptations.

Standardisation:

The standardisation of the system architecture has impact on:

- The efficient implementation of harmonized CONUSE and CONEMP within the TMS/CCS target system
- Reducing the technical and procedural diversity and complexity of today's systems and processes
- Provisioning a compelling business case for Infrastructure Managers, Railway Undertakings, and Industry partners to accelerate and expand the rollout of ETCS Level 2 throughout Europe
- The opportunity to Industry partners to manufacture standardised products for a European market.

Modularity

The modularity of the system architecture has several important impacts:

- Enhancing integration and maintenance efforts by decoupling the life cycles of individual components, allowing them to be developed, tested, and updated independently.
- Reducing dependencies and complexity within the system, which facilitates the implementation of adaptations and evolutions.
- Improving competitiveness by enabling faster innovation cycles and quicker responses to market demands.
- Promoting long-term sustainability through the use of adaptable components that can evolve alongside changing technologies and operational requirements

Performance and Scalability:

The performance and scalability of the system architecture has impact on:

- Ensuring optimal performance and scalability for different traffic volumes and traffic densities.
- Ensuring optimal performance and scalability for different dimensions of infrastructure data.

Reliability and Availability:

The allocation of functionality based on the reliability and availability requirements within the system architecture has impact on:

- Ensuring that each subsystem is designed to meet only the necessary reliability and availability levels, optimising performance and resource allocation.
- Allowing targeted maintenance strategies that focus on the individual reliability needs of each subsystem, thereby reducing overall maintenance efforts and costs.

Safety:

The allocation of functionality based on the safety requirements within the system architecture has impact on:

- Isolating safety implementation efforts and safety approval efforts to specific subsystem(s), reducing overall safety approval efforts and manufacturing costs of the TMS/CCS target system.

Migration Strategies:

2.4 Design Decision

2.4-1 - System Architecture Traffic CS

Please note:

- The figure also does not show all existing interfaces of neighbouring systems such as TMS or Train CS, as the focus of this diagram is on Traffic CS.
- The safety criticality shown in the figure corresponds to the current assumptions of Traffic CS. However, these assumptions might change in the progress of the system design process.
- The figure shows only the handover interface to adjacent SERA interface. Please find more details on connection to legacy systems in the System Concept.

ID	SPT2TRAFFIC-8620
----	------------------

Figure 3 - Traffic CS System Architecture

It is decided to allocate safety-critical functionality to a single subsystem, European Trackside Protection System.

ID	SPT2TRAFFIC-11050
----	-------------------

It is decided to allocate non-safety-critical functionality to the subsystems Plan Execution System and ATO-Trackside.

ID	SPT2TRAFFIC-11056
----	-------------------

2.4-5 - Allocation of Automatic Train Operation Trackside functionality to separate subsystem

It is decided to allocate the Automatic Train Operation Trackside functionality to a separate subsystem, ATO-Trackside.

ID	SPT2TRAFFIC-11057
----	-------------------

2.4-6 - Use of the specification standard ETCS for the interface to Train CS ETCS-OB

It is decided to use the specification standard ETCS from TSI CCS 2023 for the interface to Train CS ETCS-OB.

ID	SPT2TRAFFIC-11060
----	-------------------

2.4-7 - Use of the specification standards ATO for the interface to Train CS ATO-OB

It is decided to use the specification standard ATO from TSI CCS 2023 for the interface to Train CS ATO-OB.

ID	SPT2TRAFFIC-11059
----	-------------------

2.4-8 - Use of the specification standards EULYNX SCI-xx for the interface to Trackside Assets Object Controller

It is decided to use the specification standards EULYNX SCI-xx as the basis for the interface to Trackside Assets Object Controller.

ID	SPT2TRAFFIC-11058
----	-------------------

2.4-9 - Use of the specification standards EULYNX SMI-xx, EULYNX SDI-xx, EULYNX SSI-xx for the interfaces to Transversal Systems

It is decided to use the specification standards EULYNX SMI-xx, EULYNX SDI-xx, EULYNX SSI-xx as the basis for interfaces to Transversal Systems.

ID	SPT2TRAFFIC-11064
----	-------------------

2.4-10 - Specify new standardized interfaces

It is decided to specify new standardised interfaces where needed in order to fulfil the agreed CBOs, particularly in areas where there is currently no adequate interface specification available.

ID	SPT2TRAFFIC-11063
----	-------------------

2.4.1 Detailed Description

Modular System Architecture

The following subsystem of Traffic CS have been defined:

- **ATO Trackside System (ATO-TS):** ATO-TS facilitates the communication between the automatic train operation systems and the trackside infrastructure, translating operational plans into journey profiles for the onboard systems and managing the overall automation of train movements.
- **Plan Execution System (PES):** PES is responsible for processing operational plans received from the Traffic Management System (TMS) and managing the interaction with the European Trackside Protection System (ETPS), ensuring that train movements are executed efficiently.
- **European Trackside Protection System (ETPS):** The core safety critical functionality within Traffic CS is to control all trackside elements connected to ETPS, for example points, level crossings, and to manage movement permissions

for trains, whilst maintaining the safety of the railway. In order to do this, Traffic CS must maintain a dynamic operating state for its area of control, containing all track occupancies and movement permissions within the Area of Control.

Allocation of safety relevant functionality to subsystems

- **Automatic Train Operation - Trackside (ATO-TS):** non-safety-critical functionality will be allocated to ATO-TS. If safety-critical functionality is identified for GoA 3/4 the allocation of this functionality needs to be further analysed.
- **Plan Execution System (PES):** non-safety-critical functionality will be allocated to PES. If safety-critical functionality is identified the allocation of this functionality needs to be further analysed.
- **European Trackside Protection System (ETPS):** safety-critical functionality will be allocated to ETPS.

Use of specification standards for interfaces

Use specification standards for the following system interfaces:

- **ETCS Airgap** (ETPS to ETCS On-Board): usage of ETCS SS-026
- **ATO Airgap** (ATO Trackside to ATO On-Board): usage of ATO SS-125, ATO SS-126 and ATO SS-148
- **EULYNX-SCI** (Traffic CS to Trackside Assets): usage of EULYNX SCI-xx as the basis
- **EULYNX-SMI** (Standard Maintenance Interface): usage of EULYNX SMI-xx as the basis
- **EULYNX-SDI** (Standard Diagnostic Interface): usage of EULYNX SDI-xx as the basis
- **EULYNX-SSI** (Standard Security Interface): usage of EULYNX SSI-xx as the basis

Establish new specification standards for interfaces

Establish new specification standards for the following system interfaces:

- **SCI-OP:** Traffic Management System to Traffic CS
- **SCI-CMD:** PES to ETPS
- **SCI-TWS:** Traffic CS to Trackworker Safety System
- **Operational Interfaces:** ATO-TS, PES, ETPS to Operator Interface
- **ETPS Handover:** ETPS to Adjacent ETPS

Migration Strategies

The following decisions were made as a basis for the support of ETCS-equipped trains and support of Trackside Assets via Object Controllers:

- **ETCS Airgap:** Traffic CS will support trains equipped with ETCS Baseline 3 and above (ETCS Level 2 only). This means Traffic CS will initially implement ETCS System Version 2. The implemented ETCS System Versions can be raised over time.
- **Radio Connection to Vehicles:** Support use of FRMCS and GSM-R as the radio connection to vehicles.
- **EULYNX-SCI:** Support of trackside assets using at least EULYNX-SCI Baseline 4 Release 2.

