




ERJU SYSTEM PILLAR

51 Risk assessment report for the System Architecture Description CCS System



Risk assessment report for the System Architecture Description CCS System

Author(s)	Morman Bettina (I-NAT-GST-CCS) , Teresa Hernandez Sanchez , Pasquale Ondino , Vlček Martin, Mgr.PhD. , BUYUKAKINCAK Emre
Abstract	The purpose of this document is to provide the results of the risk assessment of the CCS-System Architecture (according to CENELEC Phase 3
Config Item	System PRAMS Risk Assessment Report
Document ID	System Level 3_ EN50126 - CCS System/51 Risk assessment report for the System Architecture Description CCS System#726037  51 Risk assessment report for the System Architecture Description CCS System
Classification	Public
Status	In Review by System Pillar
Version	0.2
Revision	726037
Last Change Date	06.10.2025
Copyright	Brussels: Europe's Rail Joint Undertaking, 2025

© Europe's Rail Joint Undertaking, 2025

This document is drafted by and belongs to EU Rail.

EU Rail encourages the distribution and re-use of this document, the technical specifications and the information it contains. EU Rail holds several intellectual property rights, such as copyright and trade mark rights, which need to be considered when this document is used.

EU Rail authorises you to re-publish, re-use, copy and store this document without changing it, provided that you indicate its source and include the following: EU Rail trade mark, title of the document, year of publication, version of document.

EU Rail makes no representation or warranty as to the accuracy or completeness of the information contained within these documents. EU Rail shall have no liability to any party as a result of the use of the information contained herein. EU Rail will have no liability whatsoever for any indirect or consequential loss or damage, and any such liability is expressly excluded.

You may study, research, implement, adapt, improve and otherwise use the information, the content and the models in the this document for your own purposes. If you decide to publish or disclose any adapted, modified or improved version of this document, any amended implementation or derivative work, then you must indicate that you have modified this document, with a reference to the document name and the terms of use of this document. You may not use EU Rail's trade marks or name in any way that may state or suggest, directly or indirectly, that EU Rail is the author of your adaptations.

EU Rail cannot be held responsible for your product, even if you have used this document and its content. It is your responsibility to verify the quality, completeness and the accuracy of the information you use, for your own purposes.

This work is currently a work in progress. The content presented is subject to change as it undergoes further review, refinement, and development. Please do not consider this version as final or authoritative.

INFO: History table is not displayed, because this document is in status [doc_contentApproval](#).

RULE: History table is not displayed, in statuses: { draft doc_open doc_inprogress doc_contentApproval doc_contentDecision }

CONTACT: For more information contact Administrator

Approval by reviewers

(captured at end of 'In Review by System Pillar')

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

Approval by approvers

(captured at end of 'In Approval by System Pillar')

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

DRAFT

1	Preamble	5
1.1	Purpose	5
1.2	Intended Audience	5
1.3	Document Context	5
1.4	Glossary	7
1.4.1	Terms	7
1.4.2	Abbreviations	7
2	Scope	8
3	Risk analysis	10
3.1	Risk tracing report	10
3.2	Risk assessment report	10
3.3	Detailed Failure Modes and Effect Analysis	10
3.3.1	Traffic CS functions	10
3.3.1.1	Aggregate movable object information	10
3.3.1.1.1	Functional description	10
3.3.1.1.2	Failure Modes and Effects Analysis	12
3.3.1.1.3	Constraints	12
3.3.1.2	Control target state of one point	13
3.3.1.2.1	Functional description	13
3.3.1.2.2	Failure Modes and Effects Analysis	14
3.3.1.2.3	Constraints	17
3.3.1.3	Control track path allocation for movement permission	18
3.3.1.3.1	Functional description	18
3.3.1.3.2	Failure Modes and Effects Analysis	21
3.3.1.3.3	Constraints	29
3.3.1.4	Control usage restrictions	30
3.3.1.4.1	Functional description	30
3.3.1.4.2	Failure Modes and Effects Analysis	32
3.3.1.4.3	Constraints	32
3.3.1.5	Observe point status	33
3.3.1.5.1	Functional description	33
3.3.1.5.2	Failure Modes and Effects Analysis	33
3.3.1.5.3	Constraints	33
4	Appendix	34
4.1	References	34

1 Preamble

1.1 Purpose

The purpose of this document is to provide the results of the risk assessment of the CCS-System Architecture (according to CENELEC Phase 3, see [📄 SPT2TRAFFIC-13107 - ERJU PRAMS Plan]).

For a wider view on risk assessment covering safety culture as well as the variety of possible risk assessment methods, please take a look at the Safety Guideline provided by the PRAMS team [📄 SPT2TRAFFIC-4141 - ERJU Safety Guideline].

While the risk assessment has to be done in the context of Performance, RAM, Safety and Security, the first version of this document focusses on Safety and RAM topics.

1.2 Intended Audience

This document is intended for all stakeholders involved in the development, implementation, and operation of CCS systems (e.g. Business stakeholders, End users, Development and engineering teams, Assessors, etc).

1.3 Document Context

As shown in the illustration below (👤 SPP-31589 - Dependencies between Configuration Items), the Risk assessment report for the System Architecture Description of the 📄 SPMS-2098 - CCS System is based on the following inputs:

