TCCS Configuration - Operational Epics

Author(s)	Ghielmetti Cirillo (I-NAT-GST-CCS) , Ibtihel Cherif

Abstract	Definition of the Operational Epics (Use Cases) for the CCS configuration management process describing the operational needs at CCS system level from stakeholder perspective. Reviewed by the PRAMS domain.

Classification	public
Status	Open
Version	1.0
Revision	357734
Last Change Date	06.09.2024

INFO: History table is not displayed, because this document is in status **doc_open**.
RULE: History table is not displayed, in statuses: { draft doc_open doc_inprogress doc_contentApproval doc_contentDecision }
CONTACT: For more information contact Administrator

Content

Contents

1 Introduction

1.1 Document Scope and Purpose

SPT2TS-1460 - The purpose of this document is to provide an analysis of the configuration management process by means of definition of operational epics (use cases) and based on input documents and experts analyses.

This document will define operational epics (use cases) from the perspective of different stakeholders (e.g Railway Undertaking, Manufacturer, Infrastructure Manager, etc.). These operational epics (use cases) are the basis to define and standardise (to a certain extent) a configuration management solution that eases the configuration management process for CCS systems.

1.2 Goals of the Activity

SPT2TS-1459 - The main activity objectives are the provision of services for configuration management of CCS systems.
Operational epic (use case) definitions should permit to:

- participate to support configuration management of CCS components, trackside and on-board.
- ease the configuration management of the CCS onboard equipment.
- ease the configuration management of the CCS trackside equipment.

1.3 Stakeholder description

SPT2TS-1444 - The operational epics in this document are addressing the Control Command and Signalling (CCS) System within the Railway System, with a clear focus on configuration management of the CCS System. Only epics, for which it can be assumed that the CCS system is involved in the context of configuration management or the CCS system's external interfaces are impacted, are listed in this document.

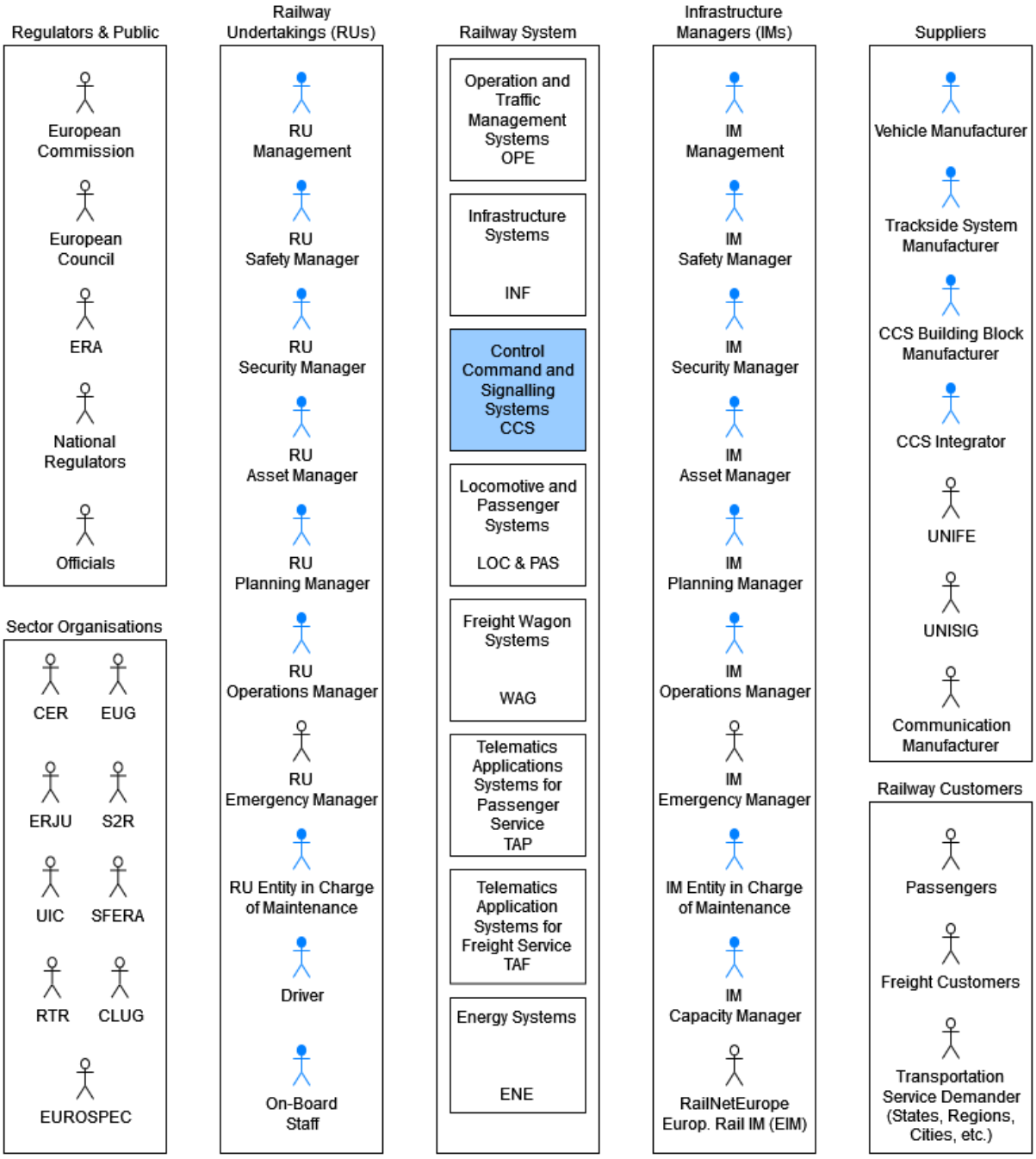

Figure 1 Railway System overview with stakeholders and their roles

Note-1: *in the above figure the railway systems and stakeholders that are relevant for the content of this document are filled-in and have a blue colour.*
Note-2: *the Railway Undertaking (RU) can be the holder of the vehicle, but it can also be just an organisation operating the vehicle. For this document we do not differentiate between the two, as it is not relevant for the development of the Configuration Management Process. For convenience we assume that RU is also the holder of the vehicle.*
The operational epics listed in this document are focussing on the needs of the Railway Undertakings (RUs), the Infrastructure Managers (IMs), and the Suppliers. They are captured, using a formal process (interview, review, approval). Epics of interest to Regulators, Sector Organisations, and Railway Customers may also be

listed in this document, but are not systematically captured. No formal interviews, reviews, or approval processes are conducted with these stakeholders.

SPT2TS-1458 - The following tables provide a brief description of the railway systems, the stakeholders and their roles.

Railway Systems	Abbr.	Description
Operation and Traffic Management Systems	OPE	Operation and traffic management systems of infrastructure managers and railway undertakings, related to the operation of trains on the rail system.
Infrastructure Systems	INF	Structural and maintenance related Infrastructure Systems.
Control Command and Signalling	CCS	Control command and signalling on-board and trackside systems.
Locomotives and Passenger Carriages Systems	LOC & PAS	Rolling stock systems of the following types of rolling stock: self-propelling thermal or electric trains, thermal or electric traction units, passenger carriages, mobile railway infrastructure construction and maintenance equipment
Freight Wagons Systems	WAG	Rolling stock systems of freight wagons including vehicles designed to carry lorries.
Telematics Applications for Passenger Service	TAP	Systems providing passengers with information before and during the journey, reservation and payment systems, luggage management and management of connections between trains and with other modes of transport.
Telematics Applications for Freight Service	TAF	Systems supporting real-time monitoring of freight and freight trains, marshalling, reservations, invoicing, payments, management of connections with other modes of transport, and production of electronic accompanying documents.
Energy Systems	ENE	Systems to supply traction energy to a train.

