




ERJU SYSTEM PILLAR

System Analysis



System Analysis

Author(s)	Zeeshan Z Ansar , Bernburg, Thomas (SMO RI R&D TC IL) , Betül Sögütlü , Steffens, Sonja (SMO RI R&D F IL) , SPANNEUT Julien (SNCF VOYAGEURS / DIRECTION DE L'INGENIERIE DU MATERIEL / CIN - DIE) , VIVARELLI, Claudio , Julian Wissmann , Klapka Štěpán RNDr. , TOBOREK Marcin , GAUTRON Mickael (SNCF VOYAGEURS / DIRECTION DE L'INGENIERIE DU MATERIEL / CIM - SBF 1) , LOSTUN Virgil
Abstract	This document presents the system analysis of the CE logical architecture including its interfaces
Config Item	System Requirements Specification
Document ID	30 Deliverables/System Analysis#723630  System Analysis
Classification	Public
Status	In Decision by Steering Group
Version	2.0
Revision	723629
Last Change Date	02.10.2025
Copyright	Brussels: Europe's Rail Joint Undertaking, 2025

© Europe's Rail Joint Undertaking, 2025

This document is drafted by and belongs to EU Rail.

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

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

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

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

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

Document History

1.2 16.05.2024	Zeeshan Z Ansar	Reviewed version including Findings from Review X.X
1.3 23.07.2025	Betül Sögütlü	Reviewed version including Findings from Review 1.2
2.0 09.09.2025	Betül Sögütlü	Approved version based on Review 1.3

SPT2CE-2759 - Document Review

full review of the document

Type of Approval	 Document Review
Approvals	Betül Sögütlü : Approved , Zeeshan Z Ansar : Approved , Bernburg, Thomas (SMO RI R&D TC IL) : Approved , GAUTRON Mickael (SNCF VOYAGEURS / DIRECTION DE L'INGENIERIE DU MATERIEL / CIM - SBF 1) : Approved , Julian Wissmann : Approved , Klapka Štěpán RNDr. : Approved , LOSTUN Virgil : Approved , SPANNEUT Julien (SNCF VOYAGEURS / DIRECTION DE L'INGENIERIE DU MATERIEL / CIN - DIE) : Approved , TOBOREK Marcin : Approved , VIVARELLI, Claudio : Approved

SPT2CE-2758 - Document Approval-System Pillar

full approval of the document

Type of Approval	 Document Approval
Approvals	Betül Sögütlü : Approved , Zeeshan Z Ansar : Approved , Bernburg, Thomas (SMO RI R&D TC IL) : Approved , GAUTRON Mickael (SNCF VOYAGEURS / DIRECTION DE L'INGENIERIE DU MATERIEL / CIM - SBF 1) : Approved , Julian Wissmann : Approved , Klapka Štěpán RNDr. : Approved , LOSTUN Virgil : Approved , SPANNEUT Julien (SNCF VOYAGEURS / DIRECTION DE L'INGENIERIE DU MATERIEL / CIN - DIE) : Approved , TOBOREK Marcin : Approved , VIVARELLI, Claudio : Approved

Table of content

1	Preamble	7
1.1	Purpose	7
1.2	Intended Audience	7
1.3	Document Context	7
2	Glossary	7
2.1	Terms and Abbreviations	7
3	System Scope	11
3.1	System under consideration	11
3.1.1	Overview	12
3.1.2	High level Capabilities	13
3.2	System Context	15
3.2.1	System Actors/Entities	16
3.2.2	Overall Context "Deployment and Update of FS"	16
3.2.3	Overall Context "Update of the Computing Platform"	18
3.2.4	Overall Context "Diagnosis"	19
3.2.5	Overall Context "Safety"	20
3.2.6	Overall Context "IT-Security"	20
3.2.6.1	IT Security stack within the FS Compartment	21
3.2.6.2	IT security stack as separate FS specific Compartment	21
3.2.6.3	IT security stack as separate standardised FS Compartment	22
3.2.6.4	IT security stack as within the CP	23
4	Scenarios	24
4.1	FS Execution	24
4.1.1	Aggregation of different kinds of FS Comp on same CP	24
4.1.2	Network Communication of a FS Comp	26
4.1.3	Running of FS Comps - safety related aspects	26
4.1.4	Running of FS Comps - IT security related aspects	27
4.2	Deployment Scenarios	28
4.2.1	Deployment of the CP Software	28
4.2.2	Deployment of the FS Software onto the CP	28
4.3	Update Scenarios	30
4.3.1	Update of the CP Software onto the CP Hardware	30
4.3.2	Update of FS software	32
4.4	Recovery Scenarios	33
4.4.1	SW Failure within a individual FS Comp	33
4.4.2	SW Failure within the CP	34
4.4.3	HW Failure within the CP	34
4.4.4	Network failure within the CP	35

5 SubSystem Capabilities	36
5.1 Application Execution Environment (AEE)	36
5.2 Computing Platform Software (CPSW)	36
5.3 Computing Platform HW (CPHW)	37
6 Functions	38
6.1 Function of the Computing Platform (CP)	38
6.1.1 CP as runtime environment for FS Comps	38
6.1.2 Configuration of the CP for usage by FS Comps	40
6.1.3 SW handling for CP Software on CP Hardware	42
6.1.4 Handling of FS Comp SW to deploy and update SMI	44
6.1.5 IT-Security SSI	45
6.1.6 Diagnostics SDI	46
6.1.7 Recovery	48
6.2 Functions of the FS Compartment (FS Comp)	50
6.3 Functions of the Shared Services (SS)	54
6.4 Function Overview	57
7 System requirements	61
7.1 Requirements for the Computing Platform	61
7.1.1 Interface I3 and CP Configuration	61
7.1.2 CP Release Management	65
7.1.3 Maintenance of the CP	66
7.1.4 Deploy and Update SMI	67
7.1.5 Diagnostics SDI	68
7.1.6 IT-Security SSI	69
7.1.7 Hardware related requirements	70
7.2 Requirements for the FS Compartment	71
7.3 Requirements for the Shared Services	74
7.3.1 Update SMI	74
7.3.2 Diagnostics SDI	77
7.4 Requirements Overview	78
8 Open Points	81
8.1 Update SMI	81
8.2 IT-Security SSI	82
8.3 Diagnostics SDI	83
8.4 Access to CP Hardware	84
8.5 RAM and Safety	84
8.6 Realtime	84
8.7 Onboard Communication Protocols	85
9 Summary and Future Work	85
10 Reference	85
11 Annex	86
11.1 Figures	86

1 Preamble

1.1 Purpose

1.2 Intended Audience

1.3 Document Context

This document presents the system analysis of the CEnv (Computing Environment) logical architecture, including its interfaces and configuration items. The analysis aims to understand the system under consideration and its objectives comprehensively. The document will also discuss the scope of the system, including its objectives and the actors or entities involved.

This third deliverable provides the system analysis, including system scenarios, capabilities, functions, and requirements. We will examine the specifications of external interface I1-shared services to analyse their applicability to the computing environment architecture and identify the gaps that need to be discussed with SP domains, including Transversal and Security.


The system analysis is based on the CEnv domain's second deliverable System Concept, including operational scenarios. The operational scenarios and requirements are transformed into system capabilities, functions, and requirements to realise the system objectives.

Note that all assessments and suggestions made, and conclusions drawn in this document assume that proprietary Functional Systems will continue to exist indefinitely. Migration from those already existing functions is not considered in this analysis, as it needs to be done case-by-case. The standardised Computing Environment shall be able to host proprietary Functional Systems (with potentially minimal change) as well as newly developed Functional Systems (fully based on the new standardised interfaces).

2 Glossary

2.1 Terms and Abbreviations

Term (Abbreviation)	
Description	Referenced
Application Execution Environment (AEE) The Application Execution Environment refers to the combination of Runtime Environment and Safety Environment. The safety environment is excluded for the basic integrity applications	here...
Application Layer (AL) The Application Layer contains Functional Applications that constitute Functional Systems.	here...
Basic Integrity Platform Independence Interface (I4) The Basic Integrity Platform Independence Interface I4 (Interface 4) is used to perform a basic integrity platform independence with the applications. In other words, this API is an interface limited to non-safety functionalities between runtime environment and applications.	here...
BBC (DR) (BBC (DR)) Building Block Configuration which contains the deployment rules for the FS.	here...

Term (Abbreviation)	
Description	Referenced
BBC (InSW) (BBC (InSW)) Building Block Configuration which contains the initial software for the Initial FS Compartment.	here...
BBC (SW-x) (BBC (SW-x)) Building Block Configuration which contains software and/or data which is part of an FS Compartment. The quantity of BBCs - BBC(SW-1), BBC(SW-2), .. - depends on the concrete solution of the FS.	here...
Building Block Configuration (BBC) Data for a Building Block, see Configuration Update Concept of Transversal.	here...
Compartment (Comp) A Compartment  is a consistent, integrated entity comprising exactly one Runtime Environment Instance, Safety Environment Task Replicas of at most one Safety Environment, and Functional Application Task Replicas of its respective Functional Applications. It can be deployed on either a Physical or a Virtual Computing Element.	here...
Compartment Execution Environment (CEE) The Compartment Execution Environment refers to the combination of Physical Computing Element and Virtualisation Environment.	here...
Computing Environment (CEnv) A computing environment encompasses the hardware, software, network resources, and services that enable the deployment, operation, and management of applications or services. Computing environment includes the application execution environment and the computing platform.	here...
Computing Platform (CP) The Computing Platform provides and manages computing resources and communication resources for functional systems (specialised IO are not included). It contains CP hardware (physical computing element(s) and communication hardware) and CP software (virtualisation environment and platform management). Note: The CP shows an abstract view and may contains several PCEs.	here...
Computing Platform Hardware (CPHW) Physical Computing Elements and network hardware.	here...
Computing Platform Software (CPSW) Provides platform-level services (e.g., resource allocation, compartment execution environment).	here...
External Diagnostic, Configuration and IT Security Interface(s) (I1) The external Diagnostic, Configuration and IT Security Interface I1 (Interface 1) comprises communication-based interfaces between rail systems and central infrastructure components such as diagnostics, IT-security services and remote update.	here...
Functional Application (FA) A Functional Application is a comprehensive set of self-contained software functions, assumed to be provided as one product by a single vendor. Depending on its role in the overall function provided by the Functional System, it has a specific SIL (BIL up to SIL4) assigned (in-line with total FS SIL definition).	here...

Term (Abbreviation)	
Description	Referenced
Functional Application Task (FAT) A Functional Application Task implements part of the functionality provided by a Functional Application. Depending on its role in the overall function provided by the Functional Application, it has a specific SIL assigned (in-line with total FA SIL definition). It may run replicated in multiple Compartments as FA Task Replicas.	here...
Functional System (FS) A Functional System is a comprehensive set of self-contained Compartments, assumed to be provided as one product by a single vendor. Depending on its overall function, it has a specific SIL assigned.	here...
Functional System Deployment Rules (FSDR) The Functional System Deployment Rules comprises all necessary information for deploying the respective Functional System onto specific approved Compartment Execution Environment(s). These deployment rules are compiled as part of the FS integration process and are part of each integrated, tested and qualified/approved Functional System along with its FS Compartments and all necessary approval documentation.	here...
Hardware Abstraction Interface (I2) The Hardware Abstraction Interface I2 (Interface 2) provides an abstraction of all technology layers above from the specific hardware used below, enabling easy replaceability of commercial off-the-shelf hardware procurable from a well-sized market of hardware vendors. Note: This is not really an interface, but rather a compatibility list of allowed hardware incl. CPU, memory, etc.	here...
Hardware Layer (HL) The Hardware Layer contains the actual Physical Computing Elements providing the compute resources to the platform.	here...
Initial FS Compartment (Initial FS Comp) It contains the minimum software which is needed to start up the FS Compartment and provide a functionality to install the BBC(SW-x) for the FS. This is the BBC (InSW). The initial FS compartment is necessary for remote load of the SW packages which are needed for the operative running mode of the FS compartment.	here...
Instance (INS) An Instance is a specific realisation of any entity.	here...
Management Compartment (MC) The management compartment provides the deployment, configuration and monitoring services through the standardised interfaces. The details will be specified in the future documents.	here...
Operational Interface (I0) The I0 is the sum of all operational interfaces used from Functional Systems (as eg. an RBC) to communicate with other Functional Systems (as eg. an IXL). Examples for these set of interfaces are the Eulynx Interfaces (SCI-xx) or interfaces like Euroradio or TSI-standardised interfaces.	here...
Operative FS Compartment (Operative FS Comp) It contains the complete SW packages (BBCs) which represent in total the FS Compartment for the operative running mode. These are the BBC(SW-x).	here...

Term (Abbreviation)	Referenced
Orchestration Interface (OI) This interface is used to manage (monitor, control, diagnose, configure) the virtual computing environments.	here...
Physical Computing Element (PCE) The Physical Computing Element refers to the physical device providing compute resources.	here...
Platform Management (PM) The platform management manages the computing platform resources and is a part of the Computing Platform software.	here...
Replica (REP) A Replica is a specific realisation of any entity in a cluster of peers used for composite fail safety and/or availability. Replicas of the same entity always run in distinct Compartments deployed to distinct Computing Elements.	here...
Runtime Environment (RTE) The Runtime Environment refers to the software needed to provide the services of the Runtime Layer in a single Compartment.	here...
Runtime Layer (RL) The Runtime Layer refers to the system services (e.g., application and computing resource orchestration, monitoring of the Functional Applications and the Application Execution Environment, tracing and logging, communication services that are not related to safety, security means incl. authentication, encryption, key storage, etc.) and the communication stack for information exchange between Functional Applications running on the same Computing Environment and with external entities. It may also include an operating system.	here...
Safe Configuration Authority (SCA) Safe Configuration Authority, see Configuration Update Concept of Transversal.	here...
Safety Environment (SE) The Safety Environment refers to all Safety Environment Tasks needed for a Functional System.	here...
Safety Environment Task (SET) A Safety Environment Task implements part of the functionality provided by a Safety Environment. Depending on its role in the overall function provided, it has a specific SIL assigned (in-line with total SE SIL definition). It may run replicated in multiple Compartments as SE Task Replicas.	here...
Safety Layer (SL) The Safety Layer implements all the technical safety principles related to fulfilling the requirements of EN 50126, EN 50716 (formerly 50128), EN 50129, EN 50159 (e.g., composite fail safety, fault tolerance, voting mechanisms, redundancy mechanisms for availability, safety communication layers etc.) that are needed to enable the execution of Functional Applications up to SIL4.	here...
Safety Platform Independence Interface (I5) The aim of introducing Safety Platform Independence Interface I5 (Interface 5), is to be able to implement platform independent Safe Functional Applications (up to SIL4) i.e., applications, based on a generalised abstraction between the application logic and the system interfaces, that will run unchanged on different platform implementations.	here...