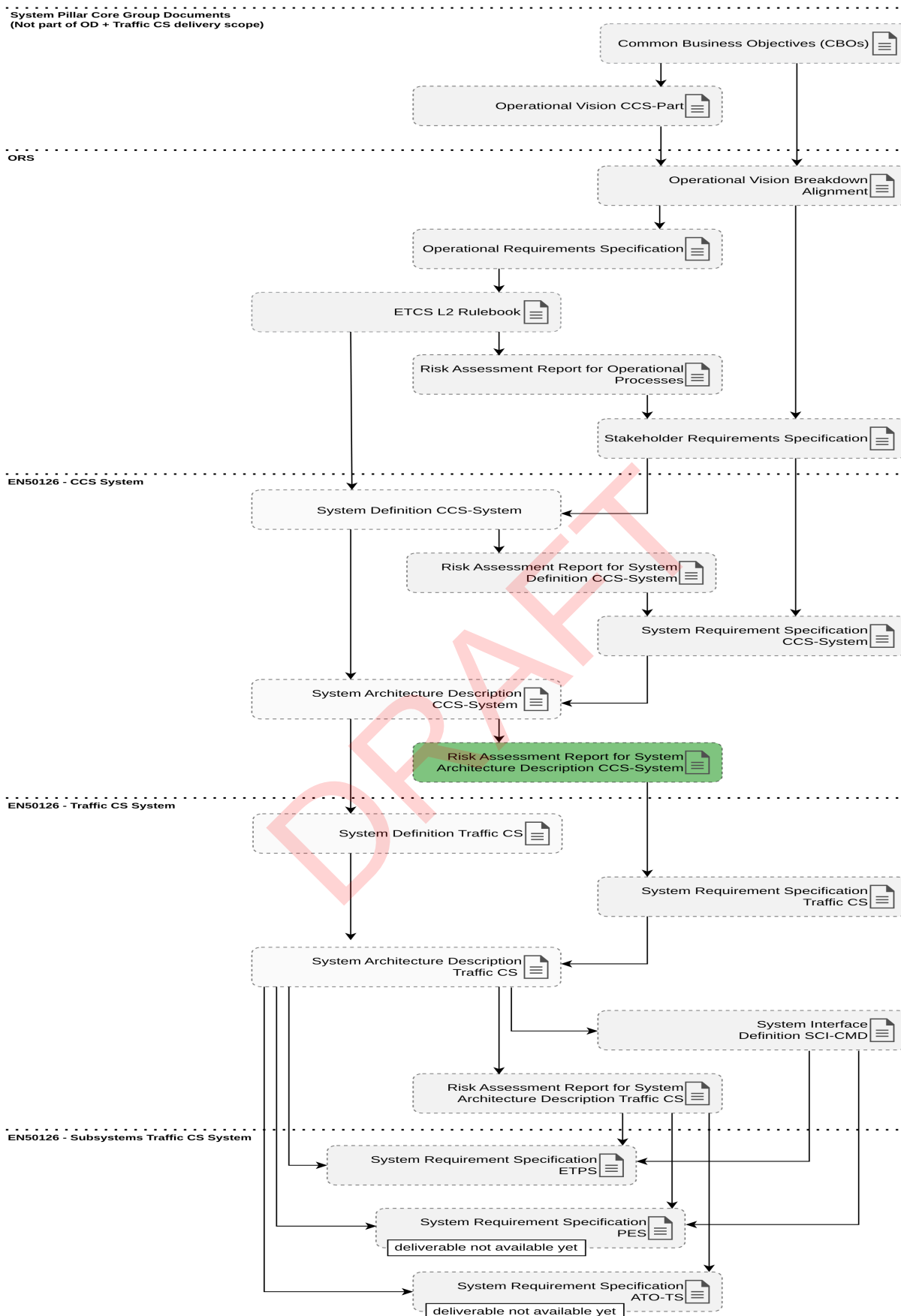
- [📄 SPP-18060 - TCS_System Architecture Description CCS System V0.3]:
This document allocates the functions and requirements identified for the CCS-Systems (System Level 3 system) to the different System Level 4 systems. Traffic CS is one of these System Level 4 systems.

Note:
The System Architecture Definition CCS contains changes in Release 1 that were not analysed yet. They will be assessed in a later point in time. In the scope of the analysis, the versions of the scenarios of the Architecture Description of the CCS System that were analysed are referenced.
- [📄 SPT2TRAFFIC-13108 - ERJU Hazard Database - Main Document]:
This document details the European Railway Harmonized Hazards Database to be used for risk assessment by ERJU SP Domains in accordance with ERJU PRAMS Plan and guidelines.

The Risk Assessment report for the System Architecture Description CCS itself is an input document for the 📄 SPP-18108 - TCS_System Requirement Specification Traffic CS_V0.2.

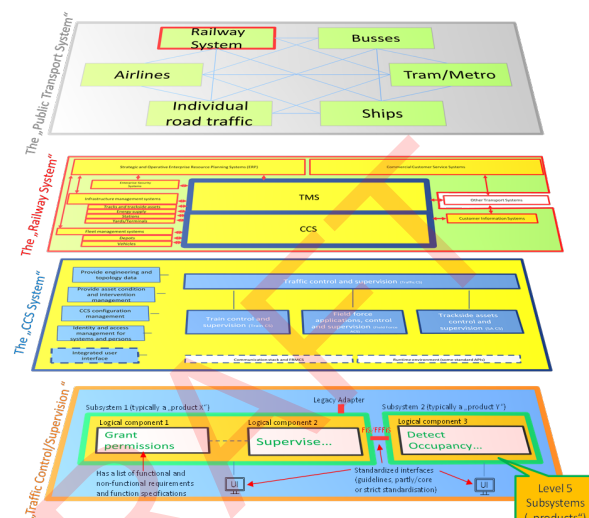
Further details regarding document independencies are described in 📄 SPP-18362 - Requirements Management Plan v2.0]. The positioning of the ETCS L2 Rulebook within the document framework is shown in 👤 SPP-31533 - Dependencies between Configuration Items.

The risk traceability report showing all system functions and their related risks that need to be allocated to the corresponding exchanges and functions on System Level 4 (logical architecture) is made available in 📄 SPP-31659 - TCS_System Architecture Description CCS System - Annex B Traceability Report Risk_V0.2. A summary of the most important results of the risk assessment of the CCS System Architectures is made available in: 📄 SPP-31654 - Risk assessment report for the System Architecture Description CCS System - Annex A Traceability Report_V0.2.



1.4 Glossary

1.4.1 Terms

Term	Definition
System Levels of the System Pillar	<p>The system of systems approach is used inside the System Pillar to recursively refine the structure of the architecture down to the level of subsystems.</p> <p>The following figure shows the decomposition of a system of systems on one consistent example spanning 5 layers of refinement. Level 5 is the actual subsystem layer and is visually integrated into the bottom layer in the following figure to be able to show the relationship to logical components.</p>  <p>Figure 1: System Level 1-5 combined view</p>

1.4.2 Abbreviations

Abbreviation	Definition
CCS	Control-Command and Signalling
FMEA	Failure Mode and Effects Analysis

2 Scope

For performing a qualitative risk analysis, the FMEA method is used, whereby FMEA stands for Failure mode and effects analysis. How to perform an FMEA is described in [SPT2TRAFFIC-13109 - ERJU Risk Assessment Process & Template]. The FMEA is conducted with the help of the Nextedy RiskSheet tool in Polarion.

FMEA represents an inductive/bottom-up risk analysis, starting with possible failure modes of a function and analysing their effects on the function itself, on the system under consideration as well as on the railway system in total. The goal of the FMEA of the CCS system definition is to:



























- Identify safety-relevant functions and interfaces,
- Identify potential new hazards,
- connect failure modes to hazards and accidents of Europe's Rail Hazard Database

































The scope of analysis are the exchanges between the Traffic CS system and the other CCS-subsystems. The analysis of the output exchanges of the Traffic CS System to the other CCS-subsystems (Train CS, Transversal CS, Trackside Assets CS) is structured by Traffic CS Logical function. Traffic CS-internal exchanges are not analysed.

