D1 CONEMP for CCS

Abstract	This document is a template for the Stakeholder Requirements deliverable which is required per EN 50126-1:2017 - phase 2 for a system under consideration.
Config Item	Document Template
Document ID	30 TCCS Deliverables/D1 CONEMP for CCS#903320 D1 CONEMP for CCS
Classification	EURAIL-internal
Status	Open
Version	0.2
Revision	903320
Last Change Date	2026-06-02

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

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

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

Type of Approval	Document Review
Comments	
Approvals	
Attachments	

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

Type of Approval	Document Approval
Comments	
Approvals	
Attachments	

Table of contents

1 Preamble 6
1.1 Purpose 6
1.2 Intended Audience 7
1.3 Glossary 7
1.3.1 Terms 7
1.3.2 Abbreviations 7
2 Inputs and Stakeholders 8
2.1 Inputs 8
2.2 Stakeholders and Operational roles 8
2.2.1 Stakeholders 8
2.2.2 Operational Actors/Entities 9
2.3 Operational Assumptions 10
2.4 Operational Requirements 10
3 Harmonisation scope proposal 11
3.1 Lifecycle definition (Commissioning - Decommissioning) 11
3.2 Analysis basis and method 11
3.3 Scope Analysis Result 12
3.3.1 Installation (Commissioning) 13
3.3.2 Maintenance (Operation & Upkeep) 13
3.3.3 Change (Modifications and Enhancements) 14
3.3.4 Incident Management (Troubleshooting) 14
3.3.5 Decommissioning (Disposal and Retirement) 15
3.4 Proposed Scope for Harmonisation 16
3.4.1 Installation (Commissioning) 16
3.4.2 Maintenance (Operation & Upkeep) 17
3.4.3 Change (Modifications and Enhancements) 18
3.4.4 Incident Management (Troubleshooting) 19
3.4.5 Decommissioning (Disposal and Retirement) 20
4 Operational Process Definition 21
4.1 First Commissioning of a device (LRU) for Trackside 21

4.1.1 Operational activities . . . 22
4.2 First Commissioning of a System for Trackside . . . 23
4.2.1 Operational activities . . . 24
4.3 First Commissioning of a System for OnBoard . . . 25
4.3.1 Operational activities . . . 26
4.4 Update of an existing System for Trackside . . . 27
4.4.1 Operational activities . . . 28
4.5 Update of an existing System for OnBoard . . . 28
4.6 Generic process for physical modification of existing track (Trackside) . . . 29
4.6.1 Operational activities . . . 31
4.7 Update Topology Data (Trackside) . . . 31
4.7.1 Operational activities . . . 33
4.8 Replacement of a broken LRU (trackside) . . . 33
4.8.1 Operational activities . . . 35
4.9 Replacement of a broken LRU (OnBoard) . . . 36
4.10 Decommissioning of a LRU (Trackside) . . . 36
4.10.1 Operational activities . . . 37
4.11 Decommissioning of a LRU (OnBoard) . . . 37
4.12 Decommissioning of a System (Trackside) . . . 37
4.12.1 Operational activities . . . 38
4.13 Perform System Asset Diagnosis for Trackside . . . 39
4.14 Perform System Asset Diagnosis for Onboard . . . 39
5 Exported Constraints and External Requirements . . . 39
6 Consistency with SL3-SL5 architecture and functions . . . 39
7 Appendix . . . 40
7.1 Standards and references . . . 40

1 Preamble

1.1 Purpose

Purpose

Deliverable D1 “Concept of Employment (CONEMP) for CCS” defines the Operational Target Concept for CCS CONEMP processes across the full lifecycle including; installation, maintenance, change, incident management, and decommissioning and covering both Trackside and Onboard.
It consolidates and aligns the existing operational analysis (e.g., Traffic CS, Train CS, TCCS, TACS) into one consistent operational concept, ensuring a shared understanding of how CCS is intended to be deployed, operated and supported.

The purpose of D1 is to translate business objectives into target operational processes and to establish a harmonized operational solution design that balances interoperability ambitions with legacy and diversity constraints. D1 also serves as the baseline for standardized operational and stakeholder requirements, including requirements that must be “exported” to external processes (e.g., Data Preparation and Validation), and ensures operational consistency with transversal functions (configuration and diagnostics) and the computing environment.

D1 enables and documents key decisions required to proceed with system analysis and subsequent specifications, including in particular:

- Harmonization scope and ambition level: which CONEMP processes will be harmonized (and to what extent), for Trackside and Onboard.
- Prioritization of harmonization candidates: evaluation and ranking of process areas to be standardized first, based on benefits, risks, and feasibility.
- Target operational process definitions: agreed end-to-end process descriptions, including roles, responsibilities, interfaces, and operational activities.
- Requirements baseline and traceability: derivation and maintenance of standardized operational and stakeholder requirements, with traceability to CBOs.
- Alignment needs for specifications and models: identification of required updates to SL3–SL5 specifications.

As such, D1 provides the approved operational reference point for CCS CONEMP processes that guides downstream system analysis activities, specification updates, and stakeholder alignment.

1.2 Intended Audience

Any EU-Rail System Pillar members and volunteers

Any EU-Rail System Pillar members and volunteers

1.3 Glossary

1.3.1 Terms

No references

1.3.2 Abbreviations

2 Inputs and Stakeholders

2.1 Inputs

Source artefacts to reuse and integrate

Input	Link	Source
CONEMP - Scope Analysis	D1 CONEMP - Scope Analysis	CONEMP Domain
Operational analysis for "Activate Configuration Data"	S2 t35 - 400 Activate Configuration Data	OD, Traffic CS, CONEMP
CONEMP - Configuration and diagnosis	TCCS CONEMP - Configuration and Diagnostics	CONEMP Domain
Configuration Operational Epics	TCCS Configuration - Operational Epics	CONEMP Domain
Configuration High Level Concept	TCCS Configuration - High Level Concept	CONEMP Domain
Diagnostics Operational Analysis	TCCS SD2 - Operational Analysis	CONEMP Domain
Diagnostics Operational Epics	TCCS SD2 - Operational Epics	CONEMP Domain

2.2 Stakeholders and Operational roles

2.2.1 Stakeholders

Stakeholder

Stakeholder in this context is an individual, organisation or institution that can affect or be affected by the railway system.

Operator

Operator is an institution operating a system through its life-cycle, in context of the document usually an Infrastructure Manager or Railway Undertaking (Train Operator).

Infrastructure Manager

Infrastructure Manager is the main rail responsible for the operation, planning, development, consistency and enhancement of the national rail network it owns.

Supplier

Supplier is a person or company that supplies another company with certain goods. The supplier will therefore provide the company with the inputs necessary for production. The company will use them to transform them into outputs. The final output can be provided directly by the supplier.

Railway Undertaking

Railway Undertaking is the entity in charge of operating train in safe and available conditions.

2.2.2 Operational Actors/Entities

CCS Trackside refers to the trackside counterpart of the CCS architecture. CCS trackside consists of all the trackside systems required to perform railway operations.

Data Preparation is responsible to prepare and validate Configuration Data required by the CCS system. This system encompasses the contributions of three types of stakeholders:
Infrastructure Manager: Provides infrastructure related Configuration Data, such as track topology.
Railway Undertaking: Provides Vehicle related Configuration Data, such as static train/vehicle characteristics used for the parametrisation of the CCS on-board.
Supplier: Delivers application specific Configuration Data, such as hardware configurations or software parameters for onboard or wayside components as well as software Configuration Data such as executable binary files.

Configuration Manager is responsible to manage and supervise the distribution of Configuration Data published by Integrators for CCS system. This role is also responsible for producing the distribution-job defining the target and when to preload and activate Configuration data. In this context it is usually an Infrastructure Manager or Train Operator/Owner

Planning Department is responsible for all planning activities including producing an operational plan, based upon the operational state and operational events. A conflict free operational plan would be sent to CCS Trackside usually at the beginning of a service day. Change of planning can be done for the next minutes up to the next year. A plan includes regular or incidence-related commands for infrastructure users (e.g. trains, construction sites), including measures to correct deviations or to stabilize the traffic flow in short term

Security Manager is responsible for security commissioning process for any new Configuration Data.

The field force is the single point of contact when maintenance activity or construction work is carried out in the field, e.g. this actor is responsible for the safety of the staff in the field.

The Signaller supervises the trains in normal operation and controls the operation of trains in degraded situations

2.3 Operational Assumptions

Planned operational restrictions for changes/updates

Changes (including configuration updates, software updates, and other approved modifications) are assumed to be planned in advance with the required operational restrictions defined upfront (e.g., maintenance window, limited speed restriction, track closure, activation of a working area..etc). A dedicated change slot (activation time) is assumed to be agreed to enable controlled implementation and to minimize impact on operations.

External processes executed in parallel or upfront

Activities belonging to external processes (e.g., construction, civil works, site preparation, or other infrastructure-related preparatory activities) are assumed to run in parallel or ahead of the CONEMP operational processes, under their own definitions and conditions. These activities are treated as prerequisites for the operational lifecycle steps covered in this deliverable.

