



ERJU SYSTEM PILLAR

# **30 Risk assessment report for the System Definition CCS System**



# Risk assessment report for the System Definition CCS System

---

DRAFT

**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	6
1.1 Purpose	6
1.2 Intended Audience	6
1.3 Document Context	6
1.4 Glossary	8
1.4.1 Terms	8
1.4.2 Abbreviations	8
2 Scope	9
3 Risk analysis	11
3.1 Risk assessment report	11
3.2 Detailed Failure Modes and Effect Analysis	11
3.2.1 CCS-System functions	11
3.2.1.1 Control position of one point	11
3.2.1.1.1 Functional description	11
3.2.1.1.2 Failure Modes and Effects Analysis	12
3.2.1.1.3 Constraints	15
3.2.1.2 Control usage restriction	16
3.2.1.2.1 Functional description	16
3.2.1.2.2 Failure Modes and Effects Analysis	17
3.2.1.2.3 Constraints	28
3.2.1.3 Ensure safe movement of trains	28
3.2.1.3.1 Functional description	28
3.2.1.3.2 Failure Modes and Effects Analysis	31
3.2.1.3.3 Constraints	41
3.2.1.4 Sense + Observe motion of one train	42
3.2.1.4.1 Functional description	42
3.2.1.4.2 Failure Modes and Effects Analysis	44
3.2.1.4.3 Constraints	50
3.2.1.5 Sense + Observe point status	51
3.2.1.5.1 Functional description	51
3.2.1.5.2 Failure Modes and Effects Analysis	52
3.2.1.5.3 Constraints	55
3.2.2 Actor functions	55
3.2.2.1 Point Machine	55
3.2.2.1.1 Functional description	55
3.2.2.1.2 Failure Modes and Effects Analysis	55
3.2.2.1.3 Constraints	59
3.2.2.2 Rolling Stock Operation System	60
3.2.2.2.1 Functional description	60
3.2.2.2.2 Failure Modes and Effects Analysis	61
3.2.2.2.3 Constraints	62

3.2.2.3 Rolling Stock Reference Point	62
3.2.2.3.1 Functional description	62
3.2.2.3.2 Failure Modes and Effects Analysis	64
3.2.2.3.3 Constraints	76
3.2.2.4 Signaller	76
3.2.2.4.1 Functional description	76
3.2.2.4.2 Failure Modes and Effects Analysis	78
3.2.2.4.3 Constraints	88
3.2.2.5 Traffic Management System	89
3.2.2.5.1 Functional description	89
3.2.2.5.2 Failure Modes and Effects Analysis	91
3.2.2.5.3 Constraints	101
3.2.2.6 Wheel	101
3.2.2.6.1 Functional description	101
3.2.2.6.2 Failure Modes and Effects Analysis	102
3.2.2.6.3 Constraints	106
4 References	107

# 1 Preamble

## 1.1 Purpose

The purpose of this document is to provide the results of the risk assessment of the CCS System (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 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

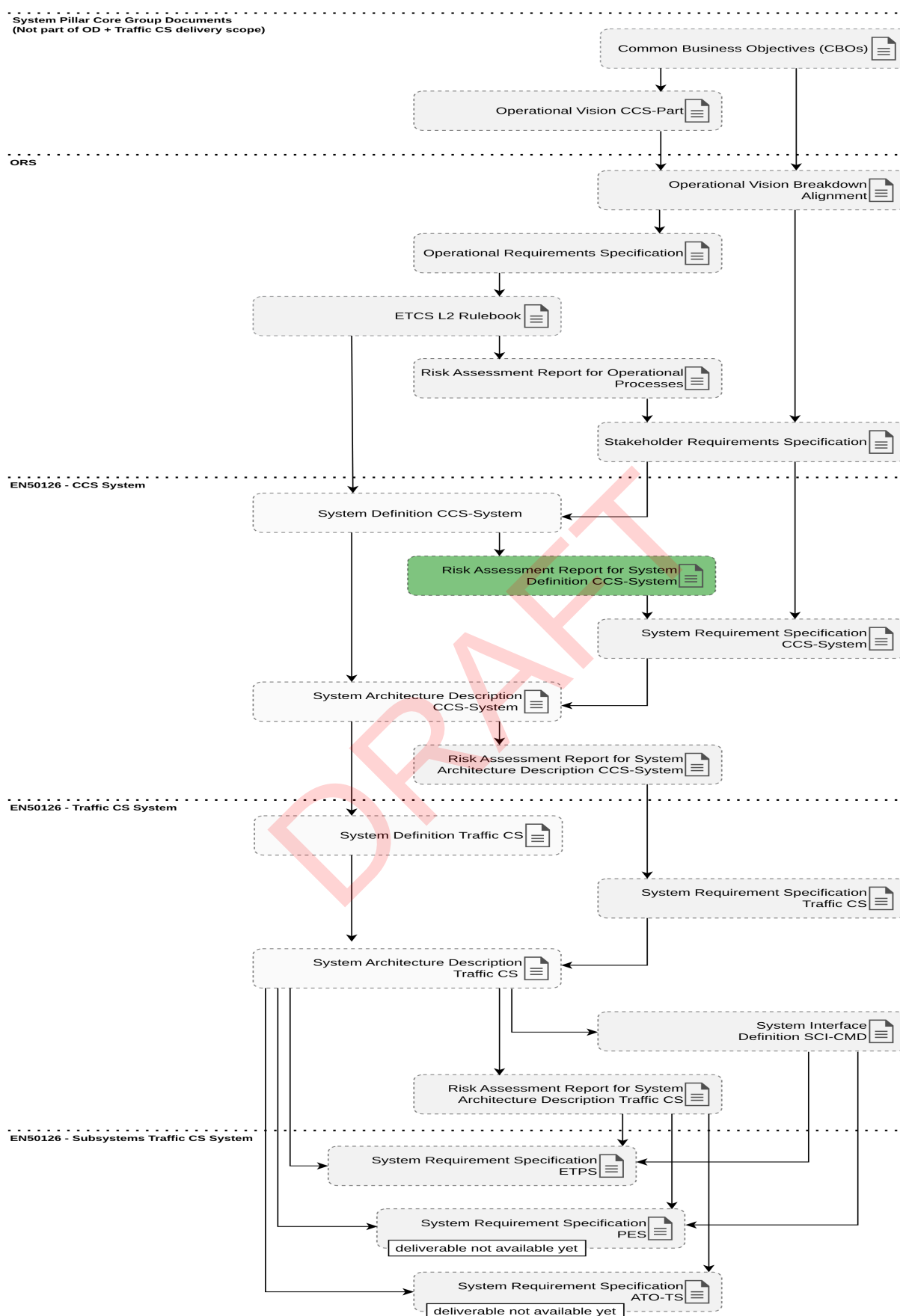
As shown in the illustration below (SPP-31533 - Dependencies between Configuration Items), the Risk assessment report for the System Definition of the SPMS-2098 - CCS System is based on the following key inputs:

- [SPP-18056 - TCS\_System Definition CCS System\_V0.3]:  
This document describes the capabilities to be provided by the CCS-System.  
  
Note:  
The System Definition of the CCS-System contains changes in Release 3 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 System Definition 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 Definition CCS itself is an input document for the SPP-18063 - TCS\_System Requirement Specification CCS System\_V0.4.

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.

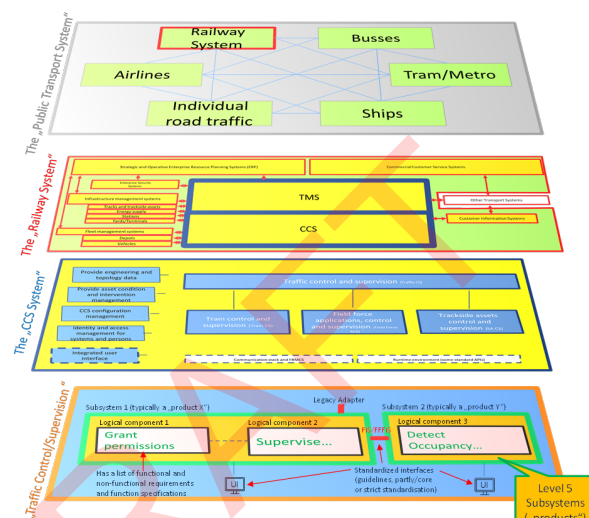
A summary of the most important results of the risk assessment of the CCS System is made available in: SPP-31652 - Risk assessment report for the System Definition CCS System - Annex A: Traceability Report\_V0.2



[SPP-31533 ]

## 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 Polaron.

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 CCS system and the physical environment, external systems and human actors. The analysis of the output exchanges of the CCS System to the physical environment, external systems and human actors is structured by CCS System function. CCS-internal exchanges are not analysed.

The analysis of the output exchanges of the physical environment, external systems and human actors to the CCS System is structured by the corresponding System Actors.

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-2438 - Activate usage restriction	  SPMS-5753 - Activate usage restriction (Planned usage restriction)   SPMS-4435 - Activate usage restriction	586189
  SPMS-2438 - Activate usage restriction	  SPMS-7226 - Activate usage restriction (Unplanned TSR)   SPMS-4435 - Activate usage restriction	690295
  SPMS-2436 - Deactivate usage restriction	  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)   SPMS-4828 - Deactivate usage restriction	588380
  SPMS-2436 - Deactivate usage restriction	  SPMS-7232 - Deactivate usage restriction (Unplanned TSR)   SPMS-4828 - Deactivate usage restriction	684834
  SPMS-5295 - Grant movement permission	  SPMS-5361 - Grant movement permission (Operational plan)   SPMS-5514 - Grant movement permission (Signaller request)	541808

System capability	Scenarios	Revision
	  SPMS-5298 - Grant movement permission (Control loop)	
  SPMS-2443 - Localise train on railway infrastructure	  SPMS-4329 - Localise train on railway infrastructure   SPMS-4438 - Localise train on railway infrastructure (Control loop)	541808
  SPMS-2440 - Perform train movement	  SPMS-4333 - Perform train movement (Full supervision)   SPMS-4447 - Perform train movement (Full supervision control loop)	541808
  SPMS-5296 - Release movement permission	  SPMS-5362 - Release movement permission   SPMS-5316 - Release movement permission (Control loop)	541808
  SPMS-2423 - Set point position	  SPMS-4342 - Set point position (Left to right, Operational plan)   SPMS-4769 - Set point position (Left to right, Signaller)   SPMS-4444 - Set point position (Control loop)	529641
  SPMS-2442 - Shorten movement permission	  SPMS-4441 - Shorten movement permission   SPMS-4326 - Shorten movement permission (Operational plan change, accepted)   SPMS-4336 - Shorten movement permission (Operational plan change, rejected)   SPMS-4334 - Shorten movement permission (Signaller request, accepted)   SPMS-4337 - Shorten movement permission (Signaller request, rejected)	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 assessment report

This Risk Assessment Report is the overview of the most important results of the Risk Analysis performed for the System definition CCS. The Risk assessment report is made available in  SPP-31652 - Risk assessment report for the System Definition CCS System - Annex A: Traceability Report\_V0.2

### 3.2 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 2-3 - Scope and presented in the linked reports above.

#### 3.2.1 CCS-System functions

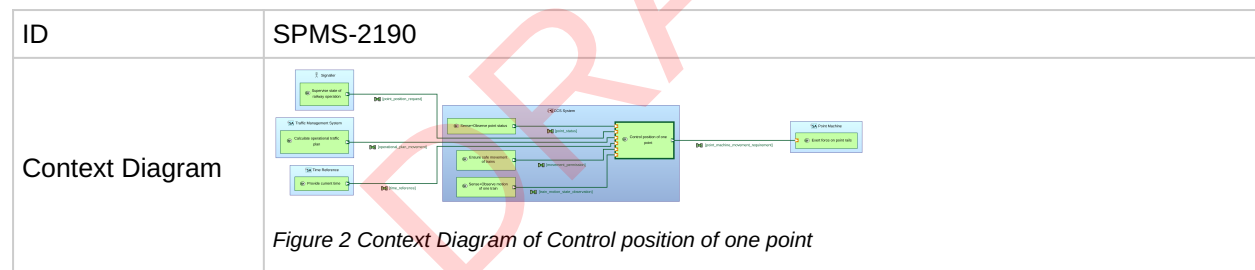
##### 3.2.1.1 Control position of one point





























##### 3.2.1.1.1 Functional description

##### Control position of one point

This function is allocated to  SPMS-2098 - CCS 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.















Input exchanges	Input exchanges	Source function	Function allocated to
	 SPMS-2311 - Observed point status <ul style="list-style-type: none"> <li> SPMS-5288 - point_status</li> </ul>	 SPMS-2108 - Sense+Observe point status	 SPMS-2098 - CCS System
	 SPMS-2301 - Estimated motion state <ul style="list-style-type: none"> <li> SPMS-2392 - train_motion_state_observation</li> </ul>	 SPMS-2192 - Sense+Observe motion of one train	 SPMS-2098 - CCS System
	 SPMS-2250 - Authorised distance and speed restriction <ul style="list-style-type: none"> <li> SPMS-2372 - movement_permission</li> </ul>	 SPMS-2137 - Ensure safe movement of trains	 SPMS-2098 - CCS System
	 SPMS-2258 - Provided current time <ul style="list-style-type: none"> <li> SPMS-2412 - time_reference</li> </ul>	 SPMS-2171 - Provide current time	 SPMS-6265 - Time Reference
	 SPMS-2350 - Required operational traffic plan <ul style="list-style-type: none"> <li> SPMS-2370 - operational_plan_movement</li> </ul>	 SPMS-2148 - Calculate operational traffic plan	 SPMS-2097 - Traffic Management System
Output exchanges	 SPMS-4628 - Requested point position <ul style="list-style-type: none"> <li> SPMS-2386 - point_position_request</li> </ul>	 SPMS-2167 - Supervise state of railway operation	 SPMS-2090 - Signaller
	Output exchanges	Target function	Function allocated to
	 SPMS-2361 - Required point machine movement <ul style="list-style-type: none"> <li> SPMS-2377 - point_machine_movement_requirement</li> </ul>	 SPMS-2125 - Sense+Observe point machine movement	 SPMS-2100 - Central Point Machine

### 3.2.1.1.2 Failure Modes and Effects Analysis












#### Early Required point machine movement to Point Machine

ID	SPRM-1301
Failure Mode (Keyword)	Commission
Failure Description	CCS system executes the operational movement too early.










Effect on Linked Functions Systems	The point machine moves when the point is occupied (by train or part of an already granted movement) or when a train is approaching. Or the point machine moves so that a movement permission cannot be granted.
Effect on Railway System	-
Risk Comment	PRAM-related considerations: CCS-System shall send the reason for rejecting an operational movement to TMS. CCS-System shall send the reason for rejecting the requested point position to Signaller.
Linked Work Items	<p>relates to :  SPMS-2190 - Control position of one point</p> <p>relates to :  SPMS-2361 - Required point machine movement</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>assesses :  SPRM-1726 - [XYZ] Undue movement of a point</p> <p>relates to :  SPMS-3008 - Required point machine position</p> <p>has parent :  SPRM-2101 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1699 - Point is free of occupancy</p>

#### Incorrect Required point machine movement to Point Machine (1)

ID	SPRM-1302
Failure Mode (Keyword)	Incorrect
Failure Description	CCS system executes an incorrect operational movement.
Effect on Linked Functions Systems	a) The point machine moves into the wrong target state (e.g. right) for the operational movement, b) The wrong point machine moves (not the requested one by TMS or Signaller).
Effect on Railway System	-
Risk Comment	PRAM-related considerations: CCS-System shall send the reason for rejecting an operational movement to TMS. CCS-System shall send the reason for rejecting the requested point position to Signaller.













Linked Work Items	<p>relates to :  SPMS-2190 - Control position of one point</p> <p>relates to :  SPMS-2361 - Required point machine movement</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>assesses :  SPRM-1726 - [XYZ] Undue movement of a point</p> <p>relates to :  SPMS-3008 - Required point machine position</p> <p>has parent :  SPRM-2101 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1699 - Point is free of occupancy</p>
-------------------	---

### Incorrect Required point machine movement to Point Machine (2)











ID	SPRM-1732
Failure Mode (Keyword)	Incorrect
Failure Description	CCS system executes an incorrect operational movement.
Effect on Linked Functions Systems	The point machine is already in the target position and could overheat by trying to move into the already reached position,
Effect on Railway System	Possible damage to point machine.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2190 - Control position of one point</p> <p>relates to :  SPMS-2361 - Required point machine movement</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</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-3008 - Required point machine position</p> <p>has parent :  SPRM-2101 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1700 - Point machine position is equal to requested point machine position.</p>

### Late Required point machine movement to Point Machine (1)

ID	SPRM-1303
Failure Mode (Keyword)	Omission
Failure Description	CCS system executes the operational movement later or not at all.
Effect on Linked Functions Systems	<p>a) The point machine moves into the wrong target state (e.g. right) for the operational movement,</p> <p>b) The point machine moves at the wrong time (too late for the movement) when it is still occupied or reserved for another operational movement.</p>

Effect on Railway System	-
Risk Comment	PRAM-related considerations: CCS-System shall send the reason for rejecting an operational movement to TMS. CCS-System shall send the reason for rejecting the requested point position to Signaller.
Linked Work Items	<p>relates to :  SPMS-2190 - Control position of one point</p> <p>relates to :  SPMS-2361 - Required point machine movement</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>assesses :  SPRM-1726 - [XYZ] Undue movement of a point</p> <p>relates to :  SPMS-3008 - Required point machine position</p> <p>has parent :  SPRM-2101 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1699 - Point is free of occupancy</p>

### Late Required point machine movement to Point Machine (2)

ID	SPRM-1733
Failure Mode (Keyword)	Omission
Failure Description	CCS system executes the operational movement later or not at all.
Effect on Linked Functions Systems	The point machine is already in the target position and could overheat by trying to move into the already reached position,
Effect on Railway System	Possible damage to point machine.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2190 - Control position of one point</p> <p>relates to :  SPMS-2361 - Required point machine movement</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</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-3008 - Required point machine position</p> <p>has parent :  SPRM-2101 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1700 - Point machine position is equal to requested point machine position.</p>

### 3.2.1.1.3 Constraints

#### 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
----	-----------

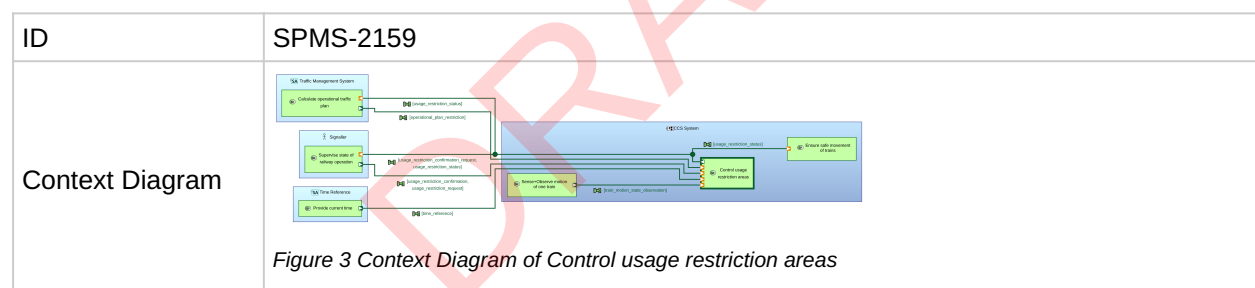
## 3.2.1.2 Control usage restriction

### 3.2.1.2.1 Functional description















#### Control usage restriction areas

This function is allocated to  SPMS-2098 - CCS System.

This function stores and controls the creation and deletion of usage restriction areas. It is responsible for the activation and deactivation of planned usage restriction areas at the planned time. If necessary, it requests the Signaller confirmation before the usage restriction is activated. This function rejects any unplanned temporary speed restriction (TSR) activation request when the train has already been authorized to enter the TSR area. It changes the output state regarding a restriction based on the input request/demand to either activate or deactivate a certain usage restriction. It keeps and shows a record of the activated usage restriction areas.





