The analysis of the output exchanges of the CCS-subsystems (Train CS, Transversal CS, Trackside Assets CS) to the Traffic CS System is done by the corresponding System Pillar domains and is not part of this document.

Please note: Following the initial hazard identification and assignment of safety requirements, quantitative risk assessment will be performed using Fault Tree Analysis when the system architecture is defined during the design and development phases, in accordance with CENELEC standards.

The base for the risk analysis are the following scenarios:


System capability	Scenarios	Revision
  SPMS-3318 - Activate usage restriction	  SPMS-4355 - Activate usage restriction (Planned usage restriction)   SPMS-4469 - Activate usage restriction	698919
  SPMS-4518 - Deactivate usage restriction	  SPMS-4363 - Deactivate usage restriction (Planned usage restriction)   SPMS-4470 - Deactivate usage restriction	698919
  SPMS-3305 - Grant movement permission	  SPMS-5368 - Grant movement permission (Operational plan)   SPMS-4462 - Grant movement permission	661872
  SPMS-3309 - Localise train on railway infrastructure	  SPMS-4364 - Localise train on railway infrastructure   SPMS-4465 - Localise train on railway infrastructure (Detect track vacancy proving section occupation)   SPMS-4474 - Localise train on railway	559486

System capability	Scenarios	Revision
	infrastructure (Determine localisation information for one train)	
  SPMS-2440 - Perform train movement	  SPMS-4333 - Perform train movement (Full supervision)   SPMS-4447 - Perform train movement (Full supervision control loop)	541808
  SPMS-5345 - Release movement permission	  SPMS-5369 - Release movement permission   SPMS-5364 - Release movement permission	559486
  SPMS-3312 - Set point position	  SPMS-4382 - Set point position (Left to right, Operational plan)   SPMS-4692 - Set point position (Left to right, Signaller request)   SPMS-4476 - Set point position	559406
  SPMS-5041 - Shorten movement permission	  SPMS-5047 - Shorten movement permission (Operational plan change, accepted)   SPMS-5131 - Shorten movement permission (Operational plan change, rejected)   SPMS-5170 - Shorten movement permission (Signaller request, accepted)   SPMS-5171 - Shorten movement permission (Signaller request, rejected)   SPMS-5426 - Shorten movement permission (Cooperative shortening of movement permission)	559406


Please refer to the scenarios listed above in order to understand the context in which the functions are analysed (e.g. which exchange items of the analysis are in scope, the target function, pre- and postconditions).

3 Risk analysis


3.1 Risk tracing report

The Risk Traceability Report is showing all system functions and their related risks that need to be allocated to the corresponding exchanges and functions on System Level 4 (logical architecture). The Risk Traceability Report is made available in  SPP-31659 - TCS_System Architecture Description CCS System - Annex B Traceability Report Risk_V0.2

3.2 Risk assessment report

This Risk Assessment Report is the overview of the most important results of the Risk Analysis performed for the CCS System Architecture. The Risk assessment report is made available in  SPP-31659 - TCS_System Architecture Description CCS System - Annex B Traceability Report Risk_V0.2.

3.3 Detailed Failure Modes and Effect Analysis

The following chapters list the detailed results of the risk analysis of the CCS system specified in the scope of the capabilities listed in  SPP-19787 - *Missing cross-reference* and presented in the linked reports above.

3.3.1 Traffic CS functions

3.3.1.1 Aggregate movable object information

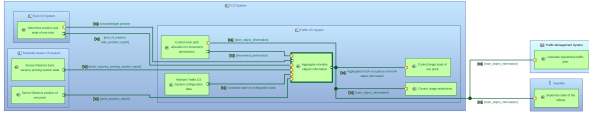
3.3.1.1.1 Functional description





















Aggregate movable objects information























This function is allocated to  SPMS-2823 - Traffic CS System.

This function aggregates and stores information (e.g. position) submitted by different actors (e.g., Trackside Asset CS, Train CS) and outputs of other functions into an operational state representation of movable objects.

Movable objects are defined as trains and wagons that either submit localisation and/or additional data (such as speed and status) or are localised by alternative technologies such as TTD systems. The scope is extended to include track workers (actor Field Force) that have an own localisation device. Further extension of the scope can be done in the following analysis steps.

ID	SPMS-2944
Context Diagram	 <p>The diagram shows a central function box labeled 'Aggregate movable objects information' with various inputs and outputs. Inputs include 'Trackside Asset CS', 'Train CS', 'Field Force', and 'TTD systems'. Outputs include 'Operational state representation of movable objects'. The diagram is titled 'Figure 2 Context Diagram of Aggregate movable objects information'.</p>

Input exchanges	Input exchanges	Source function	Function allocated to	
	 SPMS-3039 - Allocated track path <ul style="list-style-type: none">  SPMS-2372 - movement_permission 	 SPMS-2874 - Control track path allocation for movement permissions	 SPMS-2823 - Traffic CS Sy	
	 SPMS-3212 - Determined train position and state <ul style="list-style-type: none">  SPMS-7042 - end_of_mission  SPMS-6664 - train_position_report 	 SPMS-2878 - Determine position and state of one train	 SPMS-2807 - Train CS Sys	
	No exchange items allocated on  SPMS-3130 - Activated state of configuration data.	 SPMS-2840 - Maintain Traffic CS System configuration data	 SPMS-2823 - Traffic CS Sy	
	 SPMS-5268 - Observed point position <ul style="list-style-type: none">  SPMS-3283 - point_position_report 	 SPMS-2914 - Sense+Observe position of one point	 SPMS-2818 - Trackside As	
	 SPMS-4648 - Observed track vacancy proving section state <ul style="list-style-type: none">  SPMS-6569 - track_vacancy_proving_section_report 	 SPMS-2919 - Sense+Observe track vacancy proving section state	 SPMS-2818 - Trackside As	

Output exchanges	Output exchanges	Target function	Function allocated to
	 SPMS-3021 - Aggregated track occupancy and train status information <ul style="list-style-type: none">  SPMS-5562 - train_object_information 	 SPMS-2874 - Control track path allocation for movement permissions	 SPMS-2823 - Traffic CS System
	 SPMS-3028 - Aggregated track occupancy and train status information <ul style="list-style-type: none">  SPMS-5562 - train_object_information 	 SPMS-2929 - Control usage restrictions	 SPMS-2823 - Traffic CS System
	 SPMS-3050 - Aggregated track occupancy and train status information <ul style="list-style-type: none">  SPMS-5562 - train_object_information 	 SPMS-2843 - Calculate operational traffic plan	 SPMS-2813 - Traffic Management System
	 SPMS-4666 - Aggregated track occupancy and train status information <ul style="list-style-type: none">  SPMS-5562 - train_object_information 	 SPMS-2853 - Supervise state of the railway	 SPMS-2827 - Signaller
	No exchange items allocated on  SPMS-5274 - Aggregated track occupancy and train status information.	 SPMS-5265 - Control target state of one point	 SPMS-2823 - Traffic CS System
	No exchange items allocated on  SPMS-7765 - Acknowledged position.	 SPMS-2878 - Determine position and state of one train	 SPMS-2807 - Train CS System

3.3.1.1.2 Failure Modes and Effects Analysis

There are no output exchanges in scope of the analysed scenarios.