Table 1 Description of the railway systems

Roles of the Infrastructure Manager (IM)

Title	Description
IM Asset Manager	The person within the IM organisation responsible to define and plan the lifecycle for a specific asset, for instance a specific interlocking. This person will specify the asset, is involved in purchasing and acceptance activities, provides a release plan, etc.
IM Capacity Manager	The entity responsible for the coherence of projects to meet the requested performance and capacity forecast on the network.
IM Emergency Manager	The person within the IM organisation responsible to find solutions for critical issues that can occur during railways operation.
IM Entity in Charge of Maintenance	The department within the IM organisation responsible to maintain and service the infrastructure CCS components. This includes people responsible for maintenance and service of a specific interlocking as well as technicians working locally.
IM Management	The person within the IM organisation responsible to improve efficiency and reduce costs of the IM.
IM Operations Manager	The person within the IM organisation responsible for the rolling train runs planning according to schedule and current situations (e.g. occurred incidents, train delays, etc.).
IM Planning Manager	The person within the IM organisation responsible for the planning of the infrastructure usage, from the allocation of routes to the planning of the infrastructure maintenance.
IM Safety Manager	The person within the IM organisation responsible to enforce safety measures to ensure the safety of the railway system.
IM Security Manager	The person within the IM organisation responsible to enforce cyber security measures in order to protect the assets from malicious intrusions that can affect the safety or availability of the railway system.

9 items found

Roles of the Railway Undertaking (RU)

Title	Description
Driver	The Driver is a person capable and authorised to drive trains, including locomotives, shunting locomotives, work trains, maintenance railway vehicles or trains for the carriage of passengers or goods by rail in an autonomous, responsible, and safe manner. Source: Directive 2007/59/EC of the European Parliament and of the Council.
On-Board Staff	The On-Board Staff (OBS) is the personnel of the Railway Undertaking (RU), which may escort the Passenger Train. The Train Attendant is responsible for passenger and train service (e.g. indicate to the driver when he can leave a station, etc.), if present on-board he may check the passenger tickets, assist the passengers (e.g. in case of incidents), generally provide information, etc.).

RU Asset Manager	The person within the RU organisation responsible to define and plan the lifecycle for a specific asset, for instance the ETCS on-board. This person will specify the asset, is involved in purchasing and acceptance activities, provides a release plan, etc.
RU Emergency Manager	The person within the RU organisation responsible to find solutions for non-planned issues that can occur during rolling-stock operation.
RU Entity in Charge of Maintenance	The department within the RU organisation responsible to maintain and service the vehicles. This includes people responsible for maintenance and service of a whole fleet, as well as technicians working on-board the vehicles when these are in the work shop.
RU Management	The person within the RU organisation responsible to improve efficiency and reduce costs of the railway undertaking.
RU Operations Manager	The person within the RU organisation responsible to plan the operation of the single train units (which train unit operates which train run, etc.), but also the drivers schedules, the train conductors schedule, etc.
RU Planning Manager	The person within the RU organisation responsible to plan the available trains in different train runs, including the planning of maintenance activities. The planning of the available trains in different train runs is typically made on a yearly base.
RU Safety Manager	The person within the RU organisation responsible to enforce safety measures to ensure the safety of the railway system.
RU Security Manager	The person within the RU organisation responsible to enforce cyber security measures in order to protect the assets from malicious intrusions that can affect the safety or availability of the railway system.

10 items found

Roles of the Suppliers

Title	Description
CCS Building Block Manufacturer	Entity in charge of: • designing the cabinet / rack (for hosting electronic boards) and its electrical wiring, • designing, realising and validating the component (including hardware electronic boards) according to requirements including test requirements (i.e., test bench and procedures), • assembling the components in their electrical/mechanical cabinet/rack, • realising the safe integration of the selected components, • configurating the components for the concerned CCS project(s), • realising the Generic Product Safety Case (component scope), • performing the further modifications of the components according to enhanced requirements (e.g., new functionalities, improvements),

- validating the CCS System according to test requirements (i.e., test bench and procedures),
- performing the further modifications of the CCS System (e.g., new components, exchanges, new configuration...),
- export application conditions to CCS (if any),
- managing the other assessment types (e.g., ISA, NoBo, DeBo),
- submitting and obtain the Application for Placing On the Market (APOM for the supplier: official document allowing the building block as an interoperability constituent to be placed in commercial revenue) to the ERA and the National Safety Authorities (NSAs),
- describing the maintenance constraints and procedures applicable for the building block to ease its maintainability.

CCS Integrator — Entity in charge of:

- application safety cases (Specific Application on rollingstock or interlocking and network, and Generic Application on the fully equipped rollingstock or interlocking),
- realising the Generic Application Safety Case or the Specific Application Safety Case of the full CCS System,
- managing and provide the input to the other assessment types (e.g. NoBo, DeBo, etc.),
- performing the safe integration of the rollingstock or interlocking and its dedicated network (e.g., ERTMS line (n)),
- realising the safe data preparation: rollingstock or interlocking into network (main technical task),
- submitting and obtain the Application for Placing On the Market (APOM for the integrator: official document allowing the rollingstock or trackside subsystem to be placed in commercial revenue) to the ERA and the National Safety Authorities (NSAs),
- defining the functionalities required from the CCS System,
- designing the integration phase (e.g. electrical drawings, mechanical specifications),
- assigning these last tasks to the train manufacturer, CCS component manufacturer and CCS integrator,
- realising the safe integration of the CCS sub-system into the rollingstock or network,
- physically integrating the CCS sub-system into the rollingstock or the network,
- testing the complete rollingstock or network integration in the scope of TSI CCS/TSI LOC&PAS using the CCS sub-system and the rollingstock or network as black boxes,
- realising the data preparation of the CCS sub-system on the dedicated rollingstock or network.