Non intrusive monitoring and diagnostics

Monitoring and diagnostics capabilities for determining the health and status of the system are assumed to be designed and operated such that they do not interfere with operational service (e.g., passive monitoring and diagnostics). Diagnostic and monitoring data collection is therefore treated as an operational support function that does not impact the operation directly.

2.4 Operational Requirements

Operational production procedures shall allow for automated regulation of rail traffic and of deployment of CCS resources.
All the operational production needs, such as the use of available technical/physical or human resources shall be regulated with automation.

The use of infrastructure resources between train traffic and of other operational production needs - such as human or technical/physical resources availability, maintenance routines, construction management, commissioning or incidents management - shall be optimised to extract the closest possible results in relation to the planned service offer, based on the available operating state information.

3 Harmonisation scope proposal

This chapter translates the results of the D1 CONEMP - Scope Analysis into a decision-ready proposal for what to harmonise across CCS for Trackside and Onboard. Harmonisation is structured along the operational lifecycle from commissioning to decommissioning to ensure coverage of end-to-end operational responsibilities. In addition, the scoping is shaped by CONEMP domain scope activities that cut across multiple lifecycle steps which is :

- Data Standardisation,
- Configuration Management, and
- Diagnostics/Monitoring.

3.1 Lifecycle definition (Commissioning - Decommissioning)

Lifecycle phases

For the purpose of this CONEMP deliverable, the operational lifecycle is defined as the following sequence of steps.

Each step is understood as an operational phase that can contain multiple sub-processes and interfaces.

Figure 1 EU CONEMP process (lifecycle)

3.2 Analysis basis and method

Analysis Method

The harmonisation candidates in this chapter are derived from the scope analysis method defined in D 1 CONEMP - Scope Analysis . The evaluation follows a consistent three-step approach, applied to each sub-activity within the lifecycle phases:

1.Relevancy for Railway :

For each sub-activity from the generic standard (EU CONEMP process), it is assessed whether the topic is relevant for CCS railway operations in general. Non-relevant items are excluded from further harmonisation consideration.

2.Scope of System Pillar:

For sub-activities deemed relevant for railways, it is assessed whether the topic is in scope or out of scope for System Pillar standardisation. Out-of-scope items are documented explicitly as excluded and do not become harmonisation candidates.

3.Mapping to CONEMP domain (with intentional references to later design phases):
For sub-activities that are both relevant and within System Pillar scope, a mapping is established to the appropriate CONEMP activity. By intention, the mapping may refer to concrete elements of later design phases (e.g., **SL5**) to provide implementable examples and ensure that scope proposals remain technically actionable and traceable into existing work activities.

To keep the scope realistic and useful, the harmonisation candidates are assessed and prioritised based on criteria covering the expected operational benefit, criticality and the readiness of prerequisites (e.g. availability of input from Stakeholders).

The resulting prioritisation supports a realistic standardisation goal and scope: items with high benefit and available prerequisites are addressed first, while items with high benefit but significant dependencies on other Stakeholders inputs are planned for later phases or marked as conditional until required inputs are in place.

Prioritisation method
Harmonisation items are prioritised based on their expected operational benefit, criticality for safe and reliable railway operations, and the readiness of prerequisites required. This includes consideration of whether the necessary inputs, dependencies, and supporting conditions are already sufficiently available or whether further alignment is still needed.

- Priority 1: Items with high operational benefit and/or high criticality, for which the main prerequisites are already available or can be established with manageable effort.

- Priority 2: Items that are relevant for harmonisation but have lower immediate urgency and/or require additional prerequisites, external dependencies, or further maturation.

3.3 Scope Analysis Result

This section provides a high level overview and a summary of D1 CONEMP - Scope Analysis result. For detailed analysis and the complete assessment per activity, please refer to the Scope Analysis document.

3.3.1 Installation (Commissioning)

Installation (Commissioning):

Activities	IN/OUT	Priority
Planning and Requirements Analysis	OUT	--
Procurement and Environment Preparation	OUT	--
Physical Installation and Base Configuration	IN	Prio 1
Integration, Testing, and Acceptance	OUT	--
Documentation and Operational Handover	OUT	--
Security processes (PKI, IAM, etc.)	OUT	--

3.3.2 Maintenance (Operation & Upkeep)

Maintenance (Operation & Upkeep)

Activities	IN/OUT	Priority
Monitoring and Operations Management	IN	Prio1
Software Updates and Patch Management	IN	Prio1
Hardware Maintenance and Preventive Upkeep	OUT	--
Backup and Recovery Management	OUT	--
Security Management in Operations	OUT	--
Contract and License Management	OUT	--
Documentation and Logging	OUT	--

3.3.3 Change (Modifications and Enhancements)

Change (Modifications and Enhancements)

Activities	IN/OUT	Priority
Request for Change (RfC) and Assessment	OUT	--
Planning and Approval	OUT	--
Change Execution	IN :Implement the approved change (hardware add-on, software installation, configuration)	Prio1
Testing and Verification	IN: If problems occur, activate rollback.	Prio 2
Closure, Documentation, and Review	OUT	--
Security considerations	OUT	--

3.3.4 Incident Management (Troubleshooting)

Incident Management (Troubleshooting)

Activities	IN/OUT	Priority
Detection and Logging	IN	Prio1
Prioritisation and Categorisation	IN: Not directly/ the collected diagnostic data may support this activity	Prio2
Assignment and Diagnosis	OUT	--

Activities	IN/OUT	Priority
Resolution and Recovery:	IN: Apply corrective actions (e.g. patching, restarts, hardware swap, config fixes).	Prio1
Validation and Closure:	OUT	--

3.3.5 Decommissioning (Disposal and Retirement)

Decommissioning (Disposal and Retirement)

Activities	IN/OUT	Priority
Decommissioning Planning	OUT	--
Backup and Data Migration	OUT	--
Shutdown and Removal	IN: Uninstall s oftware, decommission virtual machines, and remove configurations	Prio2
Secure Data Erasure	IN: Delete data using certified methods (e.g. wiping tools, physical destruction):n : factory reset and certificate deleting (configuration + secuirty)	Prio2
Disposal or Return	OUT	--
Closure and Documentation	OUT	--

3.4 Proposed Scope for Harmonisation

This section outlines the prioritised list of harmonisation items. It consolidates the candidates identified from the scope analysis across the lifecycle based on the agreed evaluation.

3.4.1 Installation (Commissioning)

Physical Installation and Base Configuration

The first standardisation candidate covers "Physical Installation and Base Configuration" as part of commissioning and establishes a common operational baseline for bringing CCS equipment into service.

For the purpose of the standardisation candidate in D1, the focus is on the sub-activities “Install operating systems and baseline software” and “Configure key parameters (IP settings, domain integration, user accounts, and security measures such as firewalls and antivirus)”, as these define the minimum technical baseline that must be achieved in a consistent way before a CCS device/system can be integrated and commissioned.
The activity “Set up and connect hardware” is treated as a prerequisite: it is assumed to be completed first and is handled as a separate preceding process (not harmonized in D1 scope), since the operational target process described here starts once the equipment is physically installed and available for configuration.
In addition, a security commissioning baseline is assumed as part of the readiness conditions, meaning the system is already registered and authorised for operation, has network access enabled, and has the required operational security material (e.g., certificates/keys) in place, so that the subsequent configuration and activation steps can be executed.

The operational implementation of this candidate is detailed in the next chapter through the corresponding:
4.1 - First Commissioning of a device (LRU) for Trackside ,
4.2 - First Commissioning of a System for Trackside,
4.3 - First Commissioning of a System for OnBoard
including preconditions, postconditions and the end-to-end flow.

3.4.2 Maintenance (Operation & Upkeep)

Monitoring and Operations Management

For "Monitoring and Operations Management", the standardisation candidate focuses on establishing the diagnostic capability to continuously monitor performance, availability and overall system health across the relevant assets (e.g., systems, servers, clients, network devices, process control units and telecom systems) and to detect anomalies.
These activity focuses define what information must be available to ensure early detection of faults and timely reaction. The activity “perform capacity and performance management to pre-empt bottlenecks” is not addressed as a direct standardisation target in the context of D1 instead, the diagnostics capability is considered to support it indirectly by providing the required diagnostic and monitoring information.

The operational implementation of this candidate is detailed in the next chapter through the corresponding:
4.13 - Perform System Asset Diagnosis for Trackside
4.14 - Perform System Asset Diagnosis for Onboard
including preconditions, postconditions and the end-to-end flow.

Software Updates and Patch Management

For "Software Updates and Patch Management" the scope analysis confirms that all listed sub-activities are relevant for standardisation scope. The focus includes maintaining system and application software, applying security updates (including OS patches and firmware upgrades), and scheduling updates and major upgrades to minimize downtime, preferably within defined maintenance windows.
From an operational perspective, this also includes the controlled update of configuration data as part of the release, as well as the associated planning activities (e.g. coordination with planning department and affected stakeholders). The Standardisation target defines a harmonised update process with clear roles and steps, required prerequisites and approvals, and the necessary operational restrictions (e.g. activation of working area by signaller).