3.3.1.1.3 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
----	-----------

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
----	-----------

3.3.1.2 Control target state of one point



















3.3.1.2.1 Functional description

Control target state of one point

This function is allocated to  SPMS-2823 - Traffic CS System.

This function determines the target position of one point for the planned movement of the train on the intended path. Furthermore, this function receives the requested point position from the Signaller and controls the point position according to this when the respective point is not allocated to an intended path. The time it takes to set the point, and other constraints like electrical load shall be taken into account.














[illegible]

Input exchanges	Input exchange items	Source function	Function allocated to	
	<ul style="list-style-type: none"> SPMS-2370 - operational_plan_movement SPMS-5548 - operational_plan_restriction 	 SPMS-2843 - Calculate operational traffic plan	 SPMS-2813 - Traffic Manager	
	<ul style="list-style-type: none"> SPMS-3283 - point_position_report 	 SPMS-2914 - Sense+Observe position of one point	 SPMS-2818 - Trackside Assets	
	No exchange items allocated on  SPMS-5274 - Aggregated track occupancy and train status information.	 SPMS-2944 - Aggregate movable objects information	 SPMS-2823 - Traffic CS System	
	<ul style="list-style-type: none"> SPMS-2386 - point_position_request 	 SPMS-2853 - Supervise state of the railway	 SPMS-2827 - Signaller	
	<ul style="list-style-type: none"> SPMS-2412 - time_reference 	 SPMS-2922 - Synchronise current time	 SPMS-2819 - Transversal CC	
	No exchange items allocated on  SPMS-5277 - Activated state of configuration data.	 SPMS-2840 - Maintain Traffic CS System configuration data	 SPMS-2823 - Traffic CS System	
	<ul style="list-style-type: none"> SPMS-2372 - movement_permission 	 SPMS-2874 - Control track path allocation for movement permissions	 SPMS-2823 - Traffic CS System	
Output exchanges	Output exchange items	Target function	Function allocated to	
	<ul style="list-style-type: none"> SPMS-3286 - point_position_command 	 SPMS-2851 - Determine required position of one point machine	 SPMS-2818 - Trackside Assets CS System	

3.3.1.2.2 Failure Modes and Effects Analysis














Early required point position to Trackside Assets CS

ID	SPRM-1069
Failure Mode (Keyword)	Commission
Failure Description	Traffic CS sends the point position command to Trackside Assets CS too early.












Effect on Linked Functions Systems	Trackside Assets CS receives the command before Traffic CS has verified internal safety conditions (e.g. point occupancy, movement permission).
Effect on Railway System	Point movement may occur before point is free of occupancy or other, conflicting reservations, potentially leading to conflicting and unsafe movements.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-5265 - Control target state of one point</p> <p>relates to :  SPMS-3227 - Required point position</p> <p>relates to :  SPMS-4476 - Set point position</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>relates to :  SPMS-4382 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4692 - Set point position (Left to right, Signaller request)</p> <p>relates to :  SPMS-4715 - Set point position (Left to right, Operational plan - Traffic CS view)</p> <p>relates to :  SPMS-4788 - Set point position (Left to right, Signaller request - Traffic CS view)</p> <p>assesses :  SPRM-1726 - [XYZ] Undue movement of a point</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-6357 - Commanded point position state</p> <p>has parent :  SPRM-2130 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1699 - Point is free of occupancy</p> <p>_ is mitigated by : {c} SPRM-1775 - Point is reserved for one movement permission</p>

Late required point position to Trackside Assets CS (1/2)













ID	SPRM-1070
Failure Mode (Keyword)	Omission
Failure Description	Traffic CS fails to send the point position command or sends it too late to Trackside Assets CS.
Effect on Linked Functions Systems	<p>a) Trackside Assets CS does not receive the point position command, resulting in no change to the point state.</p> <p>b) Trackside Assets CS receives the point position command too late, resulting in changing the point position when the safety conditions checked by Traffic CS are not valid anymore (e.g. point was moved by another command before the late command was received).</p>
Effect on Railway System	<p>a) Point is in the incorrect position for the intended train movement, meaning that the track path cannot be secured for the train movement. This results in a potentially disturbed operation.</p> <p>b) Point movement may occur when point is occupied by a train/vehicle or other, conflicting reservations, potentially leading to conflicting and unsafe movements.</p>
Risk Comment	-

Linked Work Items	<p>relates to :  SPMS-5265 - Control target state of one point</p> <p>relates to :  SPMS-3227 - Required point position</p> <p>relates to :  SPMS-4476 - Set point position</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>relates to :  SPMS-4382 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4692 - Set point position (Left to right, Signaller request)</p> <p>relates to :  SPMS-4715 - Set point position (Left to right, Operational plan - Traffic CS view)</p> <p>relates to :  SPMS-4788 - Set point position (Left to right, Signaller request - Traffic CS view)</p> <p>assesses :  SPRM-1726 - [XYZ] Undue movement of a point</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-6357 - Commanded point position state</p> <p>has parent :  SPRM-2130 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1699 - Point is free of occupancy</p> <p>_ is mitigated by : {c} SPRM-1730 - Point position command is sent after performing the safety checks</p> <p>_ is mitigated by : {c} SPRM-1775 - Point is reserved for one movement permission</p> <p>_ is mitigated by : {c} SPRM-2281 - Point position command is executed within a defined time</p>
-------------------	---

Late required point position to Trackside Assets CS (2/2)

ID	SPRM-1734
Failure Mode (Keyword)	Omission
Failure Description	Traffic CS sends the point position command to Trackside Assets CS too late or not at all.
Effect on Linked Functions Systems	Traffic CS sends the command after the safety conditions checked by Traffic CS are not valid anymore. In case the point was moved into the requested position already, the late command will trigger a movement into the position
Effect on Railway System	Point machine overheats when trying to execute the command.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-5265 - Control target state of one point</p> <p>relates to :  SPMS-3227 - Required point position</p> <p>relates to :  SPMS-4382 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4476 - Set point position</p> <p>relates to :  SPMS-4692 - Set point position (Left to right, Signaller request)</p> <p>relates to :  SPMS-4715 - Set point position (Left to right, Operational plan - Traffic CS view)</p> <p>relates to :  SPMS-4788 - Set point position (Left to right, Signaller request - Traffic CS view)</p> <p>assesses :  SPRM-312 - [B.3.0] Other failures of the infrastructure</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-6357 - Commanded point position state</p> <p>has parent :  SPRM-2130 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1729 - Point position is equal to required point position</p>