Input exchanges	Input exchange items	Source function	Function allocated to
	<ul style="list-style-type: none"> <li>SPMS-5548 - operational_plan_restriction</li> </ul>	 SPMS-2148 - Calculate operational traffic plan	 SPMS-2097 - Traffic Management System
	<ul style="list-style-type: none"> <li>SPMS-2412 - time_reference</li> </ul>	 SPMS-2171 - Provide current time	 SPMS-6265 - Time Reference
	<ul style="list-style-type: none"> <li>SPMS-4826 - usage_restriction_confirmation</li> <li>SPMS-2407 - usage_restriction_request</li> </ul>	 SPMS-2167 - Supervise state of railway operation	 SPMS-2090 - Signaller
	<ul style="list-style-type: none"> <li>SPMS-2392 - train_motion_state_observation</li> </ul>	 SPMS-2192 - Sense+Observe motion of one train	 SPMS-2098 - CCS System
Output exchanges	Output exchange items	Target function	Function allocated to
	<ul style="list-style-type: none"> <li>SPMS-2398 - usage_restriction_status</li> </ul>	 SPMS-2137 - Sense+Observe motion of one train	 SPMS-2098 - CCS System
	<ul style="list-style-type: none"> <li>SPMS-2398 - usage_restriction_status</li> </ul>	 SPMS-2148 - Calculate operational traffic plan	 SPMS-2097 - Traffic Management System
	<ul style="list-style-type: none"> <li>SPMS-4827 - usage_restriction_confirmation_request</li> <li>SPMS-2398 - usage_restriction_status</li> </ul>	 SPMS-2167 - Supervise state of railway operation	 SPMS-2090 - Signaller










### 3.2.1.2.2 Failure Modes and Effects Analysis

#### Early confirmation request of usage restriction deactivation to Signaller

ID	SPRM-1780
Failure Mode (Keyword)	Commission
Failure Description	CCS-System sends request to confirm deactivation of usage restriction too early to Signaller.
Effect on Linked Functions Systems	Signaller receives a request to confirm deactivation of a usage restriction that it is not intended to be deactivated at this time.
Effect on Railway System	If the Signaller confirms it, possible unsafe movement of a train over an area where the usage restriction should be activated.










Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2219 - Usage restriction state</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>assesses :  SPRM-519 - [xy] Field Force on track without trackside protection</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>relates to :  SPMS-7232 - Deactivate usage restriction (Unplanned TSR)</p> <p>relates to :  SPMS-3174 - Usage restriction state</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1702 - Usage restriction area is free of field force</p> <p>_ is mitigated by :  SPRM-1740 - Confirmed usage restriction matches requested usage restriction</p> <p>_ is mitigated by :  SPRM-2240 - Track condition allows regular operation</p>

#### Early indication of usage restriction deactivation state to Signaller










ID	SPRM-1481
Failure Mode (Keyword)	Commission
Failure Description	CCS System indicates usage restriction deactivation state too early to Signaller.
Effect on Linked Functions Systems	Incoherent information on the restriction status may lead to unnecessary manual operations E.g. Signaller takes safety critical actions such as emergency brake activation. (e.g. because track workers are still on the track)
Effect on Railway System	<p>The usage restriction remains active in the CCS System, with the internal status correctly reflecting an active condition; however, this may not align with external expectations or operational assumptions.</p> <p>The train continues to comply with the active usage restriction, as it remains valid and enforced within the CCS System.</p>
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2219 - Usage restriction state</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-7232 - Deactivate usage restriction (Unplanned TSR)</p> <p>relates to :  SPMS-3174 - Usage restriction state</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p>

#### Early confirmation request of usage restriction activation to Signaller










ID	SPRM-914
----	----------

Failure Mode (Keyword)	Commission
Failure Description	CCS-System sends request to confirm the activation of usage restriction too early to Signaller.
Effect on Linked Functions Systems	Signaller would receive a request to confirm a usage restriction that it is not intended to be activated at this time. (The Signaller can confirm this request if all settings including the activation time is correct, even if the request was sent too early ).
Effect on Railway System	Overload for Signaller could lead to missing "correct" requests. Possible delays/ disturbed operations.
Risk Comment	See SPRM-958, SPRM-971 and SPRM-972 analysis for the confirmation from Signaller.
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4469 - Activate usage restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-2219 - Usage restriction state</p> <p>relates to :  SPMS-7226 - Activate usage restriction (Unplanned TSR)</p> <p>relates to :  SPMS-3174 - Usage restriction state</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p>











#### Incorrect indication of usage restriction deactivation state to Signaller

ID	SPRM-1482
Failure Mode (Keyword)	Incorrect
Failure Description	CCS System indicates deactivation of wrong usage restriction to Signaller.
Effect on Linked Functions Systems	The Signaller rejects wrong request or adapts the request according to the operational needs. Or Signaller may have incoherent information regarding the state of the usage restriction which lead to unnecessary manual operations. E.g. a new activation of the still active usage restriction could be requested.
Effect on Railway System	At CCS-System, usage restriction status is correct: the ones that should be still activated are active, and the one that was requested to be deactivated has been deactivated.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-2219 - Usage restriction state</p> <p>relates to :  SPMS-7232 - Deactivate usage restriction (Unplanned TSR)</p> <p>relates to :  SPMS-3174 - Usage restriction state</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p>










#### Incorrect confirmation request of usage restriction activation to Signaller

ID	SPRM-963
Failure Mode (Keyword)	Incorrect
Failure Description	CCS-System requests confirmation to activate wrong usage restriction to Signaller, or indicates wrong settings to be confirmed.
Effect on Linked Functions Systems	Signaller receives information not aligned with operational plan.
Effect on Railway System	Disturbed operation, wrong usage restriction activation in case Signaller confirms it.
Risk Comment	See SPRM-958, SPRM-971 and SPRM-972 analysis for the confirmation from Signaller.
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4469 - Activate usage restriction</p> <p>relates to :  SPMS-2219 - Usage restriction state</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-7226 - Activate usage restriction (Unplanned TSR)</p> <p>relates to :  SPMS-3174 - Usage restriction state</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p>










#### Incorrect indication of Usage restriction activation state to Signaller

ID	SPRM-967
Failure Mode (Keyword)	Incorrect
Failure Description	CCS-System indicates to Signaller incorrect usage restriction (wrong location/parameter) activated than what is activated.
Effect on Linked Functions Systems	Signaller may allow track workers in the area when it is not secured enough (e.g. usage restriction that only allows 0 km/h is indicated but usage restriction that allows 80 km/h is active).
Effect on Railway System	Field Force might be allowed on track by Signaller without protection.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2219 - Usage restriction state</p> <p>relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4469 - Activate usage restriction</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>assesses :  SPRM-519 - [xy] Field Force on track without trackside protection</p> <p>relates to :  SPMS-7226 - Activate usage restriction (Unplanned TSR)</p> <p>relates to :  SPMS-3174 - Usage restriction state</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1702 - Usage restriction area is free of field force</p>














### Late confirmation request of usage restriction deactivation to Signaller

ID	SPRM-1483
Failure Mode (Keyword)	Omission
Failure Description	CCS System requests to Signaller the confirmation for deactivation of a usage restriction too late or not at all.
Effect on Linked Functions Systems	Signaller would not receive a request to confirm deactivation of a usage restriction when it is expected, and the deactivation is not completed or delayed.
Effect on Railway System	Disturbed operation. Train would still respect restrictions activated.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2219 - Usage restriction state</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-3174 - Usage restriction state</p> <p>relates to :  SPMS-7232 - Deactivate usage restriction (Unplanned TSR)</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p>

### Late indication of Usage restriction deactivation state to Signaller










ID	SPRM-1484
Failure Mode (Keyword)	Omission
Failure Description	CCS System indicates usage restriction deactivation state too late or not at all to Signaller.
Effect on Linked Functions Systems	Signaller has incoherent information regarding the state of the usage restriction which lead to unnecessary manual operations. E.g. a new deactivation of the already deactivated usage restriction could be requested.
Effect on Railway System	-
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2219 - Usage restriction state</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-3174 - Usage restriction state</p> <p>relates to :  SPMS-7232 - Deactivate usage restriction (Unplanned TSR)</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p>

### Late confirmation request of usage restriction activation to Signaller










ID	SPRM-964
Failure Mode (Keyword)	Omission
Failure Description	CCS System requests to Signaller the confirmation for activation of a usage restriction too late or not at all.
Effect on Linked Functions Systems	Usage restriction activated too late.
Effect on Railway System	Possible unsafe movement of a train over an area where the usage restriction should be activated. Field Force might be allowed on track by Signaller without protection.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4469 - Activate usage restriction</p> <p>relates to :  SPMS-2219 - Usage restriction state</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>assesses :  SPRM-519 - [xy] Field Force on track without trackside protection</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>relates to :  SPMS-3174 - Usage restriction state</p> <p>relates to :  SPMS-7226 - Activate usage restriction (Unplanned TSR)</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1702 - Usage restriction area is free of field force</p> <p>_ is mitigated by : {c} SPRM-2109 - Usage restriction activation is planned</p>

#### Late indication of Usage restriction activation state to Signaller

ID	SPRM-968
Failure Mode (Keyword)	Omission
Failure Description	CCS System indicates usage restriction activation state too late or not at all to Signaller.
Effect on Linked Functions Systems	The Signaller could stop train operation due to the perception that the usage restriction is inactive.
Effect on Railway System	Disturbed operation (PRAM issue).
Risk Comment	-

Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2219 - Usage restriction state</p> <p>relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4469 - Activate usage restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-3174 - Usage restriction state</p> <p>relates to :  SPMS-7226 - Activate usage restriction (Unplanned TSR)</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p>
-------------------	--










### Early indication of Usage restriction deactivation state to TMS

ID	SPRM-1485
Failure Mode (Keyword)	Commission
Failure Description	CCS System indicates usage restriction deactivation state too early to TMS.
Effect on Linked Functions Systems	TMS has incoherend information about the deactivation state of a usage restriction and plans train movements according to incorrect information.
Effect on Railway System	<p>The usage restriction remains active in the CCS System, with the internal status correctly reflecting an active condition; however, this may not align with external expectations or operational assumptions.</p> <p>The train continues to comply with the active usage restriction, as it remains valid and enforced within the CCS System.</p>
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2215 - Usage restriction state</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-7232 - Deactivate usage restriction (Unplanned TSR)</p> <p>relates to :  SPMS-3173 - Usage restriction state</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p>










### Early indication of Usage restriction activation state to TMS

ID	SPRM-927
Failure Mode (Keyword)	Commission
Failure Description	CCS-System indicates too early to TMS that a usage restriction has been activated.
Effect on Linked Functions Systems	TMS may have incoherent information regarding the state of the usage restriction. No optimal Operational Plan is calculated.



Effect on Railway System	Disturbed operation.
Risk Comment	-
Linked Work Items	<p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2215 - Usage restriction state</p> <p>relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4469 - Activate usage restriction</p> <p>relates to :  SPMS-7226 - Activate usage restriction (Unplanned TSR)</p> <p>relates to :  SPMS-3173 - Usage restriction state</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p>
















### Incorrect indication of Usage restriction deactivation state to TMS

ID	SPRM-1487
Failure Mode (Keyword)	Incorrect
Failure Description	CCS System indicates deactivation of wrong usage restriction to TMS.
Effect on Linked Functions Systems	TMS has incoherend information about the activation state of a usage restriction and plans train movements according to incorrect information.
Effect on Railway System	CCS System internal status of the usage restrictions are correct. CCS System will not allow unsafe requests from TMS that violate active usage restriction. Disturbed operation (PRAM issue)
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2215 - Usage restriction state</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-7232 - Deactivate usage restriction (Unplanned TSR)</p> <p>relates to :  SPMS-3173 - Usage restriction state</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p>

### Early indication of Usage restriction activation state to Signaller















ID	SPRM-966
Failure Mode (Keyword)	Commission
Failure Description	CCS-System indicates usage restriction activation state too early to Signaller.












Effect on Linked Functions Systems	The Signaller is informed about the activation of usage restriction although the usage restriction is not activated. The Signaller may authorise train movements/ trackworkers assuming that the usage restriction is applied but it will not be applied.
Effect on Railway System	Possible unsafe movement of a train over an area where the usage restriction should be activated.
Risk Comment	-
Linked Work Items	<p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2219 - Usage restriction state</p> <p>relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4469 - Activate usage restriction</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>assesses :  SPRM-519 - [xy] Field Force on track without trackside protection</p> <p>relates to :  SPMS-7226 - Activate usage restriction (Unplanned TSR)</p> <p>relates to :  SPMS-2929 - Control usage restrictions</p> <p>relates to :  SPMS-3174 - Usage restriction state</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1701 - Activation process of usage restriction is completed</p>

#### Incorrect confirmation request of usage restriction deactivation to Signaller

ID	SPRM-1778
Failure Mode (Keyword)	Incorrect
Failure Description	CCS-System requests confirmation to deactivate wrong usage restriction to Signaller.
Effect on Linked Functions Systems	Signaller receives information not aligned with operational plan and safety conditions (Field Force might occupy the track).
Effect on Railway System	If Signaller confirms it, this may lead to deactivation of a usage restriction that is still needed.
Risk Comment	-










Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2219 - Usage restriction state</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>assesses :  SPRM-519 - [xy] Field Force on track without trackside protection</p> <p>causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>causes :  SPRM-74 - [A1.3] Collision of one or more rail vehicles with another rail vehicle</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>relates to :  SPMS-3174 - Usage restriction state</p> <p>relates to :  SPMS-7232 - Deactivate usage restriction (Unplanned TSR)</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1702 - Usage restriction area is free of field force</p>
-------------------	---

### Incorrect indication of Usage restriction activation state to TMS










ID	SPRM-969
Failure Mode (Keyword)	Incorrect
Failure Description	CCS-System indicates to TMS incorrect usage restriction (wrong location/parameter) than what is activated.
Effect on Linked Functions Systems	TMS may have incorrect information regarding the state of usage restriction (location, parameters like speed).
Effect on Railway System	Less performance in the operational plan because a usage restriction is taken into account which is not there at all or which imposes more restrictive driving.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2215 - Usage restriction state</p> <p>relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4469 - Activate usage restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-7226 - Activate usage restriction (Unplanned TSR)</p> <p>relates to :  SPMS-3173 - Usage restriction state</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p>

### Late indication of Usage restriction deactivation state to TMS

ID	SPRM-1486
Failure Mode (Keyword)	Omission

Failure Description	CCS System indicates usage restriction deactivation state too late or not at all to TMS.
Effect on Linked Functions Systems	TMS considers usage restriction still active when it is deactivated and plans operational movements more restrictively.
Effect on Railway System	Disturbed operation (PRAM issue)
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2215 - Usage restriction state</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-3173 - Usage restriction state</p> <p>relates to :  SPMS-7232 - Deactivate usage restriction (Unplanned TSR)</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p>

#### Late indication of Usage restriction activation state to TMS

ID	SPRM-970
Failure Mode (Keyword)	Omission
Failure Description	CCS System indicates usage restriction activation state too late or not at all to TMS.
Effect on Linked Functions Systems	TMS uses non-updated restriction information.
Effect on Railway System	Trains/Field Force are protected by usage restriction. Operational movement requests that violate usage restriction will not be executed.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2159 - Control usage restriction areas</p> <p>relates to :  SPMS-2215 - Usage restriction state</p> <p>relates to :  SPMS-4469 - Activate usage restriction</p> <p>relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction)</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-3173 - Usage restriction state</p> <p>relates to :  SPMS-7226 - Activate usage restriction (Unplanned TSR)</p> <p>has parent :  SPRM-2106 - Detailed Failure Modes and Effect Analysis</p>

### 3.2.1.2.3 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
----	-----------

#### 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
----	-----------

#### Track condition allows regular operation

The track conditions are normal and does not need restriction.

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

#### 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
----	-----------

### 3.2.1.3 Ensure safe movement of trains

#### 3.2.1.3.1 Functional description

##### Authorise motion of one train

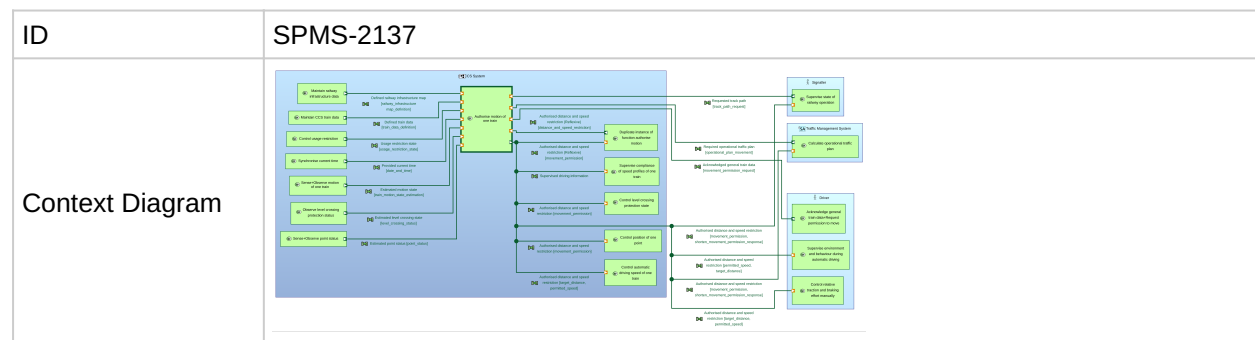
This function controls the speed-and-distance-limiting speed profile over distance for one train for every moment in time, taking all safety constraints into account.

Basic behaviour is to set speed-and-distance-limiting speed profile in a way that the train is allowed to move from its current position towards the next planned stop or a preceding train.























It determines the next section of track path that the train should be allowed to travel on and the maximum safe speed-profile along this path. One key thing to understand is that although "Authorise motion"























produces only one speed-and-distance-limiting speed profile for one train, it needs to take into account information about the whole area of control, such as the state of infrastructure elements, the speed-and-distance-limiting speed profiles of other train units (since these portions of infrastructure are already in use), temporary speed restriction (TSR) and the positions of other trains, vehicles, track workers and equipment trains. It also coordinates the use of a recently activated temporary speed restriction (TSR) to avoid a brake intervention.

There is therefore a portion of the behaviour that looks at the entire railway within the area of control.



## Input exchanges




















-  SPMS-2216 - Usage restriction state
  - Exchange items:
  -  SPMS-2398 - usage\_restriction\_status
-  SPMS-2232 - To be deleted Acknowledged indication
  - Exchange items:
  -  SPMS-2374 - movement\_permission\_request
-  SPMS-2254
  - Exchange items:
  -  SPMS-2403
-  SPMS-2259 - Provided current time
  - Exchange items:
  -  SPMS-2412 - time\_reference
-  SPMS-2272
  - Exchange items:
  -  SPMS-2388
-  SPMS-2282
  - Exchange items:
  -  SPMS-2391
-  SPMS-2303 - Estimated motion state
  - Exchange items:
  -  SPMS-2392 - train\_motion\_state\_observation
-  SPMS-2310 - Observed point status
  - Exchange items:
  -  SPMS-5288 - point\_status
-  SPMS-2315 - Observed level crossing state
  - Exchange items:
  -  SPMS-5939 - level\_crossing\_status
-  SPMS-2347 - Requested track path
  - Exchange items:
  -  SPMS-2418 - track\_path\_request
-  SPMS-2351 - Required operational traffic plan
  - Exchange items:
  -  SPMS-2370 - operational\_plan\_movement

Output exchanges	<ul style="list-style-type: none"> <li>•  SPMS-2225 - Authorised distance and speed restriction             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2373 - permitted_speed</li> <li>◦  SPMS-2375 - target_distance</li> </ul> </li> <li>•  SPMS-2248 - Authorised distance and speed restriction             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2372 - movement_permission</li> <li>◦  SPMS-5480 - shorten_movement_permission_response</li> </ul> </li> <li>•  SPMS-2249 - Authorised distance and speed restriction             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2372 - movement_permission</li> <li>◦  SPMS-5480 - shorten_movement_permission_response</li> </ul> </li> <li>•  SPMS-2250 - Authorised distance and speed restriction             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2372 - movement_permission</li> </ul> </li> <li>•  SPMS-2251</li> <li>•  SPMS-2252             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2372 - movement_permission</li> </ul> </li> <li>•  SPMS-2253 - Authorised distance and speed restriction             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2372 - movement_permission</li> </ul> </li> <li>•  SPMS-2325 - Authorised distance and speed restriction             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2373 - permitted_speed</li> <li>◦  SPMS-2375 - target_distance</li> </ul> </li> <li>•  SPMS-2326 - Authorised distance and speed restriction             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2373 - permitted_speed</li> <li>◦  SPMS-2375 - target_distance</li> </ul> </li> </ul>
------------------	--

### 3.2.1.3.2 Failure Modes and Effects Analysis

#### Early indication of Authorised distance and speed restriction to Signaller




















ID	SPRM-1053
Failure Mode (Keyword)	Commission
Failure Description	CCS-System indicates authorised distance and speed restriction too early to Signaller.