The operational implementation of this candidate is detailed in the next chapter through the corresponding:
4.4 - Update of an existing System for Trackside
4.5 - Update of an existing System for OnBoard
including preconditions, postconditions and the end-to-end flow.

3.4.3 Change (Modifications and Enhancements)

Change Execution

For "Change Execution" the standardisation candidate focuses on the sub-activity “Implement the approved change (hardware add-on, software installation, configuration)” as the operational step where an authorised change is executed in the field and brought into service under Configuration Update responsibility. This covers changes affecting infrastructure related modifications such as topology updates (e.g., adapting configuration and engineering data following a topology change) and extensions of an existing track where additional CCS elements or interfaces must be installed and configured consistently. Activities such as testing in a staging environment and general notifications/documentation are treated as out of scope in this context; the standardisation target is the controlled execution of an already approved change, including the necessary configuration updates and operational restrictions.

The operational implementation of this candidate is detailed in the next chapter through the corresponding:
4.4 - Update of an existing System for Trackside
4.5 - Update of an existing System for OnBoard
4.6 - Generic process for physical modification of existing track (Trackside)
4.7 - Update Topology Data (Trackside)
including preconditions, postconditions and the end-to-end flow.

Testing and Verification

For "Testing and Verification", the standardisation focus is limited to the sub-activity “If problems occur, activate rollback”.
In the operational target concept, a rollback does not represent a separate operational process; it is effectively the execution of an alternative, authorised update to restore the previously valid software/configuration data. The decision to trigger rollback, including its timing and conditions, remains with the responsible Configuration Manager/Operator based on the observed issues. And the rollback itself follows the same controlled update process.

The operational implementation of this candidate is detailed in the next chapter through the corresponding:
4.4 - Update of an existing System for Trackside
4.5 - Update of an existing System for OnBoard
4.6 - Generic process for physical modification of existing track (Trackside)
including preconditions, postconditions and the end-to-end flow.

3.4.4 Incident Management (Troubleshooting)

Detection and Logging

For "Detection and Logging", the standardisation candidate is limited to capability to collect diagnostic and monitoring data that reflects the health, status, and state of the CCS system and its assets. This includes the detection of incidents based on monitoring data.
The intent is to standardise what operational state and health information must be captured and made available so it can be reused across different operational scenarios (e.g., troubleshooting, maintenance actions, or operational decision making). Activities such as creating incident tickets with detailed descriptions and classifying tickets as incident/service request or security incident are not standardised within this candidate context of D1, as they are primarily part of service management and security monitoring processes and depend on organisational and tool specific practices; they are therefore treated as out of scope for this standardisation focus.

The operational implementation of this candidate is detailed in the next chapter through the corresponding:
4.13 - Perform System Asset Diagnosis for Trackside
4.14 - Perform System Asset Diagnosis for Onboard
including preconditions, postconditions and the end-to-end flow.

Prioritisation and Categorisation

For "Prioritisation and Categorisation" the scope remains aligned with the standardisation intent described for 3.4.4-1 - Detection and Logging , i.e., the provision of diagnostic and monitoring information on the health and state of assets.
While activities such as assessing impact and urgency to assign a priority and categorising tickets for routing are relevant, they are not standardised as operational processes within this candidate because they depend strongly on organisation specific service management practices and tools. Instead, the standardisation contribution is indirect: the harmonised diagnostic data and information can support consistent prioritisation and categorisation by providing standarised information.

The operational implementation of this candidate is detailed in the next chapter through the corresponding:
4.13 - Perform System Asset Diagnosis for Trackside
4.14 - Perform System Asset Diagnosis for Onboard
including preconditions, postconditions and the end-to-end flow.

Resolution and Recovery

For "Resolution and Recovery", the standardization candidate focuses on sub-activity “Apply corrective actions (e.g., patching, restarts, hardware swap, configuration fixes)” as the operational mechanism to restore the CCS service to a consistent and operationally safe state. From the D1 perspective this is primarily treated as a controlled configuration/update Process.

The operational implementation of this candidate is detailed in the next chapter through the corresponding:
4.4 - Update of an existing System for Trackside
4.5 - Update of an existing System for OnBoard
4.8 - Replacement of a broken LRU (trackside)
4.9 - Replacement of a broken LRU (OnBoard)
including preconditions, postconditions and the end-to-end flow.

3.4.5 Decommissioning (Disposal and Retirement)

Shutdown and Removal

The operational implementation of this candidate is detailed in the next chapter through the corresponding:
4.10 - Decommissioning of a LRU (Trackside)
4.12 - Decommissioning of a System (Trackside)
including preconditions, postconditions and the end-to-end flow.

Secure Data Erasure

The operational implementation of this candidate is detailed in the next chapter through the corresponding:
4.10 - Decommissioning of a LRU (Trackside)
4.12 - Decommissioning of a System (Trackside)
including preconditions, postconditions and the end-to-end flow.

4 Operational Process Definition

4.1 First Commissioning of a device (LRU) for Trackside

Op.Postcondition	- configuration data has been activated and is used by the LRU - LRU is available for production
Op.Precondition	- configuration data is available - configuration data has been authorised by the responsible authority for use in the respective LRU - LRU is already physically installed in the needed location and switched "ON" - initial configuration data is available to the device (basic data identifier (e.g. IP addresses, identifiers) - the LRU is Security commissioned
Op.Rationale	- installing a new device LRU for the first time

diagram of process activate Configuration Data (Trackside) for use case : First Commissioning of LRU

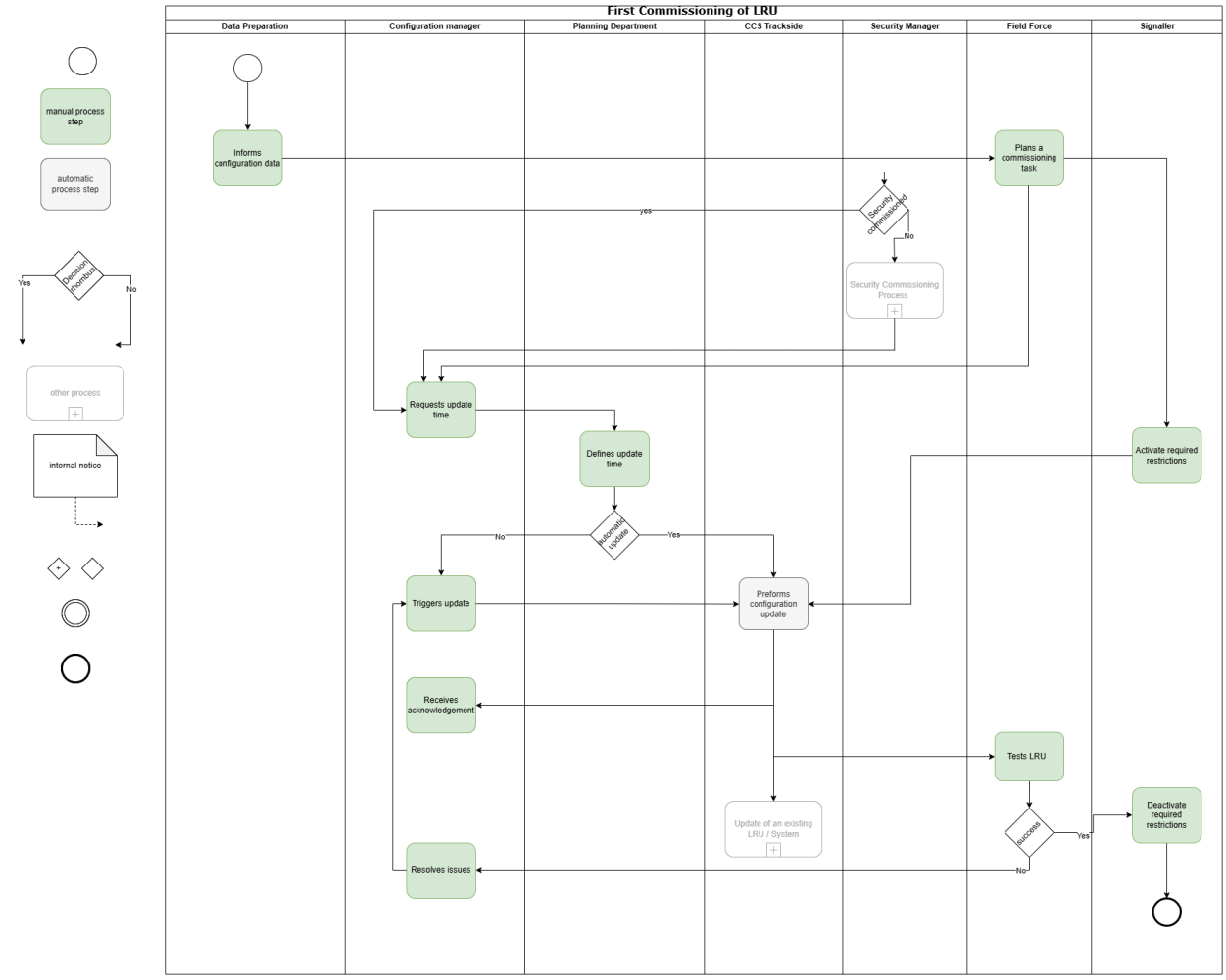

diagram template inside -> SPP-9268 - S2: Diagram template and best practices

Note for reviewers: the diagram is for visual support, the full description and main reference shall be the "operational activity" work items. **[**SPP-35389 **]**

4.1.1 Operational activities

The Data Preparation informs about new Configuration Data to be used in the CCS system. The Configuration Data is validated and authorized by the Data Preparation and ready to be used in the CCS system.