Note: The support of migration strategies and the resulting system requirements for Traffic CS will be analysed on the basis of the existing SP work by the Traffic CS Migration Group.

2.4.2 Comparison with today

The proposed Traffic CS architecture differs significantly from current systems:

- Today there is no standardised CCS system architecture for European railways. Current systems often rely on tightly coupled components, leading to increased complexity and challenges in integration. The new architecture promotes modularity and standardisation, which simplifies integration.
- Safety functions in existing systems are typically apportioned across multiple systems leading to more dependencies and integration efforts.

2.4.3 Alternative Design Options

The following alternative design decisions have been identified as potentially disadvantageous for the system architecture:

Single-component solution for Traffic CS

While opting for a single component for the entire system can simplify the implementation and integration process, this approach would limit flexibility and innovation and present several typical disadvantages associated with monolithic systems, such as reduced scalability, increased complexity, higher risk of system failure, higher maintenance efforts, slower time to market.

Retaining existing legacy systems

Maintaining existing legacy systems without moving to a standardised architecture may provide temporary stability; however, relying solely on the further development of these systems hinders interoperability as it impedes the implementation of harmonised operational processes. In addition, the further development of national legacy systems and solutions is often unpromising as progress tends to be costly and slow due to the high customisation effort and limited capacity of manufacturers, which inhibits innovation and technological progress. Ultimately, strict adherence to legacy systems undermines the potential benefits of a standardised system architecture and hinders long-term operational efficiency within SERA.

2.5 Rationale

The design decisions were taken due to the following rationales:

SPT2TRAFFIC-11072 - System Architecture Traffic CS

Common Business Objective:  SPT1RS-221 - [standardized architecture\(1\)](#)

The modular Traffic CS system architecture was defined according to granularity rules given by Domain Architecture and Release Coordination in  [ARC-D2.3 Granularity Concepts and Principles](#). Evaluation of different system architecture definitions according to given granularity rules was done in  [Topic #2: Evaluation of subsystem architecture](#).

Linked Work Items	relates to :  SPT2TRAFFIC-8620 - System Architecture Traffic CS has parent :  SPT2TRAFFIC-8624 - Rationale
-------------------	---

SPT2TRAFFIC-11073 - Allocation of safety critical functionality to European Trackside Protection System

Common Business Objective:  SPT1RS-232 - [simplified standard safety components](#)

This decision ensures that all safety-critical functions are concentrated in a dedicated subsystem, enabling a common approach to system safety. Isolating safety-critical functions into a single subsystem provides a clear scoping for safety assessment. Changes to the safety subsystem should be less frequent, as the safety functions are minimised.

Linked Work Items	relates to :  SPT2TRAFFIC-11050 - Allocation of safety-critical functionality to European Trackside Protection System has parent :  SPT2TRAFFIC-8624 - Rationale
-------------------	---

SPT2TRAFFIC-11074 - Allocation of non-safety critical functionality to Plan Execution System and ATO-Trackside

Common Business Objective:  SPT1RS-226 - [systems: extensible capacity, scalability\(2\)](#)

This decision allows for a clear distribution of responsibilities between subsystems. It enables the allocation of the entire operational logic to two subsystems ATO-TS and PES, providing the flexibility to implement future operational enhancements without the always needing to modify the safety critical functionality within the ETPS.

Linked Work Items	relates to :  SPT2TRAFFIC-11056 - Allocation of non-safety-critical functionality to Plan Execution System and ATO-Trackside has parent :  SPT2TRAFFIC-8624 - Rationale
-------------------	--

SPT2TRAFFIC-11075 - Allocation of Automatic Train Operation Trackside functionality to separate subsystem

Common Business Objective:  SPT1RS-226 - [systems: extensible capacity, scalability\(2\)](#)

This decision allows focused optimisation of ATO functionality without interfering with other subsystems. It is beneficial to isolate this functionality in a separate subsystem, as ATO is considered an optional feature, and the PRAMSS requirements are assumed to be different and also evolve differently from those of the functionality within the PES.

Linked Work Items	relates to :  SPT2TRAFFIC-11057 - Allocation of Automatic Train Operation Trackside functionality to separate subsystem has parent :  SPT2TRAFFIC-8624 - Rationale
-------------------	---

SPT2TRAFFIC-11076 - Use of specification standards for interfaces

Common Business Objective:  SPT1RS-221 - [standardized architecture\(1\)](#)

The decision to use the specification standard is based on the need for interoperability and compatibility with existing systems. By adhering to recognised standards, we can ensure seamless integration, reduce development time, and enhance system reliability. This decision also facilitates compliance with regulatory requirements and promotes stakeholder confidence.

Linked Work Items	relates to :  SPT2TRAFFIC-11060 - Use of the specification standard ETCS for the interface to Train CS ETCS-OB
	relates to :  SPT2TRAFFIC-11059 - Use of the specification standards ATO for the interface to Train CS ATO-OB
	relates to :  SPT2TRAFFIC-11058 - Use of the specification standards EULYNX SCI-xx for the interface to Trackside Assets Object Controller
	relates to :  SPT2TRAFFIC-11064 - Use of the specification standards EULYNX SMI-xx, EULYNX SDI-xx, EULYNX SSI-xx for the interfaces to Transversal Systems
	has parent :  SPT2TRAFFIC-8624 - Rationale

SPT2TRAFFIC-11077 - Establishment of new specification standard for interfaces:

Common Business Objective:  SPT1RS-226 - [systems: extensible capacity, scalability\(2\)](#)

The decision to establish new specification standard for interfaces where no adequate standards currently exist is driven by the need to address specific operational challenges and technological advancements.

Linked Work Items	relates to :  SPT2TRAFFIC-11063 - Specify new standardized interfaces has parent :  SPT2TRAFFIC-8624 - Rationale
-------------------	---

2.6 Assumptions and Precondition

The implementation of this design criterion requires fulfilment of following pre-conditions:

Conflict-free, track-accurate, and time-specific operating plans

The Traffic Management System (TMS) generates conflict-free, track-accurate, and time-specific operating plans for each planned train journey. Both the Plan Execution System (PES) and ATO-TS adhere to these operating plans. The TMS is solely responsible for deviation management, conflict detection, and conflict resolution, updating the operating plan as necessary. As a result, PES and ATO-TS do not need to directly coordinate with one another.

3 Authorisation and Supervision of Train Movements

3.1 Topic

This section addresses an item from the SC2.4 Remit: "Train-Centric Authorisation of Movements".

This design criterion is a key requirement of the rail sector aligned by the stakeholders in the CBO's.

This section also addresses the following item from the SC2.4 Remit: "Train Movements Anywhere to Anywhere".

3.2 Traffic CS Interpretation

"Train-Centric Authorization of Movements" does not imply that the train will autonomously generate the authorization to move and command trackside assets.

Instead, "Train-Centric Authorization of Movements" means that route protection and train control features are combined. Based on the operational plan obtained from the TMS, Traffic CS will allocate a Movement Permission **for the designated train** and determine the Movement Authority **for the designated train**. This is different from the current approach where train authorisations are determined for predefined routes.

Movement Permission is defined within the Glossary.

"Train Movements Anywhere to Anywhere" means that Traffic CS moves away from traditional block systems that primarily depend on signals, track occupancy, established routes, and specific national regulations. Traffic CS permits movement ending at any location on the track (as long as this movement is allowed by the set of Safety Rules), a capability that is fundamentally restricted under current block-based signalling principles.

This design decision overcomes the functional split between route control (IXL) and train control (RBC) and introduces an integrated way of authorising train movements.