Effect on Linked Functions Systems	Signaller plans actions according to incorrect information about the movement permissions (indicated as shortened or granted when the shortening or granting was not yet executed). This can result in manual requests to CCS-System being incorrect.
Effect on Railway System	-
Risk Comment	Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.
Linked Work Items	<p>relates to :  SPMS-2137 - Ensure safe movement of trains</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>relates to :  SPMS-7230 - Authorised distance and speed restriction</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-3044 - Allocated track path</p> <p>relates to :  SPMS-2874 - Control track path allocation for movement permissions</p> <p>relates to :  SPMS-6432 - Authorised movement permission</p> <p>relates to :  SPMS-6396 - Indicated track section state</p> <p>has parent :  SPRM-2112 - Detailed Failure Modes and Effect Analysis</p>

### Incorrect indication of Authorised distance and speed restriction to Signaller

















ID	SPRM-1055
Failure Mode (Keyword)	Incorrect
Failure Description	CCS-System indicates incorrect authorised distance and speed restriction to Signaller.
Effect on Linked Functions Systems	<p>Signaller has incorrect information about the status of the movement permission (e.g. executed when it is rejected, incorrect movement permission displayed) and bases his decisions on it.</p> <p>Incorrect information in this case can be</p> <p>a) incorrect to the safe side (longer movement permissions due to e.g. shortening incorrectly displayed as executed when it is rejected, higher speed than in reality)</p> <p>b) incorrect to the non-safe side (lower speed, shorter movement permission than in reality).</p> <p>This can result in manual requests to CCS-System being incorrect. Possibly unsafe operation by Signaller due to cases listed in b). For other operations of the Signaller, please refer to the Risk Comment.</p>
Effect on Railway System	-



Risk Comment	<p>Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.</p> <p>Some use cases could lead to a hazard but they are not analysed here due to a lack of information in this scenarios about these processes.</p> <p>For example, the case If Signaller sees a shortening which actually was rejected, there needs to be a safety barrier that the Signaller is not allowed to derive safety relevant decision on the information (e.g. allowing track workers to enter the area, ...), will be analysed in the respective scenarios where the communication between track worker and Signaller is described.</p>
Linked Work Items	<p>relates to :  SPMS-2137 - Ensure safe movement of trains</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>relates to :  SPMS-7230 - Authorised distance and speed restriction</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-3044 - Allocated track path</p> <p>relates to :  SPMS-2874 - Control track path allocation for movement permissions</p> <p>relates to :  SPMS-6432 - Authorised movement permission</p> <p>relates to :  SPMS-6396 - Indicated track section state</p> <p>has parent :  SPRM-2112 - Detailed Failure Modes and Effect Analysis</p>
















### Late indication of Authorised distance and speed restriction to Signaller

ID	SPRM-1054
Failure Mode (Keyword)	Omission
Failure Description	CCS system indicates authorised distance and speed restriction too late or not at all to Signaller.
Effect on Linked Functions Systems	Signaller has outdated information about the status of the movement permission shortening (executed on the train but no new indication of the shortened movement permission, rejection is not displayed) and bases his decisions on it. Outdated information in this case is to the safe side (longer movement permissions indicated), possible commands can be sent to CCS system that are not executable.
Effect on Railway System	-
Risk Comment	Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.










Linked Work Items	<p>relates to :  SPMS-2137 - Ensure safe movement of trains</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>relates to :  SPMS-7230 - Authorised distance and speed restriction</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-3044 - Allocated track path</p> <p>relates to :  SPMS-2874 - Control track path allocation for movement permissions</p> <p>relates to :  SPMS-6432 - Authorised movement permission</p> <p>relates to :  SPMS-6396 - Indicated track section state</p> <p>has parent :  SPRM-2112 - Detailed Failure Modes and Effect Analysis</p>
-------------------	--

### Early indication of Authorised distance and speed restriction to Driver

ID	SPRM-1052
Failure Mode (Keyword)	Commission
Failure Description	CCS-System sends the distance and speed restriction too early to the Driver.
Effect on Linked Functions Systems	The Driver receives the correct distance and speed restriction too early. The Driver still applies the new distance and speed restriction at the right time.
Effect on Railway System	-
Risk Comment	-

















Linked Work Items	<p>relates to :  SPMS-2137 - Ensure safe movement of trains</p> <p>relates to :  SPMS-2326 - Authorised distance and speed restriction</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4326 - 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-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-3191 - Calculated supervision limits</p> <p>has parent :  SPRM-2112 - Detailed Failure Modes and Effect Analysis</p> <p>_ is parent of :  SPRM-1401 - Early indication of Authorised distance and speed restriction to Driver</p>
-------------------	--

#### Early indication of Authorised distance and speed restriction to Driver

ID	SPRM-1401
Failure Mode (Keyword)	Commission
Failure Description	CCS-System sends the distance and speed restriction too early to the Driver.
Effect on Linked Functions Systems	The Driver receives the correct distance and speed restriction too early while supervising the automatic driving. The automatic driving will execute the new speed profile at the right time and the Driver does not need to take action.
Effect on Railway System	-
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2137 - Ensure safe movement of trains</p> <p>relates to :  SPMS-2325 - Authorised distance and speed restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-3190 - Calculated supervision limits</p> <p>relates to :  SPMS-5444 - Drive train automatically</p> <p>relates to :  SPMS-5359 - Drive train automatically</p> <p>has parent :  SPRM-1052 - Early indication of Authorised distance and speed restriction to Driver</p>











#### Incorrect indication of Authorised distance and speed restriction to Driver

ID	SPRM-1057
Failure Mode (Keyword)	Incorrect
Failure Description	CCS-System sends incorrect distance and speed restriction to the Driver.

















Effect on Linked Functions Systems	Driver applies incorrect new distance and speed restriction (e.g. new stop location closer or further away than executed by CCS system, higher or lower speed than what is authorised by CCS-System).
Effect on Railway System	Train is possibly overspeeding and will not be able to brake at its end of authority.
Risk Comment	DMI is SIL2 today.
Linked Work Items	<p>relates to :  SPMS-2137 - Ensure safe movement of trains</p> <p>relates to :  SPMS-2326 - Authorised distance and speed restriction</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-3191 - Calculated supervision limits</p> <p>has parent :  SPRM-2112 - Detailed Failure Modes and Effect Analysis</p> <p>_ is parent of :  SPRM-1402 - Incorrect indication of Authorised distance and speed restriction to Driver</p> <p>_ is mitigated by : {c} SPRM-1439 - Train located within movement permission</p> <p>_ is mitigated by : {c} SPRM-1440 - Train speed is equal or less than the authorised target speed</p>

#### Incorrect indication of Authorised distance and speed restriction to Driver











ID	SPRM-1402
Failure Mode (Keyword)	Incorrect
Failure Description	CCS system indicates incorrect distance and speed restriction to the Driver.
Effect on Linked Functions Systems	Driver supervises automatic Driving based on an incorrect new distance and speed restriction (e.g. new stop location closer or further away than executed by CCS system, higher or lower speed than what is requested by CCS system). This can lead to unnecessary actions (e.g. braking the train) or missing safety reactions by the Driver (e.g. not braking the train).
Effect on Railway System	-
Risk Comment	This exchange is not shown in the capability SPMS-5359 Drive rain automatically. There it seems that another function provides this information. Consistency to be checked by specification group.

Linked Work Items	<p>relates to :  SPMS-2137 - Ensure safe movement of trains</p> <p>relates to :  SPMS-2325 - Authorised distance and speed restriction</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-3190 - Calculated supervision limits</p> <p>relates to :  SPMS-5444 - Drive train automatically</p> <p>relates to :  SPMS-5359 - Drive train automatically</p> <p>has parent :  SPRM-1057 - Incorrect indication of Authorised distance and speed restriction to Driver</p> <p>_ is mitigated by : {c} SPRM-1439 - Train located within movement permission</p> <p>_ is mitigated by : {c} SPRM-1440 - Train speed is equal or less than the authorised target speed</p>
-------------------	--

### Late indication of Authorised distance and speed restriction to Driver

















ID	SPRM-1056
Failure Mode (Keyword)	Omission
Failure Description	CCS-System sends the distance and speed restriction to the Driver too late or not at all.
Effect on Linked Functions Systems	The Driver receives the correct distance and speed restriction too late or not at all. The Driver applies the new distance and speed restriction too late or not at all.
Effect on Railway System	Train is possibly overspeeding and will not be able to brake at its end of authority.
Risk Comment	DMI is SIL2 today.
Linked Work Items	<p>relates to :  SPMS-2137 - Ensure safe movement of trains</p> <p>relates to :  SPMS-2326 - Authorised distance and speed restriction</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-3191 - Calculated supervision limits</p> <p>has parent :  SPRM-2112 - Detailed Failure Modes and Effect Analysis</p> <p>_ is parent of :  SPRM-1403 - Late indication of Authorised distance and speed restriction to Driver</p> <p>_ is mitigated by : {c} SPRM-1439 - Train located within movement permission</p> <p>_ is mitigated by : {c} SPRM-1440 - Train speed is equal or less than the authorised target speed</p>

### Late indication of Authorised distance and speed restriction to Driver

ID	SPRM-1403
Failure Mode (Keyword)	Omission
Failure Description	CCS system indicates distance and speed restriction too late or not at all to the Driver.
Effect on Linked Functions Systems	Driver supervises automatic Driving based on an incorrect new distance and speed restriction (e.g. new stop location closer or further away than executed by CCS system, higher or lower speed than what is requested by CCS system). This can lead to unnecessary actions (e.g. braking the train) or missing safety reactions by the Driver (e.g. not braking the train).
Effect on Railway System	-
Risk Comment	This exchange is not shown in the capability SPMS-5359 Drive train automatically. There it seems that another function provides this information. Consistency to be checked by specification group.
Linked Work Items	<p>relates to :  SPMS-2137 - Ensure safe movement of trains</p> <p>relates to :  SPMS-2325 - Authorised distance and speed restriction</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-3190 - Calculated supervision limits</p> <p>relates to :  SPMS-5444 - Drive train automatically</p> <p>relates to :  SPMS-5359 - Drive train automatically</p> <p>has parent :  SPRM-1056 - Late indication of Authorised distance and speed restriction to Driver</p> <p>_ is mitigated by : {c} SPRM-1439 - Train located within movement permission</p> <p>_ is mitigated by : {c} SPRM-1440 - Train speed is equal or less than the authorised target speed</p>

### Early indication of Authorised distance and speed restriction to TMS

















ID	SPRM-1058
Failure Mode (Keyword)	Commission
Failure Description	CCS-System sends the distance and speed restriction too early to TMS.
Effect on Linked Functions Systems	TMS bases the planning of operational movements on incorrect information about the movement permission (indicated as shortened or granted when the shortening or granting was not yet executed). This can result in the calculated Operational Plan not being conflict-free or/and not optimal.
Effect on Railway System	-
Risk Comment	Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.

Linked Work Items	<p>relates to :  SPMS-2137 - Ensure safe movement of trains</p> <p>relates to :  SPMS-2249 - Authorised distance and speed restriction</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-3052 - Allocated track path</p> <p>has parent :  SPRM-2112 - Detailed Failure Modes and Effect Analysis</p>
-------------------	---

#### Incorrect indication of Authorised distance and speed restriction to TMS

ID	SPRM-1060
Failure Mode (Keyword)	Incorrect
Failure Description	CCS-System indicates incorrect authorised distance and speed restriction to the TMS.
Effect on Linked Functions Systems	TMS bases the planning of operational movements on incorrect information about the movement permission (e.g. longer or shorter movement permission than what CCS system executed, higher or lower speed of train than what is allowed by CCS system). This can result in the calculated Operational Plan not being conflict-free or/and not optimal.
Effect on Railway System	-
Risk Comment	Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.
















Linked Work Items	<p>relates to :  SPMS-2137 - Ensure safe movement of trains</p> <p>relates to :  SPMS-2249 - Authorised distance and speed restriction</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-3052 - Allocated track path</p> <p>has parent :  SPRM-2112 - Detailed Failure Modes and Effect Analysis</p>
-------------------	---

#### Late indication of Authorised distance and speed restriction to TMS

ID	SPRM-1059
Failure Mode (Keyword)	Omission
Failure Description	CCS system indicates authorised distance and speed restriction too late or not at all to TMS.
Effect on Linked Functions Systems	TMS bases the planning of operational movements on outdated information about the status of the movement permission shortening (executed on the train but no new indication of the shortened movement permission, rejection is not displayed). Outdated information in this case is to the safe side (longer movement permissions indicated). This can result in the calculated Operational Plan not being conflict-free or/and not optimal.
Effect on Railway System	-
Risk Comment	PRAM-related considerations: TMS shall not replan movements impacting a train when no response from CCS system about the execution state of a requested revocation of the movement permission for this train was received.



Linked Work Items	relates to :  SPMS-2137 - Ensure safe movement of trains relates to :  SPMS-2249 - Authorised distance and speed restriction relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted) relates to :  SPMS-4441 - Shorten movement permission relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted) assesses :  SPRM-516 - No safety hazard causes :  SPRM-517 - No accident relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected) relates to :  SPMS-5316 - Release movement permission relates to :  SPMS-5362 - Release movement permission relates to :  SPMS-4333 - Superfluous Perform train movement relates to :  SPMS-3052 - Allocated track path has parent :  SPRM-2112 - Detailed Failure Modes and Effect Analysis
-------------------	---

### 3.2.1.3.3 Constraints

#### 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
----	-----------

#### 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
----	-----------

#### 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
----	-----------

#### 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
----	-----------

#### Train speed is equal or less than the authorised target speed

Train speed is equal or less than the authorised target speed taking into account margins for slight overspeeding.

ID	SPRM-1440
----	-----------

#### Train located within movement permission

Train is located in the boundaries of its movement permission. If there is a train located without a movement permission, it is not allowed to move until it gets a movement permission or another

authorisation to move.

If a train overreached the boundaries of the movement permission, it needs to be braked.

ID	SPRM-1439
----	-----------

#### 3.2.1.4 Sense + Observe motion of one train

#### 3.2.1.4.1 Functional description




























### Sense+Observe motion of one train






































This function is allocated to  SPMS-2098 - CCS System.

This function senses the following states of one train: power on/off, cab activated/not activated.

This function senses the following states of one train: power on/off, cab activated/not activated. This function senses the passing of one wheel by infrastructure reference location, the passing of one infrastructure reference location by one train reference point and the motions parameters speed and acceleration. In order to derive an observation of the estimated motion of the train. This includes the occupation of track and all of its relevant navigation parameters, such as speed and acceleration.

[illegible]











Input exchanges	Input exchanges	Source function	Function allocated to
	 SPMS-2244 - Actual wheel passing <ul style="list-style-type: none"> <li> SPMS-6523 - actual_wheel_passing</li> </ul>	 SPMS-2141 - Has wheel position and direction in relation to track coordinates	 SPMS-2101 - Wheel
	 SPMS-2238 - Actual present geographical coordinate <ul style="list-style-type: none"> <li> SPMS-6520 - actual_geographical_coordinate</li> </ul>	 SPMS-2135 - Has position in relation to geographical coordinates	 SPMS-2091 - Rolling Stock Reference Point
	 SPMS-2239 - Actual present position and direction <ul style="list-style-type: none"> <li> SPMS-6521 - actual_position_and_direction</li> </ul>	 SPMS-2138 - Has position and direction in relation to track coordinates	 SPMS-2091 - Rolling Stock Reference Point
	 SPMS-2234 - Actual acceleration <ul style="list-style-type: none"> <li> SPMS-6519 - actual_acceleration</li> </ul>	 SPMS-2127 - Has acceleration vector in relation to rolling stock coordinates	 SPMS-2091 - Rolling Stock Reference Point
	 SPMS-2243 - Actual velocity <ul style="list-style-type: none"> <li> SPMS-6522 - actual_velocity</li> </ul>	 SPMS-2140 - Has velocity in relation to track coordinates	 SPMS-2091 - Rolling Stock Reference Point
	 SPMS-7178 - Provided driver information <ul style="list-style-type: none"> <li> SPMS-2371 - train_data</li> <li> SPMS-2414 - train_running_number</li> <li> SPMS-7169 - ETCS_level</li> <li> SPMS-7111 - train_data_validation</li> </ul>	 SPMS-2126 - Control start of mission activities manually	 SPMS-2096 - Driver

Output exchanges	Output exchanges	Target function	Function allocated to
	 SPMS-6660 - Estimated motion state <ul style="list-style-type: none"> <li> SPMS-2400 - current_speed</li> </ul>	 SPMS-2158 - Supervise guideway of one train	 SPMS-2096 - Driver
	 SPMS-6479 - Estimated motion state <ul style="list-style-type: none"> <li> SPMS-2392 - train_motion_state_observation</li> </ul>	 SPMS-2159 - Control usage restriction areas	 SPMS-2098 - CCS System
	 SPMS-2302 - Estimated motion state <ul style="list-style-type: none"> <li> SPMS-2392 - train_motion_state_observation</li> </ul>	 SPMS-2180 - Control automatic driving speed of one train	 SPMS-2098 - CCS System
	 SPMS-2308 - Estimated motion state <ul style="list-style-type: none"> <li> SPMS-2392 - train_motion_state_observation</li> </ul>	 SPMS-2160 - Calculate information to support driving	 SPMS-2098 - CCS System
	 SPMS-2300 - Estimated motion state <ul style="list-style-type: none"> <li> SPMS-2392 - train_motion_state_observation</li> </ul>	 SPMS-2148 - Calculate operational traffic plan	 SPMS-2097 - Traffic Management System
	 SPMS-2301 - Estimated motion state <ul style="list-style-type: none"> <li> SPMS-2392 - train_motion_state_observation</li> </ul>	 SPMS-2190 - Control position of one point	 SPMS-2098 - CCS System
	 SPMS-2303 - Estimated motion state <ul style="list-style-type: none"> <li> SPMS-2392 - train_motion_state_observation</li> </ul>	 SPMS-2137 - Ensure safe movement of trains	 SPMS-2098 - CCS System
	 SPMS-2336 - Estimated motion state <ul style="list-style-type: none"> <li> SPMS-2400 - current_speed</li> <li> SPMS-7177 - ETCS_mode</li> </ul>	 SPMS-2106 - Control relative traction and braking effort manually	 SPMS-2096 - Driver
	 SPMS-2330 - Estimated motion state <ul style="list-style-type: none"> <li> SPMS-2392 - train_motion_state_observation</li> </ul>	 SPMS-2167 - Supervise state of railway operation	 SPMS-2090 - Signaller

### 3.2.1.4.2 Failure Modes and Effects Analysis











#### Early indication of estimated train motion state information to TMS

ID	SPRM-1185
----	-----------











Failure Mode (Keyword)	Commission
Failure Description	CCS System sends the estimated train motion state too early to TMS.
Effect on Linked Functions Systems	TMS bases the planning of operational movements on incorrect information about the train motion state (dynamic train data like position and speed are not the actual ones). This can result in the calculated Operational Plan not being conflict-free or/and not optimal.
Effect on Railway System	--
Risk Comment	Note 1 : Failure mode "comission" is interpreted to mean that something does not happen too early in terms of time, but too early in terms of a sequence. The information is send before all aspectes for aggregation of the information to be send are finished.  Note 2: Incorrect inputs into CCS System are analysed in other risk and are not repeated here.
Linked Work Items	relates to :  SPMS-2192 - Sense+Observe motion of one train relates to :  SPMS-2300 - Estimated motion state relates to :  SPMS-4329 - Localise train on railway infrastructure relates to :  SPMS-4438 - Localise train on railway infrastructure assesses :  SPRM-516 - No safety hazard causes :  SPRM-517 - No accident relates to :  SPMS-3050 - Aggregated track occupancy and train status information relates to :  SPMS-4442 - Execute end of mission relates to :  SPMS-4344 - Execute end of mission has parent :  SPRM-2117 - Detailed Failure Modes and Effect Analysis

#### Incorrect indication of estimated train motion state information to TMS

ID	SPRM-1186
Failure Mode (Keyword)	Incorrect
Failure Description	CCS System sends incorrect train motion state to the TMS.
Effect on Linked Functions Systems	TMS bases the planning of operational movements on incorrect information about the train motion state (dynamic train data like position and speed are not the actual ones). This can result in the calculated Operational Plan not being conflict-free or/and not optimal.
Effect on Railway System	--
Risk Comment	Note: Incorrect inputs into CCS System are analysed in other risk and are not repeated here.











