



ERJU SYSTEM PILLAR

01 System Requirement Specification ETPS



01 System Requirement Specification ETPS

DRAFT

Approval by Reviewers

Type of Approval	 Document Review
------------------	---

Approval By Approvers

Type of Approval	 Document Approval
------------------	---

DRAFT

1	Preamble	6
1.1	Purpose	6
1.2	Intended Audience	6
1.3	Document Context	6
1.4	Glossary	9
1.4.1	Terms and definitions	9
1.4.2	Abbreviations	10
2	Application Conditions	11
3	System overview	12
3.1	System context	12
3.2	System interfaces	12
3.3	System states	15
4	Concepts	16
4.1	CCS/TMS Data Model	16
4.2	Switchable Trackage Assets	16
4.2.1	Introduction	16
4.2.2	Introductory example	17
4.2.2.1	Layout	17
4.2.2.2	Domain Model	18
4.2.2.3	Instantiated Domain Objects	19
4.2.3	Interface for STA	21
4.2.3.1	Retrieve position of an STA	21
4.2.3.2	Change position of an STA	21
4.3	Fouling Section	21
4.4	Movement Permission	22
4.5	Infrastructure Occupation	24
4.5.1	Safe Train Extent	25
4.5.2	Unresolved Trackbound Object Extent	27
4.5.3	Conversions between Safe Train Extent and Unresolved Trackbound Object Extent	28
4.6	Usage Restriction Area (URA)	30
5	Constraints	30
5.1	Constraints Introduction	30
5.1.1	Type of Constraints	30
5.1.2	Technical Concept Derivation	31
5.2	Constraints Authorise movement permissions	31
5.2.1	Safety Constraints	31
5.2.2	Operational Constraints	32
5.3	Constraints Authorise usage restriction areas	32
5.3.1	Safety Constraints	32
5.3.2	Operational Constraints	33
5.4	Constraints Aggregate movable object information	33
5.4.1	Safety Constraints	34

5.4.2 Operational Constraints	34
5.5 Constraints Authorise target position of point	34
5.5.1 Safety Constraints	34
5.5.2 Operational Constraints	35
5.6 Constraints Observe point status	35
5.6.1 Safety Constraints	35
6 System requirements	35
6.1 Non-functional requirements	35
6.2 Functional requirements	35
6.2.1 Functional overview	35
6.2.2 Function 'Authorise target position of point'	35
6.2.3 Function 'Observe point status'	37
6.2.4 Function 'Aggregate movable object information'	37
6.2.5 Function 'Authorise movement permission'	39
6.2.6 Function "Authorise usage restrictions areas"	43
6.2.6.1 Activation via SCI_CMD without signaller confirmation	43
6.2.6.2 Activation via SCI_CMD with signaller confirmation	45
6.2.6.3 Activation via I_Signaller	49
6.2.6.4 Deactivation via SCI_CMD without signaller confirmation	51
6.2.6.5 Deactivation via SCI_CMD with signaller confirmation	52
6.2.6.6 Deactivation via I_Signaller	53
6.2.6.7 Signaller confirmation	53
6.3 Lifecycle concepts	53
7 Appendix	55
7.1 References	55
7.2 Open Points	57

1 Preamble

1.1 Purpose

This document is the output of system requirement specification activities (phase 4) as specified in [SPPRAMSS-349 - [EN 50126-1:2017]] for the [SPMS-5062 - *European Trainside Protection System*]. The objective of this document is to specify a comprehensive and identified set of requirements for the [SPMS-5062 - *European Trainside Protection System*].

1.2 Intended Audience

Domain experts involved in the tendering, development, verification, validation or assessment of the system under consideration (e.g. System Engineers, RAMSS Engineers, Developer, Tester, Assessors, etc).

Note:

This documentation is not intended for a general audience. For a comprehensive understanding of Traffic CS, please refer to the Traffic CS System Concept [SPP-19049 - Traffic CS System Concept V1.0].

1.3 Document Context

According to the System Levels of the System Pillar described in the [SPP-18355 - EET_Systems Engineering Management Plan_V4.0], the ETPS is allocated on System Level 5.

In alignment with [SPP-8684 - System Pillar Common Business Objectives (May 2022)], the [SPMS-5062 - European Trainside Protection System] shall be based on ETCS Level 2.

Furthermore, not all section required by [SPPRAMSS-349 - [EN 50126-1:2017]] have yet been completed. Such sections are identified by the text "Will be provided in further release".

The requirements defined so far are based on technical concepts described in this document. These concepts are currently under investigation and may be subject to change. This may lead to changes of the requirements listed in this document.

The requirements defined so far are not yet agreed in Traffic CS domain. This may lead to changes of the requirements listed in this document. This is considered acceptable because the purpose of this release is to show structure and level of detail to be expected from the System Requirement Specification ETPS. It is not the purpose of this release to provide already a finally agreed set of requirements.

As shown in [SPT2TRAFFIC-12866], the System Requirement Specification ETPS is based on the following inputs:

- [SPP-18075 - TCS_System Architecture Description Traffic CS_V0.4]:
This document allocates the functions and requirements identified for the Traffic CS system (System Level 4 system) to the different System Level 5 systems of Traffic CS. The [SPMS-5062 - European Trainside Protection System] is one of these System Level 5 systems. Therefore, [SPP-18075 - TCS_System Architecture Description Traffic CS_V0.4] identifies all functions and requirements to be fulfilled by the [SPMS-5062 - European Trainside Protection System].
- [SPP-19171 - Risk assessment report for the System Architecture Traffic CS_V0.1]:
This document defines safety constraints for the [SPMS-5062 - European Trainside Protection System]. Therefore, it is an input for the System Requirement Specification ETPS.

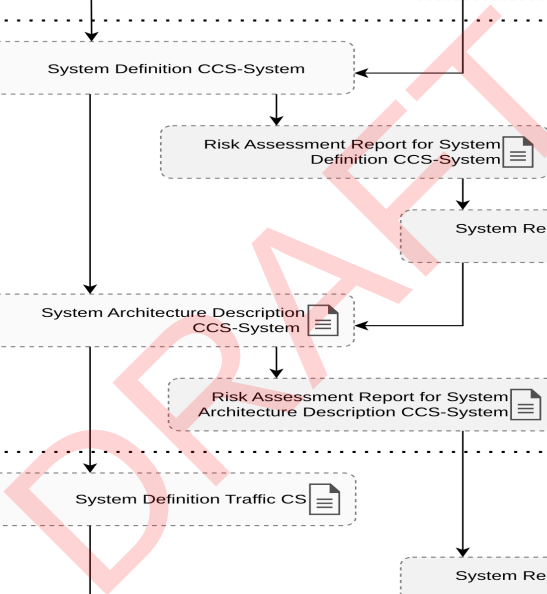
Note:

The traceability between the artefacts of the input documents and the System Requirement Specification ETPS is shown in [SPP-19939 - TCS_Traceability Report System Requirement Specification ETPS_V0.4].

The [SPP-18355 - EET_Systems Engineering Management Plan_V4.0] explains in more detail the dependencies between the different documents.

SPT2TRAFFIC-12866 below shows the System Requirement Specification ETPS in the context of the overall document list (see also [SPP-19283 - Release Note ESPR1.0]).



DRAFT






ID	SPT2TRAFFIC-12866
----	-------------------

1.4 Glossary

1.4.1 Terms and definitions

Term	Definition
Functional requirement	A  SPPR-3791 - System Requirement which specifies what the system of interest does, i.e. actions or functions that the system of interest must perform. In general, functional requirements capture the required behaviour of the system of interest.
MOVEMENT AUTHORITY	Permission for a train to run to a specific location within the constraints of the infrastructure.
Movement Permission	<p>A Movement Permission is a discrete domain object within the ETPS that defines and secures the operational path of a train. It replaces the traditional split between route setting, signalling, and train control by integrating them into one unified concept.</p> <p>Key characteristics:</p> <ul style="list-style-type: none"> · Geometric Extent: The MP specifies a linear, contiguous section of track (running path) that a train is permitted to occupy, including mandatory safety margins (Risk Buffers, Risk Paths) to prevent collisions. · Basis for Movement Authority: An MP provides the trackside foundation from which an ETCS Movement Authority (MA) is derived and transmitted to the train. · Dynamic & Risk-Based: Unlike fixed interlocking routes, an MP can start and end at any topological point and is defined according to operational needs and real-time safety checks rather than static rules. · Lifecycle: MPs are created upon request, checked against topology and safety conditions, granted, supervised, and continuously updated (extended, shortened, upgraded, or removed). · Integration: By merging route protection and movement granting, the MP enables efficient infrastructure use, reduces unnecessary locking of track elements, and supports flexible, automated operations. <p>Movement Permission is not just an “allowance to proceed” but a dynamic, safety-checked allocation of infrastructure to a specific train movement, forming the essential prerequisite for issuing a Movement Authority in ETCS.</p>
Non-functional requirement	A  SPPR-3791 - System Requirement which specifies the key system characteristics that determine how well the system performs duties and to define measurable criteria for evaluating a system function's effectiveness. They are often referred to as the performance targets and "quality attributes" of a system, which includes "-ilities," encompassing characteristics like safety, reliability, usability, serviceability, upgradeability, manufacturability, stability, portability, and more. They are essential to any specification as they emphasize measurable,

Term	Definition
	<p>quantitative criteria over vague qualitative descriptions, thereby ensuring the overall system's verifiability.</p> <p>They are specified without imposing unnecessary design constraints or prescribing specific solutions., like the system-wide non-functional characteristic such as weight, reliability, or durability However, they can specify imposed specific limitations or restriction on how the system (or component, entity) is realised to define a clear solution or implementation (rather than simply guiding design choices).</p>
Point	Assembly of rails, blades, and of auxiliaries, certain ones being movable, which effect the tangential branching of tracks and allows to run over either one track or another. Includes a Point machine and Point detector.
Safe Train Extent	<p>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.</p> <p>Remarks:</p> <ul style="list-style-type: none"> • 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
Train Object	Train Object is the object needed by the ETPS to manage the Communication with an ETCS Equipped train.  
Unresolved Trackbound Object	Unresolved Trackbound Object is the object needed by ETPS to manage occupancies of track areas where track vacancy is not proven and that cannot be associated to a Train Object 

1.4.2 Abbreviations

Abbreviation	Definition
MA	MOVEMENT AUTHORITY
MP	Movement Permission
STE	Safe Train Extent
UTO	Unresolved Trackbound Object

2 Application Conditions

Will be provided in further release.

DRAFT

3 System overview

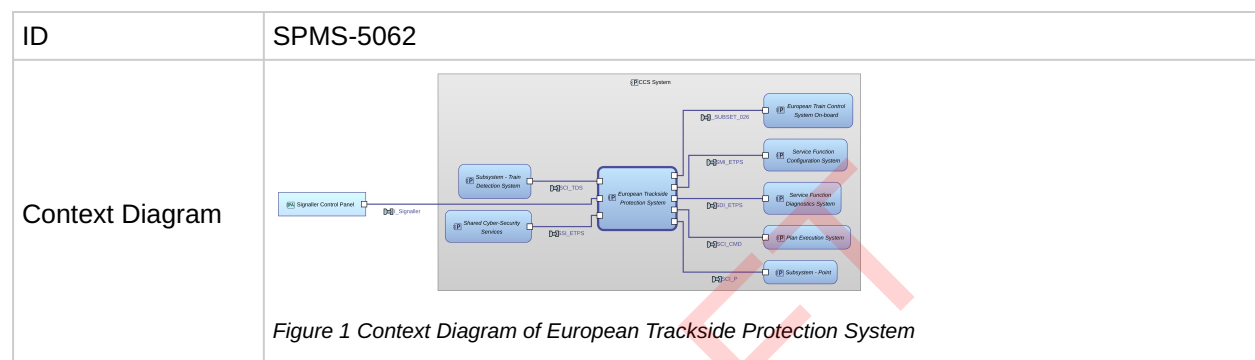
3.1 System context

European Trainside Protection System


Implements the safety-critical functionality within Traffic CS 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.

ETPS acts as a gate keeper and evaluates if the commands received via SCI_CMD interface can be implemented safely. Only if they can be implemented safely, the received commands are forwarded to the corresponding trackside element or the corresponding train.

In order to do this, ETPS maintains the Operating State for its area of control, containing all track occupancies and Movement Permissions within the area of control.



3.2 System interfaces




The interfaces of the  SPMS-5062 - European Trainside Protection System are described in the following chapters.

Note:

Further interfaces will be added in future releases of this document. At least the following interfaces will be added (list not exhaustive)

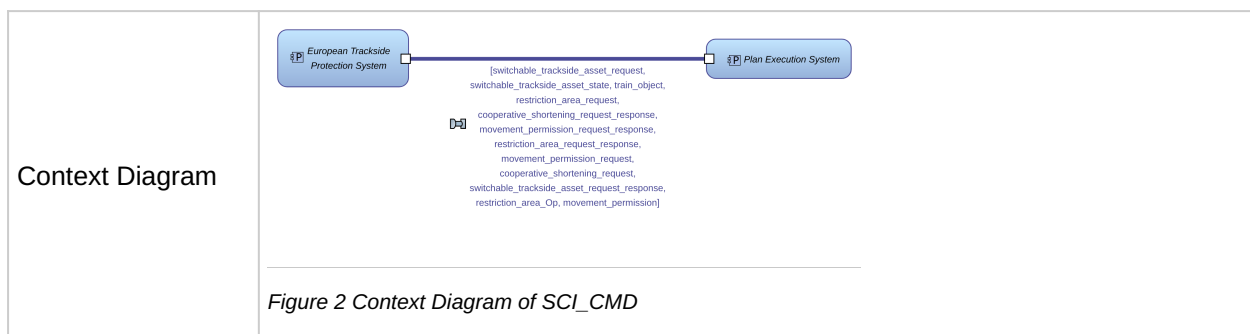
- Handover Interface to adjacent ETPS

3.2-2 - SCI_CMD

The interface  SPMS-6308 - SCI_CMD connects  SPMS-5062 - European Trainside Protection System with  SPMS-5060 - Plan Execution System.

See: [\[SPP-18094 - System Interface Description SCI-CMD\]](#).

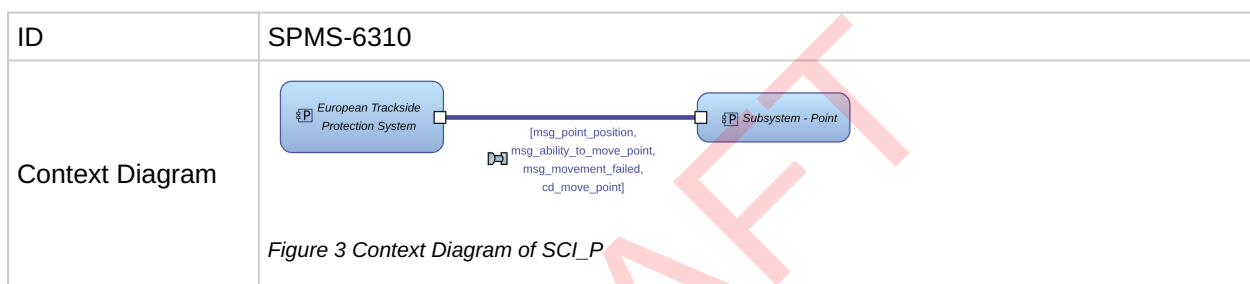
ID	SPMS-6308
----	-----------



3.2-3 - SCI_P

The interface SPMS-6310 - SCI_P connects SPMS-5062 - European Trainside Protection System with SPMS-5068 - Subsystem - Point.