Incorrect required point position to Trackside Assets CS

ID	SPRM-1071
Failure Mode (Keyword)	Incorrect
Failure Description	Traffic CS sends an incorrect point position command to Trackside Assets CS.
Effect on Linked Functions Systems	Trackside Assets CS receives incorrect command to change the point position: a) point is already in required point position state b) wrong required target position (e.g. left instead of right) is commanded.
Effect on Railway System	a) Point machine overheats when trying to execute the command. b) Point is in the incorrect position for the intended train movement, meaning that the track path cannot be secured for the train movement. This results in a potentially disturbed operation.
Risk Comment	.
Linked Work Items	<p>relates to :  SPMS-5265 - Control target state of one point</p> <p>relates to :  SPMS-3227 - Required point position</p> <p>relates to :  SPMS-4476 - Set point position</p> <p>assesses :  SPRM-312 - [B.3.0] Other failures of the infrastructure</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4382 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4692 - Set point position (Left to right, Signaller request)</p> <p>relates to :  SPMS-4715 - Set point position (Left to right, Operational plan - Traffic CS view)</p> <p>relates to :  SPMS-4788 - Set point position (Left to right, Signaller request - Traffic CS view)</p> <p>relates to :  SPMS-6357 - Commanded point position state</p> <p>has parent :  SPRM-2130 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1729 - Point position is equal to required point position</p>

3.3.1.2.3 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
----	-----------

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 Tracksides Assets CS in another constraint.

ID	SPRM-1730
----	-----------

Point position is equal to required point position

The check, if the point position is equal to the required point position is needed to avoid unnecessary commands to the point machine when their execution could damage the point machine (e.g. overheating).

ID	SPRM-1729
----	-----------

Point machine position is equal to requested point machine position.

The command to change the state of a point machine does not get executed if the point machine is already in the requested point machine position. This is to avoid overheating of PM and sending unnecessary commands to Point Machine.

ID	SPRM-1700
----	-----------

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
----	-----------

3.3.1.3 Control track path allocation for movement permission

3.3.1.3.1 Functional description

Control track path allocation for movement permissions

This function is allocated to  SPMS-2823 - Traffic CS System.





































This function performs a safe allocation of a track path for a planned train movement, i.e.




- determines track paths that need to be allocated for train movement
- checks that the track path for a planned train movement is clear
- checks whether there are no conflicting track paths already allocated to other train movements nor restrictions already defined
- supervises and verifies that the switchable trackside assets for train movement are in the required position
- locks required switchable trackside assets
- 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.
- checks if the first position reported by a train fits to the expected position from the operational plan. It means for example that before executing the operational plan this cross check is performed and that in case of deviations the operational plan is not executed. Based on this Traffic CS information, Traffic Management System would then have to update the operational plan accordingly so that it fits again and can be executed.

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).

This function also performs the safe allocation of a track path as a reaction to a failure (the requested track path is transmitted by the function "Determine reaction to failure").














The function also releases track parts that are no longer used for train movement after checking the

Input exchanges	Input exchanges	Source function	Function allocated to
	 SPMS-3220 - Observed point position <ul style="list-style-type: none">  SPMS-3283 - point_position_report 	 SPMS-2914 - Sense+Observe position of one point	 SPMS-2818 - Trackside Ass
	 SPMS-3021 - Aggregated track occupancy and train status information <ul style="list-style-type: none">  SPMS-5562 - train_object_information 	 SPMS-2944 - Aggregate movable objects information	 SPMS-2823 - Traffic CS Sys
	No exchange items allocated on  SPMS-3131 - Activated state of configuration data.	 SPMS-2840 - Maintain Traffic CS System configuration data	 SPMS-2823 - Traffic CS Sys
	 SPMS-3000 - Usage restriction state <ul style="list-style-type: none">  SPMS-2398 - usage_restriction_status 	 SPMS-2929 - Control usage restrictions	 SPMS-2823 - Traffic CS Sys
	 SPMS-5424 - Respond and request for movement authority data <ul style="list-style-type: none">  SPMS-7235 - acknowledgement_emergency_stop  SPMS-7242 - shorten_movement_authority_response 	 SPMS-2872 - Calculate safe speed profiles of one train	 SPMS-2807 - Train CS Syst
	 SPMS-3079 - Required operational traffic plan <ul style="list-style-type: none">  SPMS-2370 - operational_plan_movement 	 SPMS-2843 - Calculate operational traffic plan	 SPMS-2813 - Traffic Manag
	 SPMS-3123 - Requested track path <ul style="list-style-type: none">  SPMS-2418 - track_path_request 	 SPMS-2853 - Supervise state of the railway	 SPMS-2827 - Signaller
	 SPMS-3042 - Provided current time <ul style="list-style-type: none">  SPMS-2412 - time_reference 	 SPMS-2922 - Synchronise current time	 SPMS-2819 - Transversal C
	 SPMS-7719 - Request emergency stop <ul style="list-style-type: none">  SPMS-7137 - unconditional_emergency_stop_request 	 SPMS-2853 - Supervise state of the railway	 SPMS-2827 - Signaller

Output exchanges	Output exchanges	Target function	Function allocated to
	 SPMS-3039 - Allocated track path <ul style="list-style-type: none">  SPMS-2372 - movement_permission 	 SPMS-2944 - Aggregate movable objects information	 SPMS-2823 - Traffic CS System
	 SPMS-3044 - Allocated track path <ul style="list-style-type: none">  SPMS-2372 - movement_permission 	 SPMS-2853 - Supervise state of the railway	 SPMS-2827 - Signaller
	 SPMS-3052 - Allocated track path <ul style="list-style-type: none">  SPMS-2372 - movement_permission 	 SPMS-2843 - Calculate operational traffic plan	 SPMS-2813 - Traffic Manager
	 SPMS-5278 - Allocated track path <ul style="list-style-type: none">  SPMS-2372 - movement_permission 	 SPMS-5265 - Control target state of one point	 SPMS-2823 - Traffic CS System
	 SPMS-3065 - Allocated track path <ul style="list-style-type: none">  SPMS-5446 - shorten_movement_authority_request  SPMS-5835 - movement_authority 	 SPMS-2872 - Calculate safe speed profiles of one train	 SPMS-2807 - Train CS System
	 SPMS-3232 - Allocated track path <ul style="list-style-type: none">  SPMS-5835 - movement_authority 	 SPMS-2878 - Determine position and state of one train	 SPMS-2807 - Train CS System
	 SPMS-6982 - Allocated track path <ul style="list-style-type: none">  SPMS-5835 - movement_authority 	 SPMS-6971 - Determine proximity of station platform	 SPMS-2807 - Train CS System
	 SPMS-7661 - Allocated track path <ul style="list-style-type: none">  SPMS-5835 - movement_authority  SPMS-7234 - unconditional_emergency_stop 	 SPMS-2921 - Supervise compliance of speed profiles of one train	 SPMS-2807 - Train CS System
	 SPMS-2991 - Allocated track path <ul style="list-style-type: none">  SPMS-5835 - movement_authority 	 SPMS-2897 - Supervise standstill of one train	 SPMS-2807 - Train CS System