Term (Abbreviation)	
Description	Referenced
Standard Diagnostic Interface (SDI) Standard Diagnostic Interface as defined by EULYNX / System Pillar	here...
Standard Maintenance Interface (SMI) Standard Maintenance Interface as defined by EULYNX / System Pillar	here...
Standard Security Interface (SSI) Standard Security Interface as defined by EULYNX / System Pillar	here...
Virtual Computing Element (VCE) The Virtual Computing Element refers to virtually provided compute resources with computing resource guarantees.	here...
Virtual Trusted Platform Module (vTPM) A software-based representation of a traditional hardware-based TPM 2.0.	here...
Virtualisation Environment (VE) The Virtualisation Environment contains all software needed to provide (multiple) Virtual Computing Elements on a single Physical Computing Element.	here...
Virtualisation Interface (I3) The Virtualisation Interface I3 (Interface 3) is used to provide a standardised interface above the virtualisation layer so that applications or higher platform layers are independent of a specific implementation of the computing hardware.	here...
Virtualisation Layer (VL) The Virtualisation Layer contains mechanisms that are able to provide Virtual Computing Elements needed to run multiple Compartments on a single physical hardware underneath.	here...

3 System Scope

3.1 System under consideration

The system under consideration is a standardised computing environment designed for the railway domain. It is aimed at hosting and managing both safety-critical and non-safety-critical functional systems for both, trackside and onboard applications. This environment is engineered to enhance operational efficiency, interoperability, scalability, and security, aligned with the strategic objective of reducing dependencies and operational costs.

The system is a sophisticated computing environment designed for the railway sector, delivering seamless integration across diverse platforms and enabling remote management and configuration to minimise onsite dependencies. It offers robust scalability, allowing for adding computing elements from various suppliers and ensuring efficient resource allocation. Comprehensive security measures protect data integrity, while operational resilience is assured through automated recovery features that maintain high reliability. The system minimises dependencies between applications, runtime environments, and hardware, facilitating seamless hardware replacements and platform upgrades without vendor lock-in. It

ensures harmonised deployment processes and supports applications up to Safety Integrity Level 4 (SIL4), all while optimising operational and capital expenditures for enhanced efficiency and security.

3.1.1 Overview

This chapter describes a computing environment logical architecture. The logical architecture defines system's functional structure by grouping related functions into functional domains/subsystem. It ensures alignment with stakeholder needs while deferring implementation details to the physical architecture. The Computing Environment (CEnv) logical architecture described in Figure 1 is based on the high-level subsystem concept defined in the domain's first deliverable [1]. The logical architecture includes subsystems, external actors/systems, and interfaces with explicit separation of concerns to ensure modularity and traceability.

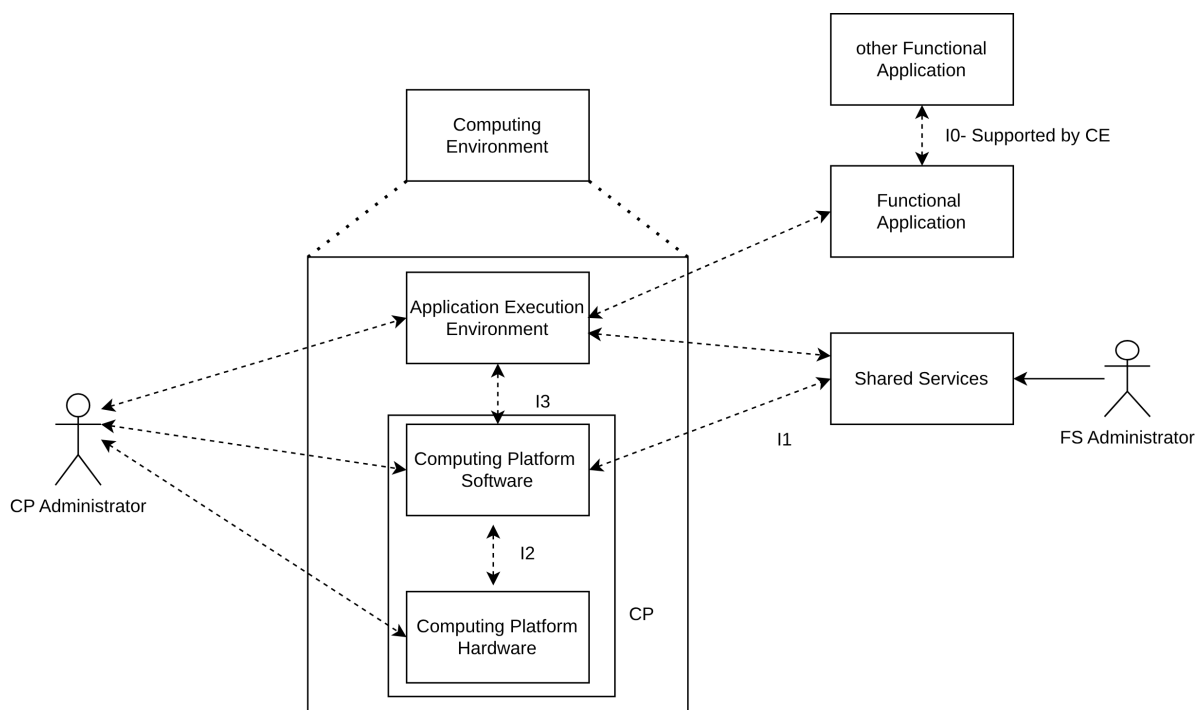



Figure 1 CEnv Logical Architecture

Subsystems:

-  SPT2CE-1239 - Application Execution Environment
-  SPT2CE-2443 - Computing Platform Software
-  SPT2CE-2442 - Computing Platform Hardware

External Actors/Systems:

- **Functional Application:** Railway application deployed on the AEE.

- **Shared Service:** Common services (e.g., Configuration, update, diagnostic, security).
- **CP Administrator:** manages Computing Platform
- **FS Administrator:** Manages Functional System





Interfaces:

- **I0:** Connects railway functions running on CEnv with other railway functions (running on CEnv or external platforms).
- **I1:** Connects external systems (Shared Service, Administrator) to the CEnv.
- **I3:** Connects the AEE to the CPSW.
- **I2:** Links the CPSW to the CPHW.

3.1.2 High level Capabilities






SPT2CE-2575 - Interoperability with Existing Systems

Enable integration with a wide range of functional systems and technologies from different suppliers.

Status	 Open
Linked Work Items	<p>is derived from :  SPT2CE-28 - Interface a Computing Platform with existing systems</p> <p>has parent :  SPT2CE-2574 - High level Capabilities</p> <p>_C2P-is parent of :  SPT2CE-2464 - Provide compartment execution environment.</p>






SPT2CE-2576 - Remote Management and Configuration

Support the deployment, updates, and configuration of functions ad-hoc during operations or in scheduled modes without requiring significant manual intervention.

Status	 Open
Linked Work Items	<p>is derived from :  SPT2CE-20 - Remotely add, modify, delete or configure functions</p> <p>is derived from :  SPT2CE-30 - System operation and update deployment without or with minimal on-site presence</p> <p>has parent :  SPT2CE-2574 - High level Capabilities</p> <p>_C2P-is parent of :  SPT2CE-2454 - Manage application lifecycle</p>

SPT2CE-2577 - Scalability and System Flexibility







Adapt to different operational scales, ranging from small deployments to large-scale integrations.

Status	 Open
Linked Work Items	<p>is derived from :  SPT2CE-24 - Planned movement/relocation of Functional Applications from one instance of a Computing Platform to another</p> <p>is derived from :  SPT2CE-27 - Add computing elements (e.g. CPUs, memory or storage) from another supplier</p> <p>has parent :  SPT2CE-2574 - High level Capabilities</p> <p>_C2P-is parent of :  SPT2CE-2464 - Provide compartment execution environment.</p>

SPT2CE-2578 - Enhanced Security and Integrity






Implement comprehensive security protocols to protect system data and functionality from unauthorised access and threats.

Note: The final security architecture are not decided and chapter 4.2.6 propose three different security architecture. Based on the final architecture different implementation are possible either as part of Platform or Functional System.

Status	 Open
Linked Work Items	<p>is derived from :  SPT2CE-29 - Add, modify, delete or configure functions related to IT/OT security and/or communication protocols</p> <p>C2P-has parent :  SPT2CE-2568 - Access to specific low-level hardware modules.</p> <p>has parent :  SPT2CE-2574 - High level Capabilities</p> <p>_C2P-is parent of :  SPT2CE-2452 - Enforce security policies.</p> <p>_C2P-is parent of :  SPT2CE-2467 - Provide low-level hardware functions.</p>





SPT2CE-2579 - Recovery and Resilience

Ensure system stability and continuous operation even during disruptions, with capabilities for automatic recovery.

Status	 Open
Linked Work Items	<p>is derived from :  SPT2CE-26 - Automatically instantiate and/or activate a Functional Application on new hardware in case all hardware on which the Functional Application runs fails (e.g., in case of a disaster affecting a whole data center)</p> <p>C2P-has parent :  SPT2CE-2469 - Provide fault tolerance.</p> <p>has parent :  SPT2CE-2574 - High level Capabilities</p> <p>_C2P-is parent of :  SPT2CE-2536 - Support redundancy</p>





SPT2CE-2582 - Resource Optimisation and Aggregation

Optimise system resources by aggregating multiple Functional Applications to enhance performance and efficiency e.g. reduce the amount of dedicated hardware.

Status	 Open
Linked Work Items	<p>is derived from :  SPT2CE-19 - Aggregate multiple Functional Applications on the same Instance of a Computing Platform</p> <p>has parent :  SPT2CE-2574 - High level Capabilities</p> <p>_C2P-is parent of :  SPT2CE-2464 - Provide compartment execution environment.</p>

SPT2CE-2581 - Minimisation of Dependencies






Provide standardised interfaces

Status	 Open
Linked Work Items	<p>is derived from :  SPT2CE-18 - Minimize overall dependencies</p> <p>has parent :  SPT2CE-2574 - High level Capabilities</p> <p>_C2P-is parent of :  SPT2CE-2453 - Manage access to platform services via Interface I3.</p>

SPT2CE-2584 - Efficient Hardware Replacement





Allows hardware updates with minimal FS certification and operation cost.

Status	 Open
--------	--

Linked Work Items	is derived from :  SPT2CE-21 - Replace the Computing Platform without vendor lock-in is derived from :  SPT2CE-25 - Replace one Hardware by another with minimal or no re-authorisation effort has parent :  SPT2CE-2574 - High level Capabilities _C2P-is parent of :  SPT2CE-2460 - Abstract hardware details from the AEE via Interface I3. _C2P-is parent of :  SPT2CE-2468 - Provide and manages compute resources (e.g. CPU, Memory, Storage, Network).
-------------------	--





SPT2CE-2583 - Harmonised Deployment Processes

Support streamlined deployment of Functional Applications across different infrastructure segments.

Status	 Open
Linked Work Items	is derived from :  SPT2CE-22 - Deploy Functional Applications through a harmonized approach C2P-has parent :  SPT2CE-2454 - Manage application lifecycle has parent :  SPT2CE-2574 - High level Capabilities

SPT2CE-2580 - Support for application up to SIL4

Computing Environment hosts applications, up to SIL4.

Status	 Open
Linked Work Items	is derived from :  SPT2CE-23 - Computing Platform suitable for Functional Applications up to SIL4 has parent :  SPT2CE-2574 - High level Capabilities _C2P-is parent of :  SPT2CE-2455 - Host applications up to SIL 4

3.2 System Context

Main objective is the definition of the overall functional architecture for Functional Systems running on a **Computing Platform**.

The overall architecture has to be defined in such a way that the processes and interfaces as defined by the **Shared Services (SMI, SDI, SSI specified by SP Transversal and Security domains)** can be used for Functional Systems running as FS compartments on the Computing Platform.

Following conditions has to be met to fulfil the system objective.

- The **Shared Services** handles maintenance, diagnosis and security related interdependencies between FS Compartments belonging to the same FS.
 Example:
 A safety related FS with 2oo3 principle consists of three FS Compartments 1/2/3.
 Each FS Compartment 1/2/3 consists of several BBCs.
 Each FS Compartment 1/2/3 provides own diagnostic data.
 Shared Services shall handle this relationships of the three FS Compartments 1/2/3 in context of update and diagnosis
- The **Computing Platform** shall handle the Compartment Execution Environment for the individual FS Compartments in context of the software installation, monitoring of running parts (software and hardware) and automated repair in case of failures. The Computing Platform shall not have the need to care about dependencies between FS compartments.

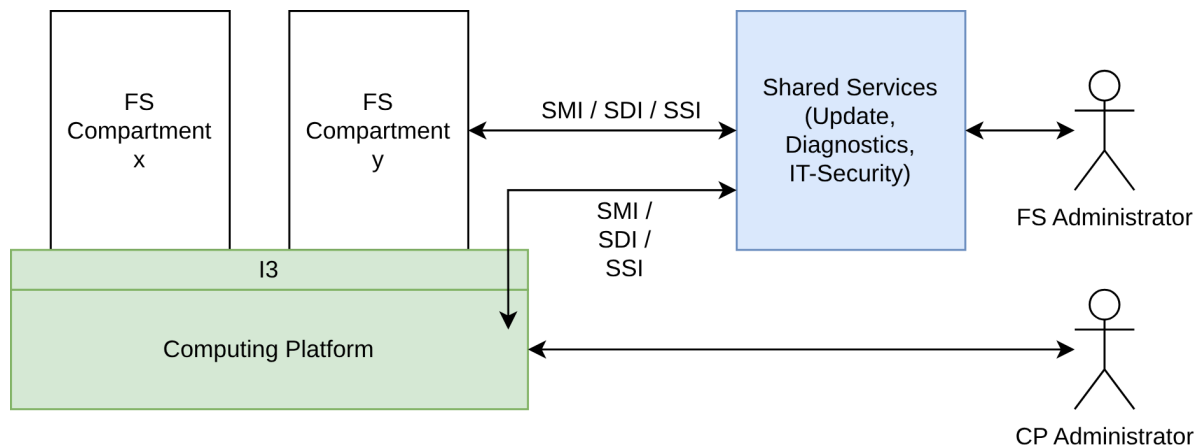


Figure 2 Overall context

Note: The Shared Services are the external IT-systems that could also be hosted on a Computing Platform.

This affects the overall architecture for

- Installation and configuration of the Computing Platform using COTS Hardware
- Deployment FS Compartments onto the Computing Platform according to **SMI**
- Update of running FS Compartments according to **SMI**
- Providing runtime environment related diagnostic data of the Computing Platform according to **SDI**
- Implementing IT-Security according to **SSI**
- Automated repair mechanism to handle SW, HW or network failures as automated as possible

3.2.1 System Actors/Entities

Actor/Entity	Type	Description
Shared Service	External System	A shared service system includes services for IT security, diagnostic and update of building block configurations defined by Transversal and Security domains.
Functional System Administrator	Human	Monitors and controls the Functional System, has safety responsibility
CP Administrator	Human	Monitor and controls the Computing Platform, has no safety responsibility

3.2.2 Overall Context "Deployment and Update of FS"

The individual software parts of a FS Compartment are handled in context of SW deployment and SW update on side of the Shared Services as **Building Block Configurations** (BBC) which are updated via **SMI** interface into the FS Compartments.