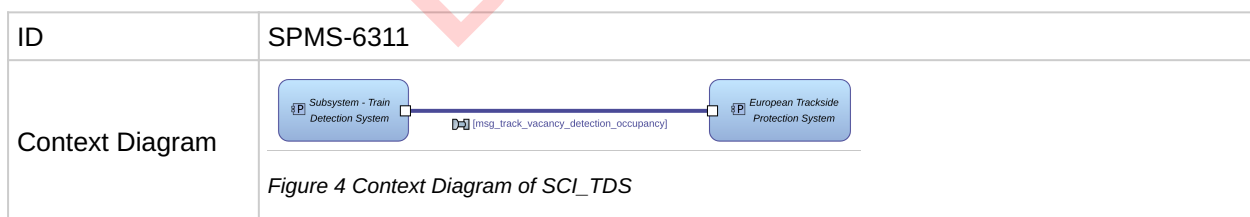
See: [SPP-18533 - Interface specification SCI-P v4.2].



3.2-4 - SCI_TDS

The interface SPMS-6311 - SCI_TDS connects SPMS-5070 - Subsystem - Train Detection System with SPMS-5062 - European Trainside Protection System.

See [SPP-18534 - Interface specification SCI-TDS v4.1].

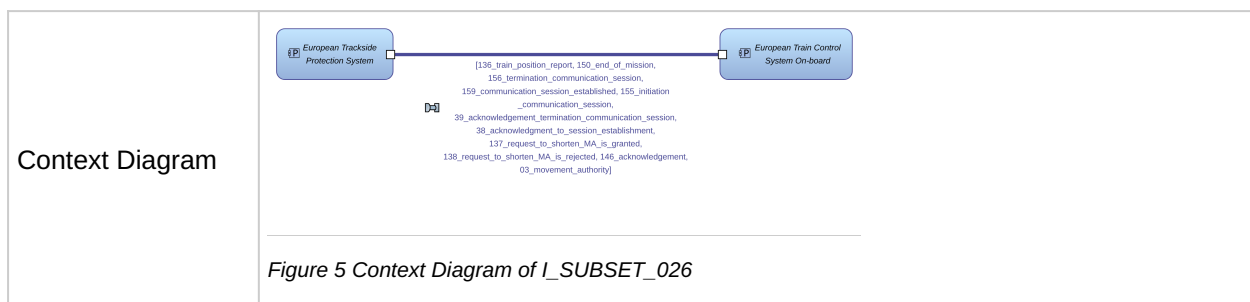


3.2-5 - I_SUBSET_026

The interface SPMS-6306 - I_SUBSET_026 connects SPMS-5062 - European Trainside Protection System with SPMS-5063 - European Train Control System On-board.

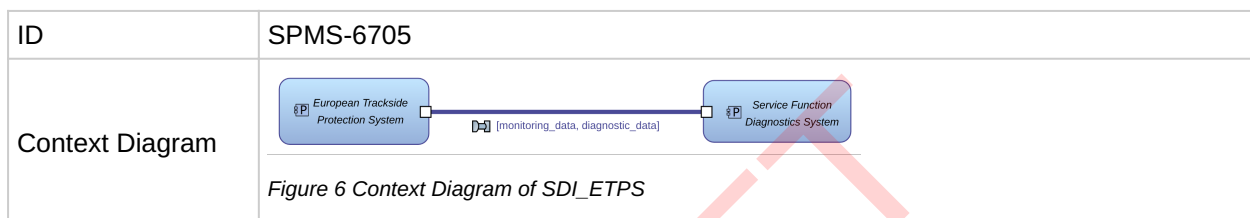
See [[SPPRAMSS-324 - [SUBSET-026]]].








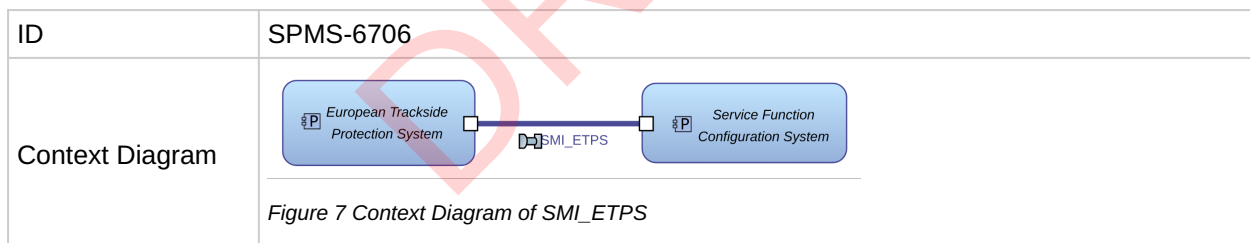
3.2-6 - SDI_ETPS

The interface  SPMS-6705 - SDI_ETPS connects  SPMS-5062 - European Trackside Protection System with  SPMS-6295 - Service Function Diagnostics System.






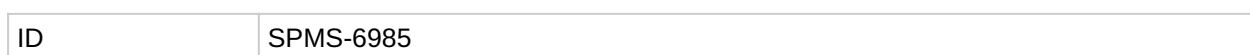
3.2-7 - SMI_ETPS

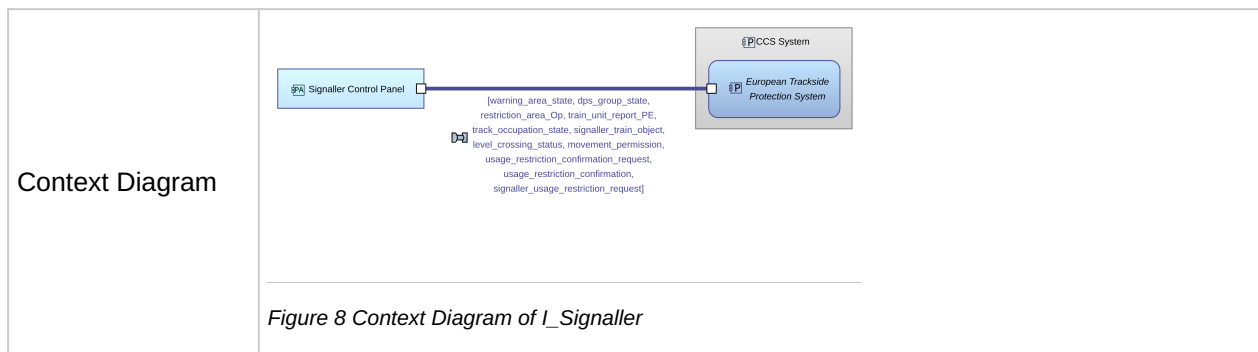
The interface  SPMS-6706 - SMI_ETPS connects  SPMS-5062 - European Trackside Protection System with  SPMS-6294 - Service Function Configuration System.



3.2-8 - I_Signaller

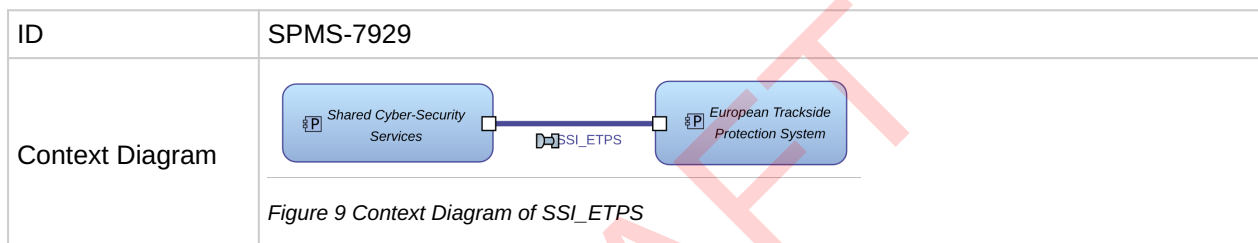
The interface  SPMS-6985 - I_Signaller connects  SPMS-6984 - Signaller Control Panel with  SPMS-5062 - European Trackside Protection System.





3.2-9 - SSI_ETPS

The interface SPMS-7929 - SSI_ETPS connects SPMS-6696 - Shared Cyber-Security Services with SPMS-5062 - European Trackside Protection System. Further described in [Shared Cybersecurity Services Specification].



3.3 System states

Will be provided in further release.

4 Concepts

This chapter describes the technical concepts the system requirements in this document are based on.

Note: These concepts are currently under investigation and may be subject to change. This may lead to changes of the requirements listed in this document.

4.1 CCS/TMS Data Model

The system requirements defined in this document are based on the CCS/TMS Data Model provided by System Pillar. See [SPP-18571 - TCCS - Data Model_00_Guide] for further information.

Note:

The following concepts are based on the CCS/TMS Data Model.

4.2 Switchable Trackside Assets

4.2.1 Introduction

Switchable Trackside Assets (STA) in the railway network can provide the continuity or discontinuity of the track path and/or can supply the possibility to join/diverge tracks.

The most prominent examples are (simple) *Points*. They can be switched to provide continuity of the track path in one or the other direction while at the same time interrupting the track path in the non-chosen direction. *Points* appear in several combinations (e.g. double/interlaced *Points*, simple/double slip *Points* with an inner crossing).

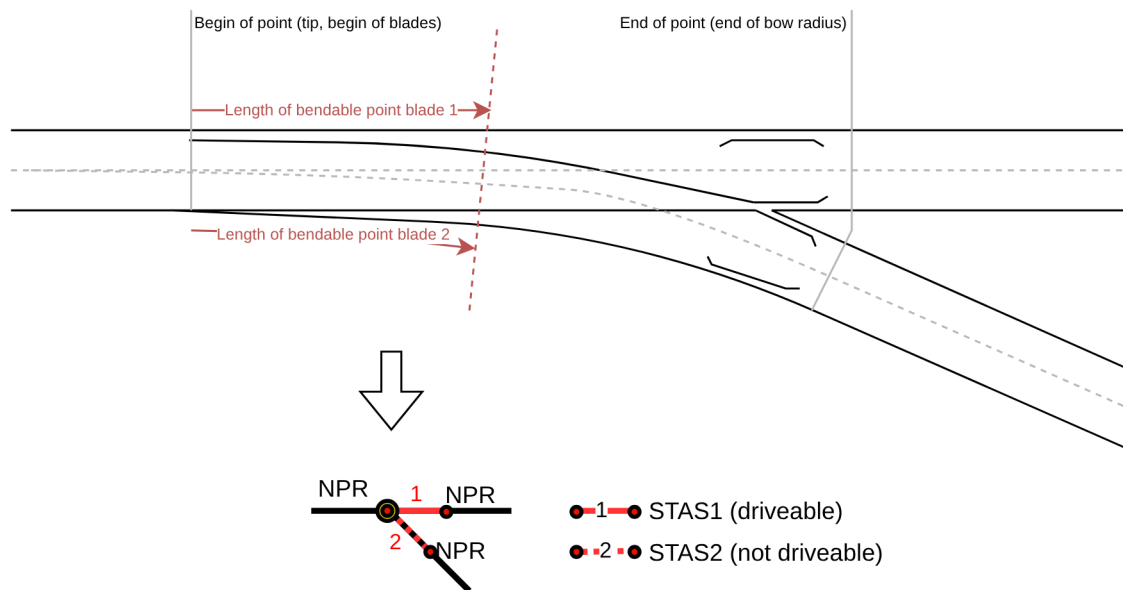
While the primary purpose of *Points* is to provide continuity, its possible discontinuity can also be used to mitigate the risk of a flank collision. This mitigation is also the main purpose of derailleurs.

Finally, there can be obstacles in the way: Movable bridges or (flood) gates.

With the *STA* concept, the following basic needs can be fulfilled:

1. Determination of the position (status) of an *STA* (cf. section SPT2TRAFFIC-16401 - Interface for *STA*);
2. Safety check before accepting a position of an *STA* for a Movement Permission.
3. Move an *STA* to the needed position (cf. section SPT2TRAFFIC-16399 - Change position of an *STA*);
4. Safety check before accepting a request to change an *STA*.

To reach a generic and easy-to-maintain Safety Logic, it is beneficial to abstract the concrete *STA* to the core characteristics which are needed for the Safety Logic. For the example of a simple *Point*,



ID	SPT2TRAFFIC-13378
----	-------------------

There are two movable parts (point blades - 'the points'). They can be moved such that they provide one position or the other, and give continuity for one or the other.

Translated to the CCS/TMS Data Model, either of the ways is represented by a LinearElementSection (*LES*, delimited by two NetPointReference, *NPR*). These *LES* will be called *STA Sections* and are engineered in the *Topology Data* with an extent that covers the movable parts of their *STA* (for a *Point* as shown above, for a movable bridge for the length of the bridge).

This means, that the **core aspect** of an *STA*, the **driveability**, is handled by *STA/STA Sections*. There are two more aspects

- Potential **structure gauge conflict**:
- Degraded situations (e.g. trailed *Point*): this will be done by the *URA* concept. As mentioned already there, the restriction imposed by a malfunction/unintended state of an *STA* leads to the (automatic) creation of a *URA*. This ensures that any (existing or later requested) *Movement Permission* obeys that restriction.

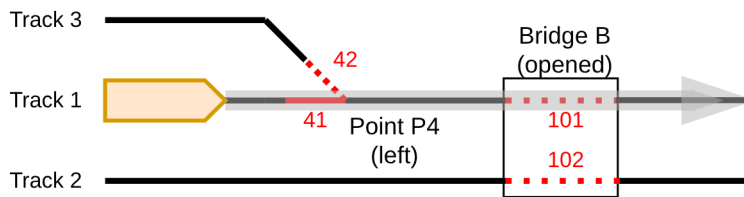
This separation into three aspects adheres to a core architectural principle: separation of concerns.

4.2.2 Introductory example

With the help of this example it should be easy to understand the concept of *STA Sections*. It is explained mainly by describing the *Point*, the most prominent *STA*. The mentioned principle is applicable also to other types of *STA*.