The Field Force plans the commissioning task for the affected LRU and coordinates the required on-site activities before the commissioning including the Configuration Data update can start

If not done automatically, the Configuration Manager manually triggers update of the Configuration Data when the defined time has been reached.

The Configuration Manger requests the planning department for an appropriate time slot for performing the update of the Configuration Data.

The Planning Department defines based on the needs CCS System the update Time for the Configuration Data.

.

On having all the required triggers and safety measures in place to perform the update, the CCS-System performs the update. This includes activation and deactivation of the Configuration Data.

The Signaller activates the required operational restrictions (e.g. planned temporary speed restriction/ working area) to secure the affected LRU before the configuration update activities is performed.

The Field Force tests the LRU after the configuration update/commissioning activity to verify that it works correctly before the required restrictions are deactivated.

The Signaller deactivates the required operational restrictions after the LRU has been successfully tested and the Configuration Data update activity is completed.

The Configuration Manager receives a status acknowledgement of the configuration data update process, indicating the current status, including any failures that may occur.

The Configuration Manager resolves issues identified during the configuration update or testing and coordinates the necessary corrections and if a rollback or new Configuration update is needed.

4.2 First Commissioning of a System for Trackside

Op.Postcondition	- configuration data has been activated and is used by the system - system is available for production
Op.Precondition	- configuration data is available - configuration data has been authorised by the responsible authority for use in the respective System - System is already physically installed in the needed location and switched "ON" - initial configuration data is available to the device (basic data identifier (e.g. IP addresses, identifiers) - The System is Security commissioned
Op.Rationale	- installing a new System for the first time

diagram of process activate Configuration Data (Trackside) for use case : First Commissioning of System

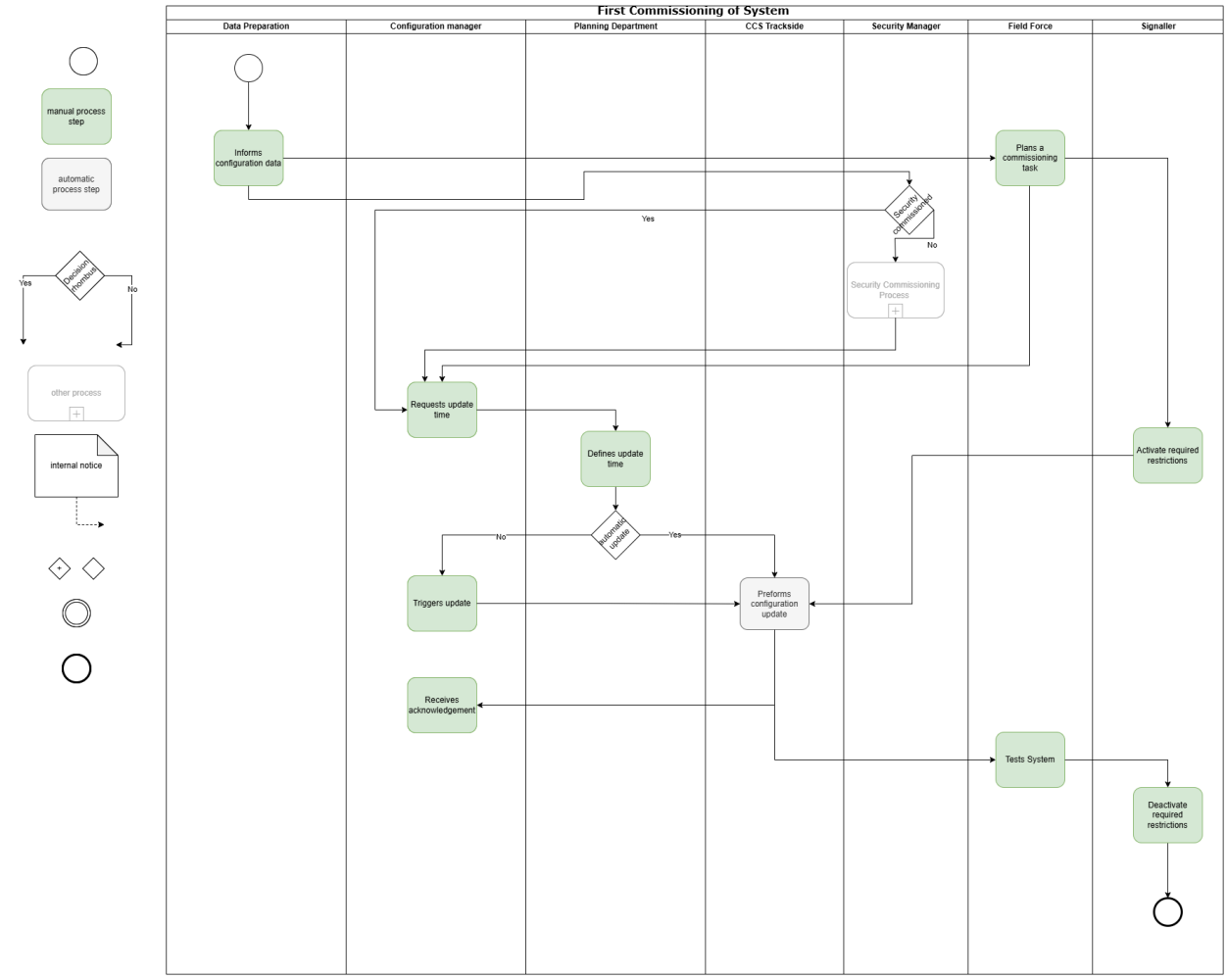

diagram template inside -> SPP-9268 - S2: Diagram template and best practices

Note for reviewers: the diagram is for visual support, the full description and main reference shall be the "operational activity" work items. **[**SPP-39968 **]**

4.2.1 Operational activities

The Data Preparation informs about new Configuration Data to be used in the CCS system. The Configuration Data is validated and authorized by the Data Preparation and ready to be used in the CCS system.

The Field Force plans the commissioning task for the affected System and coordinates the required on-site activities before the commissioning including the Configuration Data update can start.

If not done automatically, the Configuration Manager manually triggers update of the Configuration Data when the defined time has been reached.

The Configuration Manger requests the planning department for an appropriate time slot for performing the update of the Configuration Data.

The Planning Department defines based on the needs CCS System the update Time for the Configuration Data.

On having all the required triggers and safety measures in place to perform the update, the CCS-System performs the update. This includes activation and deactivation of the Configuration Data.

The Signaller activates the required operational restrictions (e.g. planned temporary speed restriction/ working area) to secure the affected System before the configuration update activities is performed.

The Field Force tests the System after the configuration update/commissioning activity to verify that it works correctly before the required restrictions are deactivated.

The Configuration Manager receives a status acknowledgement of the configuration data update process, indicating the current status, including any failures that may occur.

The Signaller deactivates the required operational restrictions after the LRU has been successfully tested and the Configuration Data update activity is completed.

4.3 First Commissioning of a System for OnBoard

First Commissioning of a System for OnBoard

Op.Postcondition	- configuration data has been activated and is used by the system - system is available for production
Op.Precondition	- configuration data is available - configuration data has been authorised by the responsible authority for use in the respective System - System is already physically installed and switched "ON" - initial configuration data is available to the System (basic data identifier (e.g. IP addresses, identifiers) - The System is Security commissioned
Op.Rationale	- installing a new System for the first time

diagram of process activate Configuration Data (OnBoard) for use case : First Commissioning of System