This process is generic and allows the remote update of basic integrity BBCs and Safe BBCs into rail systems as e.g. decentralised object controllers and centralised CCS logic as e.g. interlocking logic. Depending on the change (software and/or data, basic integrity or SIL4) individual BBCs can be updated. For rail systems running on **specific platforms** as e.g. object controllers the process is used for the update of a running software version onto a new software version. Process is not used for the first deployment of software onto the specific hardware because this is done by the system vendor before the commissioning.

For rail systems running on the **standardised CP** the process can be used not only for the update but even for the first deployment of the software onto the standardised CP. For this first deployment additional

BBCs are necessary to define the FS specific deployment rules and to provide a initial software with bootloader functionality.

The complete process is described in  **Logical Concept** of the Transversal domain [2].

Each FS Compartment consists of several BBCs:

- **BBC(DR)**

These are the deployment rules of the FS compartment as e.g. needed CPU-cores, exclusive usage of CPU cores, needed memory, needed communication.

The format of the deployment rules shall be defined as generic standard.

 SPT2CE-2329 - Fct-FS Comp - Provide FS Comp deployment rules BBC(DR)


- **BBC(InSW):**

This is the needed initial software for starting up as Initial FS compartment in a secure way and being ready to process the remote load of further BBCs via I1-Update (SMI) into the FS Compartment.

This BBC contains the boot loading functionality of the FS Compartment and with needed default data as IP addresses for first remote connection.

 SPT2CE-2319 - Fct-FS Comp - Provide BBC(InSW) with SMI client functionality

The BBC(InSW) is not safety related.

 SPT2CE-2571 - Open #SMI - handling of default data for initial FS Compartment ?

- **BBC(SW-1), BBC(SW-2), ...:**

These are the software parts which are needed for the operative running mode of the FS Compartment.

The quantity and content of BBCs are determined by the specific solution of the FS.


Example:

It depends on the concrete FS solution if the own operating system is within the BBC(InSw) and overwritten by a BBC(SW) or not.

Example:


Safety related FS with 2oo3 principle = 3 FS compartments. Each FS compartment consists of 2 SW BBCs:

- BBC(SW-1) = basic integrity OS with belonging data
- BBC(SW-2) = safety layer with safe application and belonging data

 SPT2CE-2508 - Fct-SS - SMI - Considering FS Comp related BBC structure for FS release management

For each of the three FS compartments the following steps are necessary and can be done in parallel:
At first the deploy = creation of the Initial FS Compartment as steps 1,2,3.

And the update of the BBC(SW-x) into the FS Compartments as steps 4 and 5.

1. Initiation of the creation of the Initial FS Comp 1/2/3, transfer of the BBC(DR)[1]/[2]/[3] and BBC(Initial SW)[1]/[2]/[3] via I1-SMI to the Computing Platform.
 SPT2CE-2492 - Open #SMI - deploy new FS - initiation by the admins ?
2. Configuration of the Computing Platform according to the deployment rules **BBC(DR)[1]/[2]/[3]**
3. Creation and start of the **Initial FS Comp = BBC(Initial SW)[1]/[2]/[3]**
Initial FS Comp 1/2/3 are starting up an ready to process load of BBC(SW-x)[1]/[2]/[3] via I1-SMI into the FS Compartment.
4. Update of the **BBC(SW-x)[1]/[2]/[3]** via **I1-SMI** into the FS Compartment 1/2/3.
5. In case of safe BBC(SW) the update process is safety related and requires the involvement of the **Safe Configuration Authority SCA**. In this context the safety layer within the FS Compartment ensures that an individual FS Compartment handles the update process for safety related BBC(SW-x) safely, means with dependency to safe synchronisation with neighbour compartments. This means that for the activation of a safety related BBC(SW-x) at least two FS Compartments need to be inter-synchronised. A simultaneous update of safety related BBC(SW-x) in parallel into the FS Compartments shall be considered by the Shared Services.

Specific aspects in context of SIL1 / SIL2 systems are not yet analysed.

SPT2CE-2502 - Open #SIL1/2

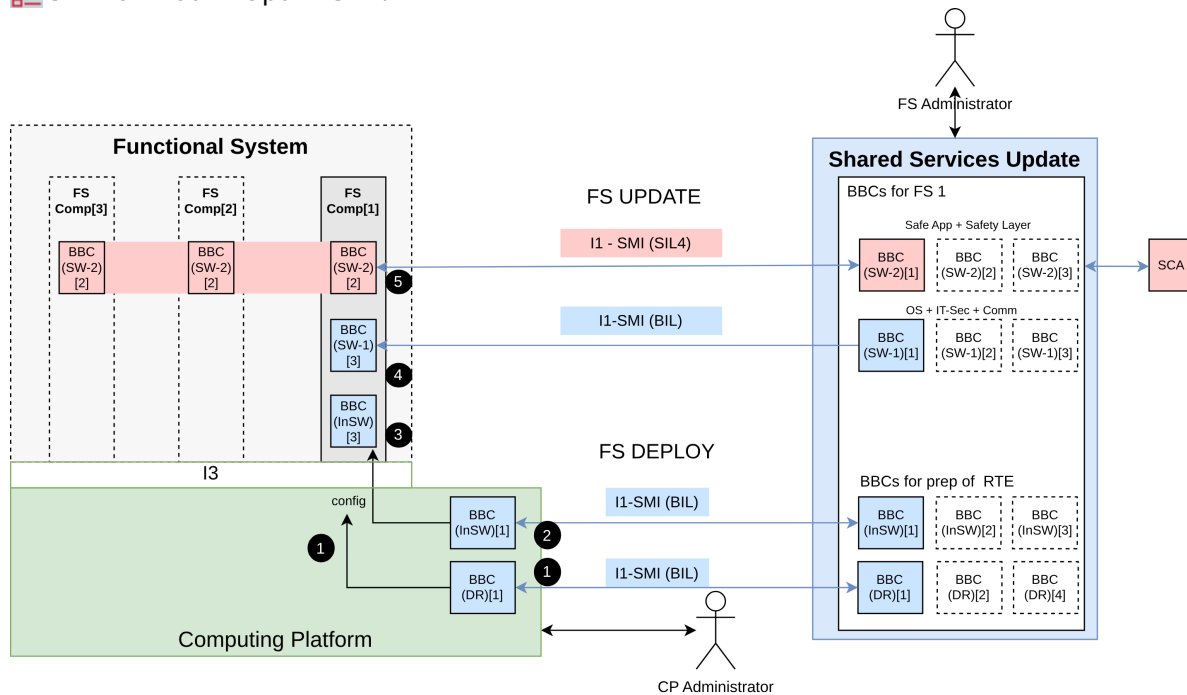


Figure 3 Overall context "Deploy the Initial FS Compartment and Update of FS"

After the deployment of the initial FS Compartment with BBC(InSW) it is possible to update the individual BBC(SW-x)s of the FS into the initial FS Compartments.

Each change of any BBC(SW-x) may have an impact on the deployment rules. It depends on the used BBC(DR) if the update can be done into the existing FS Compartment (in the case that BBC(DR) is unchanged) or if a new FS Compartment with new configuration according new BBC(DR) is necessary. Update of BIL BBCs can be automated by employing BIL tools by shared services to reduce the manual maintenance effort.

For update of Safe BBCs the automation support by the SCA is necessary.

3.2.3 Overall Context "Update of the Computing Platform"

Each SW update of the CP has to be processed by the CP Administrator.

1. A new version of the CP Software is installed by the CP Administrator
2. It depends on the details of the SW change within the new version of the CP Software if the existing FS Compartments with belonging configuration are affected or not.

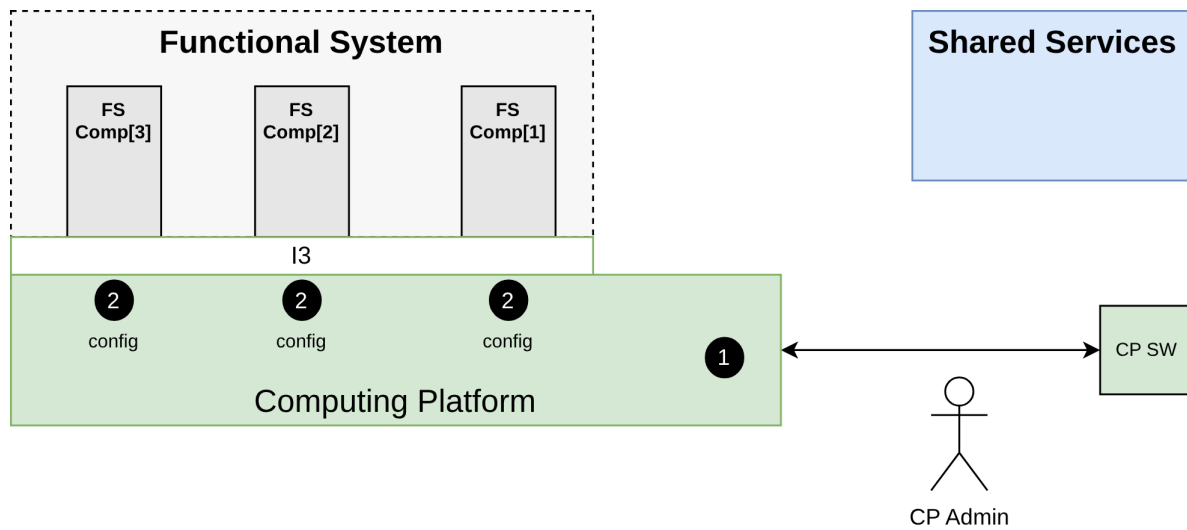


Figure 4 Overall context "Update of the Computing Platform"

Note : The SW update of the Computing Platform software could also be done via the Shared Services. This solution might be useful in some applications (onboard for example).

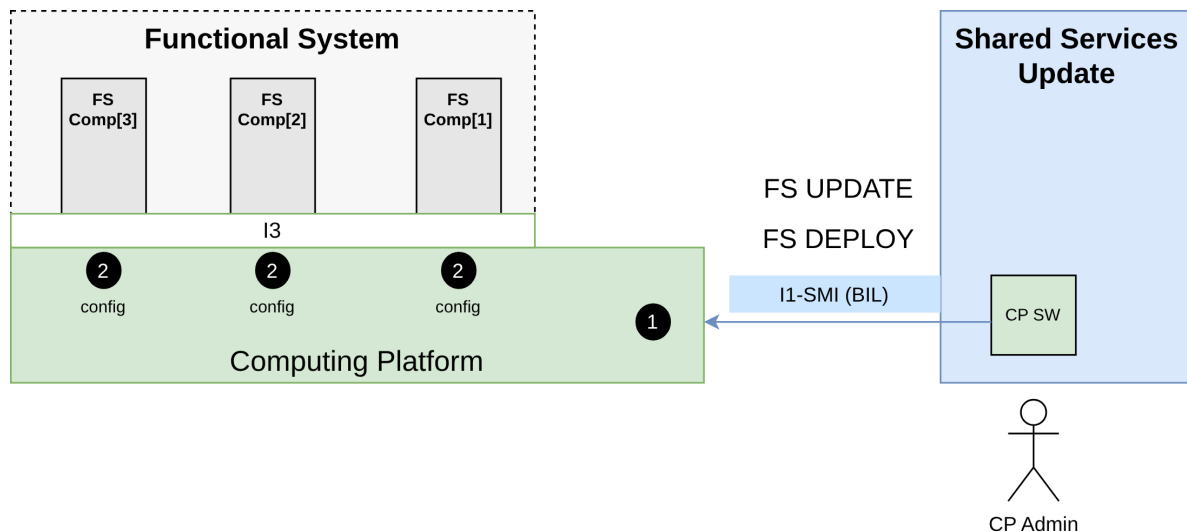


Figure 1 Overall context "Update of the Computing Platform using the Shared services"

3.2.4 Overall Context "Diagnosis"

Sources of diagnostic data:

1. Functional application, synchronised between the FS compartments
2. FS Compartment related data, individually for each FS Compartment (not synchronised and early available during the start-up phase).
3. a) FS Compartment related runtime state to CP for root cause analysis within CP
b) FS Compartment related state of the CP
4. Self-Diagnosis of the CP

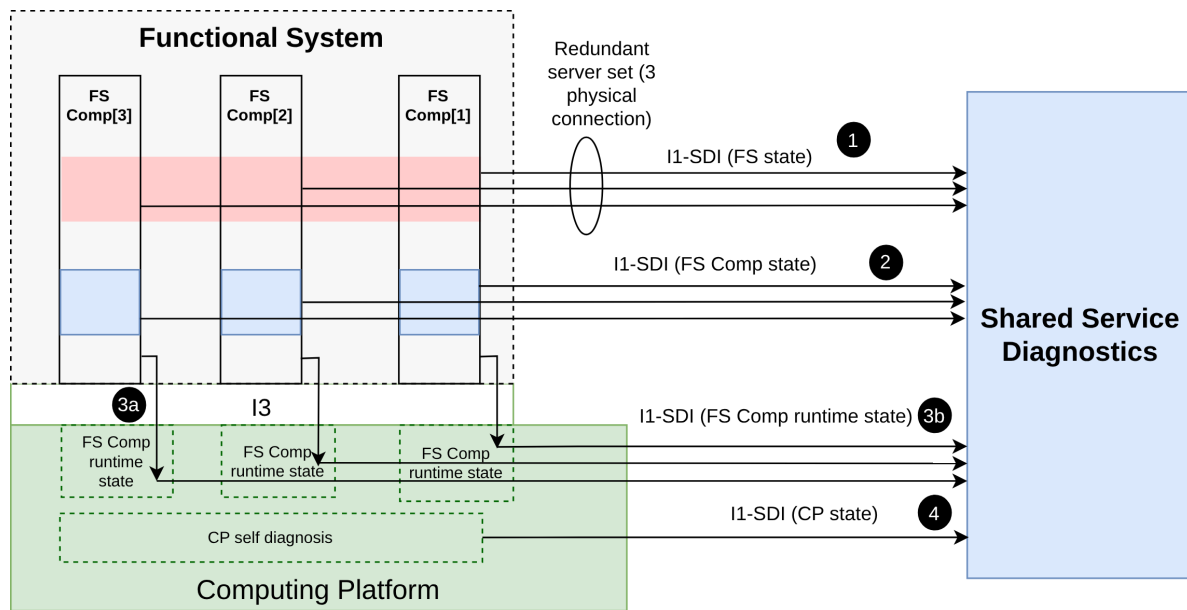



Figure 5 Overall context "Diagnosis"

3.2.5 Overall Context "Safety"


There are solutions building safe system using COTS components. The systematic HW failure is dealt through composite fail safety. The SE within the functional system has to take care of the systematic issues of the low level software from the computing platform. We leave this to the suppliers to provide the solutions. Systematic failures can be dealt through diversity. Random failures can be dealt through composite fail safety.