Linked Work Items	<p>relates to :  SPMS-2192 - Sense+Observe motion of one train</p> <p>relates to :  SPMS-2300 - Estimated motion state</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-3050 - Aggregated track occupancy and train status information</p> <p>relates to :  SPMS-4442 - Execute end of mission</p> <p>relates to :  SPMS-4344 - Execute end of mission</p> <p>has parent :  SPRM-2117 - Detailed Failure Modes and Effect Analysis</p>
-------------------	--

#### Late indication of estimated train motion state information to TMS











ID	SPRM-1187
Failure Mode (Keyword)	Omission
Failure Description	CCS System sends the estimated train motion state too late or not at all.
Effect on Linked Functions Systems	TMS bases the planning of operational movements on outdated information about the train motion state (dynamic train data like position and speed are not the actual ones). This can result in the calculated Operational Plan not being conflict-free or/and not optimal.
Effect on Railway System	--
Risk Comment	Note: Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.
Linked Work Items	<p>relates to :  SPMS-2192 - Sense+Observe motion of one train</p> <p>relates to :  SPMS-2300 - Estimated motion state</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-3050 - Aggregated track occupancy and train status information</p> <p>relates to :  SPMS-4442 - Execute end of mission</p> <p>relates to :  SPMS-4344 - Execute end of mission</p> <p>has parent :  SPRM-2117 - Detailed Failure Modes and Effect Analysis</p>

#### Early indication of estimated train area occupation information to Signaller

ID	SPRM-1188
Failure Mode (Keyword)	Commission
Failure Description	CCS System sends the estimated train area occupation too early to the Signaller.
Effect on Linked Functions Systems	Signaller plans actions based on incorrect information about the trackside occupation. Possibly requests that contradict the granted movement permissions will be send.











Effect on Railway System	--
Risk Comment	<p>Note 1 : Failure mode "comission" is interpreted to mean that something does not happen too early in terms of time, but too early in terms of a sequence. The information is send before all aspectes for aggregation of the information to be send are finished.</p> <p>Note 2: Incorrect inputs into CCS System are analysed in other risk and are not repeated here.</p>
Linked Work Items	<p>relates to :  SPMS-2192 - Sense+Observe motion of one train</p> <p>relates to :  SPMS-2330 - Estimated motion state</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4666 - Aggregated track occupancy and train status information</p> <p>relates to :  SPMS-4442 - Execute end of mission</p> <p>relates to :  SPMS-4344 - Execute end of mission</p> <p>has parent :  SPRM-2117 - Detailed Failure Modes and Effect Analysis</p>

#### Incorrect indication of estimated train area occupation information to Signaller











ID	SPRM-1189
Failure Mode (Keyword)	Incorrect
Failure Description	CCS System sends incorrect train area occupation information to the Signaller.
Effect on Linked Functions Systems	Signaller plans actions based on incorrect information about the trackside occupation. Possibly requests that contradict the granted movement permissions will be send.
Effect on Railway System	--
Risk Comment	Note: Incorrect inputs into CCS System are analysed in other risk and are not repeated here.
Linked Work Items	<p>relates to :  SPMS-2192 - Sense+Observe motion of one train</p> <p>relates to :  SPMS-2330 - Estimated motion state</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4666 - Aggregated track occupancy and train status information</p> <p>relates to :  SPMS-4442 - Execute end of mission</p> <p>relates to :  SPMS-4344 - Execute end of mission</p> <p>has parent :  SPRM-2117 - Detailed Failure Modes and Effect Analysis</p>

#### Late indication of estimated train area occupation information to Signaller

ID	SPRM-1190
Failure Mode (Keyword)	Omission











Failure Description	CCS System sends the estimated train area occupation too late or not at all.
Effect on Linked Functions Systems	Signaller plans actions according to outdated information about the trackside occupation. Possibly commands that contradict the granted movement permissions will be send.
Effect on Railway System	--
Risk Comment	Note: Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.
Linked Work Items	<p>relates to :  SPMS-2192 - Sense+Observe motion of one train</p> <p>relates to :  SPMS-2330 - Estimated motion state</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4666 - Aggregated track occupancy and train status information</p> <p>relates to :  SPMS-4442 - Execute end of mission</p> <p>relates to :  SPMS-4344 - Execute end of mission</p> <p>has parent :  SPRM-2117 - Detailed Failure Modes and Effect Analysis</p>

#### Early indication of current train speed to Driver













ID	SPRM-1191
Failure Mode (Keyword)	Commission
Failure Description	CCS System sends the current train speed too early to the train Driver.
Effect on Linked Functions Systems	Train Driver supervises the track guideway based on incorrect train speed indication on DMI (e. g. indication of less or higher speed). Not adequate actions could be performed.
Effect on Railway System	Possible overspeeding of train.
Risk Comment	<p>Note 1: Failure mode "comission" is interpreted to mean that something does not happen too early in terms of time, but too early in terms of a sequence. The information is send before all aspectes for aggregation of the information to be send are finished.</p> <p>Note 2: This DMI functionality is implemented today in SIL 2.</p>
Linked Work Items	<p>relates to :  SPMS-2192 - Sense+Observe motion of one train</p> <p>relates to :  SPMS-2336 - Estimated motion state</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-4510 - Estimated speed</p> <p>has parent :  SPRM-2117 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1717 - Integrity of train speed display</p>



### Incorrect indication of current train speed to Driver

ID	SPRM-1192
Failure Mode (Keyword)	Incorrect
Failure Description	CCS System sends incorrect speed information to the Driver.
Effect on Linked Functions Systems	Train Driver performs actions according incorrect train speed indication on DMI (e. g. indicated speed is lower than real speed).
Effect on Railway System	Possible overspeeding of train.
Risk Comment	Note: Incorrect inputs into CCS System are analysed in other risk and are not repeated here.
Linked Work Items	<p>relates to :  SPMS-2192 - Sense+Observe motion of one train</p> <p>relates to :  SPMS-2336 - Estimated motion state</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>relates to :  SPMS-4510 - Estimated speed</p> <p>has parent :  SPRM-2117 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1717 - Integrity of train speed display</p>

### Late indication of current train speed to Driver

ID	SPRM-1193
Failure Mode (Keyword)	Omission
Failure Description	CCS System sends the current train speed too late or not at all.
Effect on Linked Functions Systems	Train Driver performs actions according outdated train speed indication on DMI (e. g. indicated speed is lower than real speed).
Effect on Railway System	Possible overspeeding of train.
Risk Comment	Note: Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.
Linked Work Items	<p>relates to :  SPMS-2192 - Sense+Observe motion of one train</p> <p>relates to :  SPMS-2336 - Estimated motion state</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>assesses :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>assesses :  SPRM-78 - [A2.1] Derailment of train</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>relates to :  SPMS-4510 - Estimated speed</p> <p>has parent :  SPRM-2117 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1717 - Integrity of train speed display</p>

### 3.2.1.4.3 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
----	-----------

#### Integrity of train speed display

The Train's actual speed is displayed correctly to the Driver.

ID	SPRM-1717
----	-----------

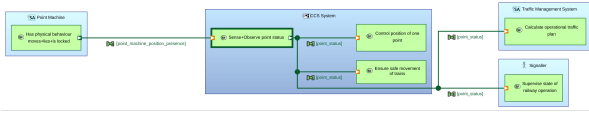




















### 3.2.1.5 Sense + Observe point status

#### 3.2.1.5.1 Functional description

##### Sense+Observe point status










This function is allocated to  SPMS-2098 - CCS System.

This function senses and observes the state of one point (on one or more point machines) based on the blades position of the Point.

ID	SPMS-2108		
Context Diagram	 <p>Figure 5 Context Diagram of Sense+Observe point status</p>		
Input exchanges	<b>Input exchanges</b>  SPMS-2237 - Actual physical point machine position <ul style="list-style-type: none"> <li> SPMS-2381 - point_machine_position_presence</li> </ul>	<b>Source function</b>  SPMS-2132 - Has physical behaviour moves+lies+is locked	<b>Function allocated to</b>  SPMS-2100 - Point Machine
Output exchanges	<b>Output exchanges</b>  SPMS-2310 - Observed point status <ul style="list-style-type: none"> <li> SPMS-5288 - point_status</li> </ul>	<b>Target function</b>  SPMS-2137 - Ensure safe movement of trains	<b>Function allocated to</b>  SPMS-2098 - CCS System
	 SPMS-5329 - Observed point status <ul style="list-style-type: none"> <li> SPMS-5288 - point_status</li> </ul>	 SPMS-2148 - Calculate operational traffic plan	 SPMS-2097 - Traffic Management System
	 SPMS-2311 - Observed point status <ul style="list-style-type: none"> <li> SPMS-5288 - point_status</li> </ul>	 SPMS-2190 - Control position of one point	 SPMS-2098 - CCS System
	 SPMS-2312 - Observed point status <ul style="list-style-type: none"> <li> SPMS-5288 - point_status</li> </ul>	 SPMS-2167 - Supervise state of railway operation	 SPMS-2090 - Signaller










### 3.2.1.5.2 Failure Modes and Effects Analysis

#### Early indication of Observed point status to Signaller










ID	SPRM-1287
Failure Mode (Keyword)	Commission
Failure Description	CCS-System indicates point status to the Signaller too early.
Effect on Linked Functions Systems	Signaller has incorrect information about the point position and bases his decisions on it. This can result in manual requests to CCS-System being incorrect.
Effect on Railway System	-
Risk Comment	<p>Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.</p> <p>Scenarios in which the Signaller bypasses CCS-System and controls other actors (e.g. written order) are not described and are out of scope in this analysis.</p>
Linked Work Items	<p>relates to :  SPMS-2108 - Sense+Observe point status</p> <p>relates to :  SPMS-2312 - Observed point status</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-3189 - Observed point status</p> <p>has parent :  SPRM-2124 - Detailed Failure Modes and Effect Analysis</p>

#### Incorrect indication of Observed point status to Signaller

ID	SPRM-1288
Failure Mode (Keyword)	Incorrect
Failure Description	CCS-System indicates incorrect point status to the Signaller.
Effect on Linked Functions Systems	Signaller has incorrect information about the point position and bases his decisions on it. This can result in manual requests to CCS-System being incorrect.
Effect on Railway System	-
Risk Comment	<p>Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.</p> <p>Scenarios in which the Signaller bypasses CCS-System and controls other actors (e.g. written order) are not described and are out of scope in this analysis.</p>










Linked Work Items	relates to :  SPMS-2108 - Sense+Observe point status relates to :  SPMS-2312 - Observed point status relates to :  SPMS-4342 - Set point position (Left to right, Operational plan) relates to :  SPMS-4769 - Set point position (Left to right, Signaller request) relates to :  SPMS-4444 - Set point position assesses :  SPRM-516 - No safety hazard causes :  SPRM-517 - No accident relates to :  SPMS-3189 - Observed point status has parent :  SPRM-2124 - Detailed Failure Modes and Effect Analysis
-------------------	---

### Late indication of Observed point status to Signaller










ID	SPRM-1291
Failure Mode (Keyword)	Omission
Failure Description	CCS-System indicates outdated point status to the Signaller.
Effect on Linked Functions Systems	Signaller has outdated information about the point position and bases his decisions on it. This can result in manual requests to CCS-System being incorrect.
Effect on Railway System	-
Risk Comment	Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.  Scenarios in which the Signaller bypasses CCS-System and controls other actors (e.g. written order) are not described and are out of scope in this analysis.
Linked Work Items	relates to :  SPMS-2108 - Sense+Observe point status relates to :  SPMS-2312 - Observed point status relates to :  SPMS-4342 - Set point position (Left to right, Operational plan) relates to :  SPMS-4769 - Set point position (Left to right, Signaller request) relates to :  SPMS-4444 - Set point position assesses :  SPRM-516 - No safety hazard causes :  SPRM-517 - No accident relates to :  SPMS-3189 - Observed point status has parent :  SPRM-2124 - Detailed Failure Modes and Effect Analysis

### Early indication of Observed point status to TMS

ID	SPRM-1289
Failure Mode (Keyword)	Commission
Failure Description	CCS-System indicates point status to TMS too early.
Effect on Linked Functions Systems	TMS bases the planning of operational movements on incorrect information about the point position. This can result in the calculated Operational Plan not being conflict-free or/and not optimal.
Effect on Railway System	-










Risk Comment	Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.
Linked Work Items	<p>relates to :  SPMS-2108 - Sense+Observe point status</p> <p>relates to :  SPMS-5329 - Observed point status</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5339 - Observed point status</p> <p>has parent :  SPRM-2124 - Detailed Failure Modes and Effect Analysis</p>

### Incorrect indication of Observed point status to TMS

ID	SPRM-1290
Failure Mode (Keyword)	Incorrect
Failure Description	CCS-System indicates incorrect point status to TMS.
Effect on Linked Functions Systems	TMS bases the planning of operational movements on incorrect information about the point position. This can result in the calculated Operational Plan not being conflict-free or/and not optimal.
Effect on Railway System	-
Risk Comment	Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.
Linked Work Items	<p>relates to :  SPMS-2108 - Sense+Observe point status</p> <p>relates to :  SPMS-5329 - Observed point status</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5339 - Observed point status</p> <p>has parent :  SPRM-2124 - Detailed Failure Modes and Effect Analysis</p>

### Late indication of Observed point status to TMS

ID	SPRM-1292
Failure Mode (Keyword)	Omission
Failure Description	CCS-System indicates outdated point status to TMS.
Effect on Linked Functions Systems	TMS bases the planning of operational movements on outdated information about the point position. This can result in the calculated Operational Plan not being conflict-free or/and not optimal.
Effect on Railway System	-
Risk Comment	Incorrect inputs into CCS-System are analysed in other risk and are not repeated here.

Linked Work Items	relates to :  SPMS-2108 - Sense+Observe point status relates to :  SPMS-5329 - Observed point status relates to :  SPMS-4342 - Set point position (Left to right, Operational plan) relates to :  SPMS-4769 - Set point position (Left to right, Signaller request) relates to :  SPMS-4444 - Set point position assesses :  SPRM-516 - No safety hazard causes :  SPRM-517 - No accident relates to :  SPMS-5339 - Observed point status has parent :  SPRM-2124 - Detailed Failure Modes and Effect Analysis
-------------------	---

### 3.2.1.5.3 Constraints

No constraints allocated to this function.

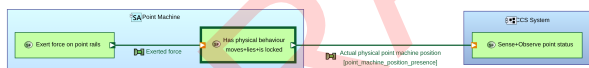



## 3.2.2 Actor functions

### 3.2.2.1 Point Machine

#### 3.2.2.1.1 Functional description

##### Has physical behaviour moves+lies+is locked















This passive function represents the mechanical blades position of the Point which can be sensed and estimated to an abstract Point Machine position.

ID	SPMS-2132
Context Diagram	 <pre> graph LR     subgraph SA_Point_Machine [SA Point Machine]         direction TB         E1((Event force on point rails))         E2((Exerted force))         E3((The physical behaviour moves+lies+is locked))         E4((Actual physical point machine position point_machine_position_presence))     end     E1 --&gt; E2     E2 --&gt; E3     E3 --&gt; E4     E4 --&gt; CCS[CCS System]     CCS --&gt; E5((Sense+Observe point status))           </pre>
Input exchanges	<ul style="list-style-type: none"> <li> SPMS-4799 - Exerted force</li> </ul>
Output exchanges	<ul style="list-style-type: none"> <li> SPMS-2237 - Actual physical point machine position             <ul style="list-style-type: none"> <li>Exchange items:</li> <li> SPMS-2381 - point_machine_position_presence</li> </ul> </li> </ul>

#### 3.2.2.1.2 Failure Modes and Effects Analysis

##### Early actual physical point machine position from Point Machine













ID	SPRM-1293
Failure Mode (Keyword)	Commission
Failure Description	Point Machine sends point machine position too early.

Effect on Linked Functions Systems	CCS-System determine the incorrect point position state, e.g. CCS assumes that the point is already in the required position for the operational movement when it is not. CCS-System is operating with an incorrect point position which can lead to and issues a movement permission over unsecured track path.
Effect on Railway System	Potentially unsafe railway operation.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2132 - Has physical behaviour moves+lies+is locked</p> <p>relates to :  SPMS-2237 - Actual physical point machine position</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5815 - Actual physical point machine position</p> <p>has parent :  SPRM-2063 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1699 - Point is free of occupancy</p>














### Early actual physical point machine position from Point Machine

ID	SPRM-1943
Failure Mode (Keyword)	Commission
Failure Description	Point Machine sends point machine position too early.
Effect on Linked Functions Systems	CCS-System determine the incorrect point position state, e.g. CCS assumes that the point is already in the required position for the operational movement when it is not. CCS-System is operating with an incorrect point position and commands point machine to move when it is not necessary (point already in required position).
Effect on Railway System	Potential overheating of the Point Machine.
Risk Comment	-
















Linked Work Items	<p>relates to :  SPMS-2132 - Has physical behaviour moves+lies+is locked</p> <p>relates to :  SPMS-2237 - Actual physical point machine position</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>assesses :  SPRM-301 - [B.3.1.0] Other failure of the track</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5815 - Actual physical point machine position</p> <p>has parent :  SPRM-2063 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1700 - Point machine position is equal to requested point machine position.</p>
-------------------	--

### Incorrect actual physical point machine position from Point Machine














ID	SPRM-1294
Failure Mode (Keyword)	Incorrect
Failure Description	Point Machine sends incorrect point machine position.
Effect on Linked Functions Systems	<p>CCS-System determine the incorrect point position state, e.g. CCS assumes that the point is already in the required position for the operational movement when it is not.</p> <p>CCS-System is operating with an incorrect point position which can lead to:</p> <p>a) CCS-System issuing a movement permission over unsecured track path</p> <p>b) CCS-System indications of point position to Signaller and TMS are wrong</p>
Effect on Railway System	Potentially unsafe railway operation.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2132 - Has physical behaviour moves+lies+is locked</p> <p>relates to :  SPMS-2237 - Actual physical point machine position</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5815 - Actual physical point machine position</p> <p>has parent :  SPRM-2063 - 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-1700 - Point machine position is equal to requested point machine position.</p>

### Incorrect actual physical point machine position from Point Machine













ID	SPRM-1945
Failure Mode (Keyword)	Incorrect
Failure Description	Point Machine sends incorrect point machine position.
Effect on Linked Functions Systems	CCS-System determine the incorrect point position state, e.g. CCS assumes that the point is already in the required position for the operational movement when it is not. CCS-System is operating with an incorrect point position and commands point machine to move when it is not necessary (point already in required position).
Effect on Railway System	Potential overheating of the Point Machine.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2132 - Has physical behaviour moves+lies+is locked</p> <p>relates to :  SPMS-2237 - Actual physical point machine position</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>assesses :  SPRM-301 - [B.3.1.0] Other failure of the track</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5815 - Actual physical point machine position</p> <p>has parent :  SPRM-2063 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1700 - Point machine position is equal to requested point machine position.</p>

### Late actual physical point machine position from Point Machine

ID	SPRM-1295
Failure Mode (Keyword)	Omission
Failure Description	Point Machine sends point machine position too late or not at all.
Effect on Linked Functions Systems	CCS-System operates with an outdated points position state maintaining the last position received. CCS-System is operating with an incorrect point position which can lead to: a). CCS-System issuing a movement permission over unsecured track path b) CCS-System indications of point position to Signaller and TMS are wrong
Effect on Railway System	Potentially unsafe railway operation.
Risk Comment	-

Linked Work Items	<p>relates to :  SPMS-2132 - Has physical behaviour moves+lies+is locked</p> <p>relates to :  SPMS-2237 - Actual physical point machine position</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5815 - Actual physical point machine position</p> <p>has parent :  SPRM-2063 - 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-1700 - Point machine position is equal to requested point machine position.</p>
-------------------	--

### Late actual physical point machine position from Point Machine

ID	SPRM-1944
Failure Mode (Keyword)	Omission
Failure Description	Point Machine sends point machine position too late or not at all.
Effect on Linked Functions Systems	CCS-System determine the incorrect point position state, e.g. CCS assumes that the point is already in the required position for the operational movement when it is not. CCS-System is operating with an incorrect point position and commands point machine to move when it is not necessary (point already in required position).
Effect on Railway System	Potential overheating of the Point Machine.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2132 - Has physical behaviour moves+lies+is locked</p> <p>relates to :  SPMS-2237 - Actual physical point machine position</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>assesses :  SPRM-301 - [B.3.1.0] Other failure of the track</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5815 - Actual physical point machine position</p> <p>has parent :  SPRM-2063 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1700 - Point machine position is equal to requested point machine position.</p>

### 3.2.2.1.3 Constraints

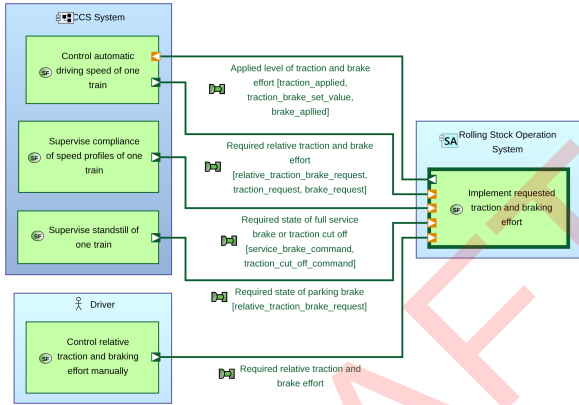














No constraints allocated to this function.