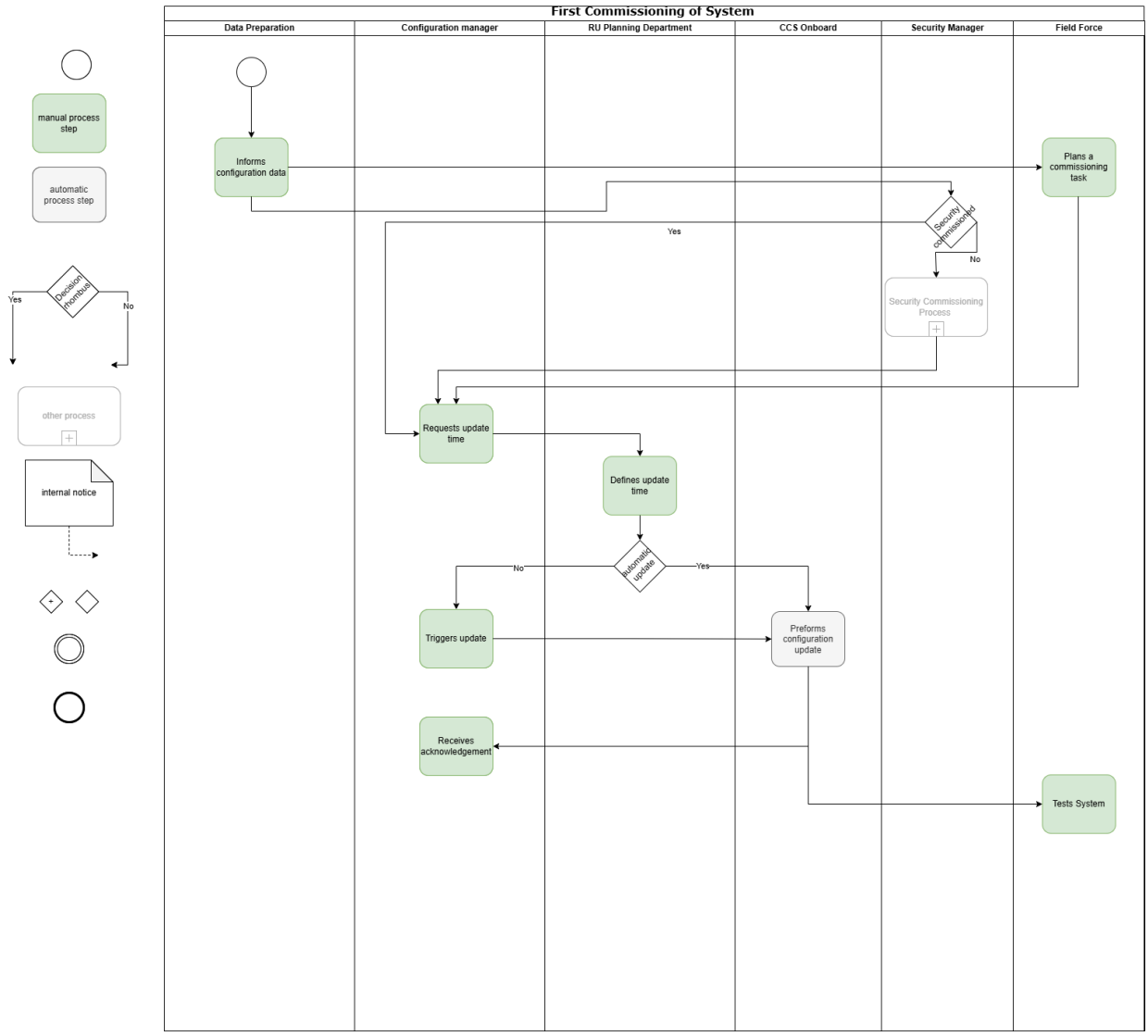

diagram template inside -> ☐ SPP-9268

Note for reviewers: the diagram is for visual support, the full description and main reference shall be the "operational activity" work items. **[**SPT2TS-132684 **]**

4.3.1 Operational activities

4.4 Update of an existing System for Trackside

Op.Postcondition	- new version configuration data has been activated and is used by the LRU/system - LRU/system is available for production
Op.Precondition	- new version configuration data is available in the system and compatible to the physical device in operation - new version configuration data has been authorised by the responsible authority for use in the System - The LRU/System is working "OK"
Op.Rationale	- updating configuration data for an existing LRU/System

diagram of process activate Configuration Data (Trackside) for use case : Update of an existing LRU / System

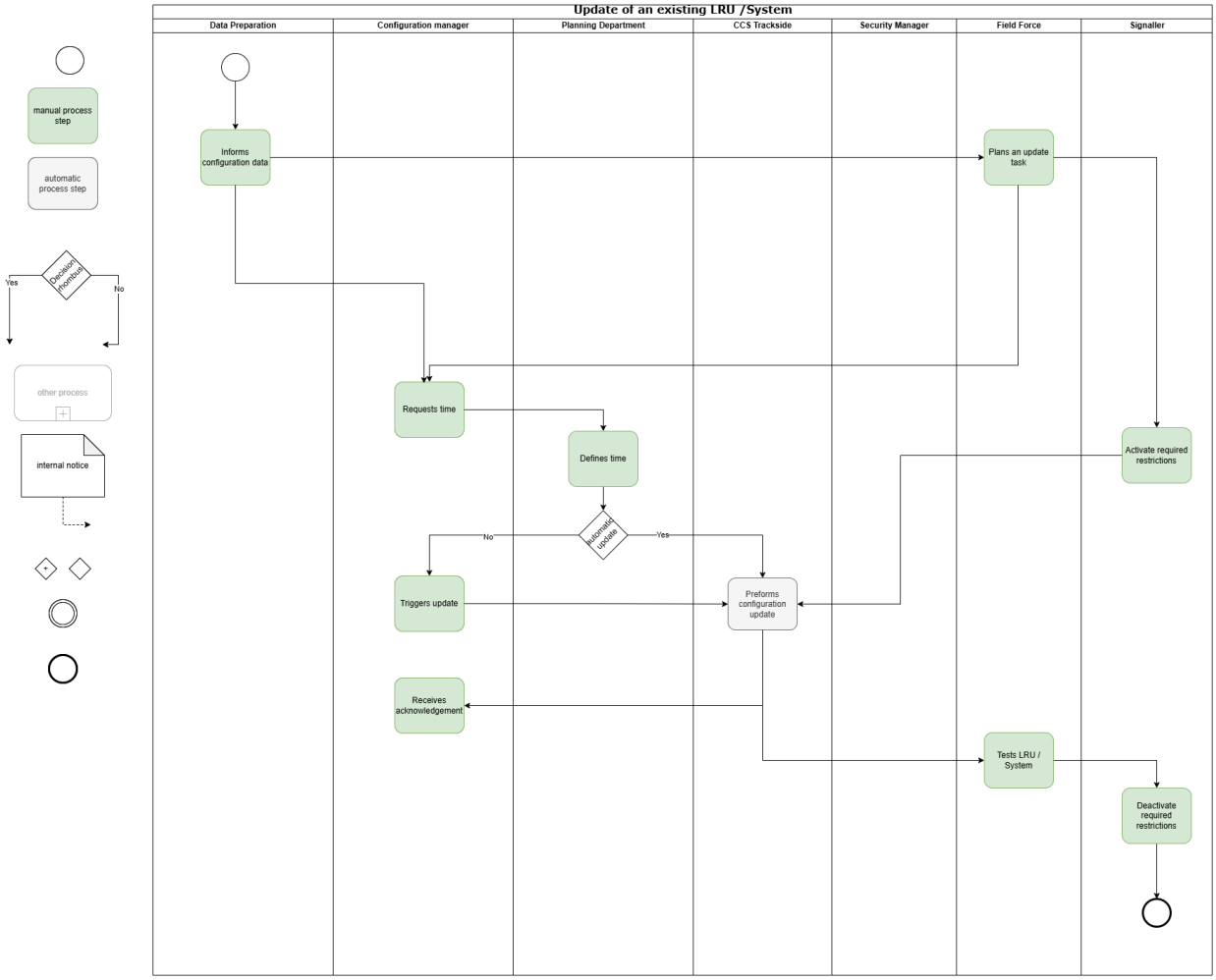

diagram template inside -> SPP-9268 - S2: Diagram template and best practices

Note for reviewers: the diagram is for visual support, the full description and main reference shall be the "operational activity" work items. **[**SPP-37545 **]**

4.4.1 Operational activities

The Data Preparation informs about new Configuration Data to be used in the CCS system. The Configuration Data is validated and authorized by the Data Preparation and ready to be used in the CCS system.

The Field Force plans the update task for the affected LRU/System and coordinates the required on-site activities before the update.

If not done automatically, the Configuration Manager manually triggers update of the Configuration Data when the defined time has been reached.

The Configuration Manger requests the planning department for an appropriate time slot for performing the update of the Configuration Data.

The Planning Department defines based on the needs CCS System the update Time for the Configuration Data.

On having all the required triggers and safety measures in place to perform the update, the CCS-System performs the update. This includes activation and deactivation of the Configuration Data.

The Signaller activates the required operational restrictions (e.g. planned temporary speed restriction/ working area) to secure the affected LRU/System before the configuration update activities is performed.

The Field Force tests the System after the configuration update activity to verify that it works correctly before the required restrictions are deactivated.

The Configuration Manager receives a status acknowledgement of the configuration data update process, indicating the current status, including any failures that may occur.

The Signaller deactivates the required operational restrictions after the LRU/System has been successfully tested and the Configuration Data update activity is completed.