Communication Manufacturer — Manufacturer of railway mobile radio, entity in charge of:

- designing the cabinet / rack (for hosting electronic boards) and its electrical wiring,
- designing the communication components,
- designing, realising and validating the component (including hardware electronic boards) according to requirements including test requirements (i.e., test bench and procedures),
- assembling the components in their electrical/mechanical cabinet/rack,
- realising the of the selected components,
- configuring the components for the concerned project(s),
- performing the further modifications of the components according to enhanced

	requirements (e.g., new functionalities, improvements), • managing other assessment types (e.g., telecom bodies), • describing the maintenance constraints and procedures applicable for the building block to ease its maintainability.
Trackside System Manufacturer	An entity that designs, produces, and integrates systems for the railway industry, ensuring they meet interoperability and safety standards like ERTMS. This includes the testing and certification of trackside equipment.
UNIFE	UNIFE is the European Rail Supply Industry Association. It represents Europe's rail supply companies, which are active in the design, manufacture, maintenance, and refurbishment of rail transport systems, subsystems, and related equipment. UNIFE also encompasses 15 national rail industry associations, advocating on behalf of over 100 of Europe's leading rail supply companies.
UNISIG	UNISIG, the Union of the Signalling Industry, was established under UNIFE to develop the technical specifications for the ERTMS/ETCS. It includes major companies in railway signalling and train control systems, contributing to the advancement of the European Rail Traffic Management System (ERTMS) through collaboration with the European Union Agency for Railways.
Vehicle Manufacturer	Entity in charge of • Specifying the vehicle system including software and hardware interfaces in line with the last European Specifications • Including in the new vehicle development LRU modules to facilitate the maintenance by the final user • Designing the vehicle and its mechanical and electrical schematics, • Testing and validating all the vehicle interfaces according to requirements including test requirements (i.e., test bench and procedures) • Realising the safety analyses with the ISA/NOBO/DeBO certifications • Configurating the components for the concerned CCS project(s), • Realising the Generic Vehicle Safety Case (vehicle scope including CCS aspects), • Performing the further modifications of the components according to enhanced requirements (e.g., new functionalities, improvements),

7 items found

Roles of the Regulators & Public

Title	Description
European Commission	The European Commission is the executive branch of the European Union, responsible for proposing legislation, implementing decisions, upholding the EU treaties, and managing the day-to-day business of the EU.
European Council	The European Council is the EU institution that defines the general political direction and priorities of the European Union.
European Union Agency for Railways (ERA)	The European Union Agency for Railways or ERA helps to create a safer and cross national European railway network. It aims at doing so through reporting on the rail safety in the European Union, and developping viable common technical standards, safety measures, and a uniform signalling system in Europe.

National Regulators	National Regulators are authorities within individual states responsible for overseeing the implementation and enforcement of European railway standards, safety regulations, and ensuring compliance with EU directives at the national level.
Officials	The person within a public organisation responsible to analyse data in case of accidents in order to identify the root cause of a specific accident, and describe the fault that resulted in the accident.

5 items found

Roles of the Sector Organisations

Title	Description
Certifiable Localisation Unit with GNSS in the railway environment (CLUG)	CLUG is a project for developing a certifiable, GNSS-based localization unit for trains to enhance navigation and safety across Europe's railways.
Community of European Railway and Infrastructure Companies (CER)	CER is a Brussels-based group that represents European railway operators, infrastructure companies, and related associations, focusing on advocacy within the EU.
ERTMS User Group (EUG)	EUG is the technical body gathering ERTMS users and leading specialised expert working group on TSI specification.
Europe's Rail Joint Undertaking (ERJU)	ERJU is an initiative under the Horizon Europe programme focusing on research and innovation to enhance the EU railway network.
European Specification for railway vehicles (EUROSPEC)	EUROSPEC, initiated by several European railway companies in 2011, develops unified technical specifications for railway vehicles and components, aiming to standardise trains and enhance their quality and procurement, without being in the competitive domain.
NBRail	NB-Rail is an international non-profit organisation comprised of various conformity assessment bodies in the European railway sector. Its main purpose is to support interoperability and safety in the railway industry, by complementing activities not covered by basic regulatory documents.
Round Table Rail (RTR)	RTR (Round Table Rail) is a European initiative focused on transforming the traditional project-oriented rolling stock procurement into a more efficient, product-oriented approach since 2018.

Shift2Rail (S2R)	Shift2Rail focuses on innovative rail solutions to double the European rail system's capacity, increase reliability and service quality by 50%, and halve life-cycle costs.
Smart communications For Efficient Rail Activities (SFERA)	SFERA focuses on standardizing languages for Driving Advisory Systems to facilitate data exchange and reduce costs, aiming to improve energy efficiency and CO2 commitments in the rail sector.
Union Internationale des Chemins de fer (UIC)	UIC is a technical body for the railway operating community.

10 items found

Roles of the Railway Customers

Title	Description
Freight Customers	Entities that use rail services to transport goods.
Passengers	Individuals or groups who use rail services for personal or business travel.
Transportation Service Demander (Steates, Regions, Cities, etc.)	Governmental bodies or regional entities that demand rail transport services for economic development, connectivity, and public welfare.

3 items found

2 Input Analysis and References

SPT2TS-1445 -

Document ID	Document description	Version
OCORA-TW07-060	Configuration Management - Concept	1.1
EULYNX Eu.Doc.18	Maintenance and data management specification	4.0
SC5 DP1.2	System Pillar Common Business Objectives	1.00
SC5 DP1.5	CCS and TMS/CMS System Architecture	1.00

SUBSET-137	On-line Key Management FFFIS	1.0.0

Table 2 List of input documents

3 Glossary

3.1 Terms and definitions

Title	Description
High level BuildingBlocks	Due to the dependency concept the BuildingBlocks can form units of unlimited size. The recursive dependency tree can have any depth. Every level of the dependency tree links to the next level - that allows to assign clear responsibilities for each of the levels. As an example a BuildingBlock "area" might refer to a number of "interlocking interiors" and "filedelements" in its next downstream dependency level. The Top-Level BuildingBlockConfiguration is the root where all dependencies start from.
Operational Epics	Operational epics refer to large-scale initiatives or projects that are focused on improving the operational aspects of a business or organization. Unlike user epics, which typically address customer or user needs, operational epics are aimed at enhancing internal processes, systems, or infrastructure to optimize efficiency, productivity, and overall performance. Operational epics often involve cross-functional collaboration and may span multiple departments or teams within an organization. They are typically strategic in nature and aligned with the overall goals and objectives of the organization. Examples of operational epics could include implementing a new supply chain management system, revamping the customer support process, or optimizing the IT infrastructure to improve data security and accessibility. The use of epics in operational contexts helps break down complex initiatives into manageable units, allowing for better planning, resource allocation, and tracking of progress. By focusing on operational improvements, organizations can streamline their workflows, reduce costs, and enhance the overall effectiveness of their operations.
Static (or semi-static) data	Static (or semi-static) data refers to information or data that remains unchanged or constant over time. It is data that does not require frequent updates or modifications. Static data typically includes reference data, constants, configuration settings, or any other data that remains consistent throughout the operation of a system or application. This type of data is often used as a foundation or reference point for various processes or calculations within a system. Static data is generally stored in a read-only format and is not subject to frequent modifications or user interactions. This is often data that requires a homologation process before it can be applied on a system going in operation. However, it can also include data that does not require a homologation like IP-address, security patches, etc. Example of statical data: software, firmware, parametrisation file, data related to the topology stored in an interlocking, braking curves stored in the ETCS on-board, etc.

3 items found

4 Operational Epics (Use Cases)

SPT2TS-1375 - Template for Operational Epic definition

As a <*stakeholder role*>, I want to <*need description*>, in order to <*expected benefit / goal / rationale*>.

Linked Work Items	has parent: SPT2TS-1347 - Operational Epics (User stories)

4.1 Generally valid epics

SPT2TS-1388 - Correct activation of an update: correct CCS field component, correct configuration data packet

As an entity in charge of maintenance, I want to ensure that the correct CCS configuration (configuration data packet - specific release or version of an entity) is put into operation by the envisaged CCS field component, in order to ensure a correct update process conform with the homologation documents (e.g. certificates covering the compatibility between genuine and updated modular components).