### 3.2.2.2 Rolling Stock Operation System

#### 3.2.2.2.1 Functional description









##### Implement requested traction and braking effort

This function controls the vehicle specific traction and braking so that the traction and braking systems create a traction and/or braking force respectively, which corresponds with the required relative traction and brake effort.

ID	SPMS-2146
Context Diagram	
Input exchanges	<ul style="list-style-type: none"> <li>•  SPMS-2211 - Required state of full service brake or traction cut off <ul style="list-style-type: none"> <li>◦ Exchange items: <ul style="list-style-type: none"> <li>◦  SPMS-2380 - service_brake_command</li> <li>◦  SPMS-2382 - traction_cut_off_command</li> </ul> </li> </ul> </li> <li>•  SPMS-2212 - Required state of parking brake <ul style="list-style-type: none"> <li>◦ Exchange items: <ul style="list-style-type: none"> <li>◦  SPMS-2393 - relative_traction_brake_request</li> </ul> </li> </ul> </li> <li>•  SPMS-2365 - Required relative traction and brake effort <ul style="list-style-type: none"> <li>◦ Exchange items: <ul style="list-style-type: none"> <li>◦  SPMS-2393 - relative_traction_brake_request</li> <li>◦  SPMS-2396 - traction_request</li> <li>◦  SPMS-5481 - brake_request</li> </ul> </li> </ul> </li> <li>•  SPMS-2366 - Required relative traction and brake effort manually</li> </ul>
Output exchanges	<ul style="list-style-type: none"> <li>•  SPMS-2245 - Applied level of traction and brake effort <ul style="list-style-type: none"> <li>◦ Exchange items: <ul style="list-style-type: none"> <li>◦  SPMS-2394 - traction_applied</li> <li>◦  SPMS-2395 - traction_brake_set_value</li> <li>◦  SPMS-5482 - brake_applied</li> </ul> </li> </ul> </li> </ul>









### 3.2.2.2.2 Failure Modes and Effects Analysis

#### Early applied level of traction and brake effort from Rolling Stock Operation System









ID	SPRM-1276
Failure Mode (Keyword)	Commission
Failure Description	Rolling Stock Operation System sends information about applied level of traction or brake effort too early.
Effect on Linked Functions Systems	CCS-System is incorrectly informed about traction or brake effort of the Rolling Stock Operation System. CCS still sends the correct information about required traction or brake effort to the Rolling Stock Operation System because calculations of the required traction or braking effort done by CCS are not affected by this information from Rolling Stock Operational System.
Effect on Railway System	No hazardous effect on Railway System expected. CCS still controls speed of the train according to the MRSP (most restrictive speed profile).
Risk Comment	Calculations of the required traction or braking effort done by CCS are not affected by this information from Rolling Stock Operational System.
Linked Work Items	<p>relates to :  SPMS-2146 - Implement specific traction and braking effort</p> <p>relates to :  SPMS-2245 - Applied level of traction and brake effort</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5359 - Drive train automatically</p> <p>relates to :  SPMS-5444 - Drive train automatically</p> <p>relates to :  SPMS-3051 - Applied level of traction and brake effort</p> <p>has parent :  SPRM-2065 - Detailed Failure Modes and Effect Analysis</p>

#### Late applied level of traction and brake effort from Rolling Stock Operation System

ID	SPRM-1277
Failure Mode (Keyword)	Omission
Failure Description	Rolling Stock Operation System sends information about applied level of traction or brake effort too late.
Effect on Linked Functions Systems	CCS-System is incorrectly informed about traction or brake effort of the Rolling Stock Operation System. CCS still sends the correct information about required traction or brake effort to the Rolling Stock Operation System because calculations of the required traction or braking effort done by CCS are not affected by this information from Rolling Stock Operational System.
Effect on Railway System	No hazardous effect on Railway System expected. CCS still controls speed of the train according to the MRSP (most restrictive speed profile).
Risk Comment	Calculations of the required traction or braking effort done by CCS are not affected by this information from Rolling Stock Operational System.

Linked Work Items	relates to :  SPMS-2146 - Implement specific traction and braking effort relates to :  SPMS-2245 - Applied level of traction and brake effort assesses :  SPRM-516 - No safety hazard causes :  SPRM-517 - No accident relates to :  SPMS-5359 - Drive train automatically relates to :  SPMS-5444 - Drive train automatically relates to :  SPMS-3051 - Applied level of traction and brake effort has parent :  SPRM-2065 - Detailed Failure Modes and Effect Analysis
-------------------	---

### Incorrect applied level of traction and brake effort from Rolling Stock Operation System

ID	SPRM-1278
Failure Mode (Keyword)	Incorrect
Failure Description	Rolling Stock Operation System sends incorrect information about applied level of traction or brake effort.
Effect on Linked Functions Systems	CCS-System is incorrectly informed about traction or brake effort of the Rolling Stock Operation System. CCS still sends the correct information about required traction or brake effort to the Rolling Stock Operation System because calculations of the required traction or braking effort done by CCS are not affected by this information from Rolling Stock Operational System.
Effect on Railway System	No hazardous effect on Railway System expected. CCS still controls speed of the train according to the MRSP (most restrictive speed profile).
Risk Comment	Calculations of the required traction or braking effort done by CCS are not affected by this information from Rolling Stock Operational System.
Linked Work Items	relates to :  SPMS-2146 - Implement specific traction and braking effort relates to :  SPMS-2245 - Applied level of traction and brake effort assesses :  SPRM-516 - No safety hazard causes :  SPRM-517 - No accident relates to :  SPMS-5359 - Drive train automatically relates to :  SPMS-5444 - Drive train automatically relates to :  SPMS-3051 - Applied level of traction and brake effort has parent :  SPRM-2065 - Detailed Failure Modes and Effect Analysis


### 3.2.2.2.3 Constraints

No constraints allocated to this function.

### 3.2.2.3 Rolling Stock Reference Point

#### 3.2.2.3.1 Functional description


##### Has position and direction in relation to track coordinates

This function is allocated to  SPMS-2091 - Rolling Stock Reference Point.

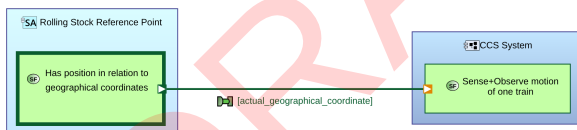












This passive function represents the position and direction in relation to track coordinates of one rolling stock reference point.

ID	SPMS-2138		
Context Diagram	<div><div><div>SA Rolling Stock Reference Point</div><div><div>Has position and direction in relation to track coordinates</div></div></div><div><div>CCS System</div><div><div>Sense+Observe motion of one train</div></div></div><div>[actual_position_and_direction]</div></div> <p>Figure 6 Context Diagram of Has position and direction in relation to track coordinates</p>		
Input exchanges	No inputs defined for this function.		
Output exchanges	<div><div>Output exchanges</div><div><div>SPMS-2239 - Actual present position and direction</div><div><div>SPMS-6521 - actual_position_and_direction</div></div></div></div>	<div><div>Target function</div><div><div>SPMS-2192 - Sense+Observe motion of one train</div></div></div>	<div><div>Function allocated to</div><div><div>SPMS-2098 - CCS System</div></div></div>


### Has position in relation to geographical coordinates

This function is allocated to  SPMS-2091 - Rolling Stock Reference Point.

This passive function represents the position in relation to geographical coordinates of one rolling stock reference point.

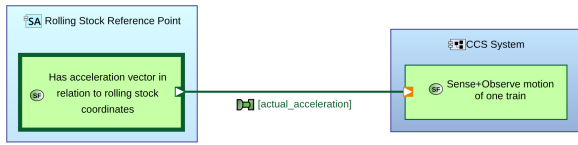




ID	SPMS-2135						
Context Diagram	<div></div> <p>Figure 7 Context Diagram of Has position in relation to geographical coordinates</p>						
Input exchanges	No inputs defined for this function.						
Output exchanges	<table><tr><th>Output exchanges</th><th>Target function</th><th>Function allocated to</th></tr><tr><td><div> SPMS-2238 - Actual present geographical coordinate<ul style="list-style-type: none"><li> SPMS-6520 - actual_geographical_coordinate</li></ul></div></td><td><div> SPMS-2192 - Sense+Observe motion of one train</div></td><td><div> SPMS-2098 - CCS System</div></td></tr></table>	Output exchanges	Target function	Function allocated to	<div> SPMS-2238 - Actual present geographical coordinate<ul style="list-style-type: none"><li> SPMS-6520 - actual_geographical_coordinate</li></ul></div>	<div> SPMS-2192 - Sense+Observe motion of one train</div>	<div> SPMS-2098 - CCS System</div>
Output exchanges	Target function	Function allocated to					
<div> SPMS-2238 - Actual present geographical coordinate<ul style="list-style-type: none"><li> SPMS-6520 - actual_geographical_coordinate</li></ul></div>	<div> SPMS-2192 - Sense+Observe motion of one train</div>	<div> SPMS-2098 - CCS System</div>					

### Has acceleration vector in relation to rolling stock coordinates


This function is allocated to  SPMS-2091 - Rolling Stock Reference Point.

This passive function represents the actual acceleration in relation to rolling stock coordinates of one rolling stock reference point.

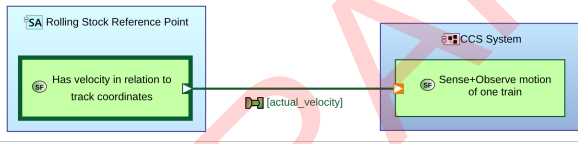




ID	SPMS-2127
----	-----------

Context Diagram	 <p>Figure 8 Context Diagram of Has acceleration vector in relation to rolling stock coordinates</p>		
Input exchanges	No inputs defined for this function.		
Output exchanges	<b>Output exchanges</b>  SPMS-2234 - Actual acceleration <ul style="list-style-type: none"> <li> SPMS-6519 - actual_acceleration</li> </ul>	<b>Target function</b>  SPMS-2192 - Sense+Observe motion of one train	<b>Function allocated to</b>  SPMS-2098 - CCS System

#### Has velocity in relation to track coordinates

This function is allocated to  SPMS-2091 - Rolling Stock Reference Point.

This passive function represents the actual velocity of one rolling stock reference point.







ID	SPMS-2140		
Context Diagram	 <p>Figure 9 Context Diagram of Has velocity in relation to track coordinates</p>		
Input exchanges	No inputs defined for this function.		
Output exchanges	<b>Output exchanges</b>  SPMS-2243 - Actual velocity <ul style="list-style-type: none"> <li> SPMS-6522 - actual_velocity</li> </ul>	<b>Target function</b>  SPMS-2192 - Sense+Observe motion of one train	<b>Function allocated to</b>  SPMS-2098 - CCS System

#### 3.2.2.3.2 Failure Modes and Effects Analysis











##### (N/A) Early acceleration information from Rolling Stock Reference Point

ID	SPRM-1173
Failure Mode (Keyword)	Commission













Failure Description	NA
Effect on Linked Functions Systems	--
Effect on Railway System	--
Risk Comment	Note: Failure mode "comission" seems to be n. a. for this information. Information cannot be send before detected, it is simply not available.
Linked Work Items	<p>relates to :  SPMS-2127 - Has acceleration vector in relation to rolling stock coordinates</p> <p>relates to :  SPMS-2234 - Actual acceleration</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-2989 - Actual acceleration</p> <p>has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis</p>

### Incorrect acceleration information from Rolling Stock Reference Point
















ID	SPRM-1174
Failure Mode (Keyword)	Incorrect
Failure Description	Rolling Stock Reference Point sends incorrect acceleration information.
Effect on Linked Functions Systems	<p>CCS System operates with incorrect acceleration information of the train and this results in a wrong estimated train motion state.</p> <p>The wrong estimated train motion state is transmitted to the TMS for further calculations for the operational traffic plan.</p> <p>Requests for operational movements and the supervision of the train motion are handled by CCS System based on wrong internal train motion state.</p>
Effect on Railway System	Possible unsafe train movement based on wrong permission to drive and failed train supervision.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2127 - Has acceleration vector in relation to rolling stock coordinates</p> <p>relates to :  SPMS-2234 - Actual acceleration</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>assesses :  SPRM-278 - [B.2.0.1] Wrong side signalling (on-board) failure</p> <p>relates to :  SPMS-2989 - Actual acceleration</p> <p>has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1736 - Integrity of received information for determining train motion state</p> <p>_ is mitigated by : {c} SPRM-1738 - Integrity of provided information for determining train motion state</p>

### Late acceleration information from Rolling Stock Reference Point

ID	SPRM-1175
Failure Mode (Keyword)	Omission
Failure Description	Rolling Stock Reference Point sends acceleration information too late or not at all.
Effect on Linked Functions Systems	CCS System operates with outdated acceleration information of the train and this results in a wrong estimated train motion state. The wrong estimated train motion state is transmitted to the TMS for further calculations for the operational traffic plan. Requests for operational movements and the supervision of the train motion are handled by CCS System based on wrong internal train motion state.
Effect on Railway System	Possible unsafe train movement based on wrong permission to drive and failed train supervision.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2127 - Has acceleration vector in relation to rolling stock coordinates</p> <p>relates to :  SPMS-2234 - Actual acceleration</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>assesses :  SPRM-278 - [B.2.0.1] Wrong side signalling (on-board) failure</p> <p>relates to :  SPMS-2989 - Actual acceleration</p> <p>has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1736 - Integrity of received information for determining train motion state</p> <p>_ is mitigated by : {c} SPRM-1738 - Integrity of provided information for determining train motion state</p>




















#### (N/A) Early geographical coordinates from Rolling Stock Reference Point

ID	SPRM-1176
Failure Mode (Keyword)	Commission
Failure Description	NA
Effect on Linked Functions Systems	--
Effect on Railway System	--
Risk Comment	Note 1: Failure mode "comission" seems to be n. a. for this information. Information cannot be send before detected, it is simple not available.











Linked Work Items	<p>relates to :  SPMS-2135 - Has position in relation to geographical coordinates</p> <p>relates to :  SPMS-2238 - Actual present geographical coordinate</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>relates to :  SPMS-3004 - Actual present geographical coordinate</p> <p>has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis</p>
-------------------	--

### Incorrect geographical coordinates from Rolling Stock Reference Point

ID	SPRM-1177
Failure Mode (Keyword)	Incorrect
Failure Description	Rolling Stock Reference Point sends incorrect geographical coordinates.
Effect on Linked Functions Systems	<p>CCS System operates with incorrect geographical coordinates of the train and this results in an wrong estimated train motion state.</p> <p>The wrong estimated train motion state is used CCS-internally to localise the train by a number of internal functions. If CCS-System operates with a wrong estimated train motion state, there are several effects for CCS-System:</p> <p>a) Authorising a train movement is based on wrong train positions - this leads possibly to a track path not being secured/reserved for a train movement (e.g. movement is granted to wrongly located train or track path of train is released before it has been passed).</p> <p>b) Incorrect train motion state is transmitted to the TMS for further calculations for the operational traffic plan which can result in operational movements not being conflict-free or optimised.</p> <p>Requests for operational movements and the supervision of the train motion are handled by CCS System based on wrong internal train motion state.</p>
Effect on Railway System	Possible unsafe train movement based on wrong permission to drive and failed train supervision.
Risk Comment	-




















Linked Work Items	<p>relates to :  SPMS-2135 - Has position in relation to geographical coordinates</p> <p>relates to :  SPMS-2238 - Actual present geographical coordinate</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>assesses :  SPRM-278 - [B.2.0.1] Wrong side signalling (on-board) failure</p> <p>relates to :  SPMS-3004 - Actual present geographical coordinate</p> <p>has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1736 - Integrity of received information for determining train motion state</p> <p>_ is mitigated by : {c} SPRM-1738 - Integrity of provided information for determining train motion state</p> <p>_ is mitigated by : {c} SPRM-1739 - Consistency between information for determining train motion state</p>
-------------------	---

### Late geographical coordinates from Rolling Stock Reference Point

ID	SPRM-1436
Failure Mode (Keyword)	Omission
Failure Description	Rolling Stock Reference Point sends geographical coordinates too late or not at all.
Effect on Linked Functions Systems	CCS System operates with outdated geographical coordinates of the train and this results in an wrong estimated train motion state. In this case of outdated train localisation information releasing the track path would happen later or not at all resulting in a track path unnecessarily staying reserved for the train movement and a loss of capacity for the railway operation.
Effect on Railway System	Disturbed operation (PRAM issue).
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2135 - Has position in relation to geographical coordinates</p> <p>relates to :  SPMS-2238 - Actual present geographical coordinate</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-3004 - Actual present geographical coordinate</p> <p>has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis</p>
















### Late geographical coordinates from Rolling Stock Reference Point

ID	SPRM-1178
Failure Mode (Keyword)	Omission
Failure Description	Rolling Stock Reference Point sends geographical coordinates too late or not at all.
Effect on Linked Functions Systems	<p>CCS System operates with outdated geographical coordinates of the train and this results in an wrong estimated train motion state.</p> <p>The outdated estimated train motion state is used CCS-internally to localise the train by a number of internal functions. If CCS-System operates with a wrong estimated train motion state, there are several effects for CCS-System:</p> <p>a) Authorising a train movement is based on wrong train positions - this leads possibly to a track path not being secured/reserved for a train movement (e.g. movement is granted to wrongly located train or unplanned entering of an occupied track path).</p> <p>b) The outdated estimated train motion state is transmitted to the TMS for further calculations for the operational traffic plan which can result in operational movements not being conflict-free or optimised.</p> <p>Requests for operational movements and the supervision of the train motion are handled by CCS System based on wrong internal train motion state.</p>
Effect on Railway System	Possible unsafe train movement based on wrong permission to drive and failed train supervision.
Risk Comment	-

Linked Work Items	<p>relates to :  SPMS-2135 - Has position in relation to geographical coordinates</p> <p>relates to :  SPMS-2238 - Actual present geographical coordinate</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>assesses :  SPRM-278 - [B.2.0.1] Wrong side signalling (on-board) failure</p> <p>relates to :  SPMS-3004 - Actual present geographical coordinate</p> <p>has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1736 - Integrity of received information for determining train motion state</p> <p>_ is mitigated by : {c} SPRM-1738 - Integrity of provided information for determining train motion state</p> <p>_ is mitigated by : {c} SPRM-1739 - Consistency between information for determining train motion state</p>
-------------------	---

#### (N/A) Early position and direction from Rolling Stock Reference Point























ID	SPRM-1179
Failure Mode (Keyword)	Commission
Failure Description	NA
Effect on Linked Functions Systems	--
Effect on Railway System	--
Risk Comment	Note 1: Failure mode "comission" seems to be n. a. for this information. Information cannot be send before detected, it is simple not available.