4.5 Update of an existing System for OnBoard

4.6 Generic process for physical modification of existing track (Trackside)

Op.Postcondition	-new version of Topology Data has been activated and is used as the only version throughout all CCS systems - CCS system is ready for production
Op.Precondition	- Configuration Data is validated and ready to use in the system: The Data Preparation prepares all required versions of the configuration data for each construction level, including intermediate configuration states that reflect the temporary construction status of the system until the final planned state is reached.
Op.Rationale	update of the Topology Data for an existing track

Generic process for physical modification of existing track

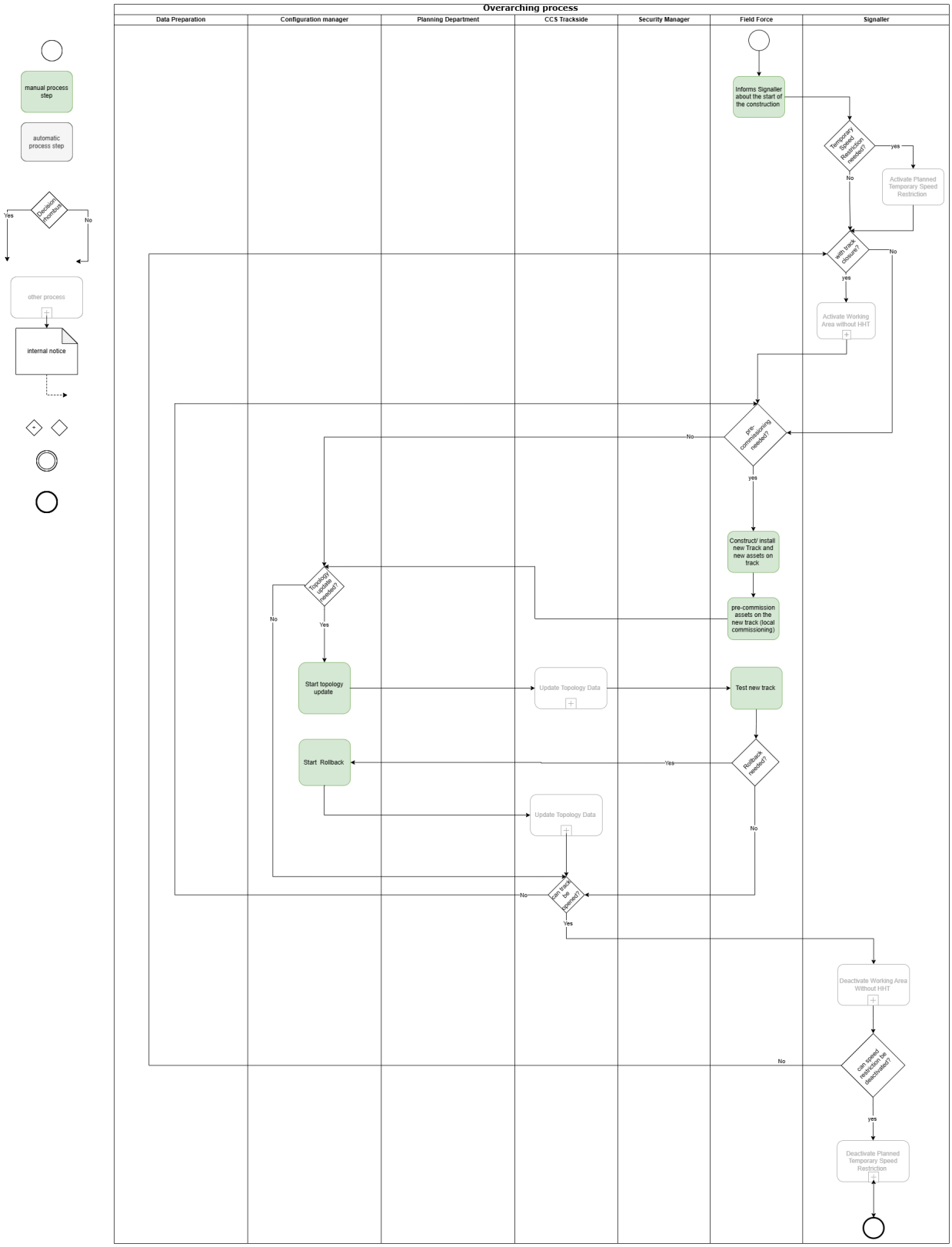

diagram template inside -> SPP-9268 - S2: Diagram template and best practices

Note for reviewers: the diagram is for visual support, the full description and main reference shall be the

"operational activity" work items. [SPP-45151]

4.6.1 Operational activities

The Field Force performs the physical construction (building) and installation of the new track and the related track assets, including setting up and connecting the necessary hardware in the field.

The Field Force performs local pre-commissioning of the new track assets in the field by installing the operating system and baseline software, configuring key technical parameters such as IP settings and domain integration, and loading preliminary certificates and security settings, for example staging certificates, using local means such as a service computer or USB stick before the final configuration is applied.

The Field Force tests the new track to ensure it meets operational and safety requirements.

The Configuration Manager initiates the topology update to reflect the planned changes in the system according to the planned Configuration Data version.

The Configuration Manager triggers a rollback to restore the previous system state if required. it is understood as rollback to the previous Configuration Data version.

The Configuration Manager receives a status acknowledgement of the configuration data update process, indicating the current status, including any failures that may occur.

4.7 Update Topology Data (Trackside)

Op.Postcondition	- new version of Topology Data has been activated and is used as the only version throughout all CCS systems - CCS system is ready for production
Op.Precondition	- new version of Topology Data has been created, validated and is ready to be used in the system CCS system is in normal mode of operation
Op.Rationale	Topology has changed, the new topology shall be used on all CCS systems and the old topology shall not be used anymore.

Update Topology Data

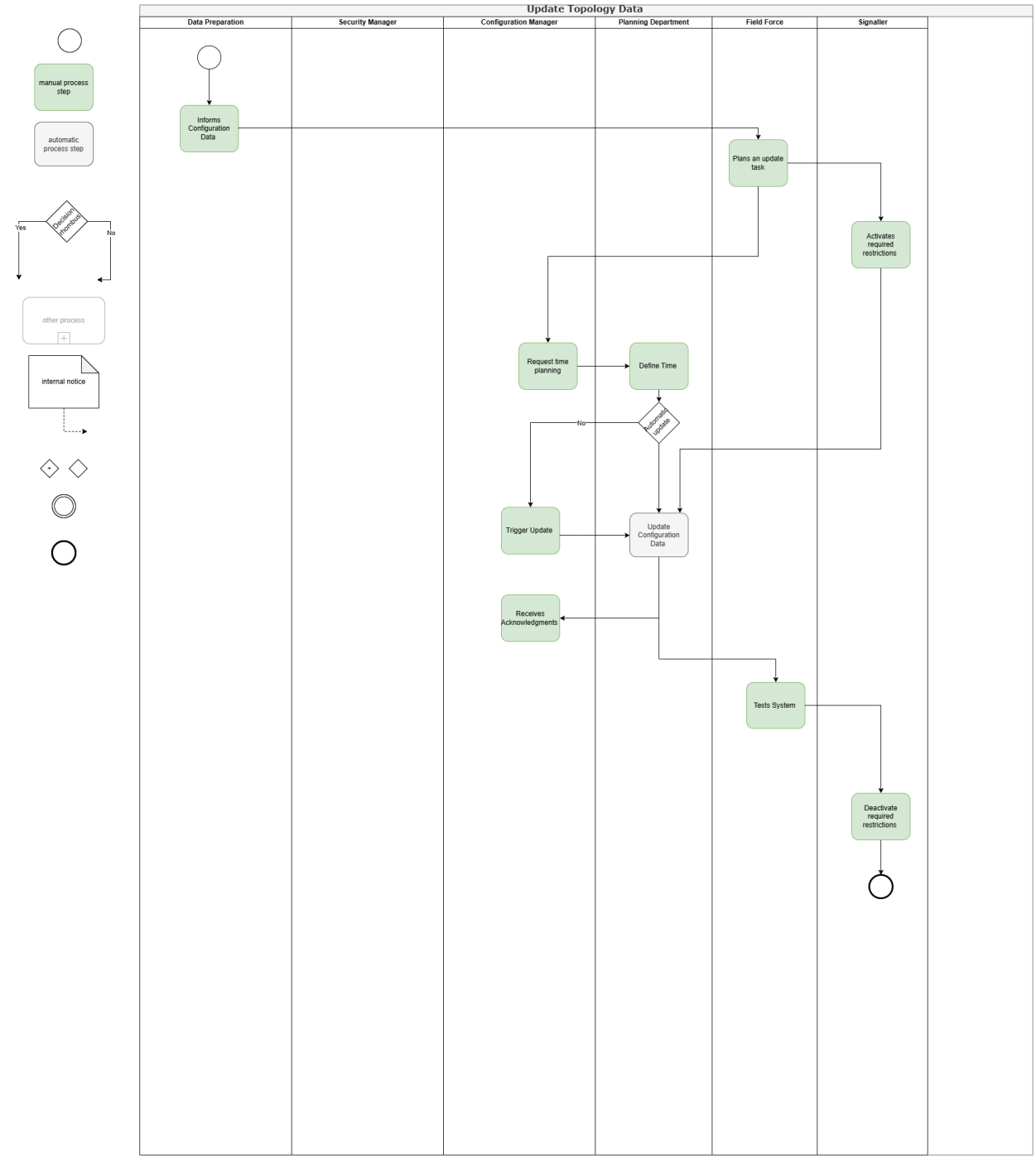

diagram template inside -> SPP-9268 - S2: Diagram template and best practices

Note for reviewers: the diagram is for visual support, the full description and main reference shall be the "operational activity" work items. **[**SPP-47590 **]**

4.7.1 Operational activities

The Data Preparation informs about new Configuration Data (Topology Data) to be used in the CCS system. The Configuration Data is validated and authorized by the Data Preparation and ready to be used in the CCS system.