4.2.2.1 Layout

Consider this simplified track layout with a *Point* and a *Movable Bridge*:



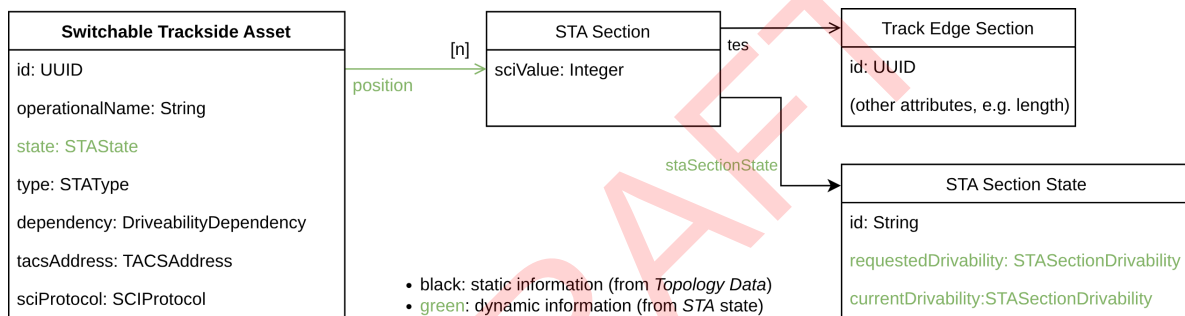
ID	SPT2TRAFFIC-13810
----	-------------------

A *Movement Permission* (grey arrow) is requested for the train to reach beyond the *Point* and the bridge. Before that could happen, *PES* had requested to set both *Switchable Trackside Assets* to the needed position. When now requesting the *Movement Permission*, the Safety Logic of *ETPS* checks if all *STAs* are in the needed position (which is not the case for the bridge).

4.2.2.2 Domain Model

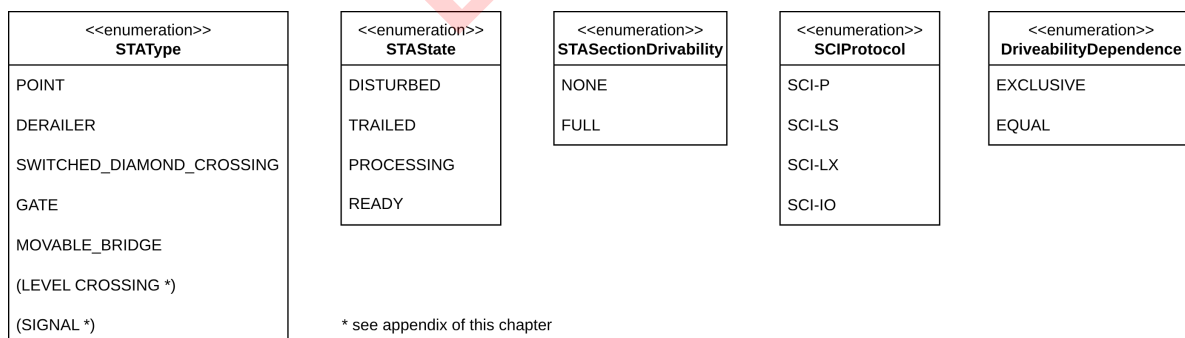
It is helpful to understand how *STAs* are modelled conceptually (only used for concept/specification purpose; the actually used *Domain Model* and *Domain Objects* can be supplier-specific).

The conceptual *Domain Model* of the analysis model is



ID	SPT2TRAFFIC-13787
----	-------------------

where n is the number of 'affected ways' (2 for a simple *Point*, 3 for a *Movable Bridge* with 3 tracks, ...), using these types



ID	SPT2TRAFFIC-13790
----	-------------------

The *Switchable Trackside Asset* has a **type**. This type is not needed for the Safety Logic (see below) but can be used to provide non-abstract, concrete diagnosis and user information (e.g. "Point 4 is disturbed" rather than "STA 4 is disturbed").

It has a number n of related *STA Sections* which represent the n different ways to pass beyond the *STA*. Each *STA Section* references a linear stretch (track segment) on the topology (*Track Edge Section*). By

this, any traversal algorithm will find the *STA Section*, e.g. when checking for safety conditions for the granting of a *Movement Permission*. These 1 to *n* *STA Sections* are referenced by the **position** attribute. Each of the *STA Sections* has the information if it is actually **driveable**.

Some information is needed to make the translation between the abstract *STA/STA Section* notion and the concrete *Trackside Asset* (e.g. a *Point*). For this, the used SCI Protocol (**sciProtocol**) is retrievable, together with the communication address of the related *Trackside Asset Control and Supervision* (*TACS*, **tacsAddress**). From this, it will be known that e.g. for a point (SCI-P) the attribute to be evaluated is *Reported Point Position*. From **sciValue** it is known which value means left (0x02) or right (0x01). The dynamic state **driveable** can then be simply retrieved from the report

$$\text{driveable} := (\text{<reported value>} == \text{sciValue})$$

or translated to the SCI parameter value to set the point

$$\text{Commanded Point Position} := \text{sciValue}$$

Example: the P4 is in left position (= 0x02) so position[0].driveable for STA Section 41 is *true* as it matches position[0].sciValue, and position[1].driveable is *false* as it does not match position[1].sciValue.

While accepting any reported value, not every combination of *STA Section* positions can be accepted. As an example for *Point 4*, *STA Section 41* and *STA Section 42* cannot be both set to driveable but only either of them. This is expressed by the **dependency**:

- **EXCLUSIVE**: exactly one *STA Section* can be requested driveable, the other must be requested non-driveable. A *Point* is an obvious example.
- **EQUAL**: all *STA Sections* must be requested with equal driveability. A *Movable Bridge* or *Gate* are examples: all the tracks (*STA Sections*) must be driveable (bridge closed, gate opened) or all non-driveable (bridge opened, gate closed).

Finally, the *Switchable Trackside Asset* has an overall status so it is clear how it can be used by *ETPS*:

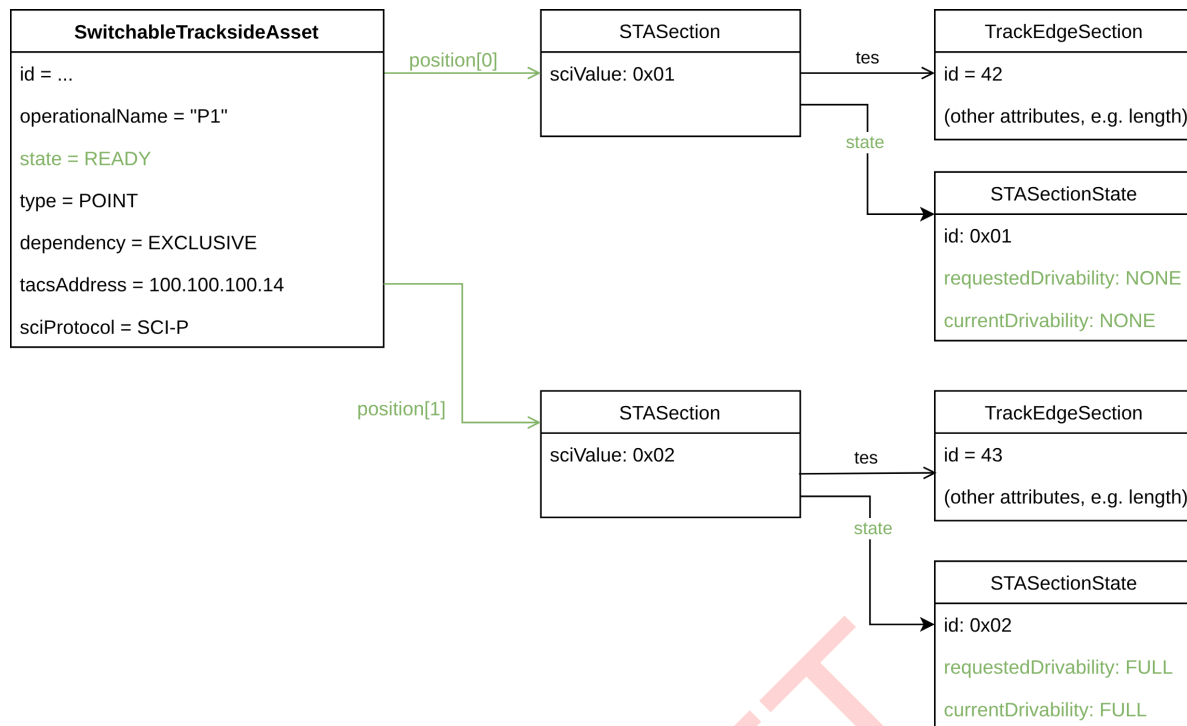
- **AVAILABLE** (regular state): The *STA* can be operated; it is ready to receive commands;
- **PROCESSING**: The *STA* is switching. A new command (for an immediate reversal) will be still accepted;
- **DISTURBED**: The *STA* cannot be operated. One example is a disturbed communication link.

This information is used to determine if switch requests are possible, but also to know if *ETPS* can trust the reported state: if the communication is broken, *ETPS* cannot guarantee the (previously) reported state is (still) correct and will have to consider all *STA Sections* (of the related *STA*) to be non-driveable.

4.2.2.3 Instantiated Domain Objects

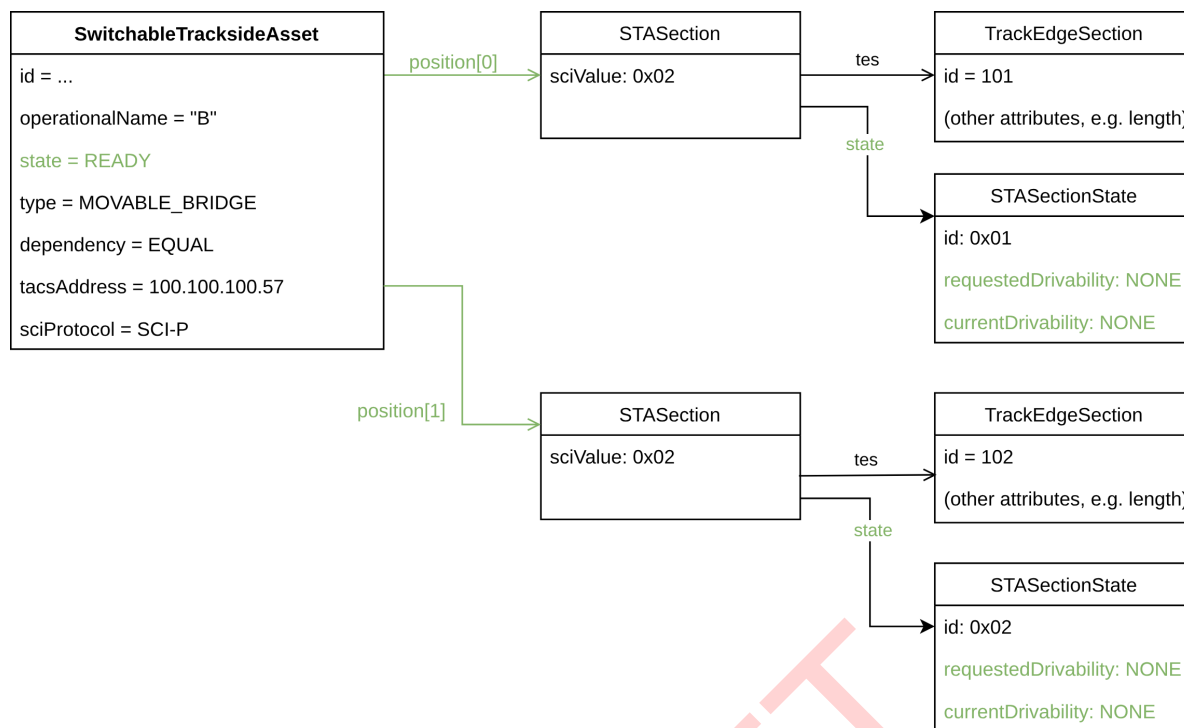
Referring to the next figure, all static information (shown in black) is built at *ETPS* startup from the static *Topology Data* and all dynamic information (shown in green) is initialised to the respective safe value. In effect, *Domain Objects* are created from the *Domain Model*'s object model. Please note again that this is still a conceptual view only used for concept/specification purpose; the actually used *Domain Model* and *Domain Objects* are implementation-specific.

For the sketched simplified layout, the instantiated *Domain Objects*, including their synchronised dynamic state, are



ID	SPT2TRAFFIC-13826
----	-------------------

for the Point and assuming that for the bridge, the 0x01 value ('right') corresponds to closed position but the bridge is actually opened (0x02 value), the dynamic state is



ID	SPT2TRAFFIC-16429
----	-------------------

4.2.3 Interface for STA

4.2.3.1 Retrieve position of an STA

By standard EULYNX SCI-XX interfaces, TACS elements (synonym for *Object Controller*) provide information about the status of STA. The provided concrete protocol (e.g. SCI-P) is known by the **sciProtocol** attribute of an STA and each **position** attribute (STA Section) maps the state value of the related SCI-P protocol.

When there is no connection to the TACS, the **status** of the STA is set accordingly, and a safe value is taken for the **position** of the related STA Sections.

4.2.3.2 Change position of an STA

By the same standard SCI-XX interfaces, an STA can be actuated to change its position. This is an asynchronous operation: After the actuation, control returns. Asynchronous status updates provide the actual position which is first undetermined (e.g. while the point blades are moving). While an STA change state command is processing, the corresponding STA sections driveable status are set to false.

This will prevent that safety checks would allow a *Movement Permission* (extension) using the STA. After the needed time, the final state will be reported and thus updated in the *ETPS Domain Model*.

4.3 Fouling Section

A Fouling Section is a defined area of track topology used to manage and mitigate clearance gauge conflicts between adjacent or intersecting railway tracks. It represents the area within a conflict zone where the physical space occupied by a train on one track could interfere with a train on another track, potentially leading to flank collisions.

Fouling Sections are derived from Fouling Points, which mark the beginning of such conflict zones. These zones arise in three base scenarios:

1. Joining tracks (e.g., Simple Points),
2. Crossing tracks (e.g., Diamond Crossings),
3. Parallel or interlaced tracks with insufficient spacing

Each Fouling Section is part of a pair, representing the mutual exclusivity of movement permissions across conflicting paths. If one section of the pair is reserved or not vacant, the other cannot be used simultaneously. This logic is enforced by the ETPS, ensuring safe train operations.

Fouling Sections are statically engineered into the Topology Data.

They are essential for automated safety checks and can be visualised in operator interfaces to aid decision-making, especially in complex or constrained track layouts.

4.4 Movement Permission

The **Movement Permission (MP)** is a safety critical object managed by ETPS.

A MP defines the reserved track path for a train (including the overrun protection and flank protection) as well as the ETCS Movement Authority (MA) that ETPS will issue to the train. An MP applies to one train and always covers at least the train's safe-train-extent.

The MP consists of three basic elements: the MP Extent, the Risk Buffer and the Risk Paths.

- The **MP Extent** represent the exact track path reserved for the train and also defines the characteristics of the MA that ETPS shall issue, for example the allowed speed profile and ETCS mode profile.
- The **Risk Buffer** represent the overrun protection for the train movement. The Risk Buffer extends the MP in the train's direction of travel. A Risk Buffer exists if there is a Danger Point or project-specific safety margin greater than zero. Its specific length depends for example on the MP's speed profile.
- The **Risk Paths** represent the required Flank protection for the train movement. The Risk Paths run alongside the MP and protect the track path in general up to the next Switchable Trackside Asset that provides flank protection (for example a set of points or a derailer). How far a risk path must extend depends for example on the MP's speed profile and on the type of Switchable Trackside Assets involved. At low speeds or specific operational use cases (for example during shunting), the Risk Path may only need to cover the fouling section of that the transversed Switchable Trackside Asset.