3.3 Impact

PES and ETPS are generic applications that require track topology information of the Area of Control to define and supervise the train movements. For instance, they necessitate the identification of Fouling Points in relation to Points and Crossings.

This information is detailed in section 7, which discusses the Use of Infrastructure Data for Topology Data.

The Generic Safety Logic (refer to Chapter 3.4) must be specified in detail to ensure that the Traffic Management System (TMS) and the PES subsystem within the Traffic Control System (CS) can submit requests with a high probability of success.

3.4 Design Decisions

The following design decision were taken regarding the authorisation and supervision of train movements:

3.4-1 - Movement Definition and Safety Approval

The Traffic CS PES defines train movements based on Operational Plan received from the Traffic Management System (TMS). In order to realize such train movement, the PES requests Trackside Asset commands and Train Movements Permission to the Traffic CS ETPS.

Given that the PES operates as a non-safety-critical system, the Traffic CS ETPS is responsible for verifying that the Trackside Asset commands and the requested train Movement Permissions meet safety requirements (see 3.4-3).

ID	SPT2TRAFFIC-9797
----	------------------

3.4-2 - Safety Supervision

The ETPS Generic Safety Logic supervises train movements and trackside assets to prevent railway accidents, e.g., collisions, derailments. ETPS Generic Safety Logic authorises train movements in safe way, enabling ETCS-OB to protect against over speed and over run.

ID	SPT2TRAFFIC-9796
----	------------------

3.4-3 - Generic Safety Logic

The Traffic CS ETPS is responsible for verifying that the Trackside Asset commands and the requested train Movement Permissions received from PES meet safety requirements before relaying them to the appropriate equipment.

This core function of the ETPS is the Generic Safety Logic.

The ETPS Generic Safety Logic incorporates a set of generic Safety Rules. To prevent accidents, Generic Safety Logic utilizes track topology to ensure there are no conflicts (e.g. overlays or incorrect point position) between Safe Train Extent, Movement Permission, and trackside asset information (such as track occupancy and point position). Generic Safety Logic is a generic application (according to CENELEC EN 50126) designed to ensure safety across various track topologies and configurations that can be configured within the application.

ID	SPT2TRAFFIC-9795
----	------------------

3.4-4 - Pure ETCS Level 2 area without Lineside Signals

The Area of Control will be a pure ERTMS/ETCS Level 2 area (as defined in SUBSET-026 4.0.0 chapter 2.6.6) with no Lineside signals in place. However, the requirement for shunting signals to facilitate shunting movements will be assessed. Shunting signals may be required if the train is not connected and has no consist information, i.e. in degraded situations or during migration.

ID	SPT2TRAFFIC-10669
----	-------------------

3.4-5 - Replacing Traditional Fixed Block Concept by movement from anywhere to anywhere

The Traffic Control System (Traffic CS) moves away from traditional systems (IXL) that primarily depend on signals, track occupancy, established routes, and specific national regulations.

The introduction of Generic Safety Logic permits movement from any location to any location on the track (as long as this movement is allowed by the set of Safety Rules), a capability that is fundamentally restricted under current signaling methods.

Movement Permission will be dynamic without predefined start (from Anywhere) or end (to Anywhere).

There are no longer routes with fixed starts and end locations. TMS nevertheless can still request trains to stop at fixed locations by the Operational Plan.

ID	SPT2TRAFFIC-9798
----	------------------

3.4.1 Detailed Description

The ETPS is responsible for maintaining safe separation of trains and trackside protection through the following mechanisms:

1. Handling Trackside Asset Control and Supervision (TACS) command requests and Movement Permission requests received from PES, based on a set of Generic Safety Rules.
2. Utilizing the track topology of specific lines as configured within the ETPS Generic Application (see 3.4-3).
3. Exchanging ETCS messages with the Train CS.
4. Exchanging EULYNX messages with the TACS (e.g. Points object controllers, TTD).

The ETPS, classified as a safety critical system, implements Generic Safety Logic to perform several critical functions:

1. Checking Trackside Asset Control and Supervision (TACS) command requests and Movement Permission requests received from PES
2. Sending commands to switchable Trackside Assets (TACS), such as points and level crossings (where applicable)
3. Sending ETCS messages, including Movement Authorities, to Train Control Systems (Train CS)
4. Supervising train movements.

As part of the verification process within the ETPS Generic Safety Logic, before approving a Movement Permission request

received from PES, ETPS Generic Safe Logic performs checks to ensure that the request does not conflict with any existing Movement Permissions that have already been assigned to other trains.

This verification process is based on the established set of Generic Safety Rules, which are specifically applied to the relevant track topology.

This process is essential for maintaining safe and efficient train operations within the network.

3.4.2 Comparison with Today

Currently, the safe supervision of train separation within mainline railway systems is achieved by subdividing tracks into sections of fixed length, referred to as Fixed Block. This method allows only one train to occupy an individual section at any given time.

In accordance with national regulations, prior to enabling a train to transit from signal A to signal B, the Interlocking System (IXL) secures routes by setting the route/signal to a specified state/aspect.

It also ensures that this state/aspect is safe with respect to other routes/signals and trackside asset information, which encompasses factors such as point position, track occupancy, and level crossing status.

The IXL employs its own Safety Logic to conduct these route checks based on several criteria:

- National regulations
- The specific logic intrinsic to the IXL product
- The specific configuration processes and data structures of the IXL product
- Information received from the Train Management System (TMS)

Subsequently, the Radio Block Centre (RBC) generates movement authorities for the train based on information received from the IXL and data exchanged with on-board subsystems.

The RBC is responsible for appropriately allocating trains to routes and ensuring that the movement authorities correspond with the route settings and signals sent by the IXL. This makes RBCs overly complex, especially for judging sudden stop aspects on signals or figuring out, which proceed aspect shall lead to an MA for which train.

The RBC also possesses its own Safety Logic to oversee train movements according to:

- National regulations
- The specific logic relevant to the RBC product, which includes assigning trains to routes, verifying and defining movement authorities before dispatch, and determining the timing and content of messages to send to trains
- The specific configuration processes and data structures for the RBC product
- Information procured by the IXL through non standardised interface
- Optionally, information received from the Train Management System (TMS)

This structure delineates the safety logic into two distinct domains: the RBC, which is mainly train-centric, and the IXL, which is track-centric, within the current framework.

Moreover, there is a lack of harmonization in safety logic between different Infrastructure Managers (IM) and various suppliers.

The proposed solution advocates for a Generic Safety Logic within a single domain: the European Trackside Protection System (ETPS).

This harmonized Generic Safety Logic will be established for SERA and will adhere to:

- Standardized Safety Rules
- Track topology specified in a standard format
- Standardized interfaces between Systems

Additionally, the operational management of train movement will be overseen by the PES (non-safety-critical level system), functioning independently from the Generic Safety Logic.

By implementing this Generic Safety Logic, movement will be possible from any location to any location, and all movements will be authorized as long as they comply with the established Safety Rules.

Connection to existing TMS solutions using fixed block can be done via an adapter as described in the migration section of

the System Concept.

3.4.3 Alternative Design Option

There are alternative design options:

Maintaining current separation between IXL and RBC

The alternative presented here involves maintaining the current separation of knowledge between route control (IXL) and train control (RBC).

The significant drawback of this approach is that it limits our ability to address the operational and safety challenges arising from the increased number of interfaces to be considered as a result of this division.