The SIL1/SIL2 use cases and Safety requirements currently being written by the PRAMS team have not been taken into account in this version of the document  SPT2CE-2502 - Open #SIL1/2

 SPT2CE-2565 - PRAMS Requirements

3.2.6 Overall Context "IT-Security"

From the perspective of the SSI overall architecture, each CP hardware, along with all the software operating on it (including CP software and FS compartments), is considered as a 'secure device.' This means that the certification for the secure device needs to be done for each individual CP hardware and all the running software parts provided by different suppliers. The allocation of FS Compartments onto to a CP hardware is not "static", in context of maintenance activities it shall be possible to re-allocate FS Comps onto another CP hardware.

 SPT2CE-2529 - Open #SSI - Secure device with frequent software and configuration





The COTS based CP itself must fulfil the IT security standards for rail systems.

 SPT2CE-2721 - Open #SSI - IT security of the COTS based CP

For the realisation of the IT security stack different software architectures are possible.

The IT security stack can be realised within each FS compartment, as separate FS Compartment or within the CP.

3.2.6.1 IT Security stack within the FS Compartment

1. Each FS Compartment contains its own IT security stack and provides the interface I1-IT sec SSI.
 SPT2CE-2339 - Fct-FS Comp - Provide I1-SSI by FS Comp .
2. The IT-security stack within the FS Compartment accesses the TPM of the CP hardware. The TPM is used to store security certificates for authentication and encryption.
 SPT2CE-2325 - Fct-CP SSI - Provide access to HW-based security solution e.g. TPM
 SPT2CE-2570 - Open #SSI - Usage of vTPM (virtual TPM)
3. The communication to other systems in context of diagnosis (I1-SDI), update (I1-SMI) and operative communication (I0-SCI) is encrypted according architecture definition SSI.
 This encryption is applied universally, regardless of whether the communication partner operates within a different secure device or within the same secure device.
 SPT2CE-2474 - Fct-FS Comp - Provide secure communication for I1 SDI, SMI and I0 SCI

The figure below illustrates the detailed steps specifically for FS-3. This approach is also applicable to FS-1 and FS-2, although the details are not fully shown to maintain clarity in the figure.

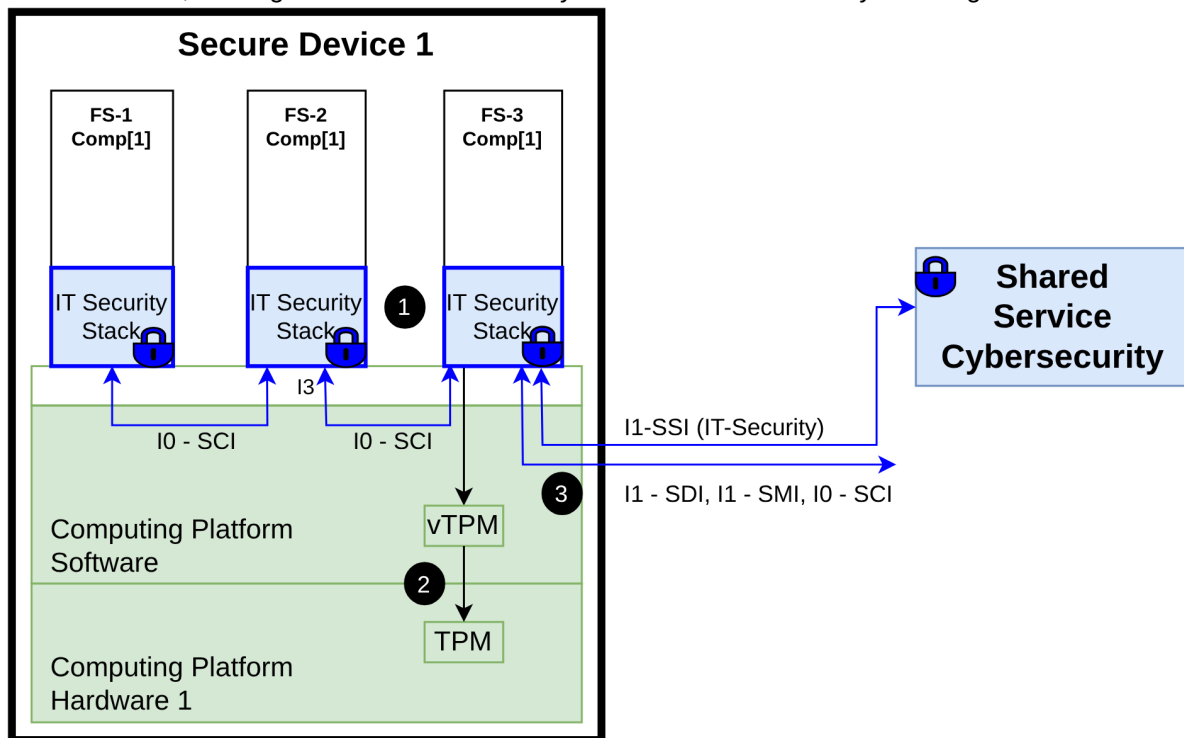






Figure6 Overall context "IT Security stack within each FS Compartment of the FS"


3.2.6.2 IT security stack as separate FS specific Compartment

For efficient FS related handling of IT-security related software it shall be possible to separate the IT security stack (with short lifecycle) from the functional FS Compartment (with long life cycle).

1. The IT-security stack is realised as separate FS related FS-IT Comp.
 The FS-IT Comp belongs to the FS and provides the interface I1-IT security SSI.
 SPT2CE-2339 - Fct-FS Comp - Provide I1-SSI by FS Comp .
 The functional FS Comp and the FS-IT Comp belong together to same FS.
 SPT2CE-2493 - Open #SSI - IT-Security stack as own FS-IT-Comp ?
2. The complete communication of the functional FS Comp to any other system (even to neighbour FS Comps of the same FS) is done via the FS-IT Comp.
 SPT2CE-2494 - Open #SSI - FS-IT-Comp latencies

3. The communication between the functional FS Comp (without IT security stack) and the FS-IT Comp is protected by mechanisms within the CP software.

 SPT2CE-2449 - Fct-CP SSI - Restriction and protection of the device-internal communication |

 SPT2CE-2495 - Open #SSI - CP protection for internal communication - what exactly ? |

The figure below shows the detailed steps exemplarily for the FS-3. This is in same way relevant for FS-1 and FS2, but not shown to keep the figure simple.

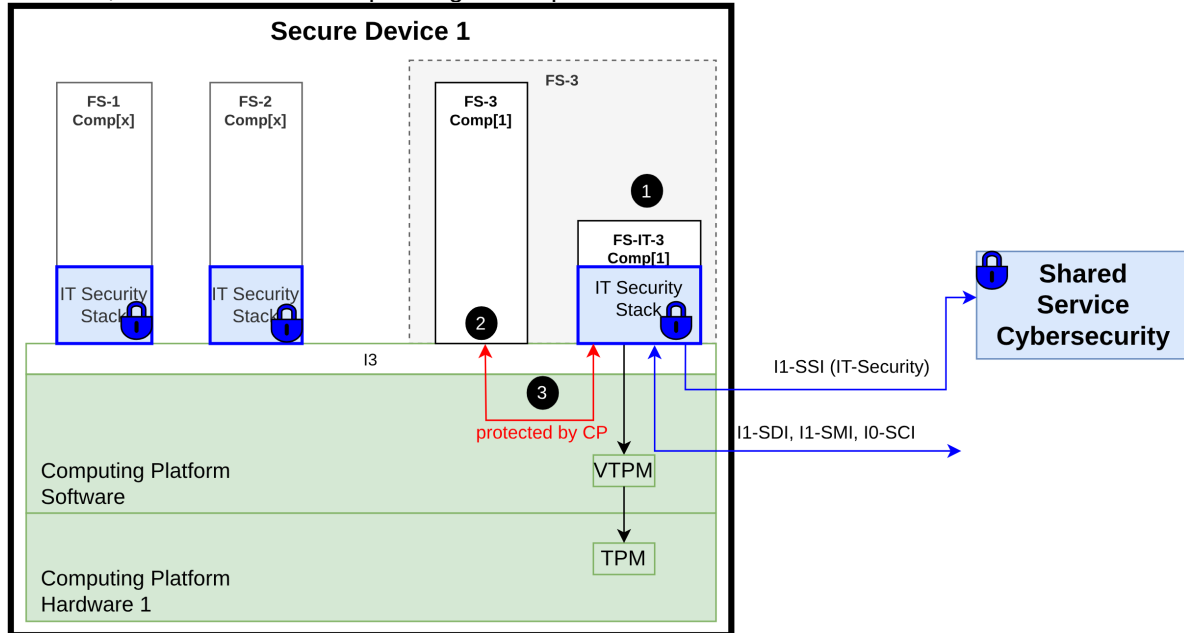








Figure 7 Overall context "IT Security stack as separate FS related FS-IT Comp"

3.2.6.3 IT security stack as separate standardised FS Compartment

For efficient generic handling of IT-security related software the IT security stack (with short lifecycle) can be realised as generic separate FS-IT Comp with standardised interface.

1. The IT-security stack is realised as separate generic FS-IT Comp.
The FS-IT Comp belongs to the CP and provides the interface I1-IT security SSI.
 SPT2CE-2564 - Open #SSI - CP Standardisation I3-SSI ?
 SPT2CE-2493 - Open #SSI - IT-Security stack as own FS-IT-Comp ?
2. The complete communication of each FS Comp to any other system (even to neighbour FS Comps of the same FS) is done via the FS-IT Comp.
The interface between the FS Comps and the FS-IT Comp is standardised as I3-SSI.
 SPT2CE-2494 - Open #SSI - FS-IT-Comp latencies
3. The communication between the functional FS Comps (without IT security stack) and the FS-IT Comp is protected by mechanisms within the CP software.
 SPT2CE-2449 - Fct-CP SSI - Restriction and protection of the device-internal communication |
 SPT2CE-2495 - Open #SSI - CP protection for internal communication - what exactly ?

 SPT2CE-2339 - Fct-FS Comp - Provide I1-SSI by FS Comp .

The functional FS compartment and the FS-IT compartment belong together to same FS.

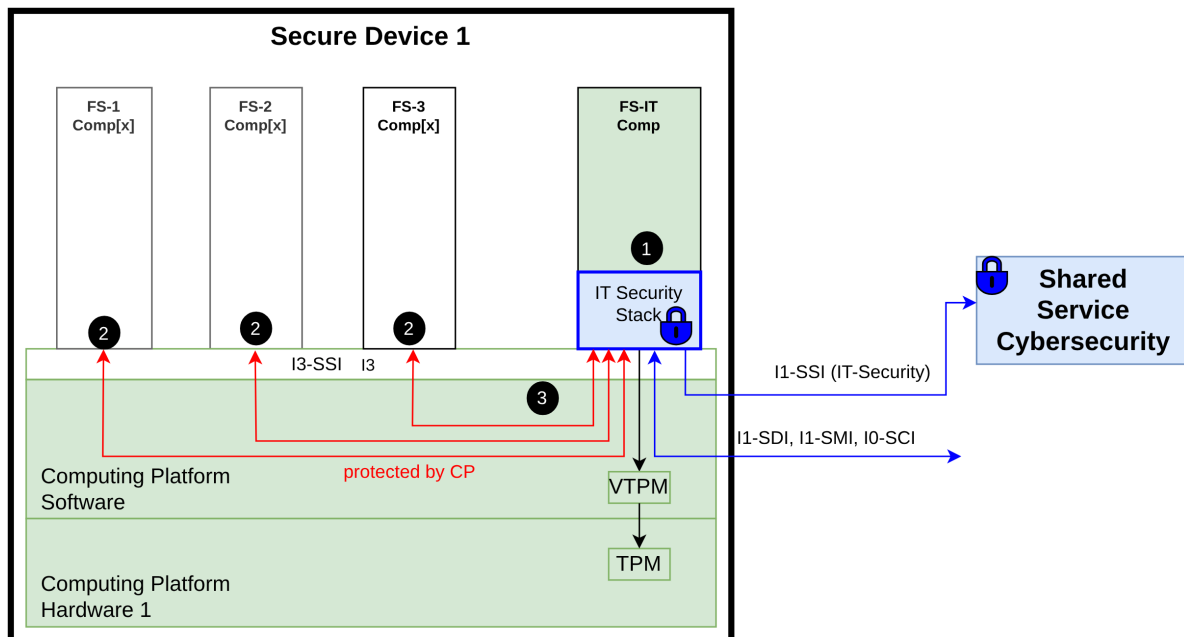









Figure 8 Overall context "IT security stack as separate generic (standardised) FS-IT Comp"

3.2.6.4 IT security stack as within the CP

The security stack can be applied with several possible configurations. The following configuration elaborates the IT-security stack as part of computing platform subsystem.

1. The IT-security stack is realised as part of the CP with standardised interface to the FS Comps.
 -  SPT2CE-2562 - Fct-CP SSI - Provide I3 with interface for secure communication of the FS Comp
 -  SPT2CE-2563 - Fct-CP SSI - Provide I1-SSI by CP
 -  SPT2CE-2564 - Open #SSI - CP Standardisation I3-SSI ?
 -  SPT2CE-2494 - Open #SSI - FS-IT-Comp latencies
2. The device internal communication between FS Comps is protected by the CP.
 -  SPT2CE-2495 - Open #SSI - CP protection for internal communication - what exactly ?
 -  SPT2CE-2537 - Open #SSI - IT-Security stack within the CP with standardised I3 to FS Comps ?
 -  SPT2CE-2564 - Open #SSI - CP Standardisation I3-SSI ?