Life cycle:

- The MP is requested through the SCI-CMD interface. In automatic operation the request is send from PES to ETPS; in manual operation the signaller can send the request using the Operator Panel to ETPS.
- The Requester is thereby responsible for setting Switchable Trackside Assets to the required position in advance to ensure the drivability and flank protection of the trackpath to be reserved. The request includes the MP Extent, required Risk Buffer and optionally Switchable Trackside Assets to be excluded from flank protection, whereas ETPS will determine and manage the required flank protection of the MP.
- An MP is requested initially and then extended forward as the train moves, so the train can continue moving along the track path. The MP must take into account all relevant limits from the infrastructure, the train, the operational use cases and the current operational situation to ensure safe movement.
- ETPS checks the requested MP against all safety criteria. It either approves the MP or rejects it and gives a reason. If approved, ETPS saves the MP in its Operating State, and generates and issues the corresponding ETCS MA to the train.
- To keep traffic running smoothly, PES must keep extending the MP forward as needed. At the same time ETPS shortens the rear end of the MP to match the train's safe rear end automatically.

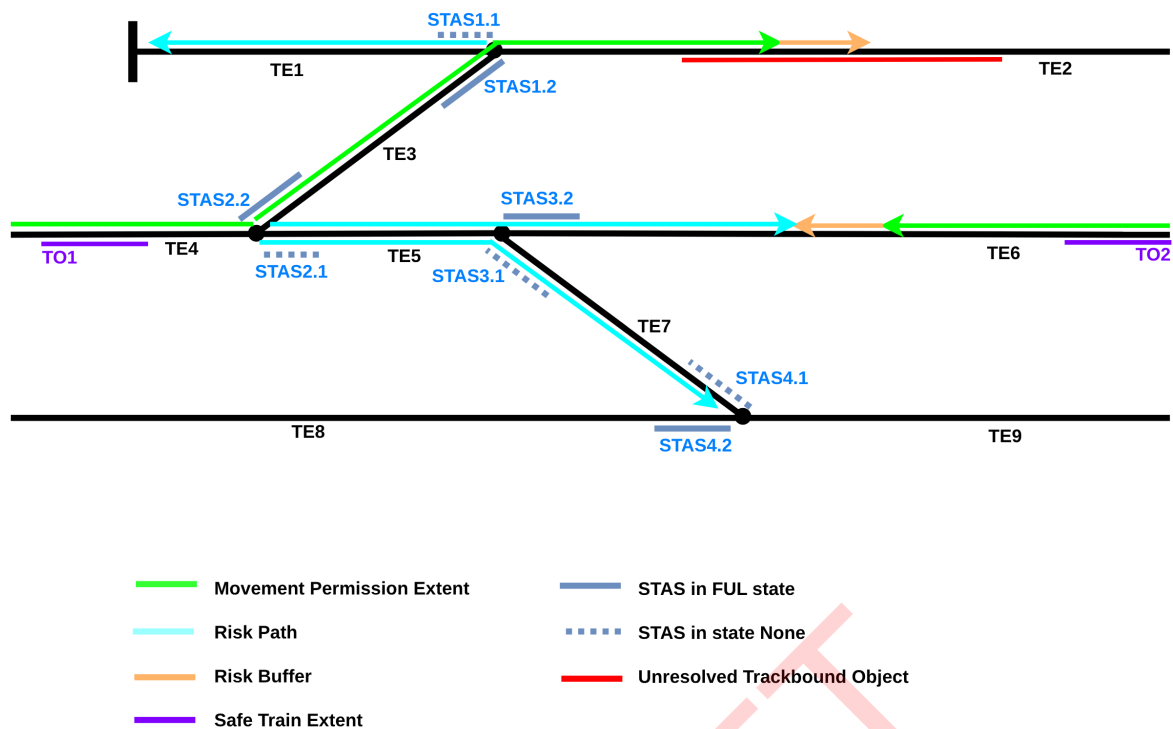
- ETPS removes an MP automatically when the corresponding Train Object is deleted, for example at the train's End of Mission.

 SPT2TRAFFIC-16420 - shows the different elements of a Movement Permission.

The Movement Permission defines the part of the track that is reserved for the movement of a train. It includes:

- Extent
 - Risk Buffer
 - Risk Path(s)
 - Requested Maximum Speed
 - ETCS Movement Mode
 - List of STA's that must not be used as flank protection measure
- **Extent**
An Extent is a linear contiguous stretch of track that is reserved for the movement of a train. The Extent is translated to an authorisation (e.g. Movement Authority) that is transmitted to the train. The Extent is part of the Movement Permission.
 - **Risk Buffer**
A Risk Buffer is a linear contiguous stretch of track that serves as the overrun protection and as a safety buffer in the event of a rollback of a chased train. It is part of a Movement Permission. A Risk Buffer exists if there is a Danger Point or project-specific safety margin greater than zero.
 - **Risk Path**
A Risk Path is one potential path (a linear contiguous stretch of track) by which a non-permitted vehicle movement could result in a flank collision with a vehicle moving along the Movement Permission Extent. A Movement Permission can contain zero or more Risk Paths.

 SPT2TRAFFIC-16420 - shows the different elements of a Movement Permission.



ID	SPT2TRAFFIC-16420
----	-------------------

4.5 Infrastructure Occupation

Infrastructure occupation represents all parts of the track network where physical objects might be located on or close to the tracks preventing safe passage of railway vehicles.

Within ETPS, there are two different concepts to determine track occupancy:

1. Safe Train Extent

This is used to represent areas of track occupied by localised communicating ETCS trains. Each Safe Train Extent will be associated with a specific ETCS train (represented as Train Object).

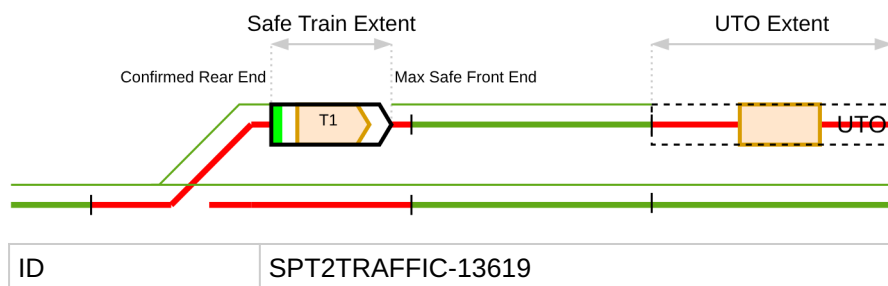
2. Unresolved Trackbound Object Extent

This is used to represent all areas of track which are not proven clear but cannot be linked to a localised communicating ETCS train (i.e., a Safe Train Extent).

For example, an Unresolved Trackbound Object Extent (UTO Extent) could be present for:

- An ETCS train which has ceased to communicate with the trackside, either under failure conditions (after 5 minutes, when the session is considered as closed), or after the termination of the communication session
- An Occupied TTD section which cannot be uniquely associated with any communicating ETCS train (e.g. trains not equipped with ETCS, uncoupled wagons)

In the following example, the Safe Train Extent, UTO extent, and the clear area of the track at a given time are represented. The clear area of the track represented by the green thin line corresponds to the absence of any occupation, which includes neither the Safe Train Extent nor the UTO extent.



Note that as the train could be moving, the Safe Train Extent represents the occupation of a train based on the most recently received information (e.g. the last position report sent by Train CS). Therefore, the Safe Train Extent then represents the **last known position** of the train and does not necessarily represent the current location of the train. This has to be considered in the Traffic CS design.

For example, if the train is not at standstill and/or the train has received a Movement Authorisation, the track ahead of the Safe Train Extent must not be used for other train movements. The Movement Authorisation sent to the train shall be considered as a reservation of that track for the train.

4.5.1 Safe Train Extent

Safe Train Extent is the concept needed by the ETPS to manage track occupancy attributed to a reporting railway vehicle. It is the ETPS interpretation of the occupation of a *Train Object*.

Example: For an ETCS-Equipped train, *Safe Train Extent* is based on ETCS Train Position Reports, ETCS Validated Train Data and other inputs if available, e.g. TTD.

In ETCS, Safe Train Extent is determined as follows:

- one end of the Safe Train Extent is the closest position for the **rear of the train** that can be safely confirmed, in the direction opposite to the train orientation, based on ETCS Train Position Reports, ETCS Validated Train Data, and other inputs, e.g. TTDs.
- the other end of the *Safe Train Extent*, is the closest position for the **front of the train** that can be safely confirmed, in the same direction as to the train orientation, based on ETCS Train Position Reports and other inputs, e.g. TTD section.
- the Safe Train Extent is oriented from the Rear to the Front of the train.

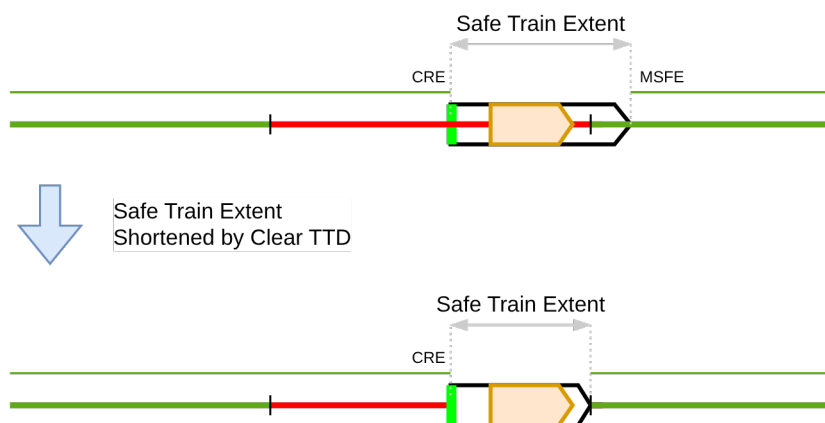
For a train with integrity confirmed inside a TTD reported as occupied, the Safe Train Extent is from the Confirmed Rear End (CRE) to the Max Safe Front End (MSFE).

For a train with Train Integrity confirmed, if the CRE is within a TTD section, then only that part covered by the Safe Train Extent is considered as Occupied although the complete TTD is reported as occupied (provided that no other trackbound object is located in this occupied TTD section):

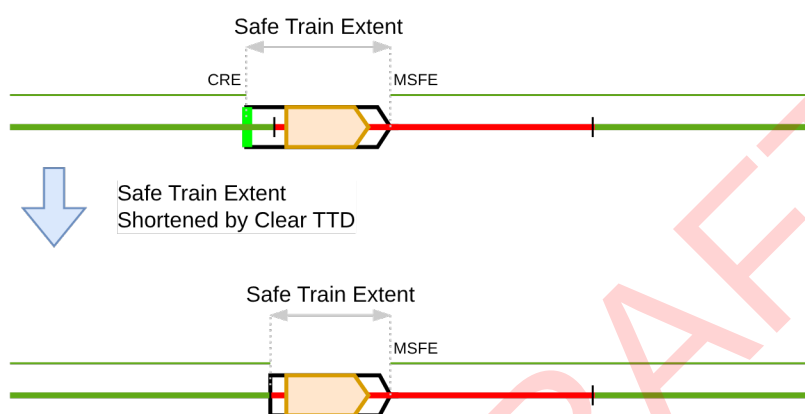


ID	SPT2TRAFFIC-13321
----	-------------------

TTD section status must be used to adjust the Safe Train Extent at the boundaries of the TTD sections, if the confidence interval of the position reported by the train is within a Clear TTD section:

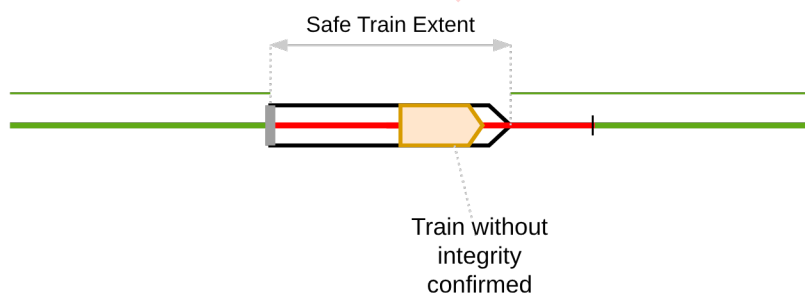


ID	SPT2TRAFFIC-13318
----	-------------------



ID	SPT2TRAFFIC-14933
----	-------------------

For a train without Train Integrity confirmed, there is no Confirmed Rear End derived from Train Position Reports, and the rear end of the Safe Train Extent is therefore at the TTD section boundary to the next free TTD section:



ID	SPT2TRAFFIC-13317
----	-------------------

The information received by ETPS from Train Position Reports and TTD sections is asynchronous, and will have different latencies. This must be managed within ETPS.

For example, from the information received by ETPS, it will occur that a train physically occupies a TTD section before it has reported its position within the TTD section (or vice versa). Similarly, the train may physically leave a TTD section before it has reported its position beyond the TTD section (or vice versa).

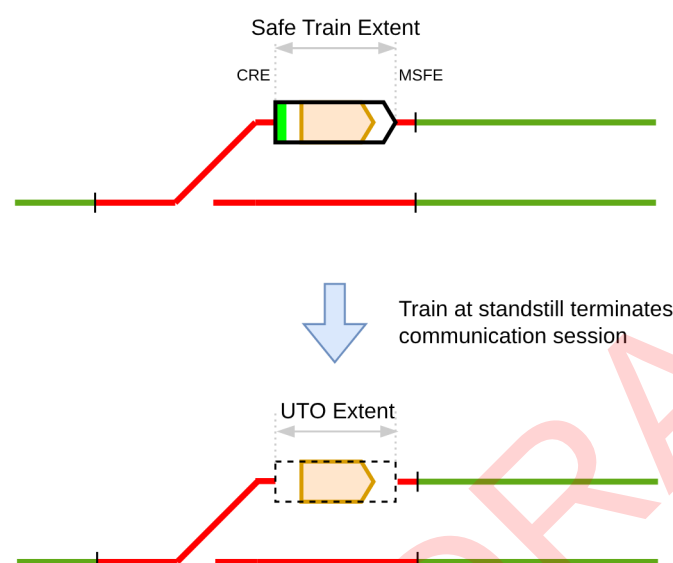
4.5.2 Unresolved Trackbound Object Extent

Unresolved Trackbound Object Extent is the extent of the track that may be occupied by a railway vehicle not associated to a Train Object, i.e. it cannot be directly associated to a Safe Train Extent.

- An Unresolved Trackbound Object Extent may exist due to a specific train, for example for an ETCS train which has ceased to communicate with the trackside.
- An Unresolved Trackbound Object Extent may also exist not associated to a specific train, for example for an Occupied TTD section which cannot be associated with any communicating ETCS train.