The Field Force plans the update task for the affected System and coordinates the required on-site activities before the update.

If not done automatically, the Configuration Manager manually triggers update of the Configuration Data when the defined time has been reached.

The Configuration Manger requests the planning department for an appropriate time slot for performing the update of the Configuration Data.

The Planning Department defines based on the needs CCS System the update Time for the Configuration Data.

On having all the required triggers and safety measures in place to perform the update, the CCS-System performs the update. This includes activation and deactivation of the Configuration Data.

The Signaller activates the required operational restrictions (e.g. planned temporary speed restriction/ working area) to secure the affected System before the configuration update activities is performed.

The Field Force tests the System after the configuration update activity to verify that it works correctly before the required restrictions are deactivated.

The Configuration Manager receives a status acknowledgement of the configuration data update process, indicating the current status, including any failures that may occur.

The Signaller deactivates the required operational restrictions after the LRU/System has been successfully tested and the Configuration Data update activity is completed.

4.8 Replacement of a broken LRU (trackside)

Op.Postcondition	- Configuration data has been activated in the replaced device and is used by the system - System is available for production

Op.Precondition	- Broken LRU(s) replaced by a new one. - Initial configuration data is available for LRU (basic data identifier (e.g. IP addresses, identifiers) - Commissioning process from security perspective is done (registered in asset inventory, keys / certificates loaded, access to network granted) - Configuration data is available in the CCS system (same data from broken device /no new Configuration data is prepared)
Op.Rationale	Replacement of a broken LRU

diagram of process activate Configuration Data (Trackside) for use case : Replacement of a broken LRU

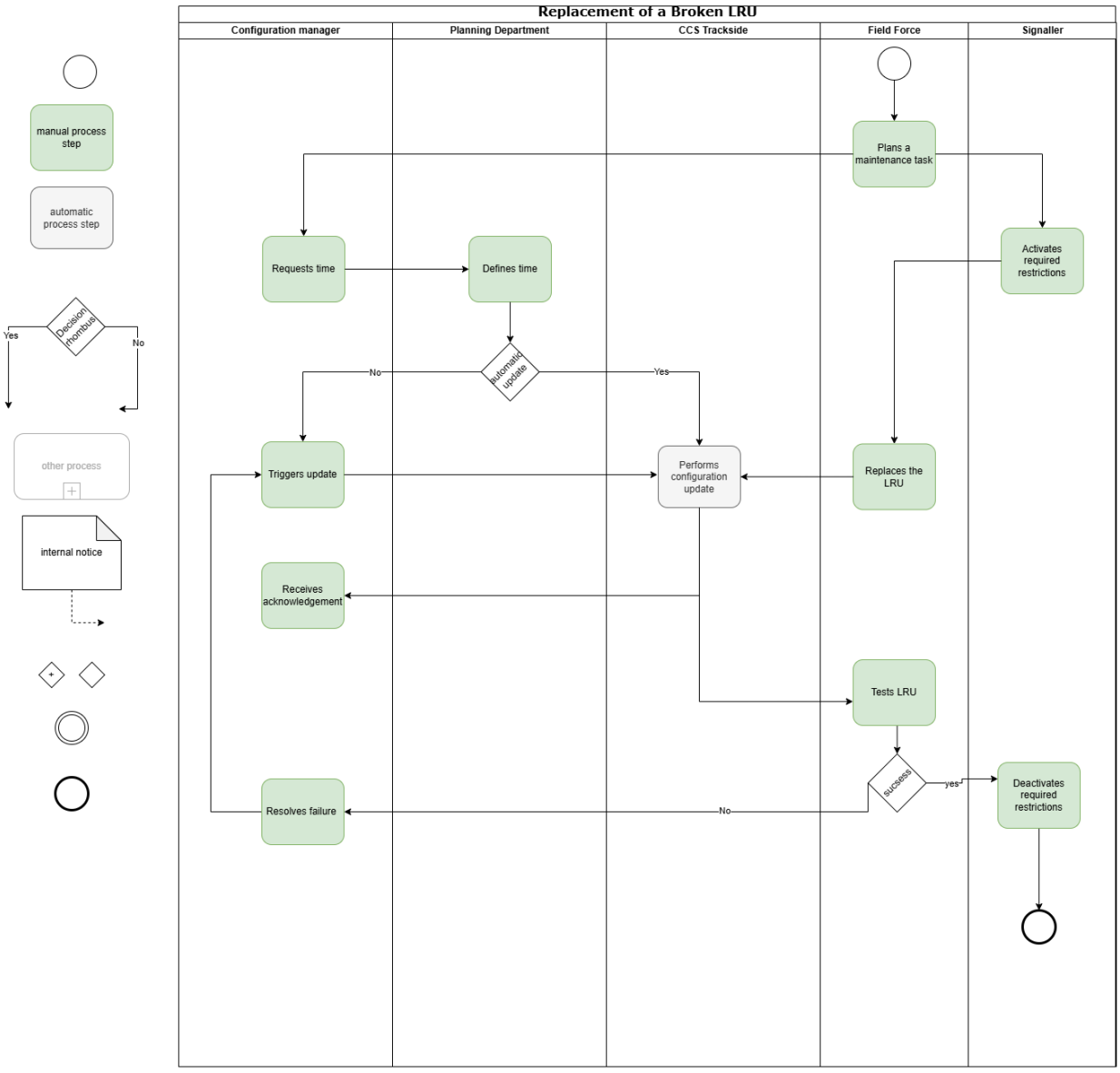

diagram template inside -> SPP-9268 - S2: Diagram template and best practices

Note for reviewers: the diagram is for visual support, the full description and main reference shall be the "operational activity" work items. **[**SPP-36205 **]**

4.8.1 Operational activities

The Field Force plans the maintenance task for replacing the broken LRU and coordinates the required on-site activities.

If not done automatically, the Configuration Manager manually triggers update of the Configuration Data when the defined time has been reached.

The Configuration Manger requests the planning department for an appropriate time slot for performing the update of the Configuration Data.

The Planning Department defines based on the needs CCS System the update Time for the Configuration Data.

.

On having all the required triggers and safety measures in place to perform the update, the CCS-System performs the update. This includes activation and deactivation of the Configuration Data.

The Signaller activates the required operational restrictions (e.g. planned temporary speed restriction/ working area) to secure the affected LRU before the configuration update activities is performed.

The Field Force tests the LRU after the configuration update/commissioning activity to verify that it works correctly before the required restrictions are deactivated.

The Signaller deactivates the required operational restrictions after the LRU has been successfully tested and the Configuration Data update activity is completed.

The Configuration Manager receives a status acknowledgement of the configuration data update process, indicating the current status, including any failures that may occur.

The Configuration Manager resolves issues identified during the configuration update or testing and coordinates the necessary corrections and if a rollback or new Configuration update is needed.

4.9 Replacement of a broken LRU (OnBoard)

4.10 Decommissioning of a LRU (Trackside)

Op.Postcondition	- Active version of Configuration data is deactivated - LRU is decommissioned
Op.Precondition	- LRU is running - LRU has active version of configuration data
Op.Rationale	- decommission LRU

diagram of process activate Configuration Data (Trackside) for use case : Decommissioning of a LRU