3.3.1.3.2 Failure Modes and Effects Analysis

Early shorten movement permission request to Train CS

ID	SPRM-1073
Failure Mode (Keyword)	Commission
Failure Description	Traffic CS requests shortening of movement permission from Train CS too early.
Effect on Linked Functions Systems	Train CS will calculate safe speed profile.
Effect on Railway System	If Train CS can come to a standstill before reaching the ETCS supervision target, it will accept the request. If not, it will reject it.
Risk Comment	Traffic CS transmits new ETCS supervision target (EoA) to Train CS, before planned/required (new EOA is correct, but transmitted too early).
Linked Work Items	<p>relates to :  SPMS-2874 - Control track path allocation for movement permissions</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-3065 - Allocated track path</p> <p>relates to :  SPMS-5047 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-5426 - Shorten movement permission (Cooperative shortening of movement permission)</p> <p>relates to :  SPMS-5131 - Shorten movement permission (Operational plan change, rejected)</p> <p>relates to :  SPMS-5170 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-5171 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-5684 - Shorten movement permission (Operational plan change, accepted - Traffic CS view)</p> <p>relates to :  SPMS-5685 - Shorten movement permission (Signaller request, accepted - Traffic CS view)</p> <p>relates to :  SPMS-6393 - Authorised movement permission</p> <p>has parent :  SPRM-2127 - Detailed Failure Modes and Effect Analysis</p>















Late shorten movement permission request to Train CS

ID	SPRM-1074
Failure Mode (Keyword)	Omission
Failure Description	Traffic CS requests shortening of movement authority (due to operational reasons) from Train CS too late or not at all.
Effect on Linked Functions Systems	Train CS does not calculate a new safe speed profile or too late when shortening would only be possible with an Emergency brake.
Effect on Railway System	In case Train CS can reach the ETCS supervision target (EoA) without immediate braking, it will accept the request. If not, it will reject it.
Risk Comment	-

Linked Work Items	<p>relates to :  SPMS-2874 - Control track path allocation for movement permissions</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-3065 - Allocated track path</p> <p>relates to :  SPMS-5047 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-5426 - Shorten movement permission (Cooperative shortening of movement permission)</p> <p>relates to :  SPMS-5131 - Shorten movement permission (Operational plan change, rejected)</p> <p>relates to :  SPMS-5170 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-5171 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-5684 - Shorten movement permission (Operational plan change, accepted - Traffic CS view)</p> <p>relates to :  SPMS-5685 - Shorten movement permission (Signaller request, accepted - Traffic CS view)</p> <p>relates to :  SPMS-6393 - Authorised movement permission</p> <p>has parent :  SPRM-2127 - Detailed Failure Modes and Effect Analysis</p>
-------------------	--














Incorrect shorten movement permission request to Train CS

ID	SPRM-1075
Failure Mode (Keyword)	Incorrect
Failure Description	Traffic CS requests incorrect shortening movement authority to Train CS (more permissive than internally calculated).
Effect on Linked Functions Systems	In case Train CS can reach the ETCS supervision target (EoA) without immediate emergency braking, it will accept the request. If not, it will reject it. If Train CS accepts the request, than the EOA on-board is more permissive than in Traffic CS.
Effect on Railway System	<p>If Train CS accepts it, Train will calculate safe speed profile and update ETCS supervision target (EoA) that is further away from the train position than the EOA used by Traffic CS.</p> <p>Track path elements still used by train might be unsecured.</p> <p>If Train CS rejects it, it will keep existing movement authority, delaying shortening of movement authority.</p>
Risk Comment	-













Linked Work Items	<p>relates to :  SPMS-2874 - Control track path allocation for movement permissions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-3065 - Allocated track path</p> <p>relates to :  SPMS-5047 - Shorten movement permission (Operational plan change, accepted)</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>relates to :  SPMS-5426 - Shorten movement permission (Cooperative shortening of movement permission)</p> <p>relates to :  SPMS-5131 - Shorten movement permission (Operational plan change, rejected)</p> <p>relates to :  SPMS-5170 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-5171 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-5684 - Shorten movement permission (Operational plan change, accepted - Traffic CS view)</p> <p>relates to :  SPMS-5685 - Shorten movement permission (Signaller request, accepted - Traffic CS view)</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>relates to :  SPMS-6393 - Authorised movement permission</p> <p>has parent :  SPRM-2127 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1512 - Train moves within Movement Authority</p> <p>_ is mitigated by : {c} SPRM-1563 - Authorised speed is less or equal to the maximum allowed track speed</p>
-------------------	---

Incorrect shorten movement permission request to Train CS












ID	SPRM-1428
Failure Mode (Keyword)	Incorrect
Failure Description	Traffic CS requests incorrect shortening movement permission to Train CS (more restrictive than internally calculated).
Effect on Linked Functions Systems	<p>In case Train CS can reach the ETCS supervision target (EoA) without immediate braking, it will accept the request. If not, it will reject it. ETCS supervision target (EoA) sent to Train CS is more restrictive than the one requested by TMS. Traffic CS internally has a less restrictive EoA than the one it send out to Train CS.</p> <p>If Train CS doesn't reject the request, Emergency braking will be triggered which leads to an operational disturbance.</p>
Effect on Railway System	<p>If Train CS accepts it, it will calculate safe speed profile and update ETCS supervision target (EoA).</p> <p>If Train CS rejects it, it will keep existing movement authority, delaying shortening of movement authority.</p>
Risk Comment	-

Linked Work Items	<p>relates to :  SPMS-2874 - Control track path allocation for movement permissions</p> <p>relates to :  SPMS-3065 - Allocated track path</p> <p>relates to :  SPMS-5047 - Shorten movement permission (Operational plan change, accepted)</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5131 - Shorten movement permission (Operational plan change, rejected)</p> <p>relates to :  SPMS-5170 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-5171 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-5426 - Shorten movement permission (Cooperative shortening of movement permission)</p> <p>relates to :  SPMS-5684 - Shorten movement permission (Operational plan change, accepted - Traffic CS view)</p> <p>relates to :  SPMS-5685 - Shorten movement permission (Signaller request, accepted - Traffic CS view)</p> <p>relates to :  SPMS-6393 - Authorised movement permission</p> <p>has parent :  SPRM-2127 - Detailed Failure Modes and Effect Analysis</p>
-------------------	---