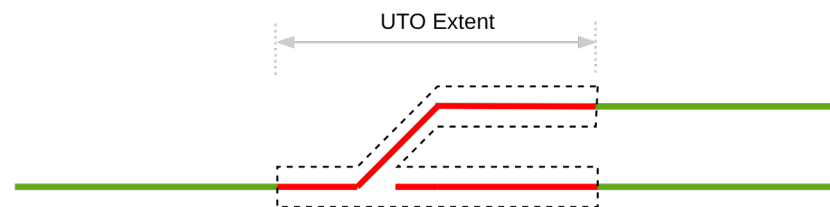
For an Unresolved Trackbound Object Extent due to a specific train, additional information can be stored as the NID_ENGINE of the Train and the Train Characteristics inside the Unresolved Train Object.

An Unresolved Trackbound Object Extent can be created due to a specific train (see also below). This is shown in the following figure:



ID	SPT2TRAFFIC-14930
----	-------------------

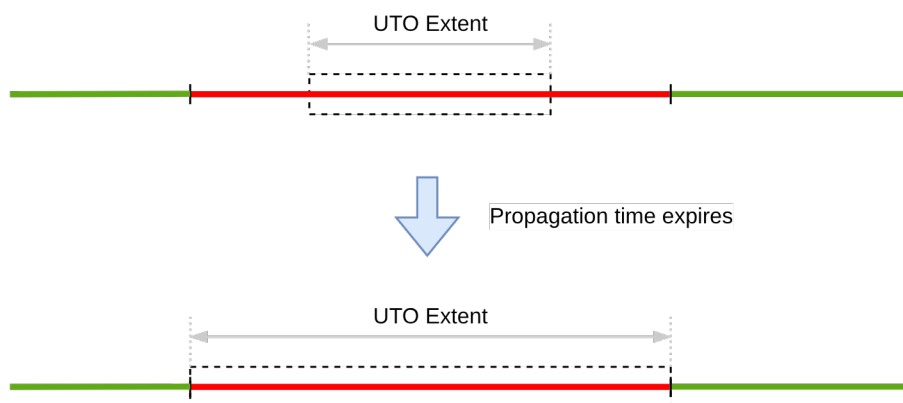
An Unresolved Trackbound Object Extent can be created to represent the possible occupation of a TTD that becomes "unexpectedly" occupied. This is shown in the following figure:



ID	SPT2TRAFFIC-14931
----	-------------------

An Unresolved Trackbound Object Extent may need to be extended, possibly after a period of time, to allow for the fact that any railway vehicles in the Unresolved Trackbound Object Extent may move without knowledge of the ETPS. This is called propagation.

The time before applying propagation can be changed in the ETPS configuration, e.g., to be applied immediately, after a certain period of time or disabled at all. This configuration parameter is valid for the whole Area of Control.



ID	SPT2TRAFFIC-13329
----	-------------------

Movements of non-reporting railway vehicles will be detected only when passing a TTD border. Movement of non-reporting railway vehicles inside one TTD are not detected.

In case of loss of communication of ETCS equipped trains, an already issued Movement Permission shall also be considered for the possible movements of non-reporting vehicles.

Measures are generally put in place at railway project level to prevent or detect and mitigate the risk of rolling vehicles moving such that they conflict with other movements:

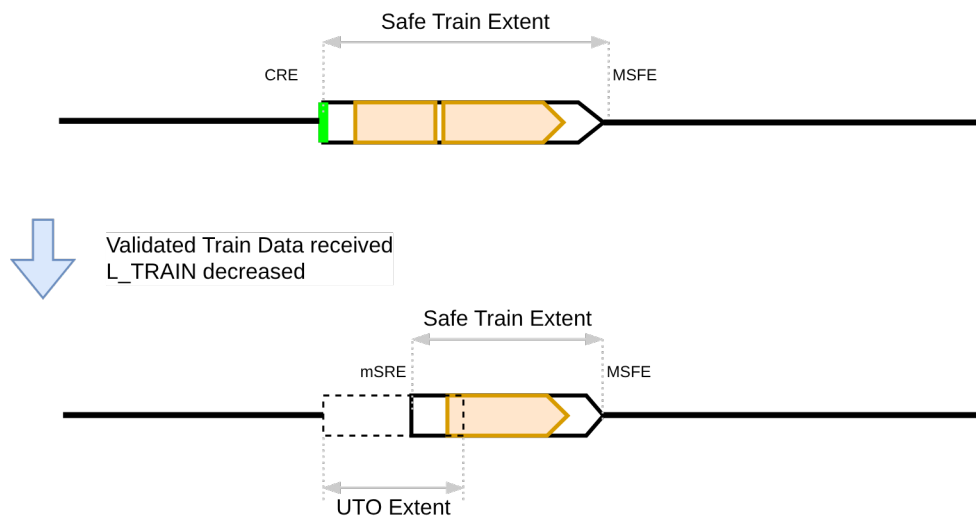
- Use of trap points or derailleurs in station areas and/or sidings
- Use of *Trackside Train Detection* in station areas and/or sidings

4.5.3 Conversions between Safe Train Extent and Unresolved Trackbound Object Extent

Some examples of conversions between Safe Train Extent and Unresolved Trackbound Object Extent are given here after.

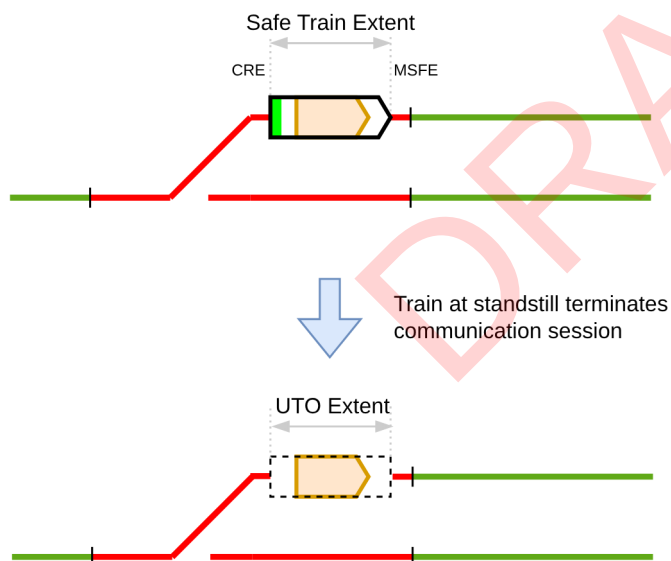
A Safe Train Extent may be totally or partly covered by an Unresolved Trackbound Object Extent due to a specific train:

- Planned Train Splitting (a shorter value of L_TRAIN is received)



ID	SPT2TRAFFIC-14940
----	-------------------

- ETCS train has ceased to communicate with the trackside, either under failure conditions, or after the termination of the communication session



ID	SPT2TRAFFIC-13552
----	-------------------

4.6 Usage Restriction Area (URA)

A **Usage Restriction Area (URA)** defines a **temporary restriction** applied to a specific portion of the railway network, affecting how trains and systems interact with that area. Unlike static topology data (e.g. Static Speed Profile), URAs allow dynamic, short-term modifications without altering the underlying infrastructure data.

URAs are used to manage constraints such as:

- **Train-related restrictions:** e.g. Temporary Speed Restrictions (TSRs), no passage zones, or track conditions like reduced adhesion or radio holes.
- **Trackside Asset-related restrictions:** e.g. preventing the switching of Switchable Trackside Assets during degraded conditions.
- **Operation-related restrictions:** e.g. handover control from automatic (PES) to manual (Signaller) operations and vice versa.

Each URA is defined by:

- **Extent:** the physical area it applies to (e.g. a stretch of track or a group of tracks even if these tracks are non-connected).
- **Direction:** An URA can be uni- or bi-directional.
- **Filter:** optional criteria to target specific trains (e.g. by train category).
- **Type of restriction:** specifying the operational impact (specific Train-related restrictions, Trackside Asset-related restriction or Operation-related restriction).

URAs are enforced by systems like ETPS (e.g. checking if URA violates with a Movement Permission Request from PES) and ETCS-on-board (e.g. supervision of ETCS Track Conditions during train run), ensuring safe and compliant train movements. They can be created manually by operators or automatically by systems responding to incidents (e.g. avalanche sensors). URAs may also be pre-defined in the pre-engineered topology for recurring use and must be persistently stored to survive system downtimes.

Grouping of URAs: Multiple URAs can be logically combined into a single grouped entity when they share a common operational context. This grouping can involve different types of restrictions applied to the same area or restrictions across different extents. Grouping simplifies management by allowing collective activation and removal of related URAs. For example, a construction site might involve a no-passage restriction in the work zone and speed reductions on adjacent tracks - both can be grouped into one URA for streamlined handling.

Note: Grouping of URAs is not yet included in the current specification, it has already been mentioned as a forecasted function for future iterations.


5 Constraints

5.1 Constraints Introduction

5.1.1 Type of Constraints

The document makes use of the following types of constraints:

- **Safety Constraints**
The Safety Constraints are generated during the safety analysis that takes place at each step of the derivation of the system functions and properties from the overall CCS system down to the ETPS system requirements outlined herein. See [SPP-19171 - Risk assessment report for the System Architecture Traffic CS_V0.1] for further information about Safety Constrains.
- **Operational Constraints**
The Operational Constraints are derived either from the operational procedures foreseen to operate such a system or from the need to describe a conditional in an exact fashion - hence values and references to established data models are created.

The linking between constraints and system requirements is described in [ SPP-19939 - TCS_Traceability Report System Requirement Specification ETPS_V0.4].

5.1.2 Technical Concept Derivation

Due to evolving understanding and continued discussion on some of the topics outlined here, there is a need to further align the content and establish links to derived concepts. As some of the technical topics were developed in parallel, some system specification items will require amending or further derivation in future releases.

5.2 Constraints Authorise movement permissions

This chapter contains all constraints defined for the  SPMS-4883 - Authorise movement permissions function.

5.2.1 Safety Constraints

All STAs in the required path are in the required position

All switchable trackside assets in the required path are in the required position.

ID	SPRM-2312
Type	{c} Constraint

Maximum authorised distance is within Movement Permission

The end of the MA has to be within the secured path for the movement (i.e. the Movement Permission).

ID	SPRM-1776
Type	{c} Constraint

Requested track path adheres to train-side restrictions

Requested track path adheres to trainside restrictions e.g. possible braking curves, maximum speed of train, train length etc.

ID	SPRM-1758
Type	{c} Constraint

Maximum authorised distance ends ahead of occupied track

Maximum authorised distance is at the most the start of the next occupied track. This means that the end of authority cannot be in an occupied track (occupied by train or by another movement permission).

ID	SPRM-1447
Type	{c} Constraint

Requested track path is distinct from other authorised track paths

Requested track path for one train does not contain any track paths already set for other trains.

ID	SPRM-1444
Type	{c} Constraint

Authorised speed is less or equal to the maximum allowed track speed

The authorised speed of the movement permission of the train is less or equal to the maximum allowed track speed.

ID	SPRM-1563
----	-----------

Type	{c} Constraint
------	----------------

Train adheres to infrastructure restrictions

The train is able to run on the infrastructure (e.g. loading gauge, train category) and does not violate the loading gauge, weight limits etc. which could cause a collision or derailment.

ID	SPRM-1442
Type	{c} Constraint

Movement permission is free of occupancies

The movement permission of the train uses only a track path that is free of occupancies by other trains and vehicles.

ID	SPRM-1561
Type	{c} Constraint

Movement permission is distinct from other Movement Permissions

The movement permission of the train uses only a track path that is distinct from movement permissions of other trains. This means that Movements Permissions do not overlap.

ID	SPRM-1562
Type	{c} Constraint

5.2.2 Operational Constraints

Movement Permission does not overlap a URA of type track closure

MovementPermission.extent overlaps RestrictionArea.linearElementSections for a RestrictionArea with "specificRestrictions.restrictedAspect.trackClosure == true"

ID	SPT2TRAFFIC-16451
Type	{c} Constraint

Authorised speed is less or equal to the maximum allowed URA speed

The authorised speed should not be higher than the limitations imposed by the URAs on the relevant section of track.

ID	SPT2TRAFFIC-16454
Type	{c} Constraint

5.3 Constraints Authorise usage restriction areas

This chapter contains all constraints defined for the  SPMS-5724 - Authorise usage restriction areas function.

5.3.1 Safety Constraints

Requested usage restriction parameters adheres to infrastructure and train-side restrictions

CCS System checks the requested usage restriction parameters. The parameters are within the limits of the static trackside and train attributes.

ID	SPRM-1747
Type	{c} Constraint

Activation process of usage restriction is completed

CCS System doesn't send to Signaller activated state of a usage restriction until the activation process has been successfully completed.

ID	SPRM-1701
Type	{c} Constraint

5.3.2 Operational Constraints

Usage restriction area is reserved for one movement permission

Usage restriction area is reserved for one movement permission

ID	SPT2TRAFFIC-16428
Type	{c} Constraint

The request is valid

The received request is valid, e.g. that it concerns existing trackside elements in a coherent way, or it refers to an existing train that is in the correct location.

ID	SPT2TRAFFIC-16433
Type	{c} Constraint

Restriction Area can be created without signaller confirmation

The Restriction Area has been introduced with the parameter that signaller confirmation is not required for creation.


ID	SPT2TRAFFIC-16526
Type	{c} Constraint

Restriction Area can be deleted without signaller confirmation

The Restriction Area has been introduced with the parameter that signaller confirmation is not required for deletion.

ID	SPT2TRAFFIC-16475
Type	{c} Constraint

5.4 Constraints Aggregate movable object information

This chapter contains all safety constraints defined for the  SPMS-4871 - Aggregate movable object information function.

5.4.1 Safety Constraints

Consistency between information for determining train motion state

A check of the consistency between wheel passing information received by the Wheel and geographical information received by a Rolling Stock Reference Point is needed.

ID	SPRM-1739
Type	{c} Constraint

Integrity of received information for determining train motion state


The CCS System handles transmission errors on received information used for determining the train motion state safely. The loss of input data is handled in a safe manner when determining the train motion state.

E.g. extending the section deemed occupied by the train.

ID	SPRM-1736
Type	{c} Constraint

5.4.2 Operational Constraints

5.5 Constraints Authorise target position of point

This chapter contains all safety constraints defined for the  SPMS-4903 - Authorise target position of point function.

5.5.1 Safety Constraints

Point is reserved for one movement permission

The points used for a movement permission are locked against switching their position. To change the state of points, first the reservation (i.e. movement permission) needs to be removed/revoked.

ID	SPRM-1775
Type	{c} Constraint

Point position command is sent after performing the safety checks

The point position command goes out promptly after performing the safety checks to avoid that the operational conditions change and the result of the safety checks is not valid anymore.

Note: Stipulating a timer should be avoided after discussing with Traffic CS. The monitoring of the time it takes to change the point position is allocated to Trackside Assets CS in another constraint.