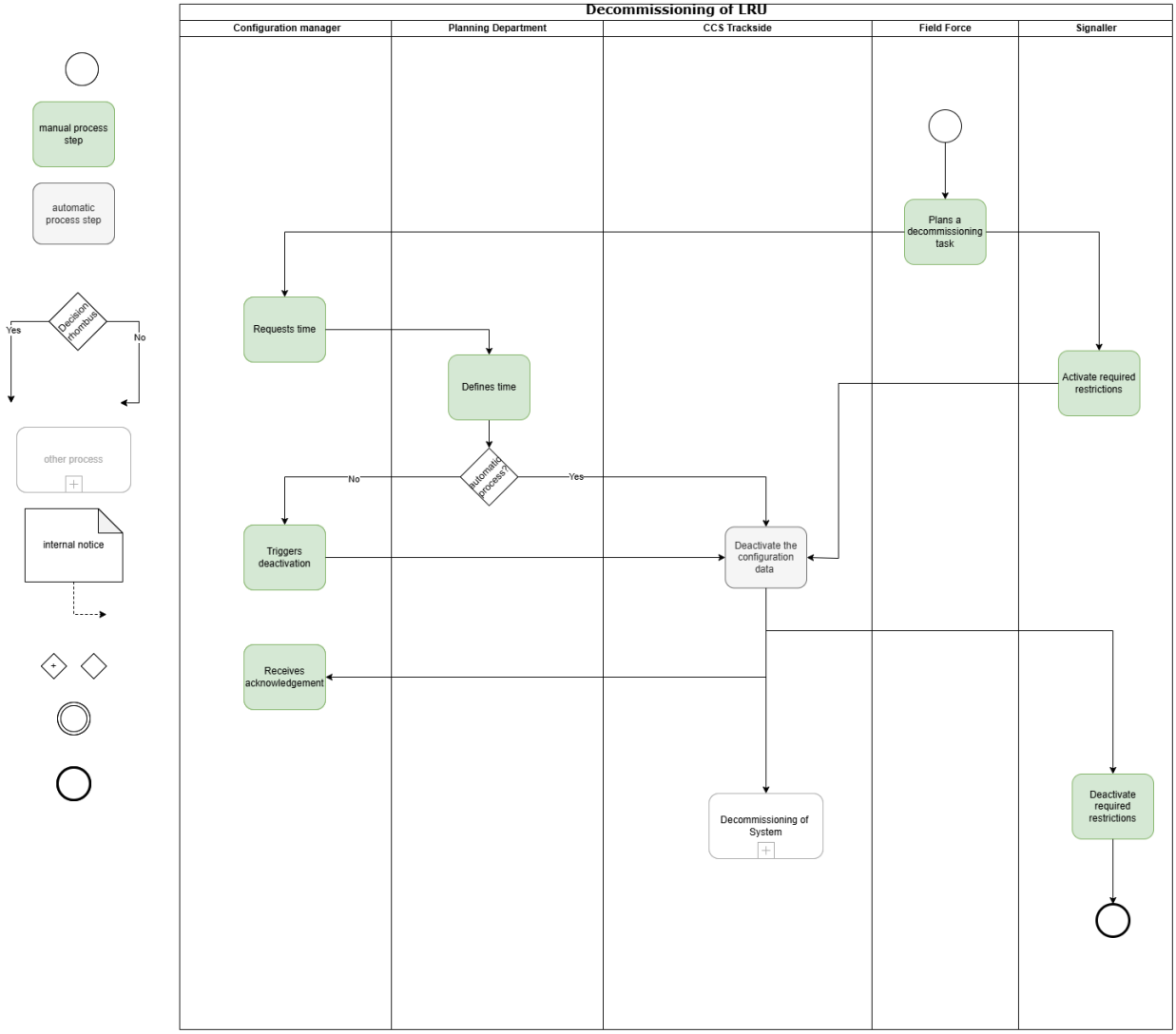

diagram template inside -> SPP-9268 - S2: Diagram template and best practices

Note for reviewers: the diagram is for visual support, the full description and main reference shall be the "operational activity" work items. **[**SPP-37551 **]**

4.10.1 Operational activities

The Field Force plans the decommissioning task for the affected LRU and coordinates the required on-site activities.

The Signaller activates the required operational restrictions (e.g. planned temporary speed restriction/ working area) to secure the affected LRU before the configuration deactivation activities is performed.

The Configuration Manager requests the Planning Department for an appropriate time slot to perform the decommissioning and configuration data deactivation.

The Planning Department defines the appropriate time slot for performing the decommissioning activity.

If not done automatically, the Configuration Manager manually triggers deactivation of the Configuration Data when the defined time has been reached.

The CCS System deactivates the configuration data related to the LRU as part of the decommissioning process.

The Configuration Manager receives an acknowledgement indicating the current status of the deactivation process, including any failures that occurred.

The Signaller deactivates the required operational restrictions after the configuration data of the LRU has been successfully deactivated.

4.11 Decommissioning of a LRU (OnBoard)

4.12 Decommissioning of a System (Trackside)

Op.Postcondition	- Active version of Configuration data is deactivated - System is decommissioned
Op.Precondition	- System is running - System has active version of configuration data
Op.Rationale	- decommission System

diagram of process activate Configuration Data (Trackside) for use case : Decommissioning of a System

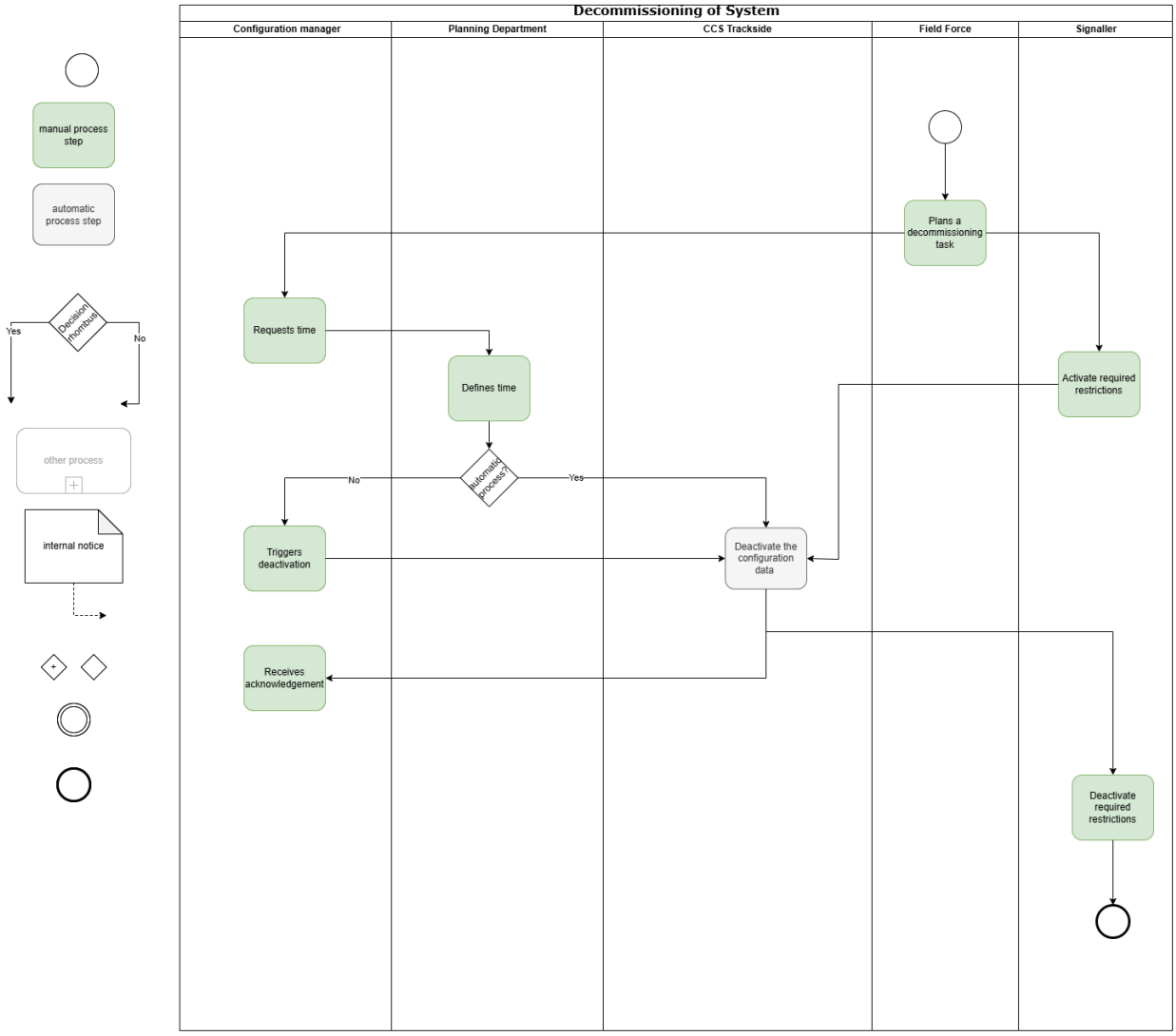

diagram template inside -> SPP-9268 - S2: Diagram template and best practices

Note for reviewers: the diagram is for visual support, the full description and main reference shall be the "operational activity" work items. **[**SPP-39941 **]**

4.12.1 Operational activities

The Field Force plans the decommissioning task for the affected System and coordinates the required on-site activities.

The Signaller activates the required operational restrictions (e.g. planned temporary speed restriction/ working area) to secure the affected System before the configuration deactivation activities is performed.

The Configuration Manager requests the Planning Department for an appropriate time slot to perform the decommissioning and configuration data deactivation.

The Planning Department defines the appropriate time slot for performing the decommissioning activity.

If not done automatically, the Configuration Manager manually triggers deactivation of the Configuration Data when the defined time has been reached.

The CCS System deactivates the configuration data related to the System as part of the decommissioning process.

The Configuration Manager receives an acknowledgement indicating the current status of the deactivation process, including any failures that occurred.

The Signaller deactivates the required operational restrictions after the configuration data of the System has been successfully deactivated.

4.13 Perform System Asset Diagnosis for Trackside

4.14 Perform System Asset Diagnosis for Onboard

5 Exported Constraints and External Requirements

exported constraints to external processes or actors (e.g. data prep, maintenance processes)

6 Consistency with SL3-SL5 architecture and functions

Mapping to SL3-SL5

- What in SL3-SL5 must be updated due to operational decisions
- Gaps found + proposed update

7 Appendix

7.1 Standards and references