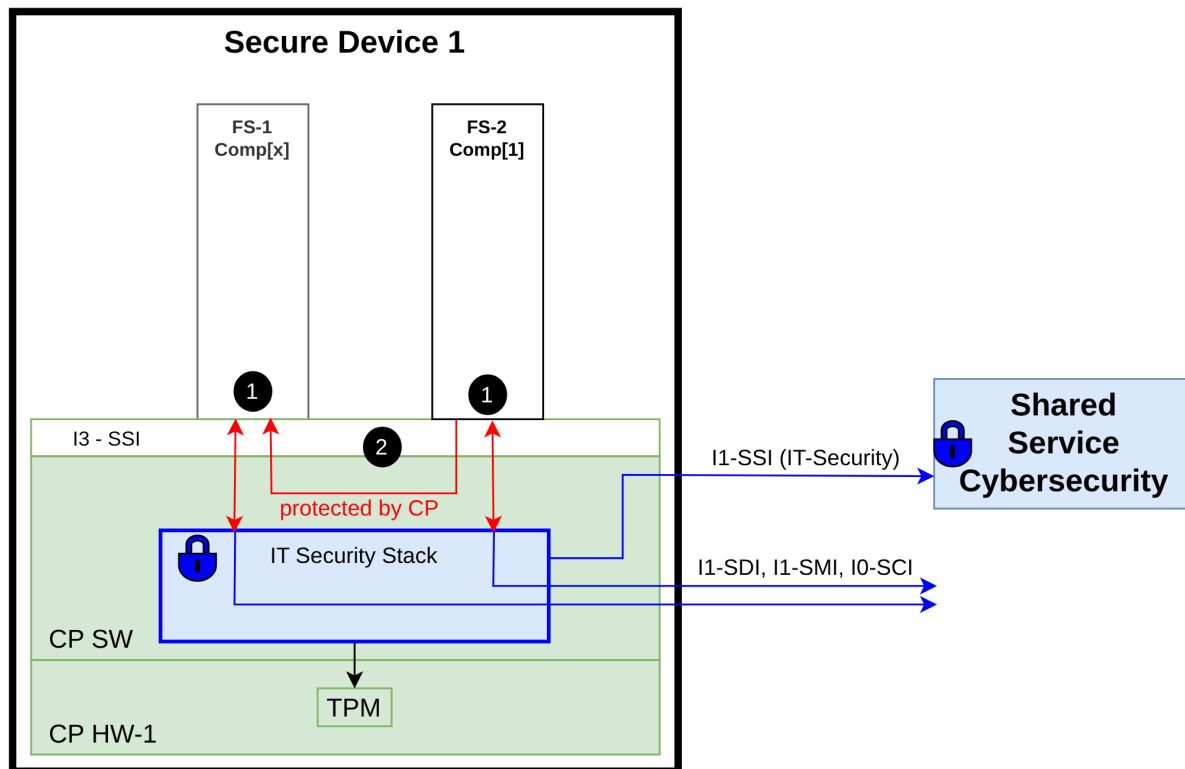


Figure 9 Overall context "IT security stack as part of the CP"

4 Scenarios

4.1 FS Execution

4.1.1 Aggregation of different kinds of FS Comp on same CP

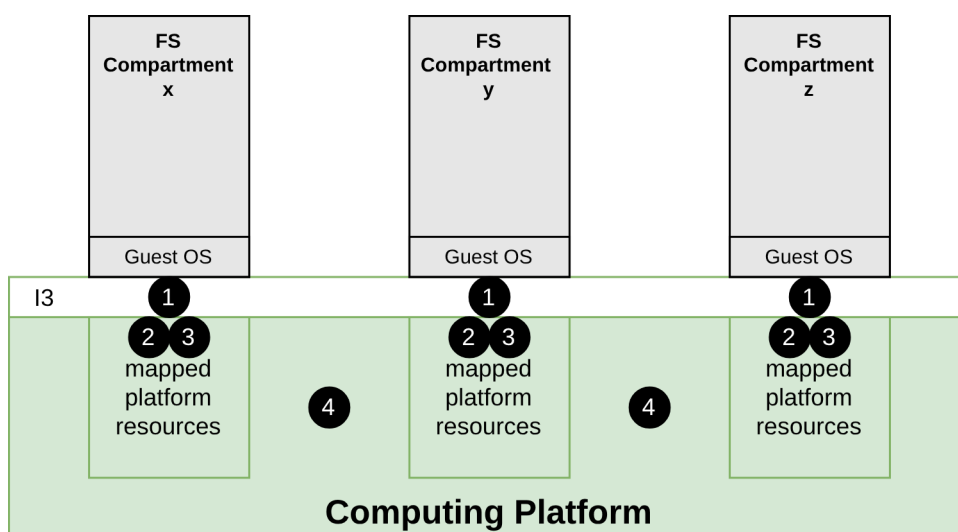


Figure 10 Scenario "Aggregation of different kinds of FS Comps on same CP"

1. Runtime Environment with flexibility in Guest OS

For the aggregation of different kinds of solutions of Functional Systems on the same Computing

Platform it shall be possible to run FS compartments with any Guest OS able to run on Computing Platform.

🔒 SPT2CE-1862 - Fct-CP Basic - Runtime environment for FS Comp

🔒 SPT2CE-2484 - Fct-CP Basic - CP as basic integrity standard solution for SW and HW

2. **FS compartment related mapping of platform runtime resources**

Each FS compartment needs its own platform runtime resources:. For this the BBC(DR) is provided for the FS compartment.

🔒 SPT2CE-2329 - Fct-FS Comp - Provide FS Comp deployment rules BBC(DR)

The Computing platform provides a mapping of the required runtime resources for the FS compartment according to the specific deployment rules described in the BBC(DR).

🔒 SPT2CE-2314 - Fct-CP Config - FS Comp related mapping of runtime resources

3. **FS compartment related network communication**

Each FS compartment needs network communication connections . The required network configuration is as well described in the FS compartment deployment rules BBC(DR).

🔒 SPT2CE-2329 - Fct-FS Comp - Provide FS Comp deployment rules BBC(DR)

Computing platform configures the required network communication for the FS compartment according to the specific deployment rules described in the BBC(DR)..

🔒 SPT2CE-2327 - Fct-CP Config - FS Comp related mapping of communication resources

4. The Computing Platform provides strict **resource isolation**

To achieve highest availability of the running FS compartments its essentially important that there are no cross-effects in context of platform resource usage between FS compartments running in parallel.

🔒 SPT2CE-2315 - Fct-CP Basic - Isolation of the resources mapped to different FS comps

Note:

Resource isolation must not affect safety but may affect availability (safety layer must assume that there could be isolation issues and must react accordingly).

CP SW is mainly not safety critical and the safety environment of the functional system shall provide the necessary safety.

The only safety related aspects in the Computing Platform are:

- a. providing of a unique HW identification to the FS Comp (safety layer) to ensure the distribution of parallel FS Compartments on different physical computing elements
- b. providing a steady clock source from the physical computing element to the FS Comp (safety layer) to create a safe clock.

🔒 SPT2CE-1901 - Fct-CP Basic - Provide steady clock from physical hardware of used CP HW node via I3-CP

- c. Additional HW related information e.g. temperature, voltage etc.

Safety related requirements from PRAMS for the behavior of a FS (as e.g. response time, ..) shall be addressed by the safety layer within the FS. Such requirements are not relevant for the underlying CP.

The PRAM requirements included in the deployment rules shall be addressed by the CP. |

4.1.2 Network Communication of a FS Comp

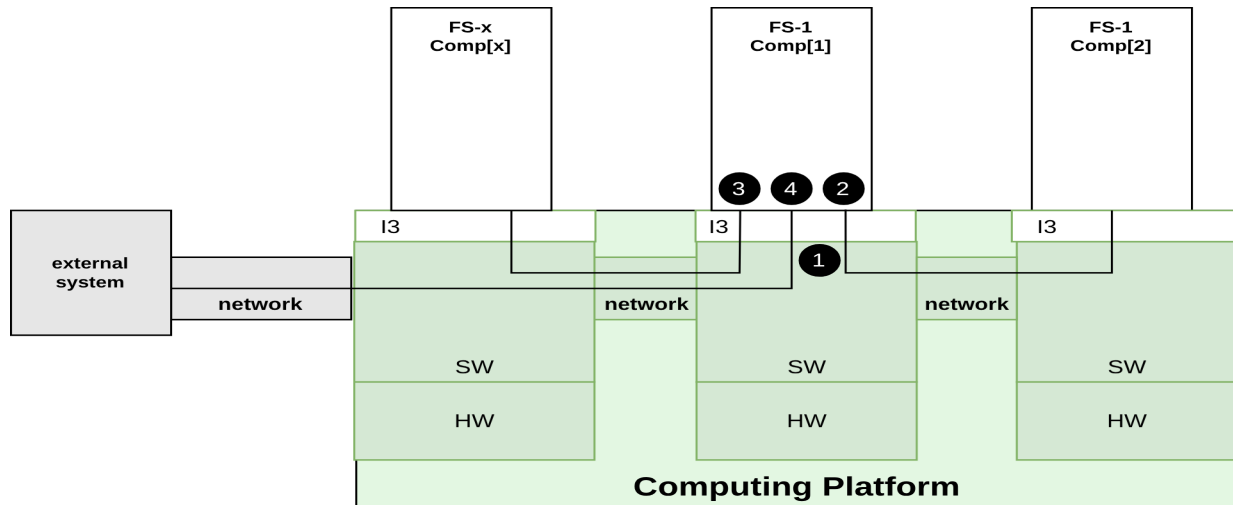


Figure 11 Scenario "Network Communication of a FS Comp"

1. Each FS Comp needs network communication connections as described in the BBC(DR).
2. The FS Comp communicates to neighbour-FS Comp(s) of the same FS
3. The FS Comp communicates to FS Compartments of other FS running on same CP
4. The FS Comp communicates to external systems which run outside of the CP (e.g. decentralised object controllers).

4.1.3 Running of FS Comps - safety related aspects

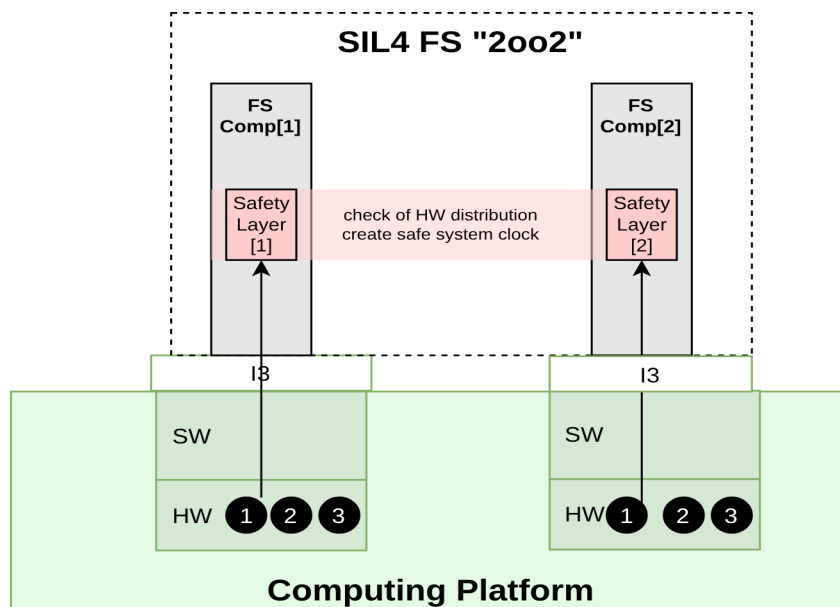


Figure 12 Scenario "Running of FS Comps of a SIL4 FS - safety related aspects"

It shall be feasible to run safety critical FS software on the computing platform. To facilitate this some safety related requirements of the Safety Layer of a FS shall be fulfilled by the Computing Platform:

1. **Distribution of safety critical FS Compartments on separate physical machines**
A basic safety principle of a SIL4 safety layer is the execution of safety critical software as parallel

channels on separated physical machines with safe voting of the channel outputs.

This means that the safety related FS compartments shall run on separate physical machines and the safety layer shall check this distribution safely.

This shall be described in the FS compartment deployment rules BBC(DR).


 SPT2CE-2329 - Fct-FS Comp - Provide FS Comp deployment rules BBC(DR)

For this a unique HW identification of the used physical machine is needed in every FS compartment to implement a safe check of the SW distribution on different hardware.


 SPT2CE-2592 - Fct-CP Basic - Provide ID of the used physical CP HW node via I3-CP

2. Steady system clock.


The safety layer must ensure a safe time behaviour and needs for this a reliable steady clock from the used physical machine. For this each FS compartment of the safety layer needs a steady clock which is created by the physical clock of the physical machine the FS compartment is running on.

 SPT2CE-1901 - Fct-CP Basic - Provide steady clock from physical hardware of used CP HW node via I3-CP

3. Additional HW related information as e.g. CPU temperature, voltage information, .. may be required by the safety layer of a FS. This depends on implementation details of the safety layer used.

 SPT2CE-2496 - Open #NHA - additional HW related information

This solution does NOT address the need of running a SIL2 application on a single hardware (common use case for onboard applications) and added as an open point

 SPT2CE-2502 - Open #SIL1/2

4.1.4 Running of FS Comps - IT security related aspects

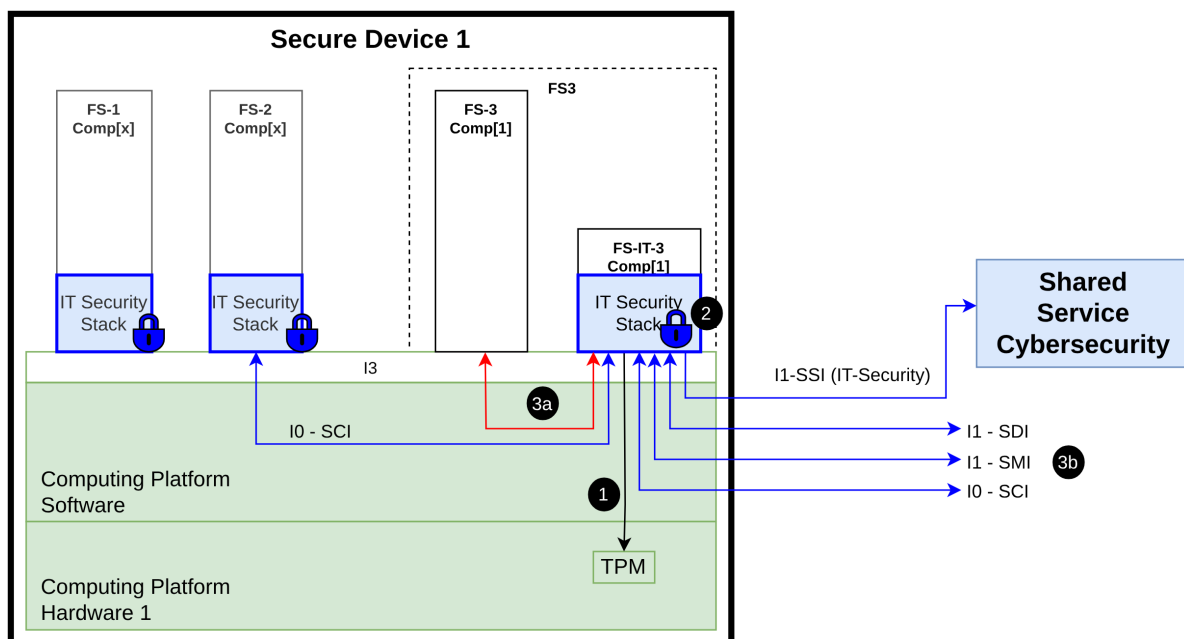








Figure 13 Scenario "Running of FS Comps - IT-security related aspects"

Several FS Comps of different FS are running in parallel on the same CP hardware within the same Secure Device.


1. The IT Security Stack accesses via interface I3 the TPM of the used Computing Platform Hardware.
 -  SPT2CE-2325 - Fct-CP SSI - Provide access to HW-based security solution e.g. TPM
2. The IT-Security Stack of the FS-IT compartment provides the interface I1-IT security SSI.
 -  SPT2CE-2339 - Fct-FS Comp - Provide I1-SSI by FS Comp
 -  SPT2CE-2539 - Fct-FS Comp - Provide I1-SSI by separate FS related FS-IT Comp
 -  SPT2CE-2530 - Open #SSI - FS Comp - which part of SSI provided by the functional FS Comp
3. The communication of the functional FS compartment to other systems is done via the FS-IT compartment.