Incorrect point position in movement permission












ID	SPRM-2311
Failure Mode (Keyword)	Incorrect
Failure Description	Traffic CS sends movement permission over a point in an incorrect position according to the required movement.
Effect on Linked Functions Systems	Train CS receives movement authority over a point in an incorrect position.
Effect on Railway System	The train runs over an unsecured path, it could lead to a collision with other trains or persons or derailment.
Linked Work Items	<p>relates to :  SPMS-2874 - Control track path allocation for movement permissions</p> <p>relates to :  SPMS-3065 - Allocated track path</p> <p>relates to :  SPMS-4462 - Grant movement permission</p> <p>relates to :  SPMS-5368 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5645 - Grant movement permission (Operational plan - Traffic CS view)</p> <p>relates to :  SPMS-5810 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5811 - Grant movement permission (Signaller request - Traffic CS view)</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>has parent :  SPRM-2136 - Risk tracing report</p> <p>_ is mitigated by : {c} SPRM-2312 - All STAs in the required path are in the required position</p>

Early movement authority to Train CS













ID	SPRM-1369
Failure Mode (Keyword)	Commission
Failure Description	Traffic CS sends movement authority to Train CS too early.
Effect on Linked Functions Systems	Train CS updates the speed profile earlier.
Effect on Railway System	Train could start its mission before the planned time resulting in disturbed operation.
Risk Comment	The correct movement authority is transmitted (track path is set and protected by Traffic CS). It's transmitted earlier than necessary resulting in the train potentially starting its movement earlier than planned.
Linked Work Items	<p>relates to :  SPMS-2874 - Control track path allocation for movement permissions</p> <p>relates to :  SPMS-3065 - Allocated track path</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5368 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5645 - Grant movement permission (Operational plan - Traffic CS view)</p> <p>relates to :  SPMS-5810 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5811 - Grant movement permission (Signaller request - Traffic CS view)</p> <p>relates to :  SPMS-4462 - Grant movement permission</p> <p>relates to :  SPMS-6393 - Authorised movement permission</p> <p>has parent :  SPRM-2127 - Detailed Failure Modes and Effect Analysis</p>

Late movement authority to Train CS

ID	SPRM-1371
Failure Mode (Keyword)	Omission
Failure Description	Traffic CS sends movement authority to Train CS too late OR not at all.
Effect on Linked Functions Systems	Train CS receives movement authority too late OR not at all. Safe speed profile is created based on outdated movement authority or not at all. This can lead to the train having to stop.
Effect on Railway System	No safety issues in normal scenario, see risk comment.
Risk Comment	The hazardous scenario only exists if the new MA is more restrictive than the one that the train is already executing. This is a case for degraded situation, which will be covered in the future. A simple lack of a MA (equal or more permissive than the existing one) would only affect operation.













Linked Work Items	<p>relates to :  SPMS-2874 - Control track path allocation for movement permissions</p> <p>relates to :  SPMS-3065 - Allocated track path</p> <p>relates to :  SPMS-5368 - Grant movement permission (Operational plan)</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5645 - Grant movement permission (Operational plan - Traffic CS view)</p> <p>relates to :  SPMS-5810 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5811 - Grant movement permission (Signaller request - Traffic CS view)</p> <p>relates to :  SPMS-4462 - Grant movement permission</p> <p>relates to :  SPMS-6393 - Authorised movement permission</p> <p>has parent :  SPRM-2127 - Detailed Failure Modes and Effect Analysis</p>
-------------------	--

Incorrect movement authority to Train CS

ID	SPRM-1370
Failure Mode (Keyword)	Incorrect
Failure Description	Traffic CS sends movement authority with incorrect speed to Train CS.
Effect on Linked Functions Systems	The speed profile calculated by Train CS may be higher than the safe speed.
Effect on Railway System	In worst case, train may drive with higher speed than allowed on track.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2874 - Control track path allocation for movement permissions</p> <p>relates to :  SPMS-3065 - Allocated track path</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-5368 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5645 - Grant movement permission (Operational plan - Traffic CS view)</p> <p>relates to :  SPMS-5810 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5811 - Grant movement permission (Signaller request - Traffic CS view)</p> <p>relates to :  SPMS-4462 - Grant movement permission</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>relates to :  SPMS-6393 - Authorised movement permission</p> <p>has parent :  SPRM-2127 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1563 - Authorised speed is less or equal to the maximum allowed track speed</p>

Incorrect movement authority to Train CS

ID	SPRM-1374
Failure Mode (Keyword)	Incorrect
Failure Description	Traffic CS sends movement authority with incorrect distance to Train CS.

Effect on Linked Functions Systems	The speed profile calculated by Train CS may be higher than the safe speed.
Effect on Railway System	In worst case, train may drive into a track which is not in a safe state, e.g. occupied, not locked, not suitable for train movement, etc.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2874 - Control track path allocation for movement permissions</p> <p>relates to :  SPMS-3065 - Allocated track path</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>relates to :  SPMS-5368 - Grant movement permission (Operational plan)</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-5645 - Grant movement permission (Operational plan - Traffic CS view)</p> <p>relates to :  SPMS-5810 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5811 - Grant movement permission (Signaller request - Traffic CS view)</p> <p>relates to :  SPMS-4462 - Grant movement permission</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>relates to :  SPMS-6393 - Authorised movement permission</p> <p>has parent :  SPRM-2127 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1447 - Maximum authorised distance ends ahead of occupied track</p> <p>_ is mitigated by : {c} SPRM-1776 - Maximum authorised distance is within Movement Permission</p>

3.3.1.3.3 Constraints

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
----	-----------

Requested track path is free of occupancies

The requested track path doesn't include occupancies by other trains or vehicles. Only the occupancy of the train for with the track path is requested is allowed.

ID	SPRM-1443
----	-----------

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
----	-----------

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
----	-----------

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
----	-----------

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
----	-----------

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
----	-----------

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
----	-----------

3.3.1.4 Control usage restrictions

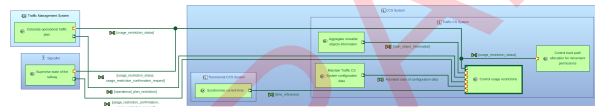
3.3.1.4.1 Functional description

Control usage restrictions

This function is allocated to  SPMS-2823 - Traffic CS System.