Linked Work Items	is derived from: SPT1RS-190 - Changeability and upgradeability(1) is derived from: SPT1RS-189 - Changeability and upgradeability(2) is derived from: SPT1RS-203 - operations/maintenance: assisted systems has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-124022 - Perform CCS System instance consistency check at runtime _ is derived by: SPT2TS-124027 - Perform automated configuration activation and installation _ is derived by: SPT2TS-124021 - Implement means to ensure consistency within one CCS System instance _ is derived by: SPT2TS-122404 - Augment CCS Configuration of Integrator with a CCS Manifest _ is derived by: SPT2TS-123907 - Implement CCS Configuration verification and validation _ is derived by: SPT2TS-123905 - Associate CCS Configuration _ is derived by: SPT2TS-122389 - Support loading procedure for distribution jobs _ is derived by: SPT2TS-124164 - Associate Distribution Jobs

SPT2TS-2250 - Secure installation of an update: configuration process facilitated by security measures

As a security manager, I want I want that the configuration management process fulfils relevant security standards to reduce security hazards.

Linked Work Items	is derived from: SPT1RS-213 - local environment cyber security is derived from: SPT1RS-212 - non invasive/noticeable cyber security is derived from: SPT1RS-189 - Changeability and upgradeability(2) has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122399 - Support update of digital certificates _ is derived by: SPT2TS-122398 - Ensure only authorised staff has system access _ is derived by: SPT2TS-122393 - Ensure only configuration data packets from trusted sources are activated and installed _ is derived by: SPT2TS-122403 - Augment BB configuration item of BB Supplier with a BB Manifest _ is derived by: SPT2TS-124129 - Verify BB Configuration from BB Supplier

SPT2TS-12680 - Installation of unaltered update: configuration process facilitated by integrity check measures

As an asset manager or as a safety manager, I want to ensure that CCS field components only install configuration data packets that have not inadvertently or maliciously been modified during the handling and distribution process, in order to prevent installation of corrupted or compromised updates resulting in component malfunctions.

Linked Work Items	is derived from: SPT1RS-193 - automate lifecycle processes is derived from: SPT1RS-189 - Changeability and upgradeability(2) is derived from: SPT1RS-199 - system robustness and robustness against weather has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122403 - Augment BB configuration item of BB Supplier with a BB Manifest _ is derived by: SPT2TS-122404 - Augment CCS Configuration of Integrator with a CCS Manifest _ is derived by: SPT2TS-124129 - Verify BB Configuration from BB Supplier

SPT2TS-2251 - Safe installation of an update: configuration process facilitated by safety measures

As a safety manager, I want to ensure that CCS field components install in a safe manner configuration packets that are intended for them, in order to ensure that safe behaviour of the system is kept. This includes that the configuration process is considered in the safety certification.

Note: in the certification process, for the system context of each individual CCS field component, at least the impact should be considered of stopping operation for installation, and starting operation with or without updated configuration (e.g. in case of failure). Furthermore, when requesting human intervention to trigger or confirm steps in the configuration management process the typical human and human machine interface error aspects should also be considered.

Linked Work Items	is derived from: SPT1RS-189 - Changeability and upgradeability(2) is derived from: SPT1RS-190 - Changeability and upgradeability(1) is derived from: SPT1RS-231 - validated system performance, robust PRAMSS framework has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122403 - Augment BB configuration item of BB Supplier with a BB Manifest _ is derived by: SPT2TS-122404 - Augment CCS Configuration of Integrator with a CCS Manifest _ is derived by: SPT2TS-124129 - Verify BB Configuration from BB Supplier

SPT2TS-2252 - Flexible installation of an update: activation time suitable for operations

As an operational manager, I want to define a time window (earliest activation time, no later activation time) defining when a configuration packet shall be activated by a specific CCS field component, in order to ensure that activation is performed when this best suits from operational perspective (e.g. timetable, traffic volume, planned staff, etc.). It shall be possible to freely define the time window (no restrictions from the technical systems, only operational restrictions would have to be considered).

Note: The Operational Epic defines to have flexibility for the activation of a configuration at the granularity level of the single CCS field component (e.g. cab radio, DMI, etc.). It is up to the operational manager to then group the different CCS field components of the same vehicle or the same CCS trackside instance/area into one time window, if needed.

Linked Work Items	is derived from: SPT1RS-237 - efficient migration based on adaptable systems is derived from: SPT1RS-190 - Changeability and upgradeability(1) is derived from: SPT1RS-189 - Changeability and upgradeability(2) has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-124027 - Perform automated configuration activation and installation

SPT2TS-1389 - Deployment of an update to multiple same CCS components in parallel

As an entity in charge of maintenance, I want to be able to deploy the same CCS configuration (configuration data packet) to multiple same CCS field components (e.g. different vehicles of the same fleet, different object controllers of the same or different interlocking instances/areas but from the same supplier) at a time, in order to have a more lean and efficient update process. This may require some kind of bulk distribution function.

Note: for the deployment the user should be able to freely select at a time the asset where the configuration data packet is needed. This can be 1 specific train, or different vehicles of the same fleet, or different vehicles from several fleets, or different components from 1 specific interlocking instance/area, or different components from several interlocking instances/areas, etc.

Linked Work Items	is derived from: SPT1RS-189 - Changeability and upgradeability(2) is derived from: SPT1RS-188 - Changeability and upgradeability(3), simpilified integration is derived from: SPT1RS-237 - efficient migration based on adaptable systems has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122391 - Support generation of many distribution jobs in parallel _ is derived by: SPT2TS-123905 - Associate CCS Configuration

SPT2TS-1390 - Receive feedback about the status of the configuration (update) process

As an entity in charge of maintenance, I want to receive a feedback about the status of the configuration (update) process for each CCS field component, in order to know if everything worked as planned, or if a specific intervention is required.

Note: with status feedback it is conceived that the entity in charge of maintenance receives the feedback information for a specific configuration (update) process that he launched. At least the following should be available: ready for activation (data is preloaded, update not activated yet but ready to be), activation (and installation) successful, activation (and installation) not successful. But it could also be other status like: activation has started, configuration data packet has been received (downloaded), no configuration data packet available (at least one should possibly always be available - the latest applied for instance), etc.

Linked Work Items	is derived from: SPT1RS-189 - Changeability and upgradeability(2) has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122405 - Provide status information for specific distribution jobs _ is derived by: SPT2TS-122406 - Provide reason for failure related to specific distribution job

SPT2TS-2253 - A configuration packet is aligned with its intended environment

As an entity in charge of maintenance, I want that a configuration packet for a specific CCS field component is aligned with the environment of the CCS field component, in order to ensure a high system availability, lean configuration process, and a proper state of the system. This means that the technical solution of the Configuration Management Process shall foresee an intermediate parametrisation step allowing smooth integration of products. The latter do not have to always be specially developed for a specific project.