3a - the communication between the functional FS Compartment and the FS-IT Compartment is protected by the CP

 SPT2CE-2495 - Open #SSI - CP protection for internal communication - what exactly ?

 SPT2CE-2449 - Fct-CP SSI - Restriction and protection of the device-internal communication .
3b - the FS-IT compartment forwards the communication traffic with encryption according the IT security architecture SSI.

This affects the interfaces in context of diagnosis (I1-SDI), update (I1-SMI) and operative communication (I0-SCI).

 SPT2CE-2474 - Fct-FS Comp - Provide secure communication for I1 SDI, SMI and I0 SCI

4.2 Deployment Scenarios

4.2.1 Deployment of the CP Software

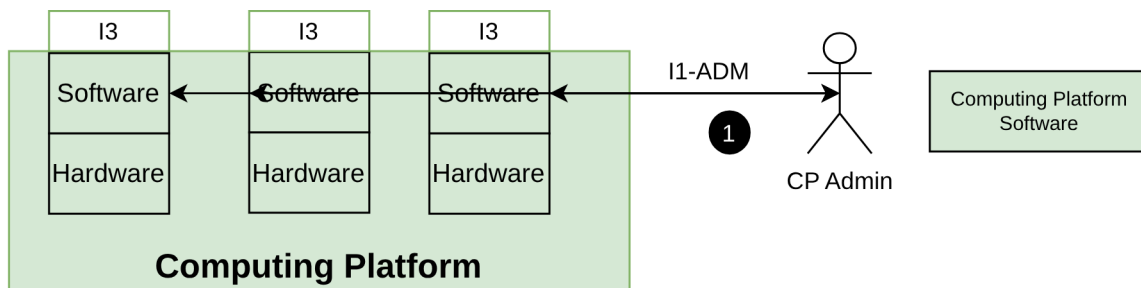




Figure 14 Scenario "Deployment of CP Software onto the CP Hardware"

1. The CP Software is deployed by the CP Admin onto the CP Hardware.

 SPT2CE-1899 - Fct-CP - Deploy CP Software onto CP Hardware

4.2.2 Deployment of the FS Software onto the CP

The FS software consists of several FS Comps and each FS Comp consists of several BBCs.

 SPT2CE-2508 - Fct-SS - SMI - Considering FS Comp related BBC structure for FS release management

Example:

Safety related FS with 2oo3 principle = 3 FS Comps.

Each FS Comp consists of 4 BBCs:

- BBC(DR) = Deployment rules for the FS Comp, used by the CP software
- BBC(InSW) = Initial software with bootloader functionality for the Initial FS Comp
- BBC(SW-1) = basic integrity OS with belonging data
- BBC(SW-2) = safety layer with safe application and belonging data

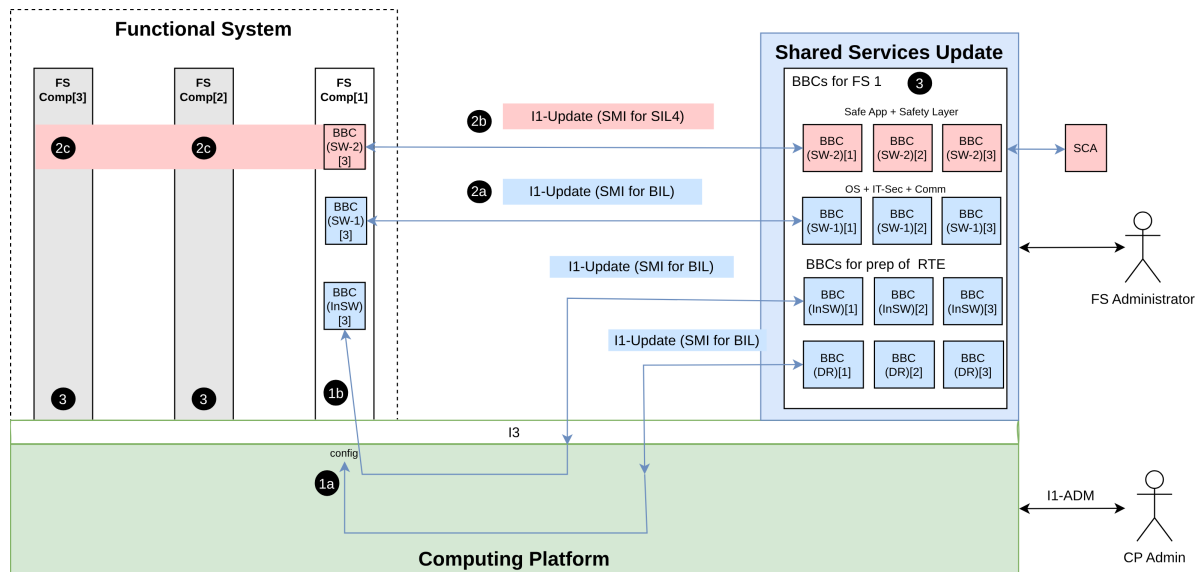


Figure 15 Scenario "Deployment of FS Software onto the CP"

The FS consists of three FS Comps, these are the steps for each FS Comp:

1. Creation of the Initial FS Comp 1:

- 5F SPT2CE-2516 - Fct-SS - SMI - Initiate the first deployment of a new FS via interface I1-SMI onto the CP
- 5F SPT2CE-2512 - Fct-CP SMI - CP with SMI service to provide interface I1-SMI for FS Comp deployment
- 5F SPT2CE-1911 - Fct-CP Config - FS related CP configuration according to deployment rules
- 5F SPT2CE-2314 - Fct-CP Config - FS Comp related mapping of runtime resources
- 5F SPT2CE-1850 - Fct-CP SMI - Creation of the Initial FS Comp with BBC(InSW)

a. Preload the FS Comp related BBC(DR) and BBC(InSW) through SMI.

- 5F SPT2CE-2329 - Fct-FS Comp - Provide FS Comp deployment rules BBC(DR)
- 5F SPT2CE-2497 - Open #SMI - How to handle dependencies?

- i. Check if the activation would be successful.
- ii. Package integrity check

b. Activation of the BBCs through SMI

i. Create FS Compartment with initial BBC(InSW) according to BBC(DR)


- 5F SPT2CE-2319 - Fct-FS Comp - Provide BBC(InSW) with SMI client functionality

- ii. Start Compartment
- iii. Verify the activation

1. Deployment of FS Comp software into FS Comp 1:

- 5F SPT2CE-1904 - Fct-FS Comp - Process update BBC(SW) into existing FS Comp according I1-SMI

- a. Preload the basic integrity **BBC(SW-1)[1]** through **SMI** into the existing FS Compartment 1
Activation of the BBC(SW-1){1} through SMI.
- b. Preload the SIL4 **BBC(SW-2)[1]** through **SMI** into the existing FS Compartment 1.
Activation of the BBC(SW-2){1} through SMI.
Confirmation for safe BBCs
This process is safety related and requires the consideration of the neighbour FS Compartments and involvement of the Safe Configuration Authority SCA.
- c. The safety related process with SCA involvement requires on side of the FS a safe state of the FS. For this least 2 FS compartments must run with synchronised safety layers.
For this the deploy and start of FS neighbour-compartments is necessary, see 3.


 SPT2CE-2337 - Fct-FS Comp - Sync with neighbour FS Comp for safe update SMI

2. Repeat 1. und 2. for FS Comp 2 and FS Comp 3.



The steps 1. and 2. need to be repeated for FS Compartment 2 and FS Compartment 3.

This is in responsibility of the Shared Services.

 SPT2CE-2335 - Fct-SS - SMI - Handling of FS Comp relationships for update of basic integrity BBCs

 SPT2CE-2336 - Fct-SS - SMI - Handling of FS Comp relationships for update of safe BBCs

For optimised SW maintenance of the CP SW during operation of the FS, it is recommended to only FS with the same redundancy principle should be deployed on the same shared hardware.

 SPT2CE-2505 - Fct-CP Config - FS Comp mapping to CP HW according to FS redundancy principle
For this see  SPT2CE-2296 - Scenario "Update of the CP Software onto the CP Hardware"

4.3 Update Scenarios

4.3.1 Update of the CP Software onto the CP Hardware

The update of the CP software on the CP hardware must be achievable without requiring the simultaneous stoppage of all FS compartments. Halting all FS compartments at once would result in a complete cessation of all FS operations. To facilitate updates during operation, the CP software can be updated incrementally for individual CP hardware nodes, adhering to the redundancy principles established for the affected FS running on the CP hardware.

The redundancy principle of an FS allows for the temporary shutdown of a single FS compartment, such as when performing a software update of the CP software. During this process, while one FS compartment is offline for the CP software update, the FS continues to operate with reduced redundancy. For instance, in a SIL4 FS utilising a 2oo3 (two out of three) principle, the system remains functional as a 2oo2 (two out of two) configuration.

Once the CP software update is complete, the affected FS compartment will restart and synchronise with the other FS compartments, restoring full redundancy to the FS. This incremental approach enables the CP software to be updated step-wise for each CP hardware node while maintaining operational continuity for the FS.

For aggregated SIL4 FS operating on the same CP hardware, it is advisable to deploy these systems according to their redundancy principles. For example, only SIL4 FS employing the 2oo3 (two out of three) principle should be hosted on the same CP hardware. This 'sorted software deployment for SIL4 systems' facilitates a structured CP software update of the redundancy channels while the SIL4 FS continues to operate.

The figure below shows as example two SIL4 FS (FS-1 and FS-2) with 2oo3 principle deployed on the same CP-HW-1/2/3.

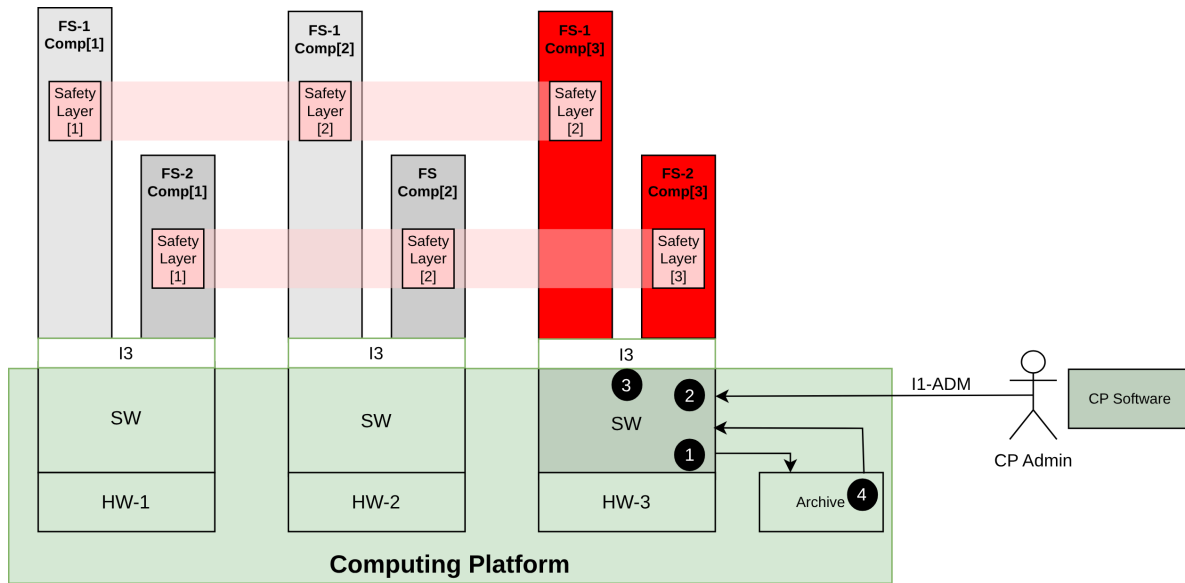


Figure 16 Scenario "Update of the CP Software onto the CP hardware"

The update for a SIL4 FS with 2oo3 principle is done in the following steps:

1. Creation of a backup of the current used CP software version and configuration.
SF SPT2CE-1978 - Fct-CP - Backup CP Software and CP Configuration
2. The CP software update is done CP hardware-wise "one after the other".
 When the CP SW update is done for one HW and the FS Comps on this CP hardware are running and synchronised with the neighbour FS Comps the CP, then the CP SW update can be done for the next CP HW.
SF SPT2CE-1984 - Fct-CP - Update CP software HW-wise
3. The new CP Software has to support the compatibility to already existing FS compartments
SF SPT2CE-2503 - Fct-CP - Update CP software with compatibility for I3 and configuration
4. If the update is not successful (does not work) a roll-back to the previous version is necessary.
SF SPT2CE-2328 - Fct-CP - Restore CP backup-version of the CP Software and CP Configuration

4.3.2 Update of FS software

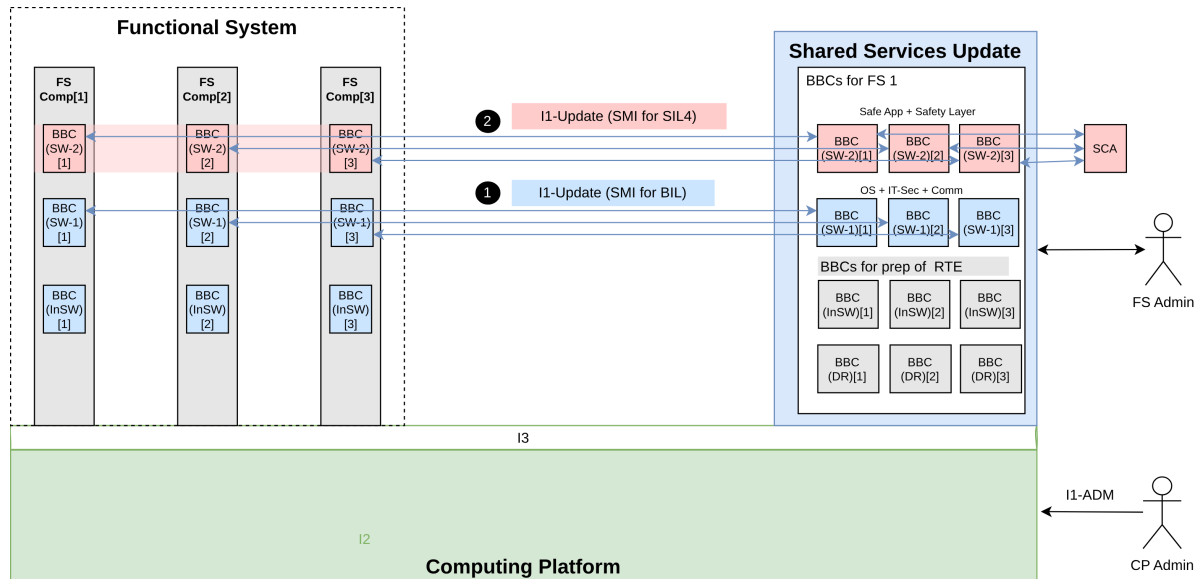


Figure 17 Scenario "Update of the FS software"

The update of a running FS with new version(s) of a BBC(SW) is done BBC-wise between Shared Services and FS Compartment without involvement of the Computing Platform.