Linked Work Items	<p>relates to :  SPMS-2138 - Has position and direction in relation to track coordinates</p> <p>relates to :  SPMS-2239 - Actual present position and direction</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>relates to :  SPMS-3007 - Actual present position and direction in track coordinates</p> <p>has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis</p>
-------------------	--

### Incorrect position and direction from Rolling Stock Reference Point

ID	SPRM-1180
Failure Mode (Keyword)	Incorrect
Failure Description	Rolling Stock Reference Point sends incorrect position and direction in track coordinates.
Effect on Linked Functions Systems	<p>CCS System operates with incorrect position and direction in track coordinates of the train and this results in an wrong estimated train motion state. The wrong estimated train motion state is used CCS-internally to localise the train by a number of internal functions. If CCS-System operates with a wrong estimated train motion state, there are several effects for CCS-System:</p> <p>a) Authorising a train movement is based on wrong train positions - this leads possibly to a track path not being secured/reserved for a train movement (e.g. movement is granted to wrongly located train or track path of train is released before it has been passed).</p> <p>b) Incorrect train motion state is transmitted to the TMS for further calculations for the operational traffic plan which can result in operational movements not being conflict-free or optimised.</p> <p>Requests for operational movements and the supervision of the train motion are handled by CCS System based on wrong internal train motion state.</p>
Effect on Railway System	Possible unsafe train movement based on wrong permission to drive and failed train supervision.
Risk Comment	-






















Linked Work Items	<p>relates to :  SPMS-2138 - Has position and direction in relation to track coordinates</p> <p>relates to :  SPMS-2239 - Actual present position and direction</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>causes :  SPRM-82 - [A3.1] Level Crossing Accident involving a train</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>assesses :  SPRM-278 - [B.2.0.1] Wrong side signalling (on-board) failure</p> <p>relates to :  SPMS-3007 - Actual present position and direction in track coordinates</p> <p>has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1736 - Integrity of received information for determining train motion state</p> <p>_ is mitigated by :  SPRM-1738 - Integrity of provided information for determining train motion state</p>
-------------------	---











### Late position and direction from Rolling Stock Reference Point

ID	SPRM-1181
Failure Mode (Keyword)	Omission
Failure Description	Rolling Stock Reference Point sends position and direction in track coordinates too late or not at all.
Effect on Linked Functions Systems	<p>CCS System operates with outdated position and direction in track coordinates of the train and this results in an wrong estimated train motion state. The outdated estimated train motion state is used CCS-internally to localise the train by a number of internal functions. If CCS-System operates with a wrong estimated train motion state, there are several effects for CCS-System:</p> <p>a) Authorising a train movement is based on wrong train positions - this leads possibly to a track path not being secured/reserved for a train movement (e.g. movement is granted to wrongly located train or unplanned entering of an occupied track path).</p> <p>b) The outdated estimated train motion state is transmitted to the TMS for further calculations for the operational traffic plan which can result in operational movements not being conflict-free or optimised.</p> <p>Requests for operational movements and the supervision of the train motion are handled by CCS System based on wrong internal train motion state.</p>
Effect on Railway System	Possible unsafe train movement based on wrong permission to drive and failed train supervision.
Risk Comment	-









Linked Work Items	<p>relates to :  SPMS-2138 - Has position and direction in relation to track coordinates</p> <p>relates to :  SPMS-2239 - Actual present position and direction</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>causes :  SPRM-82 - [A3.1] Level Crossing Accident involving a train</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-3007 - Actual present position and direction in track coordinates</p> <p>has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1736 - Integrity of received information for determining train motion state</p> <p>_ is mitigated by :  SPRM-1738 - Integrity of provided information for determining train motion state</p>
-------------------	--














### Late position and direction from Rolling Stock Reference Point

ID	SPRM-1437
Failure Mode (Keyword)	Omission
Failure Description	Rolling Stock Reference Point sends position and direction in track coordinates too late or not at all.
Effect on Linked Functions Systems	CCS System operates with outdated position and direction in track coordinates of the train and this results in an wrong estimated train motion state. In this case of outdated train localisation information releasing the track path would happen later or not at all resulting in a track path unnecessarily staying reserved for the train movement and a loss of capacity for the railway operation.
Effect on Railway System	Disturbed operation (PRAM issue).
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2138 - Has position and direction in relation to track coordinates</p> <p>relates to :  SPMS-2239 - Actual present position and direction</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-3007 - Actual present position and direction in track coordinates</p> <p>has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis</p>

### (N/A) Early train speed from Rolling Stock Reference Point














ID	SPRM-1182
Failure Mode (Keyword)	Commission
Failure Description	NA
Effect on Linked Functions Systems	--
Effect on Railway System	--
Risk Comment	Note 1: Failure mode "comission" seems to be n. a. for this information. Information cannot be send before detected, it is simple not available.
Linked Work Items	<p>relates to :  SPMS-2140 - Has velocity in relation to track coordinates</p> <p>relates to :  SPMS-2243 - Actual velocity</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-3013 - Actual velocity</p> <p>has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis</p>

### Incorrect train speed from Rolling Stock Reference Point

ID	SPRM-1183
Failure Mode (Keyword)	Incorrect
Failure Description	Rolling Stock Reference Point sends incorrect train speed.
Effect on Linked Functions Systems	<p>CCS System operates with incorrect train speed and this results in an wrong estimated train motion state. The wrong estimated train motion state is transmitted to the TMS for further calculations for the operational traffic plan. Requests for operational movements and the supervision of the train motion are handled by CCS System based on wrong internal train motion state.</p> <p>The wrong train speed is transmitted to the train driver for controlling the traction and braking effort manually (with wrong input).</p>
Effect on Railway System	Possible unsafe train movement based on wrong permission to drive and failed train supervision.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2140 - Has velocity in relation to track coordinates  relates to :  SPMS-2243 - Actual velocity  relates to :  SPMS-4329 - Localise train on railway infrastructure  relates to :  SPMS-4438 - Localise train on railway infrastructure  assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure  assesses :  SPRM-389 - KERNEL-9  assesses :  SPRM-278 - [B.2.0.1] Wrong side signalling (on-board) failure  causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle  causes :  SPRM-78 - [A2.1] Derailment of train  relates to :  SPMS-3013 - Actual velocity  has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis  _ is mitigated by :  SPRM-1736 - Integrity of received information for determining train motion state  _ is mitigated by :  SPRM-1738 - Integrity of provided information for determining train motion state</p>

### Late train speed from Rolling Stock Reference Point

ID	SPRM-1184
Failure Mode (Keyword)	Omission
Failure Description	Rolling Stock Reference Point sends train speed too late or not at all.
Effect on Linked Functions Systems	<p>CCS System operates with outdated train speed and this results in an wrong estimated train motion state. The wrong estimated train motion state is transmitted to the TMS for further calculations for the operational traffic plan. Requests for operational movements and the supervision of the train motion are handled by CCS System based on wrong internal train motion state.</p> <p>The wrong train speed is transmitted to the train driver for controlling the traction and braking effort manually (with wrong input).</p>

Effect on Railway System	Possible unsafe train movement based on wrong permission to drive and failed train supervision.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2140 - Has velocity in relation to track coordinates</p> <p>relates to :  SPMS-2243 - Actual velocity</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>assesses :  SPRM-389 - KERNEL-9</p> <p>assesses :  SPRM-278 - [B.2.0.1] Wrong side signalling (on-board) failure</p> <p>causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>relates to :  SPMS-3013 - Actual velocity</p> <p>has parent :  SPRM-2069 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1736 - Integrity of received information for determining train motion state</p> <p>_ is mitigated by :  SPRM-1738 - Integrity of provided information for determining train motion state</p>


### 3.2.2.3.3 Constraints

No constraints allocated to this function.

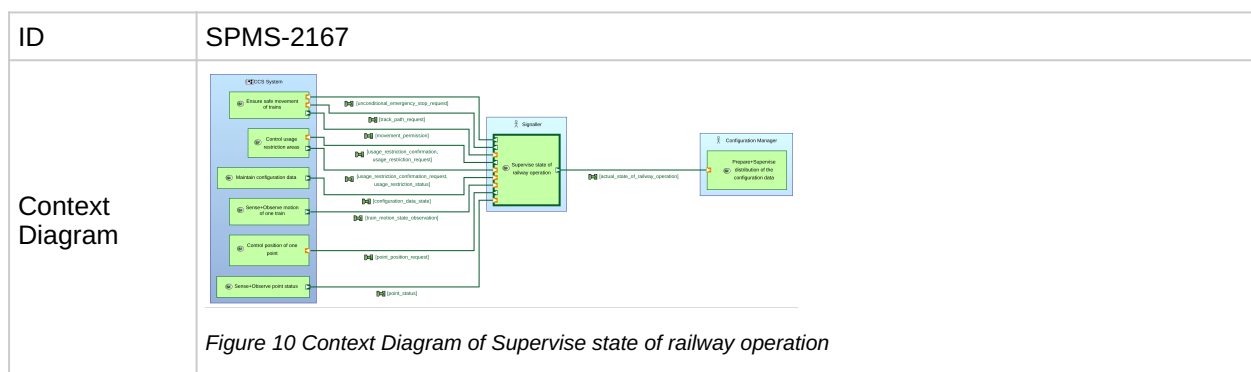
### 3.2.2.4 Signaller






















#### 3.2.2.4.1 Functional description






















#### Supervise state of railway operation

This function is allocated to  SPMS-2090 - Signaller.

This function performed by the Signaller supervises the state of railway operation and intervenes when necessary (e.g. point is indicated in different state than expected). Furthermore, it confirms (and adapt if necessary) the activation or deactivation of usage restrictions for supervised trains.














Input exchanges	Input exchanges	Source function	Function allocated to
	 SPMS-2330 - Estimated motion state <ul style="list-style-type: none"> <li> SPMS-2392 - train_motion_state_observation</li> </ul>	 SPMS-2192 - Sense+Observe motion of one train	 SPMS-2098 - CCS System
	 SPMS-2219 - Usage restriction state <ul style="list-style-type: none"> <li> SPMS-4827 - usage_restriction_confirmation_request</li> <li> SPMS-2398 - usage_restriction_status</li> </ul>	 SPMS-2159 - Control usage restriction areas	 SPMS-2098 - CCS System
	 SPMS-2312 - Observed point status <ul style="list-style-type: none"> <li> SPMS-5288 - point_status</li> </ul>	 SPMS-2108 - Sense+Observe point status	 SPMS-2098 - CCS System
	 SPMS-6037 - Actual state of configuration data <ul style="list-style-type: none"> <li> SPMS-6466 - configuration_data_state</li> </ul>	 SPMS-2182 - Maintain configuration data	 SPMS-2098 - CCS System
	 SPMS-7230 - Authorised distance and speed restriction <ul style="list-style-type: none"> <li> SPMS-2372 - movement_permission</li> </ul>	 SPMS-2137 - Ensure safe movement of trains	 SPMS-2098 - CCS System

Output exchanges	Output exchanges	Target function	Function allocated to
	 SPMS-2347 - Requested track path <ul style="list-style-type: none"> <li> SPMS-2418 - track_path_request</li> </ul>	 SPMS-2137 - Ensure safe movement of trains	 SPMS-2098 - CCS System
	 SPMS-4628 - Requested point position <ul style="list-style-type: none"> <li> SPMS-2386 - point_position_request</li> </ul>	 SPMS-2190 - Control position of one point	 SPMS-2098 - CCS System
	 SPMS-4824 - Provided usage restriction state <ul style="list-style-type: none"> <li> SPMS-4826 - usage_restriction_confirmation</li> <li> SPMS-2407 - usage_restriction_request</li> </ul>	 SPMS-2159 - Control usage restriction areas	 SPMS-2098 - CCS System
	 SPMS-6039 - Actual state of railway operation <ul style="list-style-type: none"> <li> SPMS-6772 - actual_state_of_railway_operation</li> </ul>	 SPMS-2129 - Prepare+Supervise distribution of the configuration data	 SPMS-2103 - Configuration
	 SPMS-7094 - Requested emergency stop <ul style="list-style-type: none"> <li> SPMS-7137 - unconditional_emergency_stop_request</li> </ul>	 SPMS-2137 - Ensure safe movement of trains	 SPMS-2098 - CCS System










### 3.2.2.4.2 Failure Modes and Effects Analysis

#### Early requested track path from Signaller

ID	SPRM-1049
Failure Mode (Keyword)	Commission
Failure Description	Signaller sends requested track path too early.
Effect on Linked Functions Systems	The speed-and-distance-limiting speed profile over distance for the train is calculated (e.g. with a new planned stop closer or further away from train) earlier than necessary and might be executed earlier than operationally necessary. Resources of CCS-System are blocked earlier than necessary to determine the reservation/shortening of the requested track path.
Effect on Railway System	Disturbed operation.
Risk Comment	PRAM consideration: CCS system shall send the cause for rejecting an operational movement to TMS.










Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-2347 - Requested track path</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-3123 - Requested track path</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p>
-------------------	--

### Late requested track path from Signaller (1)

ID	SPRM-1051
Failure Mode (Keyword)	Omission
Failure Description	Signaller sends requested track path too late or not at all.
Effect on Linked Functions Systems	<p>The speed-and-distance-limiting speed profile over distance for the train is recalculated with a new planned stop (the new planned stop is closer to the approaching train) too late.</p> <p>CCS-System is checking if all the conditions to shorten the movement permission are met (no brake intervention necessary because of e.g. active usage restrictions). If the conditions are not met, then the operational movement will not be executed.</p> <p>Failure of the CCS-System in performing these checks leads to the train needing to stop.</p>
Effect on Railway System	Disturbed operation (PRAM issue).
Risk Comment	<p>PRAM consideration:</p> <p>CCS shall reject the request to revoke a movement permission if the train does need to brake immediately.</p> <p>CCS system shall send the cause for rejecting an operational movement to Signaller.</p>
Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-2347 - Requested track path</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-3123 - Requested track path</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p>

### Late requested track path from Signaller (2)













ID	SPRM-1391
----	-----------

Failure Mode (Keyword)	Omission
Failure Description	Signaller sends requested track path too late or not at all.
Effect on Linked Functions Systems	The speed-and-distance-limiting speed profile over distance for the train is calculated too late or not at all. CCS-System is checking if all the conditions to authorise the movement permission are met (e.g. no conflicting occupancies, etc.). If the conditions are not met, then the requested track path will not be reserved. Failure of the CCS-System in performing these checks leads to a potentially unsafe railway operation.
Effect on Railway System	Potentially unsafe railway operation.
Risk Comment	PRAM consideration: CCS system shall send the cause for rejecting an operational movement to Signaller.
Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-2347 - Requested track path</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>assesses :  SPRM-110 - [B.1.1.1] Improper routing</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-3123 - Requested track path</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1443 - Requested track path is free of occupancies</p> <p>_ is mitigated by : {c} SPRM-1444 - Requested track path is distinct from other authorised track paths</p> <p>_ is mitigated by : {c} SPRM-1758 - Requested track path adheres to train-side restrictions</p>

### Incorrect requested track path from Signaller











ID	SPRM-1050
Failure Mode (Keyword)	Incorrect
Failure Description	Signaller sends incorrect requested track path.
Effect on Linked Functions Systems	<p>Incorrect parameters are used to calculate the speed-and-distance-limiting speed profile over distance for the train. This results in</p> <p>a) Speed profile calculated with incorrect stopping point (e.g. for shortening a stop outside of the current track path is sent), lower speed, etc. or for the wrong train</p> <p>b) Track path cannot be reserved for a train due to impossible parameters e.g. requested speed higher than allowed by track conditions/train category, movement over occupied track path, etc.</p> <p>c) shortening of track path would lead to an emergency brake on train (case is not safety critical).</p> <p>CCS-System is checking if all the conditions to grant/shorten the movement permission are met (no brake intervention necessary because of e.g. active usage restrictions). If the conditions are not met, then the operational movement will not be executed. Failure of the CCS-System in performing these checks leads to potentially unsafe railway operation.</p>
















Effect on Railway System	Potentially unsafe railway operation.
Risk Comment	PRAM consideration: CCS shall reject the request to revoke a movement permission if the train does need to brake immediately. CCS system shall send the cause for rejecting an operational movement to Signaller.
Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-2347 - Requested track path</p> <p>relates to :  SPMS-4334 - Shorten movement permission (Signaller request, accepted)</p> <p>relates to :  SPMS-4337 - Shorten movement permission (Signaller request, rejected)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>assesses :  SPRM-110 - [B.1.1.1] Improper routing</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-3123 - Requested track path</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1442 - Train adheres to infrastructure restrictions</p> <p>_ is mitigated by : {c} SPRM-1443 - Requested track path is free of occupancies</p> <p>_ is mitigated by : {c} SPRM-1444 - Requested track path is distinct from other authorised track paths</p> <p>_ is mitigated by : {c} SPRM-1758 - Requested track path adheres to train-side restrictions</p>

#### Early requested point position from Signaller

ID	SPRM-1298
Failure Mode (Keyword)	Commission
Failure Description	Signaller sends the request to change the point position too early to CCS System.
Effect on Linked Functions Systems	The target state of the point machine (e.g. left) is determined and commanded too early. CCS-System is checking if all the conditions to command the point machines are met (point not occupied or reserved for other operational movements). If the conditions are not met, then the operational movement will be rejected. Failure of the CCS-System in performing these checks leads to a potentially unsafe railway operation.
Effect on Railway System	Potentially unsafe railway operation.
Risk Comment	PRAM consideration: CCS-System shall send the reason for rejecting the requested point position to Signaller.










Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-4628 - Requested point position</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>assesses :  SPRM-1726 - [XYZ] Undue movement of a point</p> <p>relates to :  SPMS-5275 - Requested point position</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1699 - Point is free of occupancy</p>
-------------------	---

### Incorrect requested point position from Signaller (1)












ID	SPRM-1300
Failure Mode (Keyword)	Incorrect
Failure Description	Signaller sends incorrect request to change the point machine position.
Effect on Linked Functions Systems	The wrong target state of the point machine (e.g. right) is determined and commanded.
Effect on Railway System	CCS-System is checking if all the conditions to command the point machines are met (point not occupied or reserved for other operational movements). If the conditions are not met, then the request will not be executed. Failure of the CCS-System in performing these checks leads to a potentially unsafe railway operation.
Risk Comment	PRAM consideration: CCS-System shall send the reason for rejecting the requested point position to Signaller.
Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-4628 - Requested point position</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>causes :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>causes :  SPRM-115 - [X.1] Undue movement of a point nearby person</p> <p>causes :  SPRM-114 - [B.1.1.0] Other failure to operate the infrastructure</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>assesses :  SPRM-1726 - [XYZ] Undue movement of a point</p> <p>relates to :  SPMS-5275 - Requested point position</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1699 - Point is free of occupancy</p>

### Incorrect requested point position from Signaller (2)










ID	SPRM-1750
Failure Mode (Keyword)	Incorrect

Failure Description	Signaller sends incorrect request to change the point machine position.
Effect on Linked Functions Systems	The wrong target state of the point machine (e.g. right) is determined and commanded.
Effect on Railway System	The point machine is already in the target position, unnecessary command to point machine is sent. The point machine could overheat while trying to force the point into the target position which the point is already in.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-4628 - Requested point position</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>assesses :  SPRM-114 - [B.1.1.0] Other failure to operate the infrastructure</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5275 - Requested point position</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1700 - Point machine position is equal to requested point machine position.</p>










#### Late requested point position from Signaller

ID	SPRM-1299
Failure Mode (Keyword)	Omission
Failure Description	Signaller sends the request to change the point machine position to CCS System too late or not at all.
Effect on Linked Functions Systems	<p>The target state of the point machine (e.g. left) is determined and commanded too late. CCS-System is checking if all the conditions to command the point machines are met (point not occupied or reserved for other operational movements). If the conditions are not met, then the operational movement will be rejected.</p> <p>Failure of the CCS-System in performing these checks leads to a potentially unsafe railway operation.</p>
Effect on Railway System	Potentially unsafe railway operation.
Risk Comment	PRAM consideration: CCS-System shall send the reason for rejecting the requested point position to Signaller.
Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-4628 - Requested point position</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>assesses :  SPRM-1726 - [XYZ] Undue movement of a point</p> <p>relates to :  SPMS-5275 - Requested point position</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1699 - Point is free of occupancy</p>













#### Late requested point position from Signaller

ID	SPRM-1751
Failure Mode (Keyword)	Omission
Failure Description	Signaller sends the request to change the point machine position to CCS System too late or not at all.
Effect on Linked Functions Systems	Worst case: The target state of the point machine (e.g. left) is determined and commanded too late.
Effect on Railway System	The point machine is already in the target position, unnecessary command to point machine is sent. The point machine could overheat while trying to force the point into the target position which the point is already in.
Risk Comment	Not sending the command at all leads to an operational disturbance but no hazard.
Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-4628 - Requested point position</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>relates to :  SPMS-4769 - Set point position (Left to right, Signaller request)</p> <p>assesses :  SPRM-114 - [B.1.1.0] Other failure to operate the infrastructure</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-5275 - Requested point position</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1700 - Point machine position is equal to requested point machine position.</p>

### Early usage restriction activation confirmation from Signaller












ID	SPRM-958
Failure Mode (Keyword)	Commission
Failure Description	Signaller sends to CCS System confirmation of usage restriction activation too early.
Effect on Linked Functions Systems	Usage restriction will be activated too early.
Effect on Railway System	Disturbed operation. Train movement applying usage restriction unnecessarily.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-4824 - Provided usage restriction state</p> <p>relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4469 - Activate usage restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-3078 - Provided usage restriction state</p> <p>relates to :  SPMS-7226 - Activate usage restriction (Unplanned TSR)</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p>

### Incorrect usage restriction activation confirmation from Signaller










ID	SPRM-971
Failure Mode (Keyword)	Incorrect
Failure Description	Signaller sends to CCS System confirmation to activate the wrong usage restriction, or confirms wrong settings.
Effect on Linked Functions Systems	Incorrect usage restriction is activated.
Effect on Railway System	Possibly unsafe railway operation. Train movement according to usage restriction activated, which may not be the one planned by TMS (more permissive).
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-4824 - Provided usage restriction state</p> <p>relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4469 - Activate usage restriction</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>relates to :  SPMS-3078 - Provided usage restriction state</p> <p>relates to :  SPMS-7226 - Activate usage restriction (Unplanned TSR)</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1740 - Confirmed usage restriction matches requested usage restriction</p>

### Late usage restriction activation confirmation from Signaller

ID	SPRM-972
Failure Mode (Keyword)	Omission
Failure Description	Signaller sends to CCS System confirmation to activate the planned usage restriction too late or not at all.
Effect on Linked Functions Systems	Usage restriction not applied or applied later than planned.
Effect on Railway System	Possibly unsafe railway operation. Train movement not applying usage restriction when required, so it may move with more permissive information.
Risk Comment	-














Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-4824 - Provided usage restriction state</p> <p>relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4469 - Activate usage restriction</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>relates to :  SPMS-3078 - Provided usage restriction state</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1757 - Usage restriction is planned</p>
-------------------	---

### Late usage restriction activation confirmation from Signaller

ID	SPRM-2173
Failure Mode (Keyword)	Omission
Failure Description	Signaller sends to CCS System confirmation to activate the unplanned usage restriction too late or not at all.
Effect on Linked Functions Systems	Usage restriction not applied or applied later than expected.
Effect on Railway System	Possibly unsafe railway operation. Train movement not applying usage restriction when required, so it may move with more permissive information.
Risk Comment	Unplanned usage restriction as reaction from Signaller when unplanned event (e.g. Track workers on track, sudden changes in track condition etc) occurs.
Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-4824 - Provided usage restriction state</p> <p>relates to :  SPMS-7226 - Activate usage restriction (Unplanned TSR)</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-2241 - Usage restriction is requested</p>

### Early usage restriction deactivation confirmation from Signaller
















ID	SPRM-1478
Failure Mode (Keyword)	Commission
Failure Description	Signaller sends to CCS System confirmation of usage restriction deactivation too early.

Effect on Linked Functions Systems	The CCS System performs the deactivation of the usage restriction prematurely, i.e., before the required, planned, or requested time. If the confirmation is sent too early, CCS System may not yet reflect the expected operational state, potentially leading to inconsistencies in supervision. Similarly, if the request for deactivation is issued prematurely, it may not align with the actual operational context, requiring the Signaller to intervene, adapt, or reject the request accordingly.
Effect on Railway System	Possibly unsafe railway operation. Train is allowed to move over an area during maintenance works ongoing. Train overspeed over an area with restricted speed.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-4824 - Provided usage restriction state</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>assesses :  SPRM-519 - [xy] Field Force on track without trackside protection</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-3078 - Provided usage restriction state</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1702 - Usage restriction area is free of field force</p>










#### Incorrect usage restriction deactivation confirmation from Signaller

ID	SPRM-1479
Failure Mode (Keyword)	Incorrect
Failure Description	Signaller sends to CCS System confirmation to deactivate the wrong usage restriction.
Effect on Linked Functions Systems	CCS System deactivates wrong usage restriction. If the confirmation or the request is incorrectly executed, the resulting usage restriction state may not reflect the intended operational condition. 'Incorrect' may refer to a deviation in spatial extent or a misalignment in timing
Effect on Railway System	Possibly unsafe railway operation. Train is allowed to move over an area during maintenance works ongoing. Train overspeed over an area with restricted speed.
Risk Comment	-



Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-4824 - Provided usage restriction state</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>assesses :  SPRM-519 - [xy] Field Force on track without trackside protection</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-3078 - Provided usage restriction state</p> <p>relates to :  SPMS-7232 - Deactivate usage restriction (Unplanned TSR)</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1702 - Usage restriction area is free of field force</p> <p>_ is mitigated by :  SPRM-1740 - Confirmed usage restriction matches requested usage restriction</p>
-------------------	--

### Late usage restriction deactivation confirmation from Signaller

ID	SPRM-1480
Failure Mode (Keyword)	Omission
Failure Description	Signaller sends to CCS System confirmation to deactivate the usage restriction too late or not at all.
Effect on Linked Functions Systems	CCS System does not deactivate the usage restriction, the operational plan restriction continues to be active.
Effect on Railway System	Disturbed operation. Train has to keep on respecting usage restrictions.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2167 - Supervise state of railway operation</p> <p>relates to :  SPMS-4824 - Provided usage restriction state</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-3078 - Provided usage restriction state</p> <p>relates to :  SPMS-7232 - Deactivate usage restriction (Unplanned TSR)</p> <p>has parent :  SPRM-2057 - Detailed Failure Modes and Effect Analysis</p>

### 3.2.2.4.3 Constraints

#### Usage restriction activation matches operational plan.

to be checked indicated active usage restriction is according to the plan and to the data requested & confirmed.

- Usage restriction parameters



- activation time parameter

ID	SPRM-2056
----	-----------

#### Confirmation by Field Force is received

Signaller checks if the Field Force left the usage restriction area before deactivating it.

ID	SPRM-1779
----	-----------

#### Usage restriction is planned

Signaller is aware of the usage restrictions planned in his area and can identify potential failures when a usage restriction is not active when it should be.

ID	SPRM-1757
----	-----------

#### Usage restriction confirmation matches operational plan

Signaller checks if the usage restriction to be confirmed is planned. The usage restriction activation is not confirmed in case it does not match operational plan.

ID	SPRM-1746
----	-----------

#### Usage restriction area is free of field force

Field force / maintenance personal is outside of the usage restriction area.

ID	SPRM-1702
----	-----------

### 3.2.2.5 Traffic Management System

#### 3.2.2.5.1 Functional description

##### Calculate operational traffic plan

This function is allocated to  SPMS-2097 - Traffic Management System.

This function calculates the operational plans for all trains in the area of control before the train run starts and adapts it if needed during the train run. Thus, the calculation of the operational plans is based on the requirements from the capacity management, the actual operational situation (e.g. operational restrictions, delays of train runs). An Operational Movement is part of the Operational Plan, and consist of a timetable or train service specifying when and where particular events are to take place. Some of these events could be a commercial stop, a run through a certain location or even a change of train composition or a handover to another Traffic Management System. The most simple way of representation of such timetable is in a tabular form indicating station or run through location with arrival and departure time. More events could be associated at certain stations or locations depending on the Railway Undertaking needs. The Operational Movement is defined in such a way that the final user (passenger or freight company) knows if a particular timetable suits his needs.

ID	SPMS-2148
----	-----------

## Context Diagram

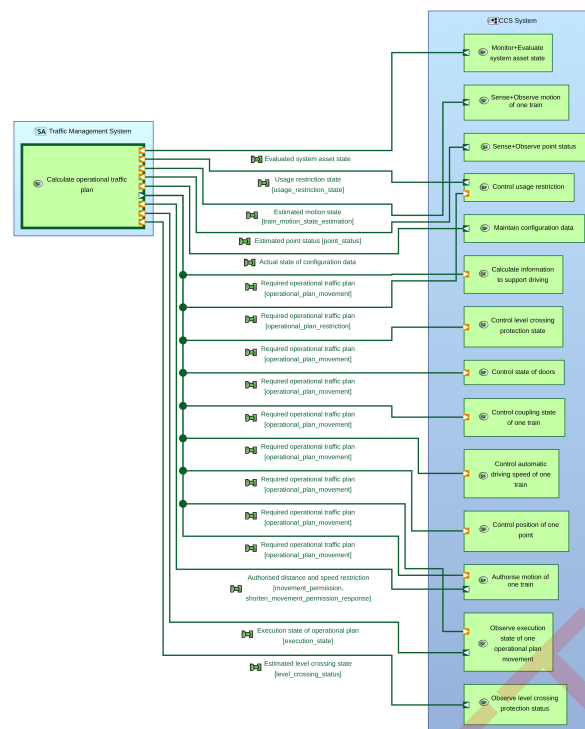



















Figure 11 Context Diagram of Calculate operational traffic plan

## Input exchanges












-  SPMS-2215 - Usage restriction state
  - Exchange items:
    -  SPMS-2398 - usage\_restriction\_status
-  SPMS-2249 - Authorised distance and speed restriction
  - Exchange items:
    -  SPMS-2372 - movement\_permission
    -  SPMS-5480 - shorten\_movement\_permission\_response
-  SPMS-2300 - Estimated motion state
  - Exchange items:
    -  SPMS-2392 - train\_motion\_state\_observation
-  SPMS-2320 - Execution state of operational plan
  - Exchange items:
    -  SPMS-2410
-  SPMS-4497 - Evaluated system asset state
-  SPMS-5329 - Observed point status
  - Exchange items:
    -  SPMS-5288 - point\_status
-  SPMS-5452 - Observed level crossing state
  - Exchange items:
    -  SPMS-5939 - level\_crossing\_status
-  SPMS-6038 - Actual state of configuration data

Output exchanges	<ul style="list-style-type: none"> <li>•  SPMS-2349 - Required operational traffic plan             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2370 - operational_plan_movement</li> </ul> </li> <li>•  SPMS-2350 - Required operational traffic plan             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2370 - operational_plan_movement</li> </ul> </li> <li>•  SPMS-2351 - Required operational traffic plan             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2370 - operational_plan_movement</li> </ul> </li> <li>•  SPMS-2354 - Required operational traffic plan             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2370 - operational_plan_movement</li> </ul> </li> <li>•  SPMS-2355 - Required operational traffic plan             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2370 - operational_plan_movement</li> </ul> </li> <li>•  SPMS-2356 - Required operational traffic plan             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2370 - operational_plan_movement</li> </ul> </li> <li>•  SPMS-2357 - Required operational traffic plan             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-5548 - operational_plan_restriction</li> </ul> </li> <li>•  SPMS-2359 - Required operational traffic plan             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2370 - operational_plan_movement</li> </ul> </li> <li>•  SPMS-2360 - Required operational traffic plan             <ul style="list-style-type: none"> <li>◦ Exchange items:</li> <li>◦  SPMS-2370 - operational_plan_movement</li> </ul> </li> </ul>
------------------	--

### 3.2.2.5.2 Failure Modes and Effects Analysis










#### Early required operational traffic plan from TMS

ID	SPRM-1043
Failure Mode (Keyword)	Commission
Failure Description	Traffic Management System sends the operational movement too early.










Effect on Linked Functions Systems	The speed-and-distance-limiting speed profile over distance for the train is calculated (e.g. with a new planned stop closer or further away from train) earlier than necessary and executed at the planned time. Resources of CCS-System are blocked earlier than necessary to determine the planned execution of the operational movement.
Effect on Railway System	-
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2148 - Calculate operational traffic plan</p> <p>relates to :  SPMS-2351 - Required operational traffic plan</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-4326 - 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-4336 - Shorten movement permission (Operational plan change, rejected)</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-3079 - Required operational traffic plan</p> <p>has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis</p>

#### Late required operational traffic plan from TMS (1)

ID	SPRM-1047
Failure Mode (Keyword)	Omission
Failure Description	Traffic Management System sends the operational movement too late or not at all.
Effect on Linked Functions Systems	The speed-and-distance-limiting speed profile over distance for the train is recalculated with a new planned stop (the new planned stop is closer to the approaching train) too late. CCS-System is checking if all the conditions to shorten the movement permission are met (no brake intervention necessary because of e.g. active usage restrictions). If the conditions are not met, then the operational movement will be rejected. Failure of the CCS-System in performing these checks leads to the train needing to stop.
Effect on Railway System	Disturbed operation (PRAM issue).
Risk Comment	<p>PRAM consideration: CCS shall reject the request to revoke a movement permission if the train does need to brake immediately. CCS system shall send the cause for rejecting an operational movement to TMS. Note: This enables TMS to adjust planning and send an executable revocation request.</p>













Linked Work Items	<p>relates to :  SPMS-2148 - Calculate operational traffic plan</p> <p>relates to :  SPMS-2351 - Required operational traffic plan</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-4336 - Shorten movement permission (Operational plan change, rejected)</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-3079 - Required operational traffic plan</p> <p>has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis</p>
-------------------	--

### Late required operational traffic plan from TMS (2)

ID	SPRM-1392
Failure Mode (Keyword)	Omission
Failure Description	Traffic Management System sends the operational movement too late or not at all.
Effect on Linked Functions Systems	<p>The speed-and-distance-limiting speed profile over distance for the train is calculated too late or not at all.</p> <p>CCS-System is checking if all the conditions to authorise the movement permission are met (e.g. no conflicting occupancies, etc.). If the conditions are not met, then the operational movement will be rejected.</p> <p>Failure of the CCS-System in performing these checks leads to a potentially unsafe railway operation.</p>
Effect on Railway System	Potentially unsafe railway operation.
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2148 - Calculate operational traffic plan</p> <p>relates to :  SPMS-2351 - Required operational traffic plan</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>assesses :  SPRM-110 - [B.1.1.1] Improper routing</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-3079 - Required operational traffic plan</p> <p>has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {C} SPRM-1442 - Train adheres to infrastructure restrictions</p> <p>_ is mitigated by : {C} SPRM-1443 - Requested track path is free of occupancies</p> <p>_ is mitigated by : {C} SPRM-1444 - Requested track path is distinct from other authorised track paths</p>









### Incorrect required operational traffic plan from TMS

ID	SPRM-1048
Failure Mode (Keyword)	Incorrect
Failure Description	Traffic Management System sends incorrect operational movement.









Effect on Linked Functions Systems	<p>The speed-and-distance-limiting speed profile over distance for the train is calculated with wrong position of the new planned stop (shorter distance or longer distance as intended) or with a wrong speed (higher or lower than safely executable) or it is recalculated for an incorrect train.</p> <p>CCS-System is checking if all the conditions to authorise the movement permission are met (no brake intervention necessary because of e.g. active usage restrictions, track paths not occupied or reserved, no conflicting occupancies, etc.). If the conditions are not met, then the operational movement will be rejected.</p> <p>Failure of the CCS-System in performing these checks leads to a potentially unsafe railway operation.</p>
Effect on Railway System	Potentially unsafe railway operation.
Risk Comment	<p>PRAM consideration:</p> <p>CCS shall reject the request to revoke a movement permission if the train does need to brake immediately.</p> <p>CCS system shall send the cause for rejecting an operational movement to TMS.</p> <p>Note: This enables TMS to adjust planning and send an executable revocation request.</p>
Linked Work Items	<p>relates to :  SPMS-2148 - Calculate operational traffic plan</p> <p>relates to :  SPMS-2351 - Required operational traffic plan</p> <p>relates to :  SPMS-4326 - Shorten movement permission (Operational plan change, accepted)</p> <p>relates to :  SPMS-4441 - Shorten movement permission</p> <p>relates to :  SPMS-4336 - Shorten movement permission (Operational plan change, rejected)</p> <p>assesses :  SPRM-110 - [B.1.1.1] Improper routing</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-3079 - Required operational traffic plan</p> <p>has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1442 - Train adheres to infrastructure restrictions</p> <p>_ is mitigated by : {c} SPRM-1443 - Requested track path is free of occupancies</p> <p>_ is mitigated by : {c} SPRM-1444 - Requested track path is distinct from other authorised track paths</p>

### Early required operational traffic plan from TMS

ID	SPRM-1448
Failure Mode (Keyword)	Commission
Failure Description	Traffic Management System sends information about planned movement according to the operational traffic plan for the train too early.
Effect on Linked Functions Systems	Normal functionality of the CCS regarding the function "Calculate information to support driver" is expected.
Effect on Railway System	-
Risk Comment	-









Linked Work Items	relates to :  SPMS-2148 - Calculate operational traffic plan relates to :  SPMS-2354 - Required operational traffic plan relates to :  SPMS-5359 - Drive train automatically relates to :  SPMS-5444 - Drive train automatically assesses :  SPRM-516 - No safety hazard causes :  SPRM-517 - No accident relates to :  SPMS-5333 - Required operational traffic plan has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis
-------------------	---

### Incorrect required operational traffic plan from TMS









ID	SPRM-1450
Failure Mode (Keyword)	Incorrect
Failure Description	Traffic Management System sends incorrect planned movement of train.
Effect on Linked Functions Systems	CCS prepares information to support driver according to wrong operational plan movement data.
Effect on Railway System	Driver could disengage the ATO by his interfering to the driving - braking or accelerating according to wrong displayed information. Train is not operated according to operational traffic plan prepared by TMS. Possible not optimal usage of the railway system regarding capacity management or timing of the trains.
Linked Work Items	relates to :  SPMS-2148 - Calculate operational traffic plan relates to :  SPMS-2354 - Required operational traffic plan relates to :  SPMS-5359 - Drive train automatically relates to :  SPMS-5444 - Drive train automatically assesses :  SPRM-516 - No safety hazard causes :  SPRM-517 - No accident relates to :  SPMS-5333 - Required operational traffic plan has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis

### Late required operational traffic plan from TMS

ID	SPRM-1451
Failure Mode (Keyword)	Omission
Failure Description	Traffic Management System sends planned movement of train too late or never at all.
Effect on Linked Functions Systems	CCS is not able to prepare information to support driver according to the operational plan movement data. No supporting information (target advice speed etc.) is displayed to the driver.
Effect on Railway System	There is a possibility that driver will intervene to the driving and stop the train when he has no information and ATO is although moving according to operational plan. Train is not operated according to operational traffic plan prepared by TMS. Possible not optimal usage of the railway system regarding capacity management or timing of the trains.
Risk Comment	-

Linked Work Items	relates to :  SPMS-2148 - Calculate operational traffic plan relates to :  SPMS-2354 - Required operational traffic plan relates to :  SPMS-5359 - Drive train automatically relates to :  SPMS-5444 - Drive train automatically assesses :  SPRM-516 - No safety hazard causes :  SPRM-517 - No accident relates to :  SPMS-5333 - Required operational traffic plan has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis
-------------------	---










### Early required operational traffic plan from TMS

ID	SPRM-1304
Failure Mode (Keyword)	Commission
Failure Description	Traffic Management System sends the operational plan too early.
Effect on Linked Functions Systems	The new target state of the point machine (e.g. left) is determined earlier than necessary and executed at the planned time. Resources of CCS-System are blocked earlier than necessary to determine the planned execution of the operational movement.
Effect on Railway System	-
Risk Comment	-
Linked Work Items	relates to :  SPMS-2148 - Calculate operational traffic plan relates to :  SPMS-2350 - Required operational traffic plan relates to :  SPMS-4342 - Set point position (Left to right, Operational plan) relates to :  SPMS-4444 - Set point position assesses :  SPRM-516 - No safety hazard causes :  SPRM-517 - No accident relates to :  SPMS-4546 - Required operational traffic plan has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis









### Incorrect required operational traffic plan from TMS

ID	SPRM-1305
Failure Mode (Keyword)	Incorrect
Failure Description	Traffic Management System sends an incorrect operational plan.
Effect on Linked Functions Systems	The wrong target state of the point machine (e.g. right) is determined and commanded.
Effect on Railway System	1. The point machine is already in the target position, unnecessary command to point machine is sent. The point machine could overheat while trying to force the point into the target position which the point is already in. 2. Train has to stop because the points are not moved at the right time to the correct position for the operational movement. Disturbed operation (PRAM issue).
Risk Comment	PRAM consideration: CCS-System shall send the reason for rejecting an operational movement to TMS. Note: A reject code enables TMS to adjust the operational plan more efficiently.