To overcome these obstacles, substantial investments would be necessary to harmonize the RBC-IXL interface, as well as to provide the associated information required for improved integration. While some solutions, such as the SCI-RBC, currently exist, they would require a major overhaul to meet the needs.

More smaller TTD Sections

The alternative to the implementation of functionalities permitting train movement to anywhere is a refinement of the fixed section solution, subdividing the lines in very short sections.

Retaining fixed blocks would probably lower the change effort for operational processes and existing products. It would however significantly increase the effort in engineering, configuration, approval and installation cost of trackside train detection equipment. Additionally, maintenance and other lifecycle costs would rise as the number of installed Trackside Assets increases.

Fixed Virtual Block or Hybrid Train Detection

The alternative to the implementation of functionalities permitting train movement to anywhere is a refinement of the fixed section solution into virtual subsections. The advantage of this would be a clearer evolution from current systems. The disadvantage of this is that Traffic CS would need to define such a system in addition the desired system without blocks, and there is limited effort available for the work within Traffic CS.

3.5 Rationale

The design decisions were taken due to the following rationales:

SPT2TRAFFIC-9802 - Generic Safety Logic

The Generic Safety Logic is fundamental to avoid operational and safety obstructions resulting from a separation of route and train control functionality. It overcomes the functional split between route control (IXL) and train control (RBC), where typical IXLs have no knowledge of trains.

Linked Work Items	relates to :  SPT2TRAFFIC-9795 - Generic Safety Logic
	relates to :  SPT2TRAFFIC-9796 - Safety Supervision
	has parent :  SPT2TRAFFIC-8364 - Rationale

SPT2TRAFFIC-9803 - Removing Fixed Block Routes

By removing traditional route based logic, we are moving from a signalling system that is designed specifically to support a limited set of operational moves, to a signalling system where all movements on the layout are theoretically possible (if allowed by the Safety Rules).

Linked Work Items	relates to :  SPT2TRAFFIC-9798 - Replacing Traditional Fixed Block Concept by movement from anywhere to anywhere
	relates to :  SPT2TRAFFIC-10669 - Pure ETCS Level 2 area without Lineside Signals
	has parent :  SPT2TRAFFIC-8364 - Rationale

SPT2TRAFFIC-9804 - Operational management of train movement

The operational management of train movement will be overseen by the PES (non-safety-critical system), functioning

independently from the Safety Logic.

Linked Work Items	relates to :  SPT2TRAFFIC-9797 - Movement Definition and Safety Approval
	has parent :  SPT2TRAFFIC-8364 - Rationale

SPT2TRAFFIC-9805 - Generic Safety Logic allows a generic approval and authorization

Common Business Objective:  [SPT1RS-230 - safety logic with generic safety approval](#)

Generic Safety Logic allows a generic approval and authorization based on a set of Generic Rules defined for SERA. Generic Safety Logic just needs a reliable input of Infrastructure Data and train information and will ensure safety on this basis, with a minimum set of validation activities to be performed during deployment. Appropriate methods, such as formal proving, must be employed to address the integration of the ETPS application with Infrastructure Data, in addition to adhering to "standard" integration methods. The safety approval will be performed independently of the operational needs that are managed by PES, so, outside the Generic Safety Logic.

Linked Work Items	relates to :  SPT2TRAFFIC-9795 - Generic Safety Logic
	relates to :  SPT2TRAFFIC-9796 - Safety Supervision
	has parent :  SPT2TRAFFIC-8364 - Rationale

SPT2TRAFFIC-10573 - Generic Safety Logic allows new technologies and harmonized processes

Common Business Objective:  [SPT1RS-169 - new technologies, harmonized processes](#)

Generic Safety Logic enhances interoperability and contributes to improved performance, such as reduced train headway, when sufficient reporting trains provide confirmed train length and confirmation of train integrity, as its set of Generic Safety Rules allows train movement from anywhere to anywhere if allowed by the Safety Rules.

Linked Work Items	relates to :  SPT2TRAFFIC-9795 - Generic Safety Logic
	has parent :  SPT2TRAFFIC-8364 - Rationale

SPT2TRAFFIC-10574 - Generic Safety Logic allows to automate lifecycle processes

Common Business Objective:  [SPT1RS-193 - automate lifecycle processes](#)

Generic Safety Logic improves asset construction, engineering, commissioning and authorisation as an important part of these activities will be performed for SERA. This is achieved by using generically specified logic, with specific track topology being provided separately from the logic, in a standardised format, thus enabling simpler processes.

Linked Work Items	relates to :  SPT2TRAFFIC-9795 - Generic Safety Logic
	has parent :  SPT2TRAFFIC-8364 - Rationale

SPT2TRAFFIC-10576 - Moving block allow to reduce train headway

Common Business Objective: [SPT1RS-177 - precise control of traffic flow, short train-ahead time](#)

Moving Block increases capacity utilisation of the rail by making use of a more precise control of traffic flow, shortening train-ahead time and increasing the numbers of trains per hour.

Linked Work Items	relates to :  SPT2TRAFFIC-9798 - Replacing Traditional Fixed Block Concept by movement from anywhere to anywhere
	has parent :  SPT2TRAFFIC-8364 - Rationale

SPT2TRAFFIC-10577 - ETPS allows to reduce the number of trackside assets

Common Business Objective: [SPT1RS-195 - less trackside assets](#)

The capability of ETPS to use train position and train integrity information may enable reduction of trackside assets such as train detection systems. The use of Moving Block may reduce the number of Marker Boards.

Linked Work Items	relates to :  SPT2TRAFFIC-9798 - Replacing Traditional Fixed Block Concept by movement from anywhere to anywhere
	relates to :  SPT2TRAFFIC-10669 - Pure ETCS Level 2 area without Lineside Signals
	has parent :  SPT2TRAFFIC-8364 - Rationale

SPT2TRAFFIC-10578 - Generic Safety Logic improves standardisation

Generic Safety Logic improves standardisation. Generic Safety Logic is only possible with standardised Operational Rules, and removal of line-side signals. The use of Generic Safety Logic contributes to the following Common Business Objectives:

-  [SPT1RS-196 - increase market size by standardisation](#)
-  [SPT1RS-221 - standardized architecture\(1\)](#)
-  [SPT1RS-232 - simplified standard safety components](#)
-  [SPT1RS-218 - modularity](#)
-  [SPT1RS-240 - systems allow simpler tender procedures](#)
-  [SPT1RS-239 - reusable and simpler contract standards](#)
-  [SPT1RS-238 - simplify certificates and their impacts](#)
-  [SPT1RS-249 - worldwide adoption](#)
-  [SPT1RS-254 - standard know how](#)

Linked Work Items	relates to :  SPT2TRAFFIC-9795 - Generic Safety Logic
	has parent :  SPT2TRAFFIC-8364 - Rationale

3.6 Assumptions and Precondition

The implementation of this design criterion requires fulfilment of following pre-conditions (see also [4.6 - Assumptions and Preconditions](#)):

TMS and PES are aware of Safety Rules

TMS and PES are also aware of the set of Safety Rules applied by the Generic Safety Logic and the Operational Plan is defined considering this logic. This is to avoid the rejection of the requests by the ETPS.

Train position for train movement from any A to any B.

The effectiveness of train movements from any point A to any point B relies on the capability of a sufficient number of trains to report their position and their train integrity. Additionally, PES must be able to request movements between any A and B.

Correct data for Balises, TTDs in the Digital Register - Infrastructure

The algorithm is dependent on ETPS being provided with correct Balise positions, and correct locations for Trackside Train Detection boundaries in the topology data to be provided by the Digital Register - Infrastructure.