SF SPT2CE-1904 - Fct-FS Comp - Process update BBC(SW) into existing FS Comp according I1-SMI
The process for this BBC related update is defined as SMI.

The quantity of BBCs and the safety criticality of the individual BBCs depend on the details of the FS solution.

1. For **basic integrity BBCs** the update is possible during runtime of the FS, using the redundancy principle of the FS.
Basic integrity BBCs run independent without synchronisation to other FS compartments. By this there is no need to run the same BBC version in different FS compartments. A change of the BBC is possible compartment-wise with shut-down and new start without affecting the other running FS compartments, means a SIL4 FS with 2oo3 principle keeps running as 2oo2 during update of a BBC in one compartment.
This relationship between the basic integrity BBCs of a FS has to be considered on side of the Shared Services.
SF SPT2CE-2335 - Fct-SS - SMI - Handling of FS Comp relationships for update of basic integrity BBCs
(Note: Lower SIL function and application are not included in the analysis, further investigation for such system would be needed.).
2. For **SIL4 BBCs** the update is mostly necessary for all FS compartments in parallel.
SIL4 BBCs are synchronised between the parallel FS channels running within the individual FS compartments with a safe synchronisation in between. This leads to the constraint that in case of change of behavior of the new SIL4 BBC this SIL4 BBC needs to be updated in parallel in all FS compartments.
This relationship between the SIL4 BBCs of a FS has to be considered on side of the Shared Services.
SF SPT2CE-2336 - Fct-SS - SMI - Handling of FS Comp relationships for update of safe BBCs

For efficient patching the Shared Services Update supports automation.

SF SPT2CE-2519 - Fct-SS - SMI - Automation of basic integrity updates for patching.

4.4 Recovery Scenarios

In the context of failure handling the CP is only able to see if a FS Comp is running actively or not. As long as the FS Comp is running the state is "ok" for the CP.

The CP does not know the dependencies and relationships between individual compartments of a FS. The CP does not know any details about failures in the behavior of a running FS Comp (as e.g. wrong time behavior, corruption of data messages, ...).

All failures which can happen for a running FS Comp must be identified by the FS Comp itself, the FS Comp is responsible for failure identification, safe reaction and providing diagnostic data via I1-SDI to Shared Services Diagnostics.

4.4.1 SW Failure within a individual FS Comp

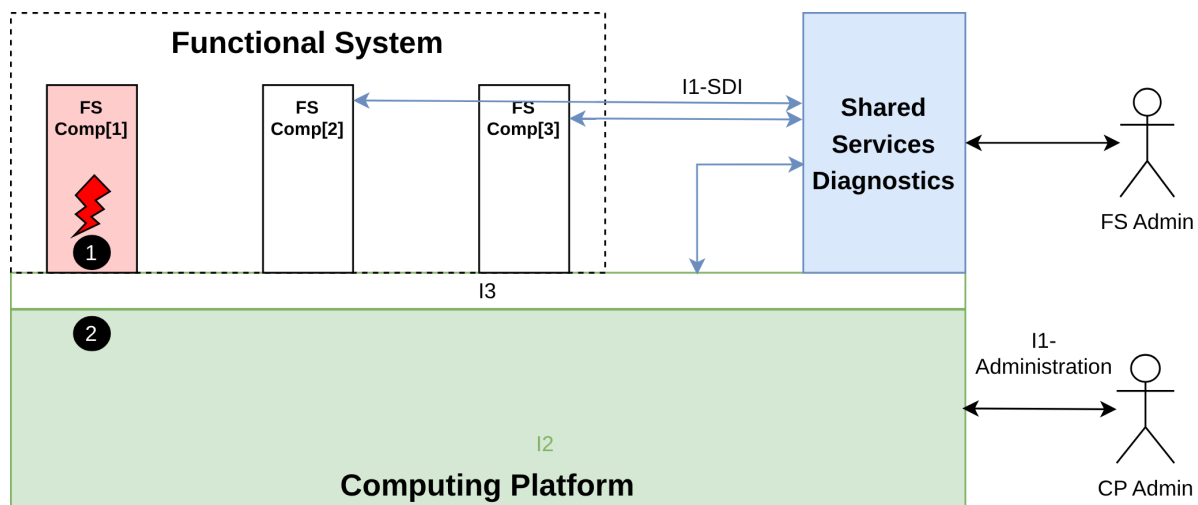




Figure 18 Scenario "SW Failure within an individual FS Compartment"


An individual FS Comp of a SIL4 FS with 2oo3 principle fails. The other FS Comp[2] and FS Comp[3] identify the failure of FS Comp[1] and provide this information via I1-diagnostics SDI


 SPT2CE-2338 - Fct-FS Comp - Provide FS state according SDI .

Shared Service aggregates the FS Comp related state to a FS state. Shared Services determine the FS state from the diagnostic data received from the respective FS Compartments.

 SPT2CE-1843 - Fct-SS - SDI - Aggregate FS Comp runtime states to FS runtime state

Root cause is a software failure within the FS Comp.


 SPT2CE-2323 - Fct-CP SDI - Process root cause analysis for FS Comp failures

 SPT2CE-1846 - Fct-SS - SDI - Provide root cause for SW failure in FS Comp

As a result, the recovery steps are focused on software repair within the same FS compartment

A repair is possible by

1. Automatic restart of the FS compartment itself


 SPT2CE-1876 - Fct-FS Comp - automatic self-restart of the FS Comp for recovery


2. Automatic restart of the FS compartment by the Computing Platform.

CP identifies the failures of the FS compartment (by missing of the FS Compartment state) and restarts the FS compartment.

 SPT2CE-1848 - Fct-CP Rec - Automatic Restart of a existing FS Comp which has failed

If a automatic restart is not successful the failed FS Comp needs to be repaired by re-installation (on same or other CP hardware).

 SPT2CE-2527 - Fct-CP Rec - Automatic deployment of a failed FS Comp on another CP location

 SPT2CE-2499 - Open #SMI - Re-install failed FS Compartment on another CP hardware ?

 SPT2CE-2528 - Open #CP #SMI - Automatic deployment of a failed FS Comp onto another CP location

4.4.2 SW Failure within the CP

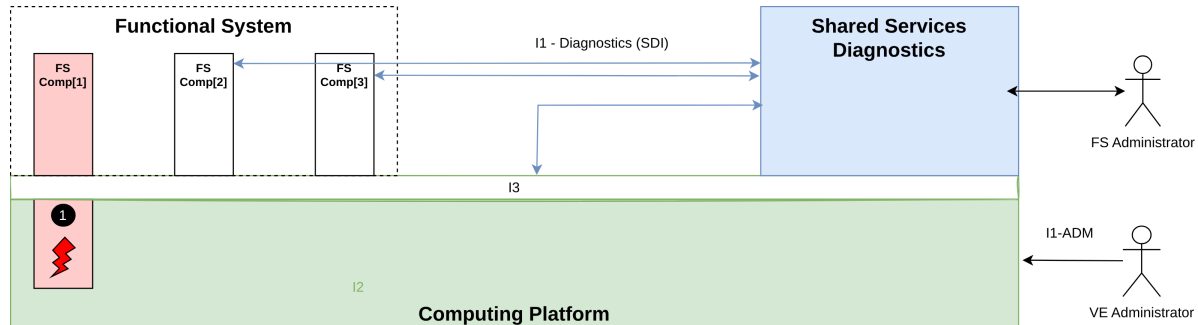





Figure 19 Scenario "SW Failure within the CP"

A SW failure within the CP leads to a failure of FS Comp[1]. The other FS Comp[2] and FS Comp[3] identify the failure of the FS Comp[1] and provide this information as diagnostic data via I1-diagnostics SDI.

 SPT2CE-2338 - Fct-FS Comp - Provide FS state according SDI

Root cause for FS Comp[1] failure is a software failure within the CP.


 SPT2CE-2323 - Fct-CP SDI - Process root cause analysis for FS Comp failures


 SPT2CE-2322 - Fct-CP SDI - Provide CP diagnostic data according I1-Diag SDI

Root cause for FS failure is a failure of FS Comp[1].


 SPT2CE-1846 - Fct-SS - SDI - Provide root cause for SW failure in FS Comp


As a result, the recovery steps focus on software repair within the Computing Platform, along with the restart of the existing FS Compartment[1].


 SPT2CE-2398 - Fct-CP Rec - Repair of a SW failure within the CP software

 SPT2CE-1848 - Fct-CP Rec - Automatic Restart of a existing FS Comp which has failed

If such a repair is not possible the failed FS Comp needs to be deployed onto another VCE of the CP

 SPT2CE-2527 - Fct-CP Rec - Automatic deployment of a failed FS Comp on another CP location

 SPT2CE-2499 - Open #SMI - Re-install failed FS Compartment on another CP hardware ?

 SPT2CE-2528 - Open #CP #SMI - Automatic deployment of a failed FS Comp onto another CP location

4.4.3 HW Failure within the CP

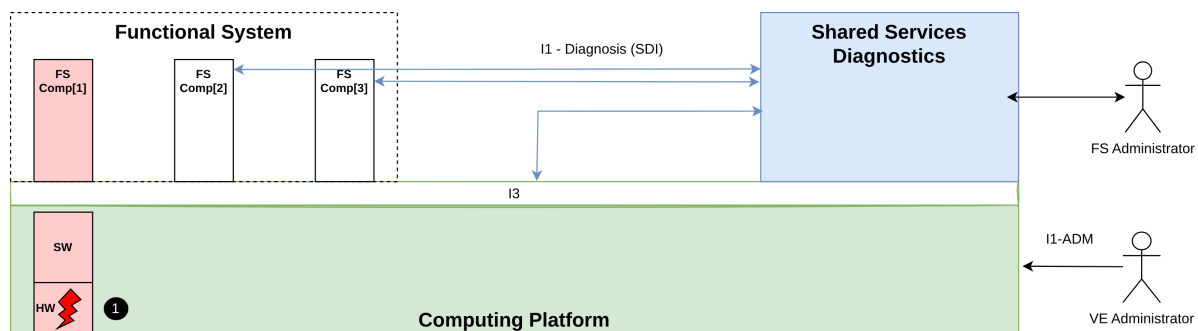





Figure 20 Scenario "HW failure within the CP"


A HW failure within the CP leads to the failure of the FS Comp[1]. FS Comp[2] and FS Comp[3] identify the failure of FS Comp[1] and provide this information as diagnostic data via I1-diagnostics SDI.

 SPT2CE-2338 - Fct-FS Comp - Provide FS state according SDI

Root cause is a hardware failure within the CP.

 SPT2CE-2431 - Fct-CP SDI - State monitoring of the CP hardware nodes


 SPT2CE-2323 - Fct-CP SDI - Process root cause analysis for FS Comp failures

 SPT2CE-2322 - Fct-CP SDI - Provide CP diagnostic data according I1-Diag SDI


 SPT2CE-1846 - Fct-SS - SDI - Provide root cause for SW failure in FS Comp

Repair by usage of a spare hardware:


1. Deactivation of the defective hardware


 SPT2CE-2402 - Fct-CP Rec - Deactivate an individual CP hardware node


2. Deploy of the CP software onto a spare hardware

 SPT2CE-2055 - Deployment of the CP Software

3. Deploy of the FS Comp[1] onto a spare hardware

 SPT2CE-2527 - Fct-CP Rec - Automatic deployment of a failed FS Comp on another CP location

 SPT2CE-2528 - Open #CP #SMI - Automatic deployment of a failed FS Comp onto another CP location

 SPT2CE-2054 - Deployment of the FS Software onto the CP

4.4.4 Network failure within the CP

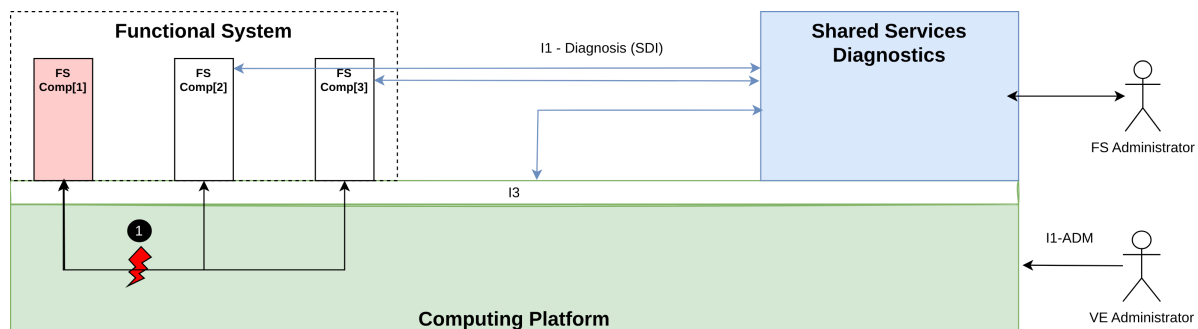





Figure 21 Scenario "Network failure within the CP"

A network failure within the CP leads to a failure "disconnection of FS Comp[1]". The other FS Comp[2] and FS Comp[3] identify the missing of FS Comp[1] and provide this information as diagnostic data via I1-diagnostics SDI.

 SPT2CE-2338 - Fct-FS Comp - Provide FS state according SDI

Root cause is a network failure within the CP.

 SPT2CE-2433 - Fct-CP SDI - State monitoring of the network communication

 SPT2CE-2323 - Fct-CP SDI - Process root cause analysis for FS Comp failures

 SPT2CE-2322 - Fct-CP SDI - Provide CP diagnostic data according I1-Diag SDI

 SPT2CE-1846 - Fct-SS - SDI - Provide root cause for SW failure in FS Comp

Depending on the root cause different repair scenarios are possible:

Reset or replacement of network components (as e.g. switches, cables, ..), replacement of network cards, restart of the CP software.




5 SubSystem Capabilities

The following capabilities describe the high-level functions of each subsystem, required to meet the objectives of the system.

5.1 Application Execution Environment (AEE)

SPT2CE-2455 - Host applications up to SIL 4





Run safety related (up to SIL4) and non-safety-related applications on the same computing platform ensuring resource allocation and isolation and necessary network communications.

Status	 Open
Linked Work Items	C2P-has parent :  SPT2CE-2580 - Support for application up to SIL4 has parent :  SPT2CE-2608 - Application Execution Environment (AEE)

SPT2CE-2454 - Manage application lifecycle

The CP manages application life cycle such as deployment, execution, update and termination.






- **Deploy:** The capability to deploy Functional System (FS) compartments on the Computing Platform (CP) using Building Block Configurations (BBC) deployment rules.
- **Update:** The capability to update existing FS compartments on the CP without interrupting the system's operation.
- **Execution:** The capability to run the FA onto the CP
- **Termination:** The capability to stop and dismantle the FS compartment on the CP without interrupting the system's operation.