Linked Work Items	is derived from: SPT1RS-190 - Changeability and upgradeability(1) is derived from: SPT1RS-189 - Changeability and upgradeability(2) is derived from: SPT1RS-188 - Changeability and upgradeability(3), simpilified integration is derived from: SPT1RS-194 - independent lifecycle, simple exchange is derived from: SPT1RS-235 - viable forward/backward compatibility has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-124022 - Perform CCS System instance consistency check at runtime _ is derived by: SPT2TS-124027 - Perform automated configuration activation and installation _ is derived by: SPT2TS-124021 - Implement means to ensure consistency within one CCS System instance _ is derived by: SPT2TS-122404 - Augment CCS Configuration of Integrator with a CCS Manifest _ is derived by: SPT2TS-123907 - Implement CCS Configuration verification and validation _ is derived by: SPT2TS-123905 - Associate CCS Configuration

SPT2TS-2263 - Homogenous configuration versions in the field

As an asset manager, I want that CCS field components I am responsible for are equipped (in operation) with homogenous configuration versions (CCS field components of the same type run with the same configuration version - e.g. software version), in order to have a leaner supervision and asset management process.

Note I: this Operational Epics to be understood as a general objective. It is not mandatory to have all components of the same type running exactly the same configuration versions, but it is desirable. The Operational Epic has also been defined from the perspective that in the future the release cycles will be shorter. This means the Configuration Management Process has to be leaner and more efficient: there will always be changes, these have to be managed adequately.

Note II: Sometimes on purpose a different configuration version may be deployed. For instance, to test a new configuration version in operation before installing it on all components.

Linked Work Items	is derived from: SPT1RS-188 - Changeability and upgradeability(3), simpilified integration is derived from: SPT1RS-190 - Changeability and upgradeability(1) is derived from: SPT1RS-198 - automate lifecycle processes, independent lifecycle is derived from: SPT1RS-237 - efficient migration based on adaptable systems has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122391 - Support generation of many distribution jobs in parallel

SPT2TS-2254 - Distribution start of a configuration packet in good time

As an entity in charge of maintenance, I want to start distribution of a specific configuration packet well ahead of its earliest activation time, in order be sure that the configuration packet is available to the foreseen CCS field component when activation time is reached, and I am comfortable from time perspective with the process. This allows me to start the distribution of the configuration packet at an early point in time that suits me, latest at the time that based on my experience is necessary for data transfer, basically the time duration required for transferring the configuration packet from the base server to the storage location from where the activation is executed.

Linked Work Items	is derived from: SPT1RS-189 - Changeability and upgradeability(2) is derived from: SPT1RS-198 - automate lifecycle processes, independent lifecycle

	is derived from: SPT1RS-188 - Changeability and upgradeability(3), simpilified integration has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122391 - Support generation of many distribution jobs in parallel _ is derived by: SPT2TS-122405 - Provide status information for specific distribution jobs

SPT2TS-1392 - Selection of the most suitable distribution channel

As an entity in charge of maintenance, I want that a specific update can optionally be distributed and activated remotely (on-line, e.g. wired connection, radio connection, etc.) or locally (off-line, e.g. USB stick, notebook, etc.) where local physical presence close to the CCS field component is needed (for instance in the workshop, when a train is undergoing a regularly planned maintenance and is only selectively powered), in order to have the possibility to plan the required activities in a way that best suits to my current situation (most efficient) and organisation.

Note: For the local activation (off-line) channel, additional security measures should be included.

Linked Work Items	is derived from: SPT1RS-189 - Changeability and upgradeability(2) is derived from: SPT1RS-188 - Changeability and upgradeability(3), simpilified integration is derived from: SPT1RS-219 - robust, comprehensible, sustainable framework is derived from: SPT1RS-237 - efficient migration based on adaptable systems has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122397 - Provide local configuration (update) capability _ is derived by: SPT2TS-122396 - Provide remote configuration (update) capability

SPT2TS-1393 - Installation of an update without the need of a manual intervention

As entity in charge of maintenance, I want that a specific update is going into operation without the need of a manual intervention locally or remotely, in order to have a configuration process that is more scalable (when maintaining a large number of CCS field components) and more efficient.

Note: this might be restricted to a certain extent by further specific criteria depending on the type of update or degraded situations. It could be that an operationally relevant CCS field component on a train can only activate (including installation) the update once this is confirmed with manual intervention by the locally present staff (e.g. driver) based on the operational situation (end of shift / mission), It will be analysed (also for safety relevant updates) during the further development of the configuration management concept.

Linked Work Items	is derived from: SPT1RS-203 - operations/maintenance: assisted systems is derived from: SPT1RS-233 - simple repeatable DevOps is derived from: SPT1RS-189 - Changeability and upgradeability(2) has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122396 - Provide remote configuration (update) capability _ is derived by: SPT2TS-124022 - Perform CCS System instance consistency check at runtime _ is derived by: SPT2TS-124027 - Perform automated configuration activation and installation _ is derived by: SPT2TS-124021 - Implement means to ensure consistency within one CCS System instance

SPT2TS-2244 - Same configuration process applicable to all CCS field components

As an entity in charge of maintenance, I want that the same configuration process is applicable to all CCS field components, independently of the supplier or the SIL of the provided component functions, in order to have a more lean process, planning and organisation.

Note: this might be restricted to the basic configuration process, for components providing safety relevant functions with safety constrains or in degraded situation, some details in the process can be different.

Linked Work Items	is derived from: SPT1RS-189 - Changeability and upgradeability(2) is derived from: SPT1RS-198 - automate lifecycle processes, independent lifecycle is derived from: SPT1RS-233 - simple repeatable DevOps has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122395 - Freedom from interference and documented separation of safety related and non-safety related functions _ is derived by: SPT2TS-122390 - Support an easy import of CCS Configurations at Operator _ is derived by: SPT2TS-122416 - Same easy export of BB Configurations at BB Supplier is applicable to all products _ is derived by: SPT2TS-122415 - Same easy import of BB Configurations at Integrator is applicable to all products _ is derived by: SPT2TS-122418 - Same easy import of CCS Configurations at Operator is applicable to all products _ is derived by: SPT2TS-122417 - Same easy export of CCS Configurations at Integrator is applicable to all products _ is derived by: SPT2TS-122419 - Same loading procedure is applicable to all products _ is derived by: SPT2TS-122389 - Support loading procedure for distribution jobs _ is derived by: SPT2TS-124161 - Same Distribution Job generation at Integrator is applicable to all products _ is derived by: SPT2TS-123910 - Implement standardised high-level modes and states for activation and installation

SPT2TS-2246 - CCS field components only enter into regular operation if these are in a defined proper state

As an entity in charge of maintenance or as a safety manager, I want that the CCS field components only enter into regular operation if configuration process has been completed and the component is in a defined and proper state, in order to ensure that the system I am responsible for is in a proper and safe state (ideally correctly working) and to ensure a high availability.

Note: If the configuration process is not completed successfully, the provisions illustrated in SPT2TS-2245 shall be adopted.

Linked Work Items	is derived from: SPT1RS-189 - Changeability and upgradeability(2) is derived from: SPT1RS-203 - operations/maintenance: assisted systems is derived from: SPT1RS-219 - robust, comprehensible, sustainable framework has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-124022 - Perform CCS System instance consistency check at runtime _ is derived by: SPT2TS-124021 - Implement means to ensure consistency within one CCS System instance _ is derived by: SPT2TS-123910 - Implement standardised high-level modes and states for activation and installation

SPT2TS-2245 - In case of failed installation during configuration process have means to remain in operation

As an entity in charge of maintenance, I want that the CCS field components, in case the installation of a new configuration packet fails, remain in regular operation, for instance by automatically applying a rollback mechanism or loading a fallback configuration (project specific), in order to ensure a higher availability of my

system.
Rollback means: the CCS field components revert back to the original situation that was present before starting the configuration process (activation).