4 Reduction of Safety Functionality

4.1 Topic

This section addresses an item from the SC2.4 Remit: "Reduction of the SIL functionality".
This design criterion is a key requirement of the rail sector aligned by the stakeholders in the CBO's.

4.2 Traffic CS Interpretation

This item is interpreted by Traffic CS to include Design Decisions relating to the following:

- Minimising the safety critical functionality within Traffic CS
- Standardising the safety critical functionality within Traffic CS

The core safety critical functionality within Traffic CS is to control all trackside elements connected to ETPS, for example points, level crossings, and to manage movement permissions for trains, whilst maintaining the safety of the railway. In order to do this, Traffic CS must maintain a dynamic operating state for its area of control. This comprises e.g all trackside elements connected to ETPS and contains all track occupancies and movement permissions within the Area of Control.

4.3 Impact

Traffic CS will contain a single generic safety system for all safety critical functionality, called "European Trackside Protection System" (ETPS), as described in Section 2 Traffic CS System Architecture.

All safety critical functions will be allocated to ETPS, and non-safety critical functions will mainly be allocated to other subsystems, for example to PES.

ETPS functions will be specified generically, independently of track layout, and in accordance with the harmonised operation concept.

This decision also affects the content of the standardised interface between PES and ETPS.

4.4 Design Decisions

The following design decision were taken regarding reduction of safety functionality:

4.4-1 - Reduction of Safety Functionality

Traffic CS will contain a single subsystem for all safety critical functionality, called "European Trackside Protection System" (ETPS), as described in Section 2 Traffic CS System Architecture. This will be achieved by restricting ETPS to safety critical functions so far as is possible, and by using the PES to perform functionality which is not safety critical.

ID	SPT2TRAFFIC-9791
----	------------------

4.4-2 - Standardisation of the safety critical functionality

Traffic CS will define the safety critical functionality within ETPS to an extent that ensures standardised behaviour at its external interfaces

ID	SPT2TRAFFIC-11326
----	-------------------

4.4.1 Detailed Description

Safety critical functions will be allocated to ETPS. The functionality of ETPS will be described in a generic manner. This will be achieved by basing the function descriptions on:

- The harmonised operation concept
- Utilisation of the track topology specified in a standard format

Functionality which is not safety critical will be allocated to other subsystems. Some functionality which is traditionally in Interlocking systems will be assigned to other subsystems. For example, separation of point commands from path locking by using PES. In this example, PES will make separate requests to ETPS:

- Point movement request ETPS will command points to move if it is safe to do so
- Movement Permissions request ETPS will assign Movement Permissions if it is safe to do so, thereby locking the path.

The safety critical function to be allocated to ETPS will include those safety critical functions required to manage degraded modes.

The main functions of the European Trackside Protection System (ETPS) are:

1. Maintain an up-to-date Operating State of the railway within the Area of Control.
2. Process requests from PES for movements of trackside infrastructure
3. Process requests from PES for Movement Permissions for trains
4. Process requests from Operator relating to manual operations, for example for Usage Restrictions
5. Release Movement Permissions based on the movement of trains
6. Detect and react to unsafe situations detected within ETPS, based on external inputs and internal Operation State, for example loss of point detection within assigned Movement Permission for a train.
7. Manage communications to Trackside Assets, Trains and adjacent ETPSs

The Operating State contains the dynamic data within ETPS, so it includes:

- Status of all Trains currently within the Area of Control
- Status of all Trackside Assets
- Track Occupancy information
- All Movement Permissions
- All Usage Restrictions, including TSR

ETPS will include some non-safety functions. For example, ETPS will support interfaces for diagnostics and maintenance.

4.4.2 Comparison with today

There are some significant differences between the architecture implied by these design decisions, and the typical architecture for trackside signalling systems today:

1. In ETCS systems today, there are typically two separate safety-critical subsystems, Interlocking (IXL) and Radio Block Centre (RBC).
In the proposed architecture, there is a single safety critical subsystem: European Trackside Protection System (ETPS).
2. In signalling systems today, there are functions within the safety-critical subsystems (IXL, RBC), which are not strictly safety functions. For example, the interface to the Interlocking is typically a Route setting interface, with the Interlocking responsible for controlling the points which need to be controlled and detected before a Route can be set.
In the proposed architecture, ETPS will only move Points in response to a request to move points from PES, so long

as it is safe to do so. In the proposed architecture, ETPS will only assign a Movement Permission for a train, in response to a request from PES, if the points are already in the required positions, so long as it is safe to do so.

3. In the signalling systems today, routes are set if the interlockings permit without reference to which train the route is being set for, and the RBC then has to determine which route is to be used for each train.

In the proposed architecture, there is a single safety critical subsystem: European Trackside Protection System (ETPS), with each Movement Permission assigned to a specific train.

4. In signalling systems today, there are different standards in different railways, because there are national Operating Rules, which require different signalling functions.

It is proposed that the new architecture is based on the harmonised operating concept, together with standardised safety functions.

5. In signalling systems today, there is bespoke data for each installation. In the proposed architecture, there will be standardised topology data (Infrastructure Data).

For an example of the typical architecture today, see the ERTMS reference architecture in Subset-026 chapter 2.5.

4.4.3 Alternative Design Options

There are alternative design options:

Fixed virtual block

There are alternative design options: It would be possible to define ETPS based on a fixed virtual block concept, with a route setting interface, based on the harmonised operating concept, possibly as an interim solution.

The advantage of this would be a clearer evolution from current systems.

The disadvantage of this is that Traffic CS would need to define such a system in addition the desired system without blocks, and there is limited effort available for the work within Traffic CS. A short-term solution of introducing HTD as a National solution is not in the scope of System Pillar. For the target SERA and ETPS specification target, no variant is foreseen for Fixed Virtual Block in the safety system. The operational scenarios described in the HTD concept will be considered in the design of the specifications for Safe Train Extend (explained also in System Concept FAQ).

Include non-safety functions in ETPS

It would be possible to define ETPS with standardised functionality, based on Infrastructure Data, but still including some non-safety functions.

For example, it could be that points would be controlled as a result of receiving a Movement Permission request, in a manner similar to a route-setting interlocking today.

The advantage of this would be a clearer evolution from current systems, in particular for the control system interface.

The disadvantage is that this does not minimise the functionality to be performed within ETPS.

The advantage can also be achieved by adapting PES to accept route setting commands from TMS.

Non standardised topology data

It would be possible to leave the definition of topology data to be defined by those implementing ETPS.

If it is still intended to use a standardised format for Digital Register - Infrastructure, then an additional off-line engineering function would be required to translate to the bespoke ETPS data format.

The advantage of this would be clearer evolution from current systems, in particular for data engineering.

The disadvantage is that this does not standardise the functionality to be performed by ETPS.

A further disadvantage is that use of bespoke topology data for ETPS hinders the sharing of topology data with other subsystems.

4.5 Rationale

The design decisions were taken due to the following rationales:

SPT2TRAFFIC-11067 - Simplified standard safety components

Common Business Objective:  [SPT1RS-232 - simplified standard safety components](#)

Safety critical components of a system should be optimized and simplified through design by moving away from bespoke solutions.