ID	SPRM-1730
Type	{c} Constraint


Point is free of occupancy

State change of a point machine only if the controlled point is not occupied by trains/vehicles/trackworkers and not reserved for other operational movement.

ID	SPRM-1699
Type	{c} Constraint


5.5.2 Operational Constraints

Point is manually operated

A usage restriction with  SPMS-7612 - RestrictedAspect.manualOperationOnly==true overlaps with one SwitchableTracksideAssetSection of the STA.


ID	SPT2TRAFFIC-16394
Type	{c} Constraint

Point is locked

A usage restriction with  SPMS-7612 - RestrictedAspect.nonSwitchability==true overlaps with one SwitchableTracksideAssetSection of the STA.

ID	SPT2TRAFFIC-16395
Type	{c} Constraint

5.6 Constraints Observe point status

This chapter contains all safety constraints defined for the  SPMS-4888 - Observe point status function.

5.6.1 Safety Constraints

No safety constraints

6 System requirements

6.1 Non-functional requirements

Will be provided in further release.

Will be provided in further release.

Note:

At least the following non-functional requirements are foreseen so fare (list non-exhaustive):

- reliability, availability, maintainability, safety, security, performance
- standards and regulations
- quality characteristics


6.2 Functional requirements

6.2.1 Functional overview

Will be provided in further release.

6.2.2 Function 'Authorise target position of point'

6.2.2-1 - Authorise target position of point




This function is allocated to  SPMS-5062 - European Trackside Protection System.

This function checks if the requested point position can be implemented safely and sends the related





command if so. In case it can not be safely implemented the request is rejected.


ID	SPMS-4903
----	-----------

Authorise point position







When [ SPMS-5062 - **European Trackside Protection System** receives  SPMS-7746 - *switchable_trackside_asset_request* via  SPMS-6308 - *SCI_CMD*


AND {c} SPRM-1699 - Point is free of occupancy
 AND NOT {c} SPRM-1775 - Point is reserved for one movement permission
 AND NOT {c} SPT2TRAFFIC-16394 - Point is manually operated
 AND NOT {c} SPT2TRAFFIC-16395 - Point is locked],

the  SPMS-5062 - European Trackside Protection System shall send  SPMS-4935 - *cd_move_point* with *commandedPointPosition* set in accordance with the information provided in the  SPMS-7746 - *switchable_trackside_asset_request* via  SPMS-6310 - *SCI_P*.




Rationale	When a point position request is received, it will check the safety conditions for setting a point position (found in a different workitem). If the safety checks clear, ETPS will command the point to the requested position (given by a translation of <i>requestedDrivability</i> into point position).
ID	SPT2TRAFFIC-11250
Type	 System Requirement

Respond to accepted point position request via SCI-CMD

When [ SPMS-5062 - **European Trackside Protection System** receives  SPMS-7746 - *switchable_trackside_asset_request* via  SPMS-6308 - *SCI_CMD*
 AND {c} SPRM-1699 - Point is free of occupancy
 AND NOT {c} SPRM-1775 - Point is reserved for one movement permission],
 the  SPMS-5062 - European Trackside Protection System shall send  SPMS-5191 - *switchable_trackside_asset_request_response* with *Response* accepted via  SPMS-6308 - *SCI_CMD*.

Rationale	When a point position request is received, ETPS will respond to PES about the outcome. The response gives the acceptance state (accepted/rejected) and the reasons for the rejection, if relevant. It should list all such reasons.
ID	SPT2TRAFFIC-11683
Type	 System Requirement

Respond to rejected point position request via SCI-CMD

When [ SPMS-5062 - **European Trackside Protection System** receives  SPMS-7746 - *switchable_trackside_asset_request* via  SPMS-6308 - *SCI_CMD*
 AND [NOT {c} SPRM-1699 - Point is free of occupancy

OR NOT {c} SPRM-1775 - Point is reserved for one movement permission]],
 the 🏠 SPMS-5062 - European Trackside Protection System shall send 📡 SPMS-5191 -
 switchable_trackside_asset_request_response with *Response* rejected via 📡 SPMS-6308 - SCI_CMD.

Rationale	When a point position request is received, ETPS will respond to PES about the outcome. The response gives the acceptance state (accepted/rejected) and the reasons for the rejection, if relevant. It should list all such reasons.
ID	SPT2TRAFFIC-16438
Type	📄 System Requirement

6.2.3 Function 'Observe point status'

6.2.3-1 - Observe point status

This function is allocated to 🏠 SPMS-5062 - European Trackside Protection System.
 This function observes the overall status of the point, including, End position, No end position.

ID	SPMS-4888
----	-----------

Report point position

When 🏠 SPMS-5062 - European Trackside Protection System receives 📡 SPMS-4933 -
 msg_point_position via 📡 SPMS-6310 - SCI_P,
 the 🏠 SPMS-5062 - European Trackside Protection System shall send 📡 SPMS-7747 -
 switchable_trackside_asset_state with *Position* set to *DriveProtectionSectionGroupState* via
 📡 SPMS-6308 - SCI_CMD.

Rationale	ETPS acts as a postman to relay trackside asset information (point position in this case) to PES.
ID	SPT2TRAFFIC-11771
Type	📄 System Requirement

6.2.4 Function 'Aggregate movable object information'




6.2.4-1 - Aggregate movable object information


This function is allocated to 🏠 SPMS-5062 - European Trackside Protection System.
 This function aggregates and stores information (e.g. position) submitted by different actors (e.g.,
 Trackside Asset CS, Train CS) and output of other functions into an operational state representation of
 movable objects. The function includes occupancies NOT allocated to a train object as well.
 Movable objects are defined as trains and wagons that either submit localisation and/or additional data
 (such as speed and status) or that are localised by alternative technologies such as TTD systems.

ID	SPMS-4871
----	-----------







Report Train Object information based on trackside detection systems


When 🏠 SPMS-5062 - European Trackside Protection System receives 📡 SPMS-3269 -
 msg_track_vacancy_detection_occupancy via 📡 SPMS-6311 - SCI_TDS,

the  SPMS-5062 - **European Trackside Protection System** shall send  SPMS-5119 - **train_object** via  SPMS-6308 - **SCI_CMD**.







Rationale	When ETPS receives information from Trackside Detection Systems, it should update the corresponding Train Object and inform PES.
ID	SPT2TRAFFIC-11902
Type	 System Requirement


Report Train Object information based on train position reports

When  SPMS-5062 - **European Trackside Protection System** receives  SPMS-4948 - **136_train_position_report** via  SPMS-6306 - **I_SUBSET_026** ,
the  SPMS-5062 - **European Trackside Protection System** shall send  SPMS-5119 - **train_object** via  SPMS-6308 - **SCI_CMD**.







Rationale	When ETPS receives train positioning information from train position reports, it should update the corresponding Train Object and inform PES.
ID	SPT2TRAFFIC-11903
Type	 System Requirement


Report Train Object information based on Start of Mission position report

When  SPMS-5062 - **European Trackside Protection System** receives  SPMS-7696 - **157_SoM_position_report** via  SPMS-6306 - **I_SUBSET_026** ,
the  SPMS-5062 - **European Trackside Protection System** shall send  SPMS-5119 - **train_object** via  SPMS-6308 - **SCI_CMD**.








Rationale	When ETPS receives train positioning information from the Start of Mission position report, it should update the corresponding Train Object and inform PES.
ID	SPT2TRAFFIC-16440
Type	 System Requirement


Report Train Object information based on End of Mission report

When  SPMS-5062 - **European Trackside Protection System** receives  SPMS-4953 - **150_end_of_mission** via  SPMS-6306 - **I_SUBSET_026** ,
the  SPMS-5062 - **European Trackside Protection System** shall send  SPMS-5119 - **train_object** via  SPMS-6308 - **SCI_CMD**.

Rationale	When ETPS receives train positioning information from the End of Mission position report, it should update the corresponding Train Object and inform PES.
ID	SPT2TRAFFIC-16439
Type	 System Requirement


Report Train Object information based on Movement Authority update

When  SPMS-5062 - **European Trackside Protection System** receives  SPMS-4951 - 146_acknowledgement for  SPMS-4945 - 03_movement_authority via  SPMS-6306 - I_SUBSET_026, the  SPMS-5062 - **European Trackside Protection System** shall send  SPMS-5119 - train_object via  SPMS-6308 - SCI_CMD.

Rationale	When ETCS receives the confirmation from the ETCS on-board that the Movement Authority has been received, it should update the corresponding Train Object and inform PES.
ID	SPT2TRAFFIC-16435
Type	 System Requirement

6.2.5 Function 'Authorise movement permission'

6.2.5-1 - Authorise movement permissions

This function is allocated to  SPMS-5062 - European Trackside Protection System. This function performs a safe allocation of a track path for planned train movements, i.e.

- supervises and verifies that the required trackside assets are in the required position
- allocates track paths over trackside assets (locking state is shown by the observe point position)
- checks whether there are no conflicting track paths already allocated to other train movements nor usage restrictions already defined
- checks that the track path for planned train movement is clear

Note: The function also involves flank protection supervision that can be either ensured by trackside assets being part of the requested track path or by logic (if railway vehicle movements close to the train can be excluded).

The function also releases track parts that are no longer planned to be used for train movement after checking the corresponding rules, e.g.,

- releases allocated portion of track path which is overpassed and therefore no more occupied by the train
- ensures that allocated portion of track in front of the train will not be released if it is still to be used by the train
- releases allocated portion of track in rear of the train if it is no longer planned to be used.




Note: The current assumption is that the function checks that all rules are fulfilled to either reserve or release a track path.

This function generates the authorisation and if relevant the track conditions for movement for one train inside the allocated track path and reports it to the train.

Note: Stopping is only a special case of a movement.

ID	SPMS-4883
----	-----------

Respond to accepted Movement Permission Request via SCI_CMD

When  SPMS-5062 - **European Trackside Protection System** receives  SPMS-4928 - movement_permission_request via  SPMS-6308 - SCI_CMD

AND {c} SPRM-1442 - Train adheres to infrastructure restrictions
 AND {c} SPRM-2312 - All STAs in the required path are in the required position
 AND {c} SPRM-1563 - Authorised speed is less or equal to the maximum allowed track speed
 AND {c} SPRM-1561 - Movement permission is free of occupancies
 AND {c} SPRM-1562 - Movement permission is distinct from other Movement Permissions
 AND {c} SPT2TRAFFIC-16454 - Authorised speed is less or equal to the maximum allowed URA speed
 AND {c} SPT2TRAFFIC-16451 - Movement Permission does not overlap a URA of type track closure,
 the 🇪🇺 SPMS-5062 - European Trackside Protection System shall send 🇮🇹 SPMS-7783 -
 movement_permission_request_response with "MovementPermissionResponseCode: Accepted" via
 🇮🇹 SPMS-6308 - SCI_CMD.

Rationale	<p>When a Movement Permission request is received, ETPS shall check against all the safety constraints. If they all pass, ETPS shall respond to PES about the acceptance of the request.</p> <p>Note: The response message does not mean that the request has been processed already, only that it will be processed.</p>
ID	SPT2TRAFFIC-12351
Type	🇮🇹 System Requirement




Send Movement Authority via I_SUBSET_026


When 🇪🇺 SPMS-5062 - European Trackside Protection System receives 🇮🇹 SPMS-4928 -
 movement_permission_request via 🇮🇹 SPMS-6308 - SCI_CMD
 AND {c} SPRM-1442 - Train adheres to infrastructure restrictions
 AND {c} SPRM-2312 - All STAs in the required path are in the required position
 AND {c} SPRM-1563 - Authorised speed is less or equal to the maximum allowed track speed
 AND {c} SPRM-1561 - Movement permission is free of occupancies
 AND {c} SPRM-1562 - Movement permission is distinct from other Movement Permissions
 AND {c} SPT2TRAFFIC-16454 - Authorised speed is less or equal to the maximum allowed URA speed
 AND {c} SPT2TRAFFIC-16451 - Movement Permission does not overlap a URA of type track closure,
 the 🇪🇺 SPMS-5062 - European Trackside Protection System shall send 🇮🇹 SPMS-4945 -
 03_movement_authority according to the 🇮🇹 SPMS-4928 - movement_permission_request and
 infrastructure restrictions via 🇮🇹 SPMS-6306 - I_SUBSET_026.

Rationale	<p>When a Movement Permission request is received, ETPS shall check against all the safety constraints. If they all pass, ETPS shall send a corresponding MA to the relevant train.</p> <p>Note: This requirement does not include the response to PES about the outcome of the safety checks.</p>
ID	SPT2TRAFFIC-12359
Type	🇮🇹 System Requirement







Respond to rejected Movement Permission Request via SCI_CMD


When 🇪🇺 SPMS-5062 - **European Trackside Protection System** receives 🇮🇹 SPMS-4928 -
 movement_permission_request via 🇮🇹 SPMS-6308 - SCI_CMD

AND [
 NOT {c} SPT2TRAFFIC-16451 - Movement Permission does not overlap a URA of type track closure
 OR NOT {c} SPRM-1442 - Train adheres to infrastructure restrictions
 OR NOT {c} SPRM-2312 - All STAs in the required path are in the required position
 OR NOT {c} SPRM-1563 - Authorised speed is less or equal to the maximum allowed track speed
 OR NOT {c} SPRM-1561 - Movement permission is free of occupancies
 OR NOT {c} SPRM-1562 - Movement permission is distinct from other Movement Permissions
 OR NOT {c} SPT2TRAFFIC-16454 - Authorised speed is less or equal to the maximum allowed URA speed],
 the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7783 - movement_permission_request_response with "MovementPermissionResponseCode: Rejected" via  SPMS-6308 - SCI_CMD.







Rationale	When a Movement Permission request is received, ETPS shall check against all the safety constraints. If at least one of them fails, ETPS will respond to PES about the rejection of the request and list all failed checks. Note: This will also include any rejection due to invalid request, e.g. due to a non-existing train or an impossible movement.
ID	SPT2TRAFFIC-16387
Type	 System Requirement


Respond to forwarded Cooperative Shortening Request via SCI_CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7786 - cooperative_shortening_request via  SPMS-6308 - SCI_CMD
 AND {c} SPRM-1776 - Maximum authorised distance is within Movement Permission
 AND {c} SPT2TRAFFIC-16433 - The request is valid,
 the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7787 - cooperative_shortening_request_response with "CooperativeShorteningResponseCode: Forwarded" via  SPMS-6308 - SCI_CMD.








Rationale	When ETPS received a valid request for a Cooperative Shortening, it shall respond to PES about the acceptance of the request.
ID	SPT2TRAFFIC-16349
Type	 System Requirement


Forward request for Cooperative Shortening via I_SUBSET_026

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7786 - cooperative_shortening_request via  SPMS-6308 - SCI_CMD
 AND {c} SPRM-1776 - Maximum authorised distance is within Movement Permission
 AND {c} SPT2TRAFFIC-16433 - The request is valid,
 the  SPMS-5062 - European Trackside Protection System shall send  SPMS-5503 - 09_request_to_shorten_MA via  SPMS-6306 - I_SUBSET_026 .