Note: If the rollback mechanism or the default configuration is also failing, it shall be possible for a technician to fix the issue by means of local / remote maintenance intervention.

Linked Work Items	is derived from: SPT1RS-237 - efficient migration based on adaptable systems is derived from: SPT1RS-219 - robust, comprehensible, sustainable framework is derived from: SPT1RS-203 - operations/maintenance: assisted systems is derived from: SPT1RS-188 - Changeability and upgradeability(3), simpilified integration has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-124205 - Perform a rollback in case of failures during installation

SPT2TS-9777 - Want to operate only one Maintenance Server Application

As an entity in charge of maintenance, I want to operate one maintenance server application for all CCS field components, independently of the component supplier or the SIL of the provided component functions, in order to only operate one server application I am familiar with. This makes my activities, people training, etc. more lean, and the whole configuration process less error prone.

Linked Work Items	is derived from: SPT1RS-194 - independent lifecycle, simple exchange is derived from: SPT1RS-197 - overall CAPEX/OPEX optimisation(1) is derived from: SPT1RS-203 - operations/maintenance: assisted systems has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122391 - Support generation of many distribution jobs in parallel _ is derived by: SPT2TS-122390 - Support an easy import of CCS Configurations at Operator _ is derived by: SPT2TS-122405 - Provide status information for specific distribution jobs _ is derived by: SPT2TS-122406 - Provide reason for failure related to specific distribution job _ is derived by: SPT2TS-122389 - Support loading procedure for distribution jobs _ is derived by: SPT2TS-124161 - Same Distribution Job generation at Integrator is applicable to all products _ is derived by: SPT2TS-124162 - Compile Distribution Job _ is derived by: SPT2TS-123910 - Implement standardised high-level modes and states for activation and installation

SPT2TS-49112 - Automatic availability of configuration data packet on maintenance server

As an asset manager, I want new configuration data packets to be automatically available on the maintenance server of my organisation, in order to have a simplified data transfer from the CCS building block supplier or the CCS integrator into my server (and is more secure), no need to have it in an email or download it from a specific website and insert it into my server application.

Linked Work Items	is derived from: SPT1RS-213 - local environment cyber security is derived from: SPT1RS-220 - overall CAPEX/OPEX optimisation(2) is derived from: SPT1RS-237 - efficient migration based on adaptable systems is derived from: SPT1RS-198 - automate lifecycle processes, independent lifecycle is derived from: SPT1RS-189 - Changeability and upgradeability(2) has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122390 - Support an easy import of CCS Configurations at Operator

	_ is derived by: SPT2TS-122401 - Support an easy import of BB Configurations at Integrator _ is derived by: SPT2TS-122400 - Support an easy export of BB Configurations at BB Supplier _ is derived by: SPT2TS-122402 - Support an easy export of CCS Configurations at Integrator _ is derived by: SPT2TS-123904 - Compile CCS Configuration

SPT2TS-127453 - Automatic notification in case of new configuration data packet

As an asset manager, I want to get an automated notification when new configuration data packets area available, in order to know the deployment strategy has to be completed.

Linked Work Items	is derived from: SPT1RS-220 - overall CAPEX/OPEX optimisation(2) is derived from: SPT1RS-237 - efficient migration based on adaptable systems is derived from: SPT1RS-198 - automate lifecycle processes, independent lifecycle is derived from: SPT1RS-189 - Changeability and upgradeability(2) has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122390 - Support an easy import of CCS Configurations at Operator _ is derived by: SPT2TS-122401 - Support an easy import of BB Configurations at Integrator _ is derived by: SPT2TS-123904 - Compile CCS Configuration

SPT2TS-49113 - Automatic distribution of data packet from building block supplier

As a CCS building block supplier, I want to have an automated distribution of a new configuration data packet release, in order to simplify the deployment process towards my customers. Furthermore, I want my customers to be aware of a new release of my product, so that they adopt it for the field.

Note: It is not about sending the new configuration data packet directly to a component for activation and installation. The distribution is from the environment of the building block supplier to the controlled environment of his customer.

Rationale: as a CCS building block supplier I have an interest that my customers operate the latest release of my product, as this contains bug fixes, security patches, new functions, etc. If latest release is adopted, I have less issues of my field components and can possibly benefit of new features.

Linked Work Items	is derived from: SPT1RS-227 - Flexible incorporation of innovations is derived from: SPT1RS-255 - roll out innovation is derived from: SPT1RS-237 - efficient migration based on adaptable systems is derived from: SPT1RS-198 - automate lifecycle processes, independent lifecycle is derived from: SPT1RS-189 - Changeability and upgradeability(2) has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-122401 - Support an easy import of BB Configurations at Integrator _ is derived by: SPT2TS-122400 - Support an easy export of BB Configurations at BB Supplier _ is derived by: SPT2TS-123904 - Compile CCS Configuration _ is derived by: SPT2TS-124129 - Verify BB Configuration from BB Supplier

SPT2TS-63817 - No or only loose coupling between configuration data packet release and operational data

As a CCS integrator or entity in charge or maintenance, I want to have high orthogonality (no or only a loose coupling) between a specific configuration data packet release (static data) and the - operational - dynamic data (e.g. moving authority, journey profile, etc.), in order to prevent a too high complexity in the maintained system, ensure scalability (if the CCS system is growing, the resources needed to maintain it are not growing exponentially) and be more efficient.

Note: The intention is that a specific configuration data packet release (e.g. software update) has no or only loose dependency to operational data (e.g. moving authority, or ATO journey profile) received by the same component. This means that the integrator can mainly concentrate on the integrity of the system he is responsible for, and do not have to also consider the integrity with operational data received during operation. The latter could mean the integrator would have to ensure that at a certain point in time the component is running a specific software version and only then a moving authority in a new format is sent to the specific component (not before that point in time).

Linked Work Items	is derived from: SPT1RS-226 - systems: extensible capacity, scalability(2) is derived from: SPT1RS-238 - simplify certificates and their impacts is derived from: SPT1RS-237 - efficient migration based on adaptable systems is derived from: SPT1RS-220 - overall CAPEX/OPEX optimisation(2) is derived from: SPT1RS-241 - efficient decision and working methodolog has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-124150 - Be backwards compatible for other than the statical configuration data _ is derived by: SPT2TS-122389 - Support loading procedure for distribution jobs

SPT2TS-124023 - Automated configuration process for a replacement unit

As an entity in charge of maintenance, I want that a replacement unit (a unit put in operation to replace another defect unit) performs automatically a configuration activation and installation process to provide the same functionality and have the same behaviour as the replaced unit, in order to have a leaner and less error prone maintenance process.

Note: It is understood that in order to perform the automated configuration activation and installation process some basic parametrisation (e.g. setting of the component unique identifier, network settings, etc.) needs to be applied. How the basic parametrisation is achieved, can be a supplier specific solution.

Linked Work Items	is derived from: SPT1RS-193 - automate lifecycle processes is derived from: SPT1RS-192 - reusable right first time work is derived from: SPT1RS-208 - automated field force communication is derived from: SPT1RS-203 - operations/maintenance: assisted systems is derived from: SPT1RS-238 - simplify certificates and their impacts has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-124026 - Perform automated configuration activation and installation for a replacement unit _ is derived by: SPT2TS-124277 - Perform automated import of basic parametrisation for a replacement unit

SPT2TS-124024 - Protection of keys / certificates in defect units

As an entity in charge of maintenance, I want that a defect unit being replaced in the field has implemented protection measures preventing a complex unit logistics (storage only in dedicated lockers or secured environment, etc.), in order to have leaner and more efficient logistic processes.