Linked Work Items	relates to :  SPT2TRAFFIC-9791 - Reduction of Safety Functionality has parent :  SPT2TRAFFIC-8305 - Rationale
-------------------	--

SPT2TRAFFIC-11070 - Safety logic with generic safety approval

Common Business Objective:  [SPT1RS-230 - safety logic with generic safety approval](#)

The safety logic shall have a generic approval and authorisation in which it is proven that it just needs a reliable input of topology information and train information and will assure safety on this basis. The target within Traffic CS is the generation of a lean, stable and generic Requirements Specification for Traffic CS subsystems, and for a set of generic Interface Specifications within Traffic CS, based on the harmonised Operational Concept. Fulfilling this target facilitates achievement of generic safety approval.

Linked Work Items	relates to :  SPT2TRAFFIC-9791 - Reduction of Safety Functionality has parent :  SPT2TRAFFIC-8305 - Rationale
-------------------	--

SPT2TRAFFIC-11071 - Deliver affordable system updates

Common Business Objective:  [SPT1RS-190 - Changeability and upgradeability\(1\)](#)

Common Business Objective:  [SPT1RS-189 - Changeability and upgradeability\(2\)](#)

The safety logic will process topology data (Infrastructure Data) provided in a standardized format by the Digital Register - Infrastructure. In order to update ETPS following changes to the physical track layout, a new version of the topology data will be required. The Traffic CS system will allow the same updated topology data to be used by different system components (ETPS, PES, ATO-TS), thus simplifying the process of updating the Traffic CS system following a changes to the physical track layout.

Linked Work Items	relates to :  SPT2TRAFFIC-9791 - Reduction of Safety Functionality has parent :  SPT2TRAFFIC-8305 - Rationale
-------------------	--

4.6 Assumptions and Preconditions

The implementation of this design criterion requires fulfilment of following pre-conditions:

There is a harmonised Operational Concept

This assumption is required in order to enable a generic specification for the safety functions within the ETPS subsystem. Furthermore, the split into vital and non-vital functions and their allocation to the respective subsystems will also base on a lean interpretation of the harmonised Operational Concept.

Engineering Data is provided by the Digital Register

Engineering data for specific locations will be provided in a standardised format by the Digital Register - Infrastructure. The Engineering data will be provided via a standardised interface based on SMI-xx.

This assumption is required in order to enable standard safety-related functions to be performed.

Strict separation of safety functionality and topological data

All topology-related data shall be part of the Digital Register only. I.e. a modification of those data e.g. caused by track layout

changes shall not affect the safety functionality and be limited to the engineering data in the Digital Register.

5 Safe Train Extent based on Sensor Fusion

5.1 Topic

This section addresses an item from the SC2.4 Remit called: "Hybrid train detection and sensor fusion".

In this context the inputs from On-Boards and Trackside are safety critical inputs to the ETPS. Both can be used together to create "Safe Train Extents". Safe Train Extents are the representation of track occupancy by trains known to ETPS.

5.2 Traffic CS Interpretation

This item is interpreted by Traffic CS to include Design Decisions relating to the maintaining Safe Train Extents within ETPS based on fusion of inputs from:

- ETCS On-Boards, for example Train Position Reports
- Trackside, for example from Trackside Train Detection

There will be a Safe Train Extent for each connected train, giving ETPS an internal representation of the track occupied by each connected train within the ETPS area of control.

The algorithm within ETPS will cover degraded modes of operation under failure conditions. For example, the algorithm within ETPS will need to retain the Safe Train Extent for a train which ceases communications from On-Board to Trackside.

5.3 Impact

This topic will have an impact at system level, as it will result in greater precision of track occupancy by a train, compared with traditional block occupancy. This greater precision can be used within the system to reduce the spacing between trains, compared with a traditional block-based approach, thus reducing headway / increasing capacity.

This topic will have impact within ETPS, which will contain the fusion algorithm to create the Safe Train Extent for a train. The algorithm to combine trackside and on-board inputs to create Safe Train Extents will be part of the core function within ETPS to retain up-to-date knowledge of track occupancy. The Safe Train Extents of trains will be part of the Operating State, used within ETPS for the safety logic.

This topic will have an impact on PES, as the Operating State will be reported to PES, and the Operating State will include Safe Train Extents for trains.

This topic will have an indirect impact on TMS, as the PES will report the Operating State to TMS.

This topic will have an impact on the definition of the interfaces between:

- ETPS and PES
- PES and TMS

5.4 Design Decisions

The following design decision were taken regarding the safe train extent based on sensor fusion:

5.4-1 - Use Safe Train Extent for Trains

Within TPS, Traffic CS will implement the concept of "Safe Train Extent". The Safe Train Extent represents the extent of the track that can be occupied by a connected train.

The Safe Train Extent will be determined by sensor fusion, based on inputs from:

- ETCS On-Boards, for example Train Position Reports
- Trackside, for example from Trackside Train Detection

ID	SPT2TRAFFIC-10086
----	-------------------

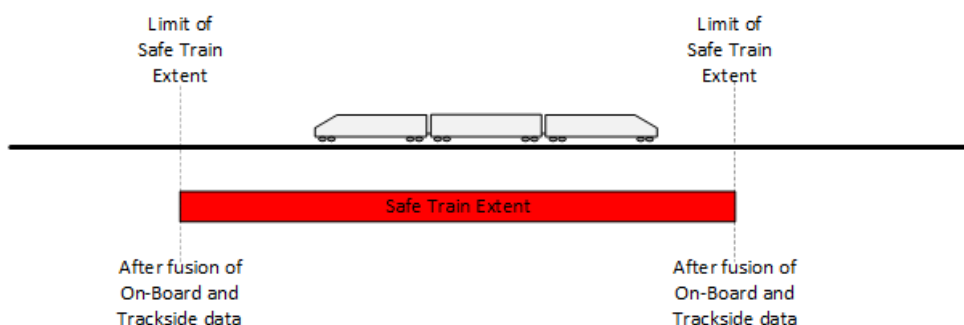
5.4.1 Detailed Description

The Traffic CS Glossary contains a definition of Safe Train Extent. The following is a summary of that definition:

The Safe Train Extent represents the extent of the track that may be occupied by a train. It is calculated from On-Board and Trackside inputs, taking into account the most recent information available from these sources.

The Safe Train Extent for a train will be updated when new information becomes available.

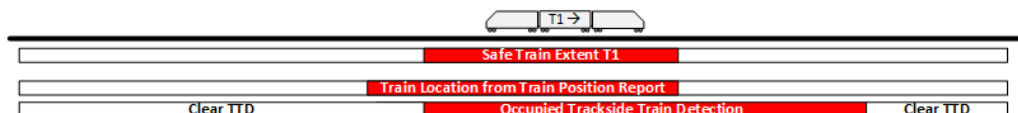
The figure below shows that the Safe Train Extent will typically be longer than the physical length of the train, as it must encompass the physical train.



The fusion algorithm to combine On-Board and Trackside inputs to create Safe Train Extent will be implemented within the ETPS subsystem, as it is a safety function.

The Safe Train Extent of a train will be used within ETPS to represent track occupancy corresponding to the train.

An example of the fusion of Train Position Report and Trackside Train Detection inputs is shown in the following figure.



The use of TTD enables the management of trains even when train integrity cannot be confirmed, specifically accommodating trains that are not equipped with a Train Integrity Monitoring System (TIMS).

This approach eliminates the need to wait for the complete retrofitting of all trains with TIMS.

This concept allows 2 or more trains to be independently localised inside the same occupied TTD.

The Safe Train Extent will also be determined for trains with no train integrity confirmed.

However, it is important to note that for trains without TIMS, the headway for the following train will be adversely affected, as the track vacancy cannot be verified between the TTD limit and the rear of the train being pursued.