Linked Work Items	<p>relates to :  SPMS-2148 - Calculate operational traffic plan</p> <p>relates to :  SPMS-2350 - Required operational traffic plan</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>causes :  SPRM-517 - No accident</p> <p>assesses :  SPRM-114 - [B.1.1.0] Other failure to operate the infrastructure</p> <p>relates to :  SPMS-4546 - Required operational traffic plan</p> <p>has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by :  SPRM-1700 - Point machine position is equal to requested point machine position.</p>
-------------------	---

### Late required operational traffic plan from TMS











ID	SPRM-1306
Failure Mode (Keyword)	Omission
Failure Description	Traffic Management System sends the operational plan later or not at all.
Effect on Linked Functions Systems	The target state of the point machine (e.g. left) is determined and commanded too late.
Effect on Railway System	Train has to stop because the points are not moved at the right time to the correct position for the operational movement. Disturbed operation (PRAM issue).
Risk Comment	PRAM consideration: CCS-System shall send the reason for rejecting an operational movement to TMS. Note: A reject code enables TMS to adjust the operational plan more efficiently.
Linked Work Items	<p>relates to :  SPMS-2148 - Calculate operational traffic plan</p> <p>relates to :  SPMS-2350 - Required operational traffic plan</p> <p>relates to :  SPMS-4342 - Set point position (Left to right, Operational plan)</p> <p>relates to :  SPMS-4444 - Set point position</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4546 - Required operational traffic plan</p> <p>has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis</p>

### Early required operational traffic plan from TMS

ID	SPRM-913
Failure Mode (Keyword)	Commission
Failure Description	Traffic Management System sends to CCS System usage restriction activation too early.
Effect on Linked Functions Systems	CCS System applies unneeded restriction and reallocation. Usage restriction wrongly activated.
Effect on Railway System	Potential traffic disruptions and reduction of performance. Operational adjustments required. Too early activation could also result to an Emergency Brake application with impact on passengers and wear of the wheels (e.g. TSR is activated while a train is moving under MA and the TSR is transmitted to the train).











Risk Comment	PRAM consideration: If a usage restriction is active, the TMS should recalculate the traffic plan cyclically, regardless of the restriction condition. This applies if such a function is not included already in its Basic Safety Integrity check.
Linked Work Items	relates to :  SPMS-2148 - Calculate operational traffic plan relates to :  SPMS-2357 - Required operational traffic plan relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction) relates to :  SPMS-4469 - Activate usage restriction assesses :  SPRM-516 - No safety hazard causes :  SPRM-517 - No accident relates to :  SPMS-2988 - Required operational traffic plan has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis

### Incorrect required operational traffic plan from TMS

ID	SPRM-956
Failure Mode (Keyword)	Incorrect
Failure Description	Traffic Management System sends to CCS System a less restrictive usage restriction activation than required, or at a wrong location.
Effect on Linked Functions Systems	CCS System implements and applies an insufficient restriction, leading to potential non-compliance with operational requirements.
Effect on Railway System	A wrong usage restriction (location or with wrong parameters) is activated and train does get the wrong usage restriction(less-restrictive).
Risk Comment	-
Linked Work Items	relates to :  SPMS-2148 - Calculate operational traffic plan relates to :  SPMS-2357 - Required operational traffic plan relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction) relates to :  SPMS-4469 - Activate usage restriction causes :  SPRM-77 - [A2] Derailments causes :  SPRM-71 - [A1] Collisions causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion assesses :  SPRM-120 - [B.1.2.4] Over-speeding relates to :  SPMS-2988 - Required operational traffic plan has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis _ is mitigated by : {c} SPRM-1746 - Usage restriction confirmation matches operational plan _ is mitigated by : {c} SPRM-1747 - Requested usage restriction parameters adheres to infrastructure and train-side restrictions












### Late required operational traffic plan from TMS

ID	SPRM-957
Failure Mode (Keyword)	Omission
Failure Description	Traffic Management System sends to CCS System usage restriction activation request too late or not at all.












Effect on Linked Functions Systems	No restriction applied in CCS System, usage restriction keeps being deactivated causing unregulated train movements. The required usage restriction keeps being deactivated.
Effect on Railway System	Train movements may proceed with less-restrictive authorizations than safety requirements. Hazardous conditions such as the missed activation of a TSR (e.g. a planned low adhesion zone)
Risk Comment	-
Linked Work Items	<p>relates to :  SPMS-2148 - Calculate operational traffic plan</p> <p>relates to :  SPMS-2357 - Required operational traffic plan</p> <p>relates to :  SPMS-4355 - Activate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-4469 - Activate usage restriction</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>assesses :  SPRM-120 - [B.1.2.4] Over-speeding</p> <p>relates to :  SPMS-2988 - Required operational traffic plan</p> <p>has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1757 - Usage restriction is planned</p> <p>_ is mitigated by : {c} SPRM-2015 - Usage restriction is active at planned time</p>

#### Early required operational traffic plan from TMS









ID	SPRM-1475
Failure Mode (Keyword)	Commission
Failure Description	Traffic Management System sends to CCS System the operational plan restriction deactivation request too early.
Effect on Linked Functions Systems	Usage restriction is wrongly deactivated differently from the actually planned or required TMS operational plan.
Effect on Railway System	Train is allowed to move over an area during maintenance works ongoing. Train overspeed over an area with restricted speed.
Risk Comment	PRAM consideration: TMS shall check the execution state of the operational plan and replan when deviations are detected.

Linked Work Items	<p>relates to :  SPMS-2148 - Calculate operational traffic plan</p> <p>relates to :  SPMS-2357 - Required operational traffic plan</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>assesses :  SPRM-519 - [xy] Field Force on track without trackside protection</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-2988 - Required operational traffic plan</p> <p>has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1742 - High quality standard for planning of usage restriction deactivation times</p> <p>_ is mitigated by : {c} SPRM-1743 - Deactivation of planned usage restrictions requested</p>
-------------------	--

### Incorrect required operational traffic plan from TMS

ID	SPRM-1476
Failure Mode (Keyword)	Incorrect
Failure Description	Traffic Management System sends to CCS System incorrect operational plan restriction deactivation request.
Effect on Linked Functions Systems	<p>The usage restriction has been deactivated either at an incorrect location, range, or operational area, or an unintended restriction type has been deactivated. This results in:</p> <p>a) Necessary usage restriction is deactivated.</p> <p>b) Unnecessary usage restriction keeps being activated.</p>
Effect on Railway System	<p>Train is allowed to move over an area during maintenance works ongoing.</p> <p>Train overspeed over an area with restricted speed.</p>
Risk Comment	PRAM consideration: TMS shall check the execution state of the operational plan and replan when deviations are detected.
Linked Work Items	<p>relates to :  SPMS-2148 - Calculate operational traffic plan</p> <p>relates to :  SPMS-2357 - Required operational traffic plan</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>assesses :  SPRM-519 - [xy] Field Force on track without trackside protection</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-77 - [A2] Derailments</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-2988 - Required operational traffic plan</p> <p>has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1742 - High quality standard for planning of usage restriction deactivation times</p> <p>_ is mitigated by : {c} SPRM-1743 - Deactivation of planned usage restrictions requested</p>

### Late required operational traffic plan from TMS

ID	SPRM-1477
Failure Mode (Keyword)	Omission
Failure Description	Traffic Management System sends to CCS System the operational restriction deactivation request too late or not at all.
Effect on Linked Functions Systems	Usage restriction keeps being activated over area with a certain extent.
Effect on Railway System	Train movement along affected track keeps being restricted unnecessarily. Disturbed operation (PRAM issue)
Risk Comment	PRAM consideration: TMS shall retry to deactivate usage restriction after XX seconds after the request has not been executed by CCS System.
Linked Work Items	<p>relates to :  SPMS-2148 - Calculate operational traffic plan</p> <p>relates to :  SPMS-2357 - Required operational traffic plan</p> <p>relates to :  SPMS-4828 - Deactivate usage restriction</p> <p>assesses :  SPRM-516 - No safety hazard</p> <p>causes :  SPRM-517 - No accident</p> <p>relates to :  SPMS-4345 - Deactivate usage restriction (Planned usage restriction)</p> <p>relates to :  SPMS-2988 - Required operational traffic plan</p> <p>has parent :  SPRM-2072 - Detailed Failure Modes and Effect Analysis</p>

### 3.2.2.5.3 Constraints

#### Usage restriction is active at planned time

TMS alerts the operator if a planned usage restriction is not activated.

ID	SPRM-2015
----	-----------

#### High quality standard for planning of usage restriction deactivation times


The IM shall ensure high quality standard for the planning of usage restriction deactivation times. Note: For example using quality measures like 4-eye principle, software tools to validate the data, etc.

ID	SPRM-1742
----	-----------

### 3.2.2.6 Wheel

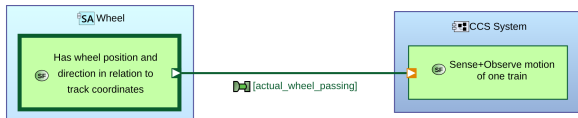




#### 3.2.2.6.1 Functional description

#### Has wheel position and direction in relation to track coordinates

This function is allocated to  SPMS-2101 - Wheel.

This passive function represents the position and passing direction in relation to track coordinates of one wheel.




















ID	SPMS-2141
----	-----------

Context Diagram	 <p>Figure 12 Context Diagram of Has wheel position and direction in relation to track coordinates</p>		
Input exchanges	No inputs defined for this function.		
Output exchanges	<b>Output exchanges</b>  SPMS-2244 - Actual wheel passing <ul style="list-style-type: none"> <li> SPMS-6523 - actual_wheel_passing</li> </ul>	<b>Target function</b>  SPMS-2192 - Sense+Observe motion of one train	<b>Function allocated to</b>  SPMS-2098 - CCS System

### 3.2.2.6.2 Failure Modes and Effects Analysis

#### Early wheel passing information from Wheel




















ID	SPRM-1134
Failure Mode (Keyword)	Commission
Failure Description	Wheel sends wheel passing information too early.
Effect on Linked Functions Systems	<p>CCS System operates with incorrect wheel passing information. Thus CCS System assumes that the train (wheels) is (are) on a position where it is actually not yet.</p> <p>The wrong estimated train motion state is used CCS-internally to localise the train.</p> <p>If CCS-System operates with a wrong estimated train motion state, there are several effects for CCS-System:</p> <p>a) Requests for operational movements are handled by CCS-System based on wrong internal train motion state. Authorising a train movement is based on wrong train positions - this leads possibly to a track path not being secured/ reserved for a train movement (e.g. movement is granted to wrongly located train or unplanned entering of an occupied track path).</p> <p>b) Track path behind the train is released too early (when train is still occupying it).</p>
Effect on Railway System	<p>Possible unsafe movement of a train.</p> <p>Track resources are seen as free / released although they are not free.</p> <p>E.g. track resources are used for a permission to drive for the following train, track resources are released too early</p>
Risk Comment	-

Linked Work Items	<p>relates to :  SPMS-2141 - Has wheel position and direction in relation to track coordinates</p> <p>relates to :  SPMS-2244 - Actual wheel passing</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>assesses :  SPRM-479 - RSSB_2.03.05 - Wrong side signalling failure - Track circuit fails to detect train</p> <p>causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>assesses :  SPRM-1726 - [XYZ] Undue movement of a point</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-3015 - Actual wheel passing</p> <p>assesses :  SPRM-314 - [B.3.0.2] Train detection equipment failure (trackside)</p> <p>has parent :  SPRM-2075 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1736 - Integrity of received information for determining train motion state</p> <p>_ is mitigated by : {c} SPRM-1739 - Consistency between information for determining train motion state</p>
-------------------	--

### Incorrect wheel passing information from Wheel

ID	SPRM-1135
Failure Mode (Keyword)	Incorrect
Failure Description	Wheel sends incorrect wheel passing information.
Effect on Linked Functions Systems	<p>CCS System operates with incorrect wheel passing information. Thus CCS System assumes that the train (wheels) is (are) on a position where it is actually not.</p> <p>The wrong estimated train motion state is used CCS-internally to localise the train.</p> <p>If CCS-System operates with a wrong estimated train motion state, there are several effects for CCS-System:</p> <p>a) Authorising a train movement is based on wrong train positions - this leads possibly to a track path not being secured/reserved for a train movement (e.g. movement is granted to wrongly located train or unplanned entering of an occupied track path).</p> <p>b) Track path behind the train is released too early (when train is still occupying it).</p>
Effect on Railway System	<p>Possible unsafe movement of a train.</p> <p>Track resources are seen as free / released. Although they are not free and are used for a permission to drive.</p>
Risk Comment	-


















Linked Work Items	<p>relates to :  SPMS-2141 - Has wheel position and direction in relation to track coordinates</p> <p>relates to :  SPMS-2244 - Actual wheel passing</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>assesses :  SPRM-479 - RSSB_2.03.05 - Wrong side signalling failure - Track circuit fails to detect train</p> <p>causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>assesses :  SPRM-1726 - [XYZ] Undue movement of a point</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>relates to :  SPMS-3015 - Actual wheel passing</p> <p>assesses :  SPRM-314 - [B.3.0.2] Train detection equipment failure (trackside)</p> <p>has parent :  SPRM-2075 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1736 - Integrity of received information for determining train motion state</p> <p>_ is mitigated by : {c} SPRM-1739 - Consistency between information for determining train motion state</p>
-------------------	---

#### Late wheel passing information from Wheel (1)


















ID	SPRM-1438
Failure Mode (Keyword)	Omission
Failure Description	Wheel sends wheel passing information too late or not at all.
Effect on Linked Functions Systems	<p>CCS System operates with outdated wheel passing information. Thus CCS System assumes that the train (wheels) is (are) on a position where it has already passed.</p> <p>1) In the case that the train has a movement permission, the train continues to move on a secure track path. Releasing the track path would happen later or not at all resulting in a track path unnecessarily staying reserved for the train movement and a loss of capacity for the railway operation.</p> <p>2) In case there is a train without a Movement Permission, CCS System would detect it later or not at all which would result in an undetected train/vehicle on the network. that can endanger other trains and makes authorising a Movement Permission unsafe.</p>
Effect on Railway System	Possible unsafe movement of a train.
Risk Comment	-



Linked Work Items	<p>relates to :  SPMS-2141 - Has wheel position and direction in relation to track coordinates</p> <p>relates to :  SPMS-2244 - Actual wheel passing</p> <p>relates to :  SPMS-5316 - Release movement permission</p> <p>relates to :  SPMS-5362 - Release movement permission</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-3015 - Actual wheel passing</p> <p>assesses :  SPRM-314 - [B.3.0.2] Train detection equipment failure (trackside)</p> <p>causes :  SPRM-71 - [A1] Collisions</p> <p>causes :  SPRM-87 - [A4] Accidents to persons involving rolling stock in motion</p> <p>has parent :  SPRM-2075 - Detailed Failure Modes and Effect Analysis</p>
-------------------	---

### Late wheel passing information from Wheel (2)









ID	SPRM-1982
Failure Mode (Keyword)	Omission
Failure Description	Wheel sends wheel passing information too late or not at all.
Effect on Linked Functions Systems	CCS System operates with outdated wheel passing information. Thus CCS System assumes that the train (wheels) is (are) on a position where it has already passed. As a result, an occupied section is assumed to be vacant which can lead to CCS System granting another train movement into the occupied section.
Effect on Railway System	Possible unsafe movement of a train. Track resources are seen as free / released. Although they are not free and are used for a permission to drive.
Risk Comment	-

Linked Work Items	<p>relates to :  SPMS-2141 - Has wheel position and direction in relation to track coordinates</p> <p>relates to :  SPMS-2244 - Actual wheel passing</p> <p>relates to :  SPMS-4329 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-4333 - Superfluous Perform train movement</p> <p>relates to :  SPMS-4438 - Localise train on railway infrastructure</p> <p>relates to :  SPMS-5298 - Grant movement permission</p> <p>relates to :  SPMS-5361 - Grant movement permission (Operational plan)</p> <p>relates to :  SPMS-5514 - Grant movement permission (Signaller request)</p> <p>assesses :  SPRM-297 - [B.3.1.3] Wrong side signalling (infrastructure) failure</p> <p>assesses :  SPRM-479 - RSSB_2.03.05 - Wrong side signalling failure - Track circuit fails to detect train</p> <p>causes :  SPRM-72 - [A1.1] Collision of train with a train/rail vehicle</p> <p>causes :  SPRM-78 - [A2.1] Derailment of train</p> <p>assesses :  SPRM-1726 - [XYZ] Undue movement of a point</p> <p>assesses :  SPRM-299 - Undue movement of a point while train is approaching</p> <p>relates to :  SPMS-3015 - Actual wheel passing</p> <p>assesses :  SPRM-314 - [B.3.0.2] Train detection equipment failure (trackside)</p> <p>has parent :  SPRM-2075 - Detailed Failure Modes and Effect Analysis</p> <p>_ is mitigated by : {c} SPRM-1736 - Integrity of received information for determining train motion state</p> <p>_ is mitigated by : {c} SPRM-1739 - Consistency between information for determining train motion state</p>
-------------------	--

### 3.2.2.6.3 Constraints

No constraints allocated to this function.

## 4 References

ID	Description
[  SPT2TRAFFIC-4141 - ERJU Safety Guideline]	The ERJU Safety Guideline practical guidance for ERJU Safety and System Engineers.
[  SPP-18056 - TCS_System Definition CCS System_V0.3]	System Definition of the CCS-System according to  SPPRAMSS-349 - [EN 50126-1:2017] .
[  SPP-18060 - TCS_System Architecture Description CCS System V0.3 ]	System Architecture of the CCS 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 <a href="#">Phase 2.EN50126-1</a> 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.