Note: storage only in dedicated lockers or secured environment is requested to prevent malicious tampering/manipulation or key / certificate extraction (download, read out, removal, etc.).

Linked Work Items	is derived from: SPT1RS-197 - overall CAPEX/OPEX optimisation(1) is derived from: SPT1RS-212 - non invasive/noticeable cyber security has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-124025 - Prevent access to secure data stored and used in a failing unit

SPT2TS-124459 - Define backwards compatible and 'future proof' interfaces

As an entity in charge of maintenance or as CCS integrator, I want that the interfaces between different units are backwards compatible and 'future proof', in order to reduce the complexity in the lifecycle management. This is based on the experience that interfaces will always evolve (for instance new variables are introduced). Basically, the interfaces should be adaptable. Furthermore, this feature provides investments protection.

Note: if the interfaces do not fulfil this operational epic there is an issue when updating different units communicating with each other. When installing an update on one unit that affects the interface, one has to synchronise the update of the other unit communicating with it, in order to ensure that the communication between the two units can still be established. This activity can become quite complex if a large number of units is being involved.

Linked Work Items	is derived from: SPT1RS-235 - viable forward/backward compatibility is derived from: SPT1RS-234 - viable migration path has parent: SPT2TS-1387 - Generally valid epics _ is derived by: SPT2TS-124471 - All building block interfaces are 'future proof' and backwards compatible.

4.2 Track side stakeholder related epics

SPT2TS-1391 - An update for CCS trackside components is in operational mode within 1 week

As an IM entity in charge of maintenance, I want that a specific update is going into operation (distribution and activation) within 1 week (this means not later than 1 week - e.g. bug fix update is operational not later than 1 week after the update has been released for mass distribution, of course this can be faster), in order to have a more efficient update process and a more homogenous asset of CCS field components (all CCS field components of the same type run with the same configuration version).

Note I: maximum duration of 1 week for an update to be in operation after release for mass distribution is based on some suppositions:

- The CCS trackside field components are always in operation (24/7), only exceptionally not operational.
- It is assumed that data distribution from start of distribution at the centralised server until the update is available on a CCS trackside field component takes not more than 1 week.
- The activation / installation and going into operation takes not more than 2 hours (relatively limited maintenance / update window). So in theory it is 1 week + 2 hours, this has been rounded to not more than 1 week.
- As recognisable from the figures above the distribution may consume most of the available time, while the activation (once the update has been distributed to all components) might take far less time.

Note II: The process is scalable, this means the time for the update to be in operation is the same independently of the railway network size.

Rationale: today, due to the long time to have an update operational (distributed and activated/installed in the field, e.g. on all interlocking blocks), the same CCS field components often have different configuration versions over a long period of time (several months up to years). This situation makes operations more complex: the configuration base needs to be verified several times, behaviour might be different between configuration versions and therefore needs to be considered when analysing issues, workarounds need to be kept in operation for longer time and differently at different locations, technicians need to be familiar with a larger number of variants, new functions take longer for being operational, etc..

Linked Work Items	is derived from: SPT1RS-236 - reduce time to market is derived from: SPT1RS-188 - Changeability and upgradeability(3), simpilified integration is derived from: SPT1RS-190 - Changeability and upgradeability(1) is derived from: SPT1RS-227 - Flexible incorporation of innovations is derived from: SPT1RS-203 - operations/maintenance: assisted systems has parent: SPT2TS-1394 - Track side stakeholder related epics _ is derived by: SPT2TS-124187 - Distribution of a new CCS Configuration to a CCS trackside building block takes less than 1 week _ is derived by: SPT2TS-124190 - Activation / installation of a new CCS Configuration in a CCS trackside building block takes less than 2 hours. _ is derived by: SPT2TS-124204 - Scalable distribution process for new CCS Configuration to CCS trackside building blocks _ is derived by: SPT2TS-122389 - Support loading procedure for distribution jobs _ is derived by: SPT2TS-124162 - Compile Distribution Job

SPT2TS-1395 - Deployment of new keys to RBCs

As an IM security manager, I want to be able to deploy within 24 hours new cryptographic keys (scope of SS-114 / SS-137) to to the Traffic CS System (today all RBCs) in operation, in order to respond to a cyber attack to the CCS system.

Note: It has to be analysed how the configuration management process addressed by TCCS-SD3 can be aligned to what is already standardized in SUBSET-137.

Linked Work Items	is derived from: SPT1RS-226 - systems: extensible capacity, scalability(2) is derived from: SPT1RS-221 - standardized architecture(1) is derived from: SPT1RS-190 - Changeability and upgradeability(1) is derived from: SPT1RS-191 - changeability has parent: SPT2TS-1394 - Track side stakeholder related epics _ is derived by: SPT2TS-122394 - Ensure only authorised configuration data packets are activated and installed _ is derived by: SPT2TS-122399 - Support update of digital certificates _ is derived by: SPT2TS-122390 - Support an easy import of CCS Configurations at Operator _ is derived by: SPT2TS-122393 - Ensure only configuration data packets from trusted sources are activated and installed _ is derived by: SPT2TS-122389 - Support loading procedure for distribution jobs _ is derived by: SPT2TS-124164 - Associate Distribution Jobs

SPT2TS-1648 - Deployment of cyber security updates to trackside components in a timely manner

As a IM security manager, I want to deploy cyber security updates within 24 hours to all trackside components in operation, in order to respond to a cyber security attack in a timely manner.

Note: the 24 hours are clocked from the point in time where the patch distribution is triggered from remote until the patch is activated in the relevant components.

Linked Work Items	is derived from: SPT1RS-232 - simplified standard safety components is derived from: SPT1RS-213 - local environment cyber security is derived from: SPT1RS-189 - Changeability and upgradeability(2) has parent: SPT2TS-1394 - Track side stakeholder related epics _ is derived by: SPT2TS-122395 - Freedom from interference and documented separation of safety related and non-safety related functions _ is derived by: SPT2TS-122394 - Ensure only authorised configuration data packets are activated and installed _ is derived by: SPT2TS-122391 - Support generation of many distribution jobs in parallel _ is derived by: SPT2TS-122390 - Support an easy import of CCS Configurations at Operator _ is derived by: SPT2TS-122393 - Ensure only configuration data packets from trusted sources are activated and installed _ is derived by: SPT2TS-122389 - Support loading procedure for distribution jobs _ is derived by: SPT2TS-124163 - Augment CCS Manifest with Distribution Job parameters

4.3 On Board stakeholder related epics

SPT2TS-49111 - An update for CCS on-board components is in operational mode within 2 weeks

As an RU entity in charge of maintenance, I want that a specific update is going into operation (distribution and activation) within 2 weeks (this means not later than 2 weeks - e.g. bug fix update is operational on a specific fleet not later than 2 weeks after the update has been released for mass distribution, of course this can be faster), in order to have a more efficient update process and a more homogenous asset of CCS field components (all CCS field components of the same type run with the same configuration version).