Rationale	When ETPS received a valid request for a Cooperative Shortening, it shall forward it to the relevant train. Note: The request should still be checked for validity (train exists, movement is a shortening of the original movement etc.).
ID	SPT2TRAFFIC-16352
Type	 System Requirement


Respond to invalid Cooperative Shortening Request via SCI_CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7786 - cooperative_shortening_request via  SPMS-6308 - SCI_CMD AND NOT  SPT2TRAFFIC-16433 - The request is valid, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7787 - cooperative_shortening_request_response with "CooperativeShorteningResponseCode: Invalid" via  SPMS-6308 - SCI_CMD







Rationale	When ETPS received an invalid request for a Cooperative Shortening, it shall respond to PES to inform about the invalidity of the request.
ID	SPT2TRAFFIC-16354
Type	 System Requirement

Respond to accepted Cooperative Shortening Request via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-4949 - 137_request_to_shorten_MA_is_granted via  SPMS-6306 - I_SUBSET_026, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7787 - cooperative_shortening_request_response with "CooperativeShorteningResponseCode: Accepted" via  SPMS-6308 - SCI_CMD.

Rationale	When ETPS received an acceptance of the Cooperative Shortening request from the relevant ETCS on-board, it shall inform PES of this result.
ID	SPT2TRAFFIC-16350
Type	 System Requirement

Respond to rejected Cooperative Shortening Request via SCI-CMD


When  SPMS-5062 - European Trackside Protection System receives  SPMS-4950 - 138_request_to_shorten_MA_is_rejected via  SPMS-6306 - I_SUBSET_026, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7787 - cooperative_shortening_request_response with "CooperativeShorteningResponseCode: Rejected" via  SPMS-6308 - SCI_CMD.

Rationale	When ETPS received a rejection of the Cooperative Shortening request from the relevant ETCS on-board, it shall inform PES of this result.
-----------	---

ID	SPT2TRAFFIC-16356
Type	 System Requirement

6.2.6 Function "Authorise usage restrictions areas"

6.2.6-1 - Authorise usage restriction areas









This function is allocated to  SPMS-5062 - European Trackside Protection System.

This function checks if the requested usage restriction area creation or deletion can be implemented safely and executes it if so. In case it cannot be safely implemented the request is rejected.

ID	SPMS-5724
----	-----------









6.2.6.1 Activation via SCI_CMD without signaller confirmation

Respond to accepted Usage Restriction Request (activate track closure without confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: False" AND "SpecificRestriction.RestrictedAspect.trackClosure: True" via  SPMS-6308 - SCI_CMD AND  SPT2TRAFFIC-16433 - The request is valid AND NOT  SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: accepted" via  SPMS-6308 - SCI_CMD.








ID	SPT2TRAFFIC-13752
Type	 System Requirement

Respond to rejected Usage Restriction Request (activate track closure without confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: False" AND "SpecificRestriction.RestrictedAspect.trackClosure: True" via  SPMS-6308 - SCI_CMD AND [ SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission OR NOT  SPT2TRAFFIC-16433 - The request is valid], the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: rejected" via  SPMS-6308 - SCI_CMD.








ID	SPT2TRAFFIC-14358
Type	 System Requirement

Respond to accepted Usage Restriction Request (activate non-switchability without confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: False" AND "SpecificRestriction.RestrictedAspect.nonSwitchability: True" via  SPMS-6308 - SCI_CMD AND  SPT2TRAFFIC-16433 - The request is valid, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: accepted" via  SPMS-6308 - SCI_CMD.











ID	SPT2TRAFFIC-16407
Type	 System Requirement

Respond to rejected Usage Restriction Request (activate non-switchability without confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: False" AND "SpecificRestriction.RestrictedAspect.nonSwitchability: True" via  SPMS-6308 - SCI_CMD AND NOT  SPT2TRAFFIC-16433 - The request is valid, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: rejected" via  SPMS-6308 - SCI_CMD.








ID	SPT2TRAFFIC-16409
Type	 System Requirement


Respond to accepted Usage Restriction Request (activate manually operated point without confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-2407 - usage_restriction_request with "RequestType: Activation" AND "SignallerConfirmation: False" AND "SpecificRestriction.RestrictedAspect.manualOperationOnly: True" via  SPMS-6308 - SCI_CMD AND  SPRM-1699 - Point is free of occupancy AND NOT  SPRM-1775 - Point is reserved for one movement permission AND NOT  SPT2TRAFFIC-16395 - Point is locked AND  SPT2TRAFFIC-16433 - The request is valid, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: accepted" via  SPMS-6308 - SCI_CMD.

ID	SPT2TRAFFIC-16390
Type	 System Requirement







Respond to rejected Usage Restriction Request (activate manually operated point without confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: False" AND "SpecificRestriction.RestrictedAspect.manualOperationOnly: True" via  SPMS-6308 - SCI_CMD AND NOT [
 SPRM-1699 - Point is free of occupancy
OR  SPT2TRAFFIC-16433 - The request is valid],
the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 -

restriction_area_request_response with "restrictionAreaResponseCode: rejected" via  SPMS-6308 - SCI_CMD.







ID	SPT2TRAFFIC-16391
Type	 System Requirement

Respond to accepted Usage Restriction Request (activate temporary speed restriction without confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: False" AND "SpecificRestriction.RestrictedAspect.speedRestriction: True" via  SPMS-6308 - SCI_CMD AND NOT {c} SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission AND {c} SPRM-1747 - Requested usage restriction parameters adheres to infrastructure and train-side restrictions, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: accepted" via  SPMS-6308 - SCI_CMD.

ID	SPT2TRAFFIC-13994
Type	 System Requirement






Respond to rejected Usage Restriction Request (activate temporary speed restriction without confirmation) via SCI-CMD


When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: False" AND "SpecificRestriction.RestrictedAspect.speedRestriction: True" via  SPMS-6308 - SCI_CMD AND [{c} SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission OR NOT {c} SPRM-1747 - Requested usage restriction parameters adheres to infrastructure and train-side restrictions], the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: rejected" via  SPMS-6308 - SCI_CMD.

ID	SPT2TRAFFIC-14374
Type	 System Requirement

6.2.6.2 Activation via SCI_CMD with signaller confirmation






Respond to forwarded Usage Restriction Request (activate track closure with confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: True" AND "SpecificRestriction.RestrictedAspect.trackClosure: True" via  SPMS-6308 - SCI_CMD AND {c} SPT2TRAFFIC-16433 - The request is valid AND NOT {c} SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 -

restriction_area_request_response with "restrictionAreaResponseCode: forwarded" via  SPMS-6308 - SCI_CMD.







ID	SPT2TRAFFIC-16463
Type	 System Requirement

Request signaller confirmation for Usage Restriction Request (activate track closure)

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: True" AND "SpecificRestriction.RestrictedAspect.trackClosure: True" via  SPMS-6308 - SCI_CMD AND {c} SPT2TRAFFIC-16433 - The request is valid AND NOT {c} SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission, the  SPMS-5062 - European Trackside Protection System shall send URAConfirmationRequest via  SPMS-6985 - I_Signaller.







ID	SPT2TRAFFIC-16570
Type	 System Requirement

Respond to invalid Usage Restriction Request (activate track closure with confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: True" AND "SpecificRestriction.RestrictedAspect.trackClosure: True" via  SPMS-6308 - SCI_CMD AND [{c} SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission OR NOT {c} SPT2TRAFFIC-16433 - The request is valid], the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: invalid" via  SPMS-6308 - SCI_CMD.

ID	SPT2TRAFFIC-16472
Type	 System Requirement







Respond to forwarded Usage Restriction Request (activate non-switchability with confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: True" AND "SpecificRestriction.RestrictedAspect.nonSwitchability: True" via  SPMS-6308 - SCI_CMD AND {c} SPT2TRAFFIC-16433 - The request is valid, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: forwarded" via  SPMS-6308 - SCI_CMD.

ID	SPT2TRAFFIC-16471
----	-------------------








Type	 System Requirement
------	--

Request signaller confirmation for Usage Restriction Request (activate non-switchability)

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: True" AND "SpecificRestriction.RestrictedAspect.nonSwitchability: True" via  SPMS-6308 - SCI_CMD AND  SPT2TRAFFIC-16433 - The request is valid, the  SPMS-5062 - European Trackside Protection System shall send URAConfirmationRequest via  SPMS-6985 - I_Signaller.











ID	SPT2TRAFFIC-16572
Type	 System Requirement

Respond to invalid Usage Restriction Request (activate non-switchability with confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: True" AND "SpecificRestriction.RestrictedAspect.nonSwitchability: True" via  SPMS-6308 - SCI_CMD AND NOT  SPT2TRAFFIC-16433 - The request is valid, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: invalid" via  SPMS-6308 - SCI_CMD.




ID	SPT2TRAFFIC-16470
Type	 System Requirement



Respond to forwarded Usage Restriction Request (activate manually operated point with confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-2407 - usage_restriction_request with "RequestType: Activation" AND "SignallerConfirmation: True" AND "SpecificRestriction.RestrictedAspect.manualOperationOnly: True" via  SPMS-6308 - SCI_CMD AND  SPRM-1699 - Point is free of occupancy AND NOT  SPRM-1775 - Point is reserved for one movement permission AND NOT  SPT2TRAFFIC-16395 - Point is locked AND  SPT2TRAFFIC-16433 - The request is valid, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: forwarded" via  SPMS-6308 - SCI_CMD.

ID	SPT2TRAFFIC-16469
Type	 System Requirement







Request signaller confirmation for Usage Restriction Request (activate manually operated point)

When  SPMS-5062 - European Trackside Protection System receives  SPMS-2407 - usage_restriction_request with "RequestType: Activation" AND "SignallerConfirmation: True" AND "SpecificRestriction.RestrictedAspect.manualOperationOnly: True" via  SPMS-6308 - SCI_CMD

AND {c} SPRM-1699 - Point is free of occupancy
 AND NOT {c} SPRM-1775 - Point is reserved for one movement permission
 AND NOT {c} SPT2TRAFFIC-16395 - Point is locked
 AND {c} SPT2TRAFFIC-16433 - The request is valid,
 the  SPMS-5062 - European Trackside Protection System shall send URAConfirmationRequest via
 SPMS-6985 - I_Signaller.







ID	SPT2TRAFFIC-16571
Type	 System Requirement

Respond to invalid Usage Restriction Request (activate manually operated point with confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 -
 restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: True" AND
 "SpecificRestriction.RestrictedAspect.manualOperationOnly: True" via  SPMS-6308 - SCI_CMD
 AND NOT [
 {c} SPRM-1699 - Point is free of occupancy
 OR {c} SPT2TRAFFIC-16433 - The request is valid],
 the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 -
 restriction_area_request_response with "restrictionAreaResponseCode: invalid" via  SPMS-6308 -
 SCI_CMD.




ID	SPT2TRAFFIC-16467
Type	 System Requirement



Respond to forwarded Usage Restriction Request (activate temporary speed restriction with confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 -
 restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: True" AND
 "SpecificRestriction.RestrictedAspect.speedRestriction: True" via  SPMS-6308 - SCI_CMD
 AND NOT {c} SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission
 AND {c} SPRM-1747 - Requested usage restriction parameters adheres to infrastructure and train-
 side restrictions,
 the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 -
 restriction_area_request_response with "restrictionAreaResponseCode: forwarded" via  SPMS-6308 -
 SCI_CMD.

ID	SPT2TRAFFIC-16466
Type	 System Requirement







Request signaller confirmation for Usage Restriction Request (activate temporary speed restriction)

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 -
 restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: True" AND
 "SpecificRestriction.RestrictedAspect.speedRestriction: True" via  SPMS-6308 - SCI_CMD
 AND NOT {c} SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission
 AND {c} SPRM-1747 - Requested usage restriction parameters adheres to infrastructure and train-

side restrictions,
the  SPMS-5062 - European Trackside Protection System shall send URAConfirmationRequest via  SPMS-6985 - I_Signaller.

ID	SPT2TRAFFIC-16573
Type	 System Requirement






Respond to invalid Usage Restriction Request (activate temporary speed restriction with confirmation) via SCI-CMD

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SignallerConfirmation: True" AND "SpecificRestriction.RestrictedAspect.speedRestriction: True" via  SPMS-6308 - SCI_CMD AND [
{c} SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission
OR NOT {c} SPRM-1747 - Requested usage restriction parameters adheres to infrastructure and train-side restrictions],
the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: invalid" via  SPMS-6308 - SCI_CMD.

ID	SPT2TRAFFIC-16468
Type	 System Requirement





6.2.6.3 Activation via I_Signaller

Respond to accepted Usage Restriction Request (activate track closure) via I_Signaller

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SpecificRestriction.RestrictedAspect.trackClosure: True" via Signaller_Interface AND NOT {c} SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission AND {c} SPT2TRAFFIC-16433 - The request is valid,
the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: accepted" via  SPMS-6985 - I_Signaller.

ID	SPT2TRAFFIC-13977
Type	 System Requirement







Respond to rejected Usage Restriction Request (activate track closure) via I_Signaller

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SpecificRestriction.RestrictedAspect.trackClosure: True" via Signaller_Interface AND [{c} SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission OR NOT {c} SPT2TRAFFIC-16433 - The request is valid],
the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 -

restriction_area_request_response with "restrictionAreaResponseCode: rejected" via I_Signaller.







ID	SPT2TRAFFIC-14371
Type	 System Requirement

Respond to accepted Usage Restriction Request (activate non-switchability) via I_Signaller

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SpecificRestriction.RestrictedAspect.nonSwitchability: True" via Signaller_Interface AND  SPT2TRAFFIC-16433 - The request is valid, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: accepted" via  SPMS-6985 - I_Signaller.







ID	SPT2TRAFFIC-16410
Type	 System Requirement

Respond to rejected Usage Restriction Request (activate non-switchability) via I_Signaller

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SpecificRestriction.RestrictedAspect.nonSwitchability: True" via Signaller_Interface AND NOT  SPT2TRAFFIC-16433 - The request is valid, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: rejected" via  SPMS-6985 - I_Signaller.




ID	SPT2TRAFFIC-16411
Type	 System Requirement




Respond to accepted Usage Restriction Request (activate manually operated point) via I_Signaller

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SpecificRestriction.RestrictedAspect.manualOperationOnly: True" via Signaller_Interface AND  SPT2TRAFFIC-16433 - The request is valid, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: accepted" via  SPMS-6985 - I_Signaller.

ID	SPT2TRAFFIC-14369
Type	 System Requirement






Respond to rejected Usage Restriction Request (activate manually operated point) via I_Signaller

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SpecificRestriction.RestrictedAspect.manualOperationOnly: True" via Signaller_Interface AND NOT  SPT2TRAFFIC-16433 - The request is valid,

the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: rejected" via  SPMS-6985 - I_Signaller.