The use of TTD is not mandatory. However, for areas without TTD, there will be consequences for recovery from degraded situations, and for the extent of track occupation by trains which are not able to provide confirmation of train integrity.

5.4.2 Comparison with today

In current main line signalling systems, track occupancy is typically determined using the status of fixed blocks, typically using Trackside Train Detection (track circuits or axle counters). Each block can be "Clear" or "Occupied". In addition, when using axle counters, a block can be "Disturbed". The status of the fixed blocks is then used within the signalling logic, for example in interlockings and control systems.

5.4.3 Alternative Design Options

There are alternative design options:

More smaller physical TTD Sections

To achieve higher capacity the track could be segregated into smaller TTD sections requiring more physical equipment.

Disadvantage:

Such a procedure would contradict to CBO aiming on reduction of CAPEX/OPEX of wayside infrastructure.

Migrate to the SERA solution only when all trains are equipped with TIMS

A significant headway decrease could be achieved if all trains were equipped with TIMS enabling usage of on-board localisation only. However, by including use of TTDs, it is not necessary for all trains to be equipped with TIMS. See section 5.4.1.

Disadvantage 1:

There will be a gradually rollout of trains with TIMS in a migration phase taking a very long time. Such migration rollout plannings must base on common business cases of IM's and RU's and will take time. In the meantime trains which are already equipped with TIMS would not contribute to capacity increase until the last train is fitted and the line is converted to make use of confirmed train length.

Disadvantage 2:

If only on-board localisation is used, the recovery mechanism provided by also using Trackside Train Detection is not available.

Even if all trains are fitted with TIMS equipment, there are still scenarios where Trackside Train Detection is required, for example detection of unplanned movements, such as rolling wagons.

5.5 Rationale

The design decisions were taken due to the following rationales:

SPT2TRAFFIC-10543 - Greater precision of track occupancy

The use of Safe Train Extents based on sensor fusion enables greater precision of track occupancy and therefore permits more efficient use of the railway infrastructure (decreased headway, faster release of trackside assets).

Linked Work Items	relates to :  SPT2TRAFFIC-10086 - Use Safe Train Extent for Trains has parent :  SPT2TRAFFIC-8374 - Rationale
-------------------	--

SPT2TRAFFIC-11117 - Support of mixed fleets

The use of Trackside Train Detection as part of the sensor fusion enables trains which cannot provide confirmed train length, or which cannot confirm train integrity (e.g. with no TIMS, failed TIMS), to use the railway. The use of TTD will need to be assessed within each project, depending on the requirements for mixed traffic, and for recovery from degraded situations.

Linked Work Items	relates to :  SPT2TRAFFIC-10086 - Use Safe Train Extent for Trains has parent :  SPT2TRAFFIC-8374 - Rationale
-------------------	--

SPT2TRAFFIC-11118 - Fallback mechanism

The use of Trackside Train Detection as part of the sensor fusion provides a fallback mechanism for degraded operation in the event of a failure of radio communications with one or more trains. The use of TTD will need to be assessed within each project, depending on the requirements for mixed traffic, and for recovery from degraded situations.

Linked Work Items	relates to :  SPT2TRAFFIC-10086 - Use Safe Train Extent for Trains has parent :  SPT2TRAFFIC-8374 - Rationale
-------------------	--

SPT2TRAFFIC-11119 - Detect unexpected track occupancy

The use of Trackside Train Detection as part of the sensor fusion enables Traffic CS to detect unexpected track occupancy, and to implement safety reactions. The use of TTD will need to be assessed within each project, depending on the requirements for mixed traffic, and for recovery from degraded situations.

Linked Work Items	relates to :  SPT2TRAFFIC-10086 - Use Safe Train Extent for Trains has parent :  SPT2TRAFFIC-8374 - Rationale
-------------------	--

SPT2TRAFFIC-11107 - Capacity Increase

Common Business Objective:  [SPT1RS-170 - increase capacity](#)

Common Business Objective:  [SPT1RS-409 - implement a full system optimisation approach for better capacity](#)

The greater precision of the track extent occupied by each train permits an increase of capacity, for example by reducing the separation between trains, thus increasing capacity.

Linked Work Items	relates to :  SPT2TRAFFIC-10086 - Use Safe Train Extent for Trains has parent :  SPT2TRAFFIC-8374 - Rationale
-------------------	--

SPT2TRAFFIC-11110 - Reduce trackside assets

Common Business Objective:  [SPT1RS-195 - less trackside assets](#)

The use of sensor fusion can permit the reduction in the number of Trackside Train Detection sections, depending on the required recovery from degraded situations, and required support for mixed fleets (with / without train integrity).

For example, consider a degraded situation where a train is no longer able to confirm train integrity. If slower recovery is acceptable, there can be a smaller number of longer Trackside Train Detection sections. If fast recovery is required, then it is necessary to have a larger number of shorter Trackside Train Detection sections.

Linked Work Items	relates to :  SPT2TRAFFIC-10086 - Use Safe Train Extent for Trains has parent :  SPT2TRAFFIC-8374 - Rationale
-------------------	--

5.6 Assumptions and Preconditions

The implementation of this design criterion requires fulfilment of following pre-conditions:

Trackside Train Detection (TTDs) may not be present

Although the subject of this topic is sensor fusion, the system should be defined such that TTDs may not cover all the railway.

Not all trains can provide confirmed train length or can confirm train integrity in the medium term

For some trains it will not be possible. For other trains, there will be some time before the trains are fitted with TIMS. The system should be defined such a mixture of trains with and without the ability to provide confirmed train length can use the railway.

Correct data for Balises, TTDs in the Digital Register - Infrastructure

The fusion algorithm is dependent on ETPS being provided with correct Balise positions, and correct locations for Trackside Train Detection boundaries in the topology data to be provided by the Digital Register - Infrastructure.

6 Management of Configuration Data

6.1 Topic

This section addresses an item from the SC2.4 Remit: 'Efficient change of topology data'.

This design criterion is a key requirement of the rail sector aligned by the stakeholders in the Common Business Objectives (CBO).

6.2 Traffic CS Interpretation

Since the topology data is part of the Configuration Data provided to Traffic CS by centralised services (SP Domain Transversal CCS), and the design decision and rationales for managing topology data do also refer to the management of Configuration Data in general, this chapter therefore refers to the 'Management of Configuration Data' by Traffic CS.

6.3 Impact

The implementation of a centralized service for managing Configuration Data is expected to have a significant positive impact on railway operations:

- **Consistency and Quality:** Centralized management will enhance data consistency and quality across all Traffic CS subsystems, reducing errors and discrepancies that can arise from using multiple data sources.
- **Efficiency in Operations:** By allowing updates to configuration data during runtime with minimal impact on operations, the system will improve operational efficiency, enabling quicker responses to changing conditions.
- **Accelerated Rollout:** Streamlined engineering, testing and approval processes for safety logic will facilitate a faster rollout of ETCS Level 2, helping to meet regulatory deadlines and operational requirements.
- **Cost Reduction:** The reduction in engineering and testing efforts associated with system deployment and modifications will lead to lower overall lifecycle costs, benefiting both Infrastructure Managers and Railway Operators.
- **Enhanced Safety:** With a clear separation of safety cases for generic application and specific application, the overall safety of railway operations will be improved.
- **Data-Driven Safety Assurance:** The effectiveness of the safety logic will heavily depend on the accuracy and reliability of data. Therefore, the centralized service for managing Configuration Data is critical to safety, as it includes processes for feeding new or updated data into the European Trackside Protection System (ETPS).