Note I: maximum duration of 2 weeks for an update to be in operation after release for mass distribution is based on some suppositions

- The CCS on-board components are not always in operation (not 24/7), sometimes the vehicles are not operational (also not powered).
- It is assumed that data distribution from start of distribution at the centralised server until the update is available on a CCS on-board component takes not more than 10 days, if the vehicle is in regular operation.
- To have a suitable activation / maintenance window takes not more than 4 days, if the vehicle is in regular operation.
- The installation and going into operation takes not more than 2 hours. So in theory it is 10 days + 4 days + 2 hours, this has been rounded to not more than 2 weeks.
- CCS on-board components of vehicles undergoing a mid-life renewal, or other long lasting taking out of operation processes, might not be operational for a period of time longer than 2 weeks. The requested time target is not applicable to such CCS on-board components.

Note II: The process is scalable, this means the time for the update to be in operation is the same

independently of the fleet size: 3 or 30 or 300 vehicles.

Rationale: today, due to the long time to have an update operational (distributed and activated/installed in the field, e.g. on all vehicles of a specific fleet), the same CCS field components often have different configuration versions over a long period of time (several months up to years). This situation makes operations more complex: the configuration base needs to be verified several times, behaviour might be different between configuration versions and therefore needs to be considered when analysing issues, workarounds need to be kept in operation for longer time and differently for different vehicles, technicians need to be familiar with a larger number of variants, new functions take longer for being operational, etc..

Linked Work Items	is derived from: SPT1RS-188 - Changeability and upgradeability(3), simpilified integration is derived from: SPT1RS-190 - Changeability and upgradeability(1) is derived from: SPT1RS-203 - operations/maintenance: assisted systems is derived from: SPT1RS-227 - Flexible incorporation of innovations is derived from: SPT1RS-236 - reduce time to market is derived from: SPT1RS-226 - systems: extensible capacity, scalability(2) has parent: SPT2TS-1396 - On Board stakeholder related epics _ is derived by: SPT2TS-124191 - Distribution of a new CCS Configuration to a CCS on-board building block takes less than 10 days _ is derived by: SPT2TS-124192 - Activation / installation of a new CCS Configuration in a CCS on-board building block takes less than 2 hours. _ is derived by: SPT2TS-124203 - Scalable distribution process for new CCS Configuration to CCS on-board building blocks _ is derived by: SPT2TS-122389 - Support loading procedure for distribution jobs _ is derived by: SPT2TS-124162 - Compile Distribution Job

SPT2TS-1397 - Deployment of new keys to CCS on-board equipment

As a RU security manager, I want to deploy within 72 hours new cryptographic keys (scope of SS-114 / SS-137) to all CCS on-board equipment in operation, in order to respond to a cyber attack to the CCS system.

Note: It has to be analysed how the configuration management process addressed by TCCS-SD3 can be aligned to what is already standardized in SUBSET-137.

Linked Work Items	is derived from: SPT1RS-190 - Changeability and upgradeability(1) is derived from: SPT1RS-191 - changeability is derived from: SPT1RS-221 - standardized architecture(1) is derived from: SPT1RS-226 - systems: extensible capacity, scalability(2) has parent: SPT2TS-1396 - On Board stakeholder related epics _ is derived by: SPT2TS-122394 - Ensure only authorised configuration data packets are activated and installed _ is derived by: SPT2TS-122399 - Support update of digital certificates _ is derived by: SPT2TS-122390 - Support an easy import of CCS Configurations at Operator _ is derived by: SPT2TS-122393 - Ensure only configuration data packets from trusted sources are activated and installed _ is derived by: SPT2TS-122389 - Support loading procedure for distribution jobs _ is derived by: SPT2TS-124164 - Associate Distribution Jobs

SPT2TS-1647 - Deployment of cyber security updates to vehicles in a timely manner

As a RU security manager, I want to deploy cyber security updates within 24 hours to all vehicles in operation, in order to respond to a cyber security attack in a timely manner.

Note: the 24 hours are clocked from the point in time where the patch distribution is triggered from remote until the patch is activated in the relevant components.

Linked Work Items	is derived from: SPT1RS-232 - simplified standard safety components is derived from: SPT1RS-213 - local environment cyber security is derived from: SPT1RS-189 - Changeability and upgradeability(2) has parent: SPT2TS-1396 - On Board stakeholder related epics _ is derived by: SPT2TS-122395 - Freedom from interference and documented separation of safety related and non-safety related functions _ is derived by: SPT2TS-122394 - Ensure only authorised configuration data packets are activated and installed _ is derived by: SPT2TS-122391 - Support generation of many distribution jobs in parallel _ is derived by: SPT2TS-122390 - Support an easy import of CCS Configurations at Operator _ is derived by: SPT2TS-122393 - Ensure only configuration data packets from trusted sources are activated and installed _ is derived by: SPT2TS-122389 - Support loading procedure for distribution jobs _ is derived by: SPT2TS-124163 - Augment CCS Manifest with Distribution Job parameters

SPT2TS-1398 - One single service point on-board

As an RU entity in charge of maintenance responsible for a fleet, I want to have one single access point on-board the vehicles (connector, service point) from where the technicians can interact with all different CCS and non-CCS on-board components, this in order to simplify the access for the people working on-board.

Note: from remote there is logically one service point, for the remote user / operator it does not matter if technically one or more communications channels are used as long as he can execute all his activities out of one remote server application.
Locally the technician does not want to physically have to connect his service notebook to different connectors (located at different places, possibly with large distances between each other) depending on what activity he has to execute.

Linked Work Items	is derived from: SPT1RS-221 - standardized architecture(1) has parent: SPT2TS-1396 - On Board stakeholder related epics _ is derived by: SPT2TS-122397 - Provide local configuration (update) capability _ is derived by: SPT2TS-122420 - In vehicles only one common local service point for all different on-board systems

5 Status of the work, open points, issues

High level concept description for the configuration management

In order to define the System Requirements with regard to the CCS configuration management process we need to develop a high level process describing the different involved actors, how these actors interact between each other and with the system. This high level concept is the basis to define the System Requirements for the CCS system.

It has to be clarified which Domain in SP attacks the formal safety certification and homologation process

During the weekly meeting on 27.04.2023 it was agreed that the configuration management with regard to formal safety certification and homologation process is not in the scope of TCCS-SD3 (Configuration). This SD3 is attacking the configuration management process from a technical perspective.
It has been recognised that the technical separation of non-safety related changes (e.g. network and security related changes) compared to safety related changes within the same building block needs to be addressed by the building block supplier --> This capability needs to be supported by future building block.
Beside the technical implementation also the the formal safety certification and homologation process needs to be attacked, more specifically for the very lean and light installation of non-safety related CCS configurations (e.g. network and security related changes).
Question to the domain lead: which domain will attack this topic within the System Pillar? At a certain point in time we will need to align with this domain. Answer on 16.08.2024: allegedly the topic is in the scope of PRAMS.
Possibly this question needs to be aligned with Core-group.

6 Tables

Please update the table of figures.

Please update the table of figures.

7 Document checklist, open points, issues

Checklist Render Error: The document checklist custom field 'docChecklist' is not of type 'Text' but it is: PrimitiveTypetypeName=java.lang.String, subtype=null. (or the custom fields is not defined). Please, configure this custom field properly.