This function:

- Creates a planned usage restriction area according to the operational plan restriction and stores it until the time for the activation has been reached.
- Creates an unplanned usage restriction area on a Signaller request.
- checks if all conditions for the activation/deactivation of usage restrictions are fulfilled taking into account feedback from Signaller as well as already active usage restriction areas and the current operational state i.e. states of trackside assets and trains currently using the infrastructure (e.g. track occupancies, train-specific authorisations, allocated track paths)).
- If necessary request trackside asset states or derive additional usage restrictions associated to specific usage restrictions.
- informs the respective functions about the activation or deactivation of a relevant usage restrictions (e.g. "request target state of one trackside asset" about a blocked trackside asset).
- provides information about the execution state of usage restrictions
- stores the activated usage restrictions

ID	SPMS-2929
Context Diagram	 <p>Figure 5 Context Diagram of Control usage restrictions</p>

Input exchanges	Input exchanges	Source function	Function allocated to
	No exchange items allocated on SPMS-3135 - Activated state of configuration data.	SPMS-2840 - Maintain Traffic CS System configuration data	SPMS-2823 - Traffic CS System
	SPMS-2988 - Required operational traffic plan • SPMS-5548 - operational_plan_restriction	SPMS-2843 - Calculate operational traffic plan	SPMS-2813 - Traffic Management System
	SPMS-3028 - Aggregated track occupancy and train status information • SPMS-5562 - train_object_information	SPMS-2944 - Aggregate movable objects information	SPMS-2823 - Traffic CS System
	SPMS-3078 - Provided usage restriction state • SPMS-4826 - usage_restriction_confirmation • SPMS-2407 - usage_restriction_request	SPMS-2853 - Supervise state of the railway	SPMS-2827 - Signaller
Output exchanges	SPMS-3045 - Provided current time • SPMS-2412 - time_reference	SPMS-2922 - Synchronise current time	SPMS-2819 - Transversal CCS System
	Output exchanges	Target function	Function allocated to
	SPMS-3000 - Usage restriction state • SPMS-2398 - usage_restriction_status	SPMS-2874 - Supervise state of the railway	SPMS-2823 - Traffic CS System
	SPMS-3173 - Usage restriction state • SPMS-2398 - usage_restriction_status	SPMS-2843 - Calculate operational traffic plan	SPMS-2813 - Traffic Management System
	SPMS-3174 - Usage restriction state • SPMS-2398 - usage_restriction_status • SPMS-4827 - usage_restriction_confirmation_request	SPMS-2853 - Supervise state of the railway	SPMS-2827 - Signaller

3.3.1.4.2 Failure Modes and Effects Analysis

There are no output exchanges in scope of the analysed scenarios.

3.3.1.4.3 Constraints

Track condition allows regular operation

The track conditions are normal and does not need restriction.

ID	SPRM-2240
----	-----------

Usage restriction activation is planned

Time-sensitive, planned usage restriction not involving track workers are activated by CCS-System without Signaller confirmation.

Rational: No confirmation of e.g. a low adhesion area will lead to a hazard. In such cases, CCS-System can activate the usage restriction at the planned time automatically.

ID	SPRM-2109
----	-----------

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
----	-----------

Deactivation of planned usage restrictions requested

The deactivation of planned usage restrictions is unavailable in CCS System if TMS/Signaller did not request it previously. This mitigates the risk that CCS system wrongfully deactivates a restriction on its own.

ID	SPRM-1743
----	-----------

Confirmed usage restriction matches requested usage restriction

CCS System checks if the confirmation from Signaller matches the requested usage restriction by TMS/Signaller for deactivation and activation.

ID	SPRM-1740
----	-----------

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
----	-----------

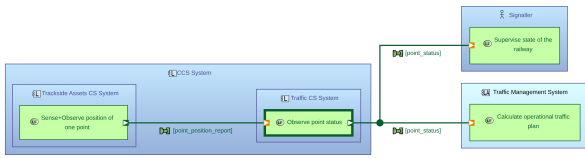












3.3.1.5 Observe point status

3.3.1.5.1 Functional description

Observe point status

This function is allocated to  SPMS-2823 - Traffic CS System.

This function observes the overall state of one point including its availability and its position compared to the required point position.

ID	SPMS-2886		
Context Diagram	<div><p>The context diagram shows the 'Observe point status' function within the 'Traffic CS System' boundary. It receives an input 'point_position_report' from the 'Trackside Assets CS System' and sends an output 'point_status' to the 'Signaller' and the 'Traffic Management System'.</p></div>		
Figure 6 Context Diagram of Observe point status			
Input exchanges	Input exchanges	Source function	Function allocated to
	<div> SPMS-3209 - Observed point position<ul style="list-style-type: none"> SPMS-3283 - point_position_report</div>	<div> SPMS-2914 - Sense+Observe position of one point</div>	<div> SPMS-2818 - Trackside Assets CS System</div>
Output exchanges	Output exchanges	Target function	Function allocated to
	<div> SPMS-3189 - Observed point status<ul style="list-style-type: none"> SPMS-5288 - point_status</div>	<div> SPMS-2853 - Supervise state of the railway</div>	<div> SPMS-2827 - Signaller</div>
	<div> SPMS-5339 - Observed point status<ul style="list-style-type: none"> SPMS-5288 - point_status</div>	<div> SPMS-2843 - Calculate operational traffic plan</div>	<div> SPMS-2813 - Traffic Management System</div>

3.3.1.5.2 Failure Modes and Effects Analysis









There are no output exchanges in scope of the analysed scenarios.

3.3.1.5.3 Constraints

No constraints allocated to this function.

4 Appendix

4.1 References

ID	Description
[ SPT2TRAFFIC-4141 - ERJU Safety Guideline]	The ERJU Safety Guideline practical guidance for ERJU Safety and System Engineers.
[ SPP-18060 - TCS_System Architecture Description CCS System V0.3]	System Architecture of the CCS System according to [ SPPRAMSS-349 - [EN 50126-1:2017].
[ SPP-18076 - System Definition Traffic CS]	System Definition of the Traffic CS System according to [ SPPRAMSS-349 - [EN 50126-1:2017].
[ SPT2TRAFFIC-13108 - ERJU Hazard Database - Main Document]	This document details the European Railway Harmonized Hazards Database to be used for risk assessment by ERJU SP Domains in accordance with ERJU PRAMS Plan and guidelines.
[ SPT2TRAFFIC-13107 - ERJU PRAMS Plan]	This Safety Plan according to Phase 2.EN50126-1 shows the planned safety activities of ERJU System Pillar. It reflects the discussion in the ERJU Workgroup RAMS.
[ SPT2TRAFFIC-13109 - ERJU Risk Assessment Process & Template]	This document describes the basic steps for performing risk assessment (focus safety) within ERJU. In addition it provides templates and examples for the risk assessment to be done by the ERJU System Pillar Domain Safety Managers.