ID	SPT2TRAFFIC-13978
Type	 System Requirement

Respond to accepted Usage Restriction Request (activate temporary speed restriction) via I_Signaller

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SpecificRestriction.RestrictedAspect.speedRestriction: True" via Signaller_Interface AND NOT {c} SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission AND {c} SPRM-1747 - Requested usage restriction parameters adheres to infrastructure and train-side restrictions, the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: accepted" via  SPMS-6985 - I_Signaller.

ID	SPT2TRAFFIC-14335
Type	 System Requirement







Respond to rejected Usage Restriction Request (activate temporary speed restriction) via I_Signaller

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Activation" AND "SpecificRestriction.RestrictedAspect.speedRestriction: True" via Signaller_Interface AND [{c} SPT2TRAFFIC-16428 - Usage restriction area is reserved for one movement permission OR NOT {c} SPRM-1747 - Requested usage restriction parameters adheres to infrastructure and train-side restrictions], the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7801 - restriction_area_request_response with "restrictionAreaResponseCode: rejected" via  SPMS-6985 - I_Signaller.

ID	SPT2TRAFFIC-14373
Type	 System Requirement








6.2.6.4 Deactivation via SCI_CMD without signaller confirmation

Respond to accepted Usage Restriction Request via SCI_CMD without signaller confirmation

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Deactivation" via  SPMS-6308 - SCI_CMD AND {c} SPT2TRAFFIC-16475 - Restriction Area can be deleted without signaller confirmation the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7837 - Draft_RestrictionAreaRequestResponse with "restrictionAreaRequestResponse: accepted" via  SPMS-6308 - SCI_CMD.

ID	SPT2TRAFFIC-16476
Type	 System Requirement








Respond to rejected Usage Restriction Request via SCI_CMD without signaller confirmation

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Deactivation" via  SPMS-6308 - SCI_CMD AND  SPT2TRAFFIC-16475 - Restriction Area can be deleted without signaller confirmation the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7837 - Draft_RestrictionAreaRequestResponse with "restrictionAreaRequestResponse: rejected" via  SPMS-6308 - SCI_CMD.

ID	SPT2TRAFFIC-16477
Type	 System Requirement







6.2.6.5 Deactivation via SCI_CMD with signaller confirmation

Respond to forwarded Usage Restriction Request (deactivation) via SCI_CMD with signaller confirmation

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Deactivation" via  SPMS-6308 - SCI_CMD AND NOT  SPT2TRAFFIC-16475 - Restriction Area can be deleted without signaller confirmation the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7837 - Draft_RestrictionAreaRequestResponse with "restrictionAreaRequestResponse: forwarded" via  SPMS-6308 - SCI_CMD.





ID	SPT2TRAFFIC-16478
Type	 System Requirement




Request signaller confirmation for Usage Restriction Request (deactivation)

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Deactivation" via  SPMS-6308 - SCI_CMD AND NOT  SPT2TRAFFIC-16475 - Restriction Area can be deleted without signaller confirmation the  SPMS-5062 - European Trackside Protection System shall send URAConfirmationRequest via  SPMS-6985 - I_Signaller.

ID	SPT2TRAFFIC-16480
Type	 System Requirement

Respond to invalid Usage Restriction Request (deactivation) via SCI_CMD with signaller confirmation







When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Deactivation" via  SPMS-6308 - SCI_CMD AND NOT  SPT2TRAFFIC-16475 - Restriction Area can be deleted without signaller confirmation

the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7837 - Draft_RestrictionAreaRequestResponse with "restrictionAreaRequestResponse: invalid" via  SPMS-6308 - SCI_CMD.

ID	SPT2TRAFFIC-16479
Type	 System Requirement

6.2.6.6 Deactivation via I_Signaller






Respond to accepted Usage Restriction Request (deactivation) via I_Signaller

When  SPMS-5062 - European Trackside Protection System receives  SPMS-7754 - restriction_area_request with "RequestType: Deactivation" via  SPMS-6985 - I_Signaller the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7837 - Draft_RestrictionAreaRequestResponse with "restrictionAreaRequestResponse: rejected" via  SPMS-6985 - I_Signaller.

ID	SPT2TRAFFIC-14379
Type	 System Requirement






6.2.6.7 Signaller confirmation

Respond to confirmed Usage Restriction Request

When  SPMS-5062 - European Trackside Protection System receives URAConfirmationRequestResponse with "Confirmed: True" via  SPMS-6985 - I_Signaller the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7837 - Draft_RestrictionAreaRequestResponse with "restrictionAreaRequestResponse: accepted" via  SPMS-6308 - SCI_CMD.

ID	SPT2TRAFFIC-16481
Type	 System Requirement

Respond to unconfirmed Usage Restriction Request

When  SPMS-5062 - European Trackside Protection System receives URAConfirmationRequestResponse with "Confirmed: False" via  SPMS-6985 - I_Signaller the  SPMS-5062 - European Trackside Protection System shall send  SPMS-7837 - Draft_RestrictionAreaRequestResponse with "restrictionAreaRequestResponse: rejected" via  SPMS-6308 - SCI_CMD.

ID	SPT2TRAFFIC-16482
Type	 System Requirement





6.3 Lifecycle concepts







Will be provided in further release.


DRAFT

7 Appendix

7.1 References

Id	Description	Reference
[ SPP-18362 - EET_Requirements Management Plan Version_1.0]	For System Pillar the plan describes a strategy for traceability between requirements levels, architecture elements and application conditions. Further the type of requirements and their related workflows are defined.	Link
[ SPP-18355 - EET_Systems Engineering Management Plan_V4.0]	The purpose of this Systems Engineering Management Plan (SEMP) is to outline the systems engineering activities of the EU-Rail System Pillar, by providing guidelines, rules and best practices	Link
[ SPP-19283 - Release Note ESPR1.0]	This Release Note describes the scope of the ESPR1.0.	Link
[ SPP-19171 - Risk assessment report for the System Architecture Traffic CS_V0.1]	This document provides the results of the risk assessment of the System Architecture of Traffic CS (according to CENELEC Phase 3, see PRAMS Plan CP 3).	Link

Id	Description	Reference
[ SPP-8684 - System Pillar Common Business Objectives (May 2022)]	Common Business Objectives (CBO) – targets and improvements - to guide the development of the outputs of the System Pillar within Europe's Rail Joint Undertaking.	Link
[ SPP-18571 - TCCS - Data Model_00_Guide]	The document gives guidance for CCS/TMS Data Model specified by SP TCCS SD1	Link
[ SPP-18545 - TCCS - Data Model_11_TP]	This document extends the SD1 data model with the content required by the Train Protection use case for Traffic CS Domain.	Link
[ SPP-18075 - TCS_System Architecture Description Traffic CS_V0.4]	System Architecture Description of the Traffic CS System according to.	Link
[ SPP-19939 - TCS_Traceability Report System Requirement Specification ETPS_V0.4]	This report shows the linking between the System Architecture Description of the Traffic CS system and the System Requirement Specification ETPS.	Link
[ SPP-19049 - Traffic CS System Concept V1.0]	Traffic CS prepared this document to summarise the most	Link

Id	Description	Reference
	important system requirements for Traffic CS and the solution concept how it is foreseen to fulfil these requirements. Furthermore, assumptions and expectations to external systems outside of Traffic CS are stated and roadmap is presented.	
[EN 50126-1:2017">  SPPRAMSS-349 - EN 50126-1:2017]	Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process	-

7.2 Open Points

Required internal actions

There is a clear need for ETPS to perform certain actions that do not include an action related to an external (sub)system, or to perform them before the external action can/should happen. For example, when a new train position report is received, ETPS should use that data together with the already existing state of the system to update the position of said train and release the track behind it and only then should it send this new information to PES. From a pure black-box approach, this internal behaviour should not be considered, and only the in and out of the system are to be described. However, that makes the requirements quite incomplete and missing essential functions. The way to represent this internal action, with a proper deterministic output, is to be considered.

Note: It could also be possible that new information is send to PES on an interval instead of at every update. This is an open point.

Changing variables while checking conditions (between requirements)

Once ETPS is triggered to perform an action, while it is processing this action, it is quite possible that any data about the operating state changes in the meantime. This can be due to new information being received, or due to parallel actions changing this state of the system. This is not an issue for single, stand-alone requirements, but becomes problematic with related, linked requirements. For example, an MP request is received, triggering the two requirements about the action towards the train (sending an MA if possible) and the feedback to PES (accepted/rejected). These two requirements are triggered by the same event, and have the same conditions to be checked. It is therefore likely any supplier

implementation performs it only once for both requirements, however this is not a requirement per se and up to the supplier. If the information changes (for example track occupancy changes) between the two requirements being checked, it could give a different response between the two actions. For example, it might tell PES it is rejected, while still sending an MA to the train, or vice versa. Or if ETPS processed the MP first, and then checks the conditions to send an MA to the train, it might refuse because of the MP stored for the train itself. This last problem is an example, and this specific one might be solved by ignoring the MP for the train itself in the safety conditions, which would help also for the case of MA extension.

Note: this situation does not have a direct impact on safety for single requirements, as long as ETPS takes action on the new information accordingly. For example, ETPS receives an MP request and shortly after there is an unexpected track occupancy. Depending on the exact timing and the way the communication is processed, the MA might be given or not. This might seem like a problem at first, however this is inevitable with non-instantaneous processes, as it will always have to work with slightly outdated information. The important part is of course that after processing the correct action is taken (UES or MA shortening etc) to ensure ETPS react properly to this new information.

General system conditions not included

For a wide range of requirements, there might be some basic/general conditions that have to be met before the action can or should be performed. This can be from the very basic condition the system is on and active, to conditions that the communication session is established so a message can be sent to a train. It is unclear if and how these conditions should be included here.

Edge case/degraded situations not considered

The requirements are assuming a system is working properly, or not working at all. However, in reality there are likely situations where some actions might be possible or allowed, even if the conditions are not fully met. For example, it might be possible for a point to be disturbed, but with a confirmed position. In this case it could be considered to allow train movement to pass, potentially with a lower level of supervision. These cases are not considered, and any such scenarios have to be defined by the Operational Design domain.

Signaller bypass of safety conditions

It might be foreseen for a signaller to have a direct access to ETPS, where it can command ETPS to perform certain actions even if the required safety conditions are not met. This is currently not considered, and any such scenarios have to be defined by the Operational Design domain.

Rejection responses not yet defined

There are multiple requirements (MP request, point position request) where there are multiple reasons for rejection, which should all be included into the rejection to PES. This allows PES to identify all issues to be solved, instead of just one. However, this has to be supported by the SCI-CMD Data Model, with responses allowing to communicate both the acceptance state (accepted/rejected) and the reasons for a rejection.

Required SIL for requirements

The requirements should have a SIL attached to them, based on the outcome of the risk analysis.

Safe conditions for implementing a URA

There are uncertainties about the activation of URAs and the impact on existing trains. If a URA is ignored for existing trains (for example a TSR), this can give the false impression of ETPS supervising a restriction but that is not the case for all trains. Also, when an MA is extended, the TSR could be activated retroactively, leading to a brake intervention. Therefore ETPS should only accept a URA when all trains in the area meet the restriction. This of course depends on the type of restriction, for some an update is sufficient (e.g. maxCurrent).

Quick reaction after safety checks

ETPS checks if a requested point position can be implemented safely. It is then important that the point position command is sent promptly after performing the safety checks to avoid that the operational conditions change and the result of the safety checks is not valid anymore.

Note: Stipulating a timer should be avoided after discussing with Traffic CS. The monitoring of the time it takes to change the point position is allocated to Trackside Assets CS in another constraint.


Train Detection Points still not managed

According to the EULYNX SCI-TDS specification, the Trackside Asset subsystem can send a Train

Detection Point message to inform ETPS that a train has passed a defined track location. This information is currently not managed by the function "Aggregate moveable object information".

Releasing track section behind a train

The release of the track behind a train (technically that would be updating the Movement Permission to not include this section) could be a better fit in another function, as it is completely dependent on the aggregation of the movable object information and the update of the Train Object. As the Movement Permission is currently considered as a part of a Train Object, the current requirement

 SPT2TRAFFIC-11903 - Report Train Object information based on train position reports already implicitly updates the extent of the Movement Permission behind the train, by sending the updated Train Object. This idea, or its rejection, should be properly defined in the technical concepts for resolving track occupancy information and position reports, for the Movement Permission and for the Train Object.

Overlap of riskPath and riskBuffer

While it is clear that the extent of a Movement Permission should never overlap another riskPath or RiskBuffer, as that would defeat the purpose of such an additional reservation, it is not clear whether it is allowed for two riskBuffer to overlap. In such a case in the nominal case neither train will use that part of the track, and even if one of the two trains needs this buffer area, the second train will not occupy that space. So for it to become an issue, both train will have to overpass their supervised End of Authority. This scenario should be considered in a risk analysis, after which a conclusion on this can be made. This should also be considered for the riskPath, and for a combination of riskPath and riskBuffer.

Check for Allocation Section -> Fouling sections

The conditions do not check for any Allocation Sections explicitly. Whether or not this is needed, depends on the way it is being modeled. For example, one way to do it, would be for ETPS to check for any Allocation Sections when it receives the Movement Permission request and include that section as a riskPath section in the Movement Permission. This will ensure it is properly checked for every future condition checking the riskPath. Another is to check for Allocation Sections every time any safety checks have to be done. This would need an extra condition in the requirement.

Route suitability checks

There is currently no consideration for route suitability in whether or not an MP can be accepted. While not all route incompatibilities have an direct impact on safety, for example a wrong traction system might lead to a stranded train with only operational and/or asset impact, there should be a risk analysis to see if there are any checks that require a SIL. If so, those checks should be done by ETPS, while checks with basic integrity can happen in TMS and/or PES.

ETPS Requirements for Shorten MP

- 1) it needs to be clarified where to specify how the path reservation is handled depending on the feedback of Train CS (e.g. how can the track path be released when the request to shorten MP was accepted by Train CS).
- 2) Even if we currently do only consider good weather scenarios, for a robust ETPS we need to specify also the handling if message 137/138 is received but cannot be mapped to any previously sent request to Shorten MA (i.e. T_TRAIN)
- 3) ETPS also needs to remember T_TRAIN in the message of the request to shorten MA to be able to map later any answer from Train CS to this specific request. Therefore, dimensioning rules (e.g. how many requests to shorten MAs should ETPS be able to handle at minimum at the same time) should be specified.

Multiplicity of Restricted Aspects when only some aspects are considered

When, as an example, a URA is requested for the NonSwitchability of a point, the rest of the possible restricted aspects are not relevant. This is easy for the restriction using a boolean type, but currently also the speedRestriction needs to have an input. This should not be necessary, as it creates extra steps and options for failure. Proposal would be to either have the restricted aspects optional, only when applicable, or to have an identifier to state whether this aspect is applicable for this URA.

Also, the model seems to have multiple 'SpecificRestriction' instances for each single restriction.

Signaller interface not modelled

The Interface between ETPS and Signaller ist not yet modelled. Therefore, exchange items are missing.