6.4 Design Decisions

The following design decision were taken regarding the management of configuration data:

6.4-1 - Acquire Configuration Data from a centralized service

It is decided that Traffic CS subsystems will acquire Configuration Data from a centralized service via a standardised interface based on EULYNX SMI-xx and on a harmonized process which allows updates of Configuration Data during runtime, with minimal impact on railway operation.

ID	SPT2TRAFFIC-11083
----	-------------------

6.4-2 - Independence of application logic from specific Configuration Data

It is decided that the application logic of the Traffic CS subsystems will be generic with regard to the Configuration Data used. This means that the logic is independent of the specific Configuration Data as long as it complies with the standardized TMS/CCS data model defined by Domain Transversal CCS - SD1.

ID	SPT2TRAFFIC-11085
----	-------------------

6.4-3 - Data representations based on the standardized data model

It is decided that all Traffic CS data representations will be based on the standardized TMS/CCS data model defined by Domain Transversal CCS - SD1.

ID	SPT2TRAFFIC-11084
----	-------------------

6.4-4 - Restricting SMI to authorised Configuration Data

It is decided that Traffic CS will only obtain authorised Configuration Data through the Standard Maintenance Interface (SMI-xx).

ID	SPT2TRAFFIC-11129
----	-------------------

6.4.1 Detail Description

Acquire Configuration Data from a centralized service

The configuration data will initially be provided by the Digital Register - Infrastructure (DR-I) and the Digital Register - Vehicle (DR-V) systems. This data will be transferred to the Configuration Management System (MDM) and subsequently supplied to Traffic CS via the Standard Maintenance Interface (SMI-xx). The Traffic CS subsystems and SMI-xx will be implemented to support the preloading and activation of configuration data according to a harmonised process. This process will allow updates to the configuration data during runtime with minimal impact on railway operations.

Independence of application logic from specific Configuration Data

The Traffic CS will implement a clear separation of safety cases between its subsystems (Plan Execution System (PES), European Trainside Protection System (ETPS), and ATO-Trackside) and the Configuration Data used.

Data representations based on the harmonized data model

The TMS/CMS data model defined by Domain Transversal - SD1 contains the data models of:

- Configuration Data
 - Application Configuration Data (Infrastructure Data, Vehicle Data)
 - System Configuration Data (Parameter Data)
- Interface specifications of SPRA

Restricting SMI to authorised Configuration Data

This decision establishes a clear distinction between the provision of authorised Configuration Data and Operational Data. The Standard Maintenance Interface (SMI-xx) will be designed for the reliable exchange and synchronous activation of authorised Configuration Data. The Operational Data will be exchanged through the Standard Communication Interfaces of SPRA, which will be designed for asynchronous, real-time data exchange.

6.4.2 Comparison with today

The management of configuration data for today's railway systems is fragmented, lacking a centralized service with a standardized interface, which complicates data consistency, quality, and accuracy. This inefficiency hinders the digitalisation of railway operations across various systems, such as TMS, CTC, Interlocking, RBC, and ATO-TS.

Today's CCS systems require tailored safety logic that must undergo rigorous testing and approval, which slows down the rollout of ETCS Level 2 (ETCS Level 2). A generic application logic that is independent of specific Configuration Data enables the creation of a generic safety case, thereby facilitating faster testing and approval processes.

6.4.3 Alternative Design Option

There are alternative design options:

Decentralising the management of configuration data

An alternative design option could involve decentralising the management of configuration data across individual subsystems within the Traffic CS system. In this model, each subsystem would maintain its own configuration data repository, allowing for faster updates and tailored data management specific to each subsystem's requirements.

While this approach could enhance responsiveness to operational changes, it may also introduce significant challenges.

These include increased complexity in ensuring data consistency and quality, as well as heightened integration efforts among subsystems. Additionally, the need for each subsystem to implement its own data management processes could lead to higher engineering and maintenance costs.

Ultimately, although decentralisation offers potential benefits in flexibility and speed, it poses substantial risks to data integrity and operational coherence, which are vital for the effective functioning of the Traffic CS system. Therefore, the decision has been made to pursue a centralized approach, ensuring consistency and reliability across all components.

6.5 Rationale

The design decisions were taken due to the following rationales:

SPT2TRAFFIC-11087 - Acquire Configuration Data from a centralized service

Common Business Objective:  SPT1RS-189 - [Changeability and upgradeability\(2\)](#)

The implementation of a centralized service for configuration data will ensure consistent data updates across Traffic CS subsystems and the entire TMS/CSS target system. Additionally, it will reduce the effort required to install and update Traffic CS subsystems and other components of the TMS/CSS target system.

Linked Work Items	relates to :  SPT2TRAFFIC-11083 - Acquire Configuration Data from a centralized service has parent :  SPT2TRAFFIC-8564 - Rationale
-------------------	---

SPT2TRAFFIC-11092 - Generic implementation logic for Traffic CS subsystems

Common Business Objective:  SPT1RS-233 - [simple repeatable DevOps](#)

Reduction of repetitive engineering and testing and safety approval efforts for system commissioning and system modification.

Linked Work Items	relates to :  SPT2TRAFFIC-11085 - Independence of application logic from specific Configuration Data has parent :  SPT2TRAFFIC-8564 - Rationale
-------------------	--

SPT2TRAFFIC-11093 - Standardised data formats for Configuration Data

Common Business Objective:  SPT1RS-230 - [safety logic with generic safety approval](#)

Defining standardised data formats for Configuration Data contributes towards the generic safety approval of Traffic CS subsystems.

Linked Work Items	relates to :  SPT2TRAFFIC-11084 - Data representations based on the standardized data model has parent :  SPT2TRAFFIC-8564 - Rationale
-------------------	---

SPT2TRAFFIC-11131 - Restricting SMI to Configuration Data provision

Common Business Objective:  SPT1RS-154 - [availability, robustness, reliability](#)

Limiting the transversal systems (Digital Register - Infrastructure, Digital Register - Vehicle, and Configuration Management System) to validating, compiling, and providing only Configuration Data—rather than Operational Data—helps to reduce the

performance, availability, and maintenance requirements of these systems. Unlike Operational Data, Configuration Data is not updated in real-time, meaning that system failures will not directly impact railway operations. This approach not only streamlines data management processes but also enhances the overall integrity of the system, ensuring reliable and consistent data provision across Traffic CS subsystems.

Linked Work Items	has parent :  SPT2TRAFFIC-8564 - Rationale _ is related to :  SPT2TRAFFIC-11129 - Restricting SMI to authorised Configuration Data
-------------------	---

6.6 Assumption and Preconditions

The implementation of this design criterion requires fulfilment of following pre-conditions:

Commitment to Standardisation

It is assumed that all stakeholders will adhere to the harmonised TMS/CCS data model and established standards, ensuring compatibility and interoperability across subsystems.

Regulatory Compliance

It is assumed that the centralized service will comply with all relevant safety and operational regulations, enabling timely approval and authorisation processes.

Data Integrity

The integrity of data provided by the Digital Register - Infrastructure (DR-I) and Digital Register - Vehicle (DR-V) systems is assumed to be reliable and accurate, as this data forms the basis for configuration management.

Data Security

It is assumed that robust security measures will be implemented to protect the integrity and confidentiality of Configuration Data provided via SMI-xx.

Data Authorisation

It is assumed that Configuration Data provided via SMI-xx is authorised to be utilized in Traffic CS.