Status	 Open
Linked Work Items	C2P-has parent :  SPT2CE-2576 - Remote Management and Configuration has parent :  SPT2CE-2608 - Application Execution Environment (AEE) _C2P-is parent of :  SPT2CE-2583 - Harmonised Deployment Processes

5.2 Computing Platform Software (CPSW)




SPT2CE-2464 - Provide compartment execution environment.

Provide compartment execution environments that are isolated from each other and allow hosted applications to communicate using virtualised hardware resources, enabling interfacing with existing systems.

Status	 Open
Linked Work Items	C2P-has parent :  SPT2CE-2577 - Scalability and System Flexibility C2P-has parent :  SPT2CE-2582 - Resource Optimisation and Aggregation C2P-has parent :  SPT2CE-2575 - Interoperability with Existing Systems has parent :  SPT2CE-2607 - Computing Platform Software (CPSW)


SPT2CE-2453 - Manage access to platform services via Interface I3.

Provides services such as resource allocation and native hardware access.

Status	 Open
Linked Work Items	C2P-has parent :  SPT2CE-2581 - Minimisation of Dependencies has parent :  SPT2CE-2607 - Computing Platform Software (CPSW)




SPT2CE-2460 - Abstract hardware details from the AEE via Interface I3.

Provides virtualised and abstract hardware to host functional applications

Status	 Open
Linked Work Items	C2P-has parent :  SPT2CE-2584 - Efficient Hardware Replacement has parent :  SPT2CE-2607 - Computing Platform Software (CPSW)




SPT2CE-2568 - Access to specific low-level hardware modules.

Provide access to low level hardware modules e.g. TPM, sensors etc.

Status	 Open
Linked Work Items	has parent :  SPT2CE-2607 - Computing Platform Software (CPSW) _C2P-is parent of :  SPT2CE-2578 - Enhanced Security and Integrity


SPT2CE-2468 - Provide and manages compute resources (e.g. CPU, Memory, Storage, Network).

The Computing Platform Software shall provide the equivalent amount of HW resources as configured by the Application for each compartment.

Status	 Open
Linked Work Items	C2P-has parent :  SPT2CE-2584 - Efficient Hardware Replacement has parent :  SPT2CE-2607 - Computing Platform Software (CPSW)




SPT2CE-2469 - Provide fault tolerance.

The Computing Platform Software provides mechanisms to enable fault tolerance for maintaining system reliability. The FS should be responsible to implement and ensure fault tolerance.

Status	 Open
Linked Work Items	has parent :  SPT2CE-2607 - Computing Platform Software (CPSW) _C2P-is parent of :  SPT2CE-2579 - Recovery and Resilience

SPT2CE-2452 - Enforce security policies.




Implement IT security measures to protect FS compartments and the Computing Platform

Status	 Open
Linked Work Items	C2P-has parent :  SPT2CE-2578 - Enhanced Security and Integrity has parent :  SPT2CE-2607 - Computing Platform Software (CPSW)

5.3 Computing Platform HW (CPHW)**SPT2CE-2467 - Provide low-level hardware functions.**


CP may provide the following HW components among others:

- HW health monitoring (e.g. temperature and voltage monitoring);
- Dedicated HW security module (e.g. TPM etc) for IT security purposes;
- I/O resources

Status	 Open
Linked Work Items	C2P-has parent :  SPT2CE-2578 - Enhanced Security and Integrity has parent :  SPT2CE-2609 - Computing Platform HW (CPHW)

SPT2CE-2536 - Support redundancy

The Computing Platform shall provide sufficient HW resources to enable the implementation of fault tolerance in the FS to ensure service continuity according to deployment rules for specific FS. Availability requirements are typically mandatory for both safety-related and non-safety-related applications.

Status	 Open
Linked Work Items	C2P-has parent :  SPT2CE-2579 - Recovery and Resilience has parent :  SPT2CE-2609 - Computing Platform HW (CPHW)

6 Functions




6.1 Function of the Computing Platform (CP)

6.1.1 CP as runtime environment for FS Comps

SPT2CE-2484 - Fct-CP Basic - CP as basic integrity standard solution for SW and HW

Provide a Computing Platform as basic integrity standard solution to run FS compartments aggregated on the same standard hardware.

- Safety: No
- Security: No







Allocated to	CP software CP hardware Interface I3 Interface I2
Rationale	no usage of specific solutions for platform parts with short lifecycles
Linked Work Items	has parent :  SPT2CE-2550 - CP as runtime environment for FS Comps _ is related to :  SPT2CE-2307 - Scenario "Aggregation of different kinds of FS Comps on the same CP" _ is derived by :  SPT2CE-2485 - REQ-CP - Use standard solutions for software and hardware

SPT2CE-1862 - Fct-CP Basic - Runtime environment for FS Comp

Provide runtime environment to run FS Compartments with flexibility in usage of guest OS within the FS Compartment.


- Safety: No
- Security: No




Allocated to	CP FS-Compartments I3-runtime
Rationale	Different solutions of FS may use different operating systems as Linux or Windows or something else as "Guest OS". By this it's necessary that the Computing Platform supports this flexibility.

Linked Work Items	has parent :  SPT2CE-2550 - CP as runtime environment for FS Comps _ is related to :  SPT2CE-2307 - Scenario "Aggregation of different kinds of FS Comps on the same CP" _ is derived by :  SPT2CE-2366 - REQ-CP - Provide runtime environment for any compatible GuestOS based FS Compartments _ is derived by :  SPT2CE-2382 - REQ-FS - Safety concept for usage of basic integrity CP _ is derived by :  SPT2CE-2385 - REQ-FS - Safety check of correct SW deployment on different physical computing elements _ is derived by :  SPT2CE-2386 - REQ-FS - Consistency check of safety related software parts
-------------------	---

SPT2CE-2315 - Fct-CP Basic - Isolation of the resources mapped to different FS comps

Provide a reliable resource isolation for the FS compartments. Each FS compartment shall use it's own mapped resources. The freedom from interference between the aggregated FS compartments shall be demonstrated through generic test environment.




- Safety: no (only availability in case of interference)
- Security:  SPT2CE-2591 - Open #SSI - Isolation of TPM content for content with access by different FS Comp ?

Allocated to	CP FS Compartments I3-runtime
Rationale	to avoid any interference between aggregated running FS Compartments.
Linked Work Items	has parent :  SPT2CE-2550 - CP as runtime environment for FS Comps _ is related to :  SPT2CE-2307 - Scenario "Aggregation of different kinds of FS Comps on the same CP" _ is derived by :  SPT2CE-2371 - REQ-CP - Provide isolation of the mapped runtime resources

SPT2CE-2592 - Fct-CP Basic - Provide ID of the used physical CP HW node via I3-CP

Provide a unique HW identification of the currently used physical machine to the FS Compartment.

- Safety: Yes
- Security: No





Allocated to	CP FS Comps I3-runtime SPT2CE-2521 - Open #NHA - HW identification standardisable ?
Rationale	needed by the safety layer within the FS Comp to ensure the distribution of FS Comp onto different physical HW nodes.
Linked Work Items	has parent :  SPT2CE-2550 - CP as runtime environment for FS Comps _ is related to :  SPT2CE-2303 - Scenario "Running of FS Comps of a SIL4 FS - safety related aspects" _ is derived by :  SPT2CE-2368 - REQ-CP - NHA - Provide unique identification of the used CP hardware to the FS Comps

SPT2CE-1901 - Fct-CP Basic - Provide steady clock from physical hardware of used CP HW node via I3-CP

Provide steady (monotonous) system clock from the physical machine to the FS Compartment.

- Safety: Is safety related, safety layer of the FS compartments needs this steady clock to create a "safe system clock".

- Security: No




Allocated to	CP FS Compartments I3-data SPT2CE-2522 - Open #NHA - Access physical hardware - how ?
Rationale	This steady clock is needed by the safety layer within the FS Compartment to create a safe clock on basis of at least 2 independent input sources provided by separate physical hardware devices.
Linked Work Items	has parent :  SPT2CE-2550 - CP as runtime environment for FS Comps _ is related to :  SPT2CE-2303 - Scenario "Running of FS Comps of a SIL4 FS - safety related aspects" _ is related to :  SPT2CE-2307 - Scenario "Aggregation of different kinds of FS Comps on the same CP" _ is derived by :  SPT2CE-2369 - REQ-CP - NHA - Provide steady system clock from physical hardware to FS Compartments

6.1.2 Configuration of the CP for usage by FS Comps

SPT2CE-2505 - Fct-CP Config - FS Comp mapping to CP HW according to FS redundancy principle

Mapping of the FS Comps to CP hardware according to the FS redundancy principle as defined in the FS Comp deployment rules BBC(DR).

- Safety: No
- Security: No










Allocated to	CP BBC(DR)
Rationale	To achieve identical redundancy principles in the FS running on same CP hardware
Linked Work Items	has parent :  SPT2CE-2552 - Configuration of the CP for usage by FS Comps _ is related to :  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP" _ is derived by :  SPT2CE-2506 - REQ-CP - Mapping of FS Comps to CP hardware according to redundancy principle of the FS

SPT2CE-1911 - Fct-CP Config - FS related CP configuration according to deployment rules

Configure the Computing Platform according to the FS Comp related deployment rules BBC(DR)

- needed runtime resources (CPU cores, memory, ..)
- needed communication resources
- connections to communication partners on separate physical machine (neighbour compartments of SIL4 FS)
- connections to communication partners on any physical machine of the same own Computing Platform
- connections to external communication partners (as e.g. decentralised object controllers)

- Safety: No
- Security: SPT2CE-2495 - Open #SSI - CP protection for internal communication - what exactly ?







Allocated to	FS Admin Shared Services CP BBC(DR) via I1-Update (SMI)
Rationale	It's necessary to configure the Computing Platform as preparation to be ready to deploy a FS compartment.
Linked Work Items	<p>has parent :  SPT2CE-2552 - Configuration of the CP for usage by FS Comps</p> <p>_ is related to :  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP"</p> <p>_ is derived by :  SPT2CE-2355 - REQ-CP - Configuration of the runtime resources for the AEE according BBC(DR)</p> <p>_ is derived by :  SPT2CE-2359 - REQ-CP - Configuration of the communication resources for the AEE according BBC(DR)</p> <p>_ is derived by :  SPT2CE-2360 - REQ-CP - SMI - Receive the BBC(DR) via I1-Update SMI from the Shared Services</p> <p>_ is derived by :  SPT2CE-2361 - REQ-CP - Configuration of communication connections for the AEE according BBC(DR)</p> <p>_ is derived by :  SPT2CE-2362 - REQ-CP - Consider HW distribution for safety related FS Comps</p> <p>_ is derived by :  SPT2CE-2391 - REQ-CP - Modularity of FS Comp related CP configuration</p> <p>_ is derived by :  SPT2CE-2394 - REQ-CP - Defined and stable user interfaces for CP configuration</p>

SPT2CE-2314 - Fct-CP Config - FS Comp related mapping of runtime resources

Provide FS Compartment related resource mapping according to deployment rules which are provided by the FS Compartments.

- needed cores
- needed memory

- Safety: No. shall not affect safety (only availability)
- Security: No

Allocated to	CP FS Compartment BBC(DR) = FS Deployment Rules
Rationale	For the aggregation of different FS on the same Computing Platform it's essential to map the needed computing resource individually to the FS compartments.
Linked Work Items	<p>has parent :  SPT2CE-2552 - Configuration of the CP for usage by FS Comps</p> <p>_ is related to :  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP"</p> <p>_ is related to :  SPT2CE-2307 - Scenario "Aggregation of different kinds of FS Comps on the same CP"</p> <p>_ is derived by :  SPT2CE-2372 - REQ-CP - Provide FS Comp related exclusive mapping of runtime resources</p> <p>_ is derived by :  SPT2CE-2392 - REQ-CP - Guarantee for the CPU resources for each timepoint</p> <p>_ is derived by :  SPT2CE-2393 - REQ-CP - FS Comp independency of FS Comp related mapping of CPU resources</p>






SPT2CE-2327 - Fct-CP Config - FS Comp related mapping of communication resources

Provide FS Compartment related mapping of the communication resources.

The mapping shall be stable for running FS compartments.

The installation of additional FS compartments may not have an impact to the resource mapping of the already installed FS compartments.

- Safety: No
- Security: No





Allocated to	CP FS Compartments BBC(DR) = FS Deployment Rules
Rationale	For the aggregation of different FS on the same Computing Platform it's essential to map the needed communication resources individually to the FS compartments.
Linked Work Items	<p>has parent :  SPT2CE-2552 - Configuration of the CP for usage by FS Comps</p> <p>_ is related to :  SPT2CE-2307 - Scenario "Aggregation of different kinds of FS Comps on the same CP"</p> <p>_ is related to :  SPT2CE-2334 - Scenario "Network Communication of a running FS Comp"</p> <p>_ is derived by :  SPT2CE-2373 - REQ-CP - Provide FS Comp related mapping of communication resources</p> <p>_ is derived by :  SPT2CE-2374 - REQ-CP - Provide FS Comp related mapping of network communication resources</p>

6.1.3 SW handling for CP Software on CP Hardware

SPT2CE-1899 - Fct-CP - Deploy CP Software onto CP Hardware

Create an instance of the Computing Platform Software onto a Computing Platform Hardware.

- Safety: No
- Security: No




Allocated to	Actor: CP Administrator
Linked Work Items	<p>has parent :  SPT2CE-2551 - SW handling for CP Software on CP Hardware</p> <p>_ is related to :  SPT2CE-2300 - Scenario "Deployment of the CP Software onto the CP Hardware"</p> <p>_ is derived by :  SPT2CE-2403 - REQ-CP - HW abstraction</p> <p>_ is derived by :  SPT2CE-2404 - REQ-CP - Mixture of HW variants</p>

SPT2CE-2503 - Fct-CP - Update CP software with compatibility for I3 and configuration

Support CP software update with compatibility at the I3 interface and configuration of existing FS compartments.

- Safety: No
- Security: No




Allocated to	CP I3
--------------	----------

Linked Work Items	has parent :  SPT2CE-2551 - SW handling for CP Software on CP Hardware _ is related to :  SPT2CE-2296 - Scenario "Update of the CP Software onto the CP Hardware" _ is derived by :  SPT2CE-2479 - REQ-CP - Compatibility of I3 in context of CP SW update
-------------------	---

SPT2CE-1984 - Fct-CP - Update CP software HW-wise

Support CP hardware-wise update of the CP software with compatibility at the I3 interface to existing FS compartments.





- Safety: No
- Security: No

Allocated to	CP Admin CP CP internal
Rationale	This function is necessary for CP SW update during operation
Linked Work Items	has parent :  SPT2CE-2551 - SW handling for CP Software on CP Hardware _ is related to :  SPT2CE-2296 - Scenario "Update of the CP Software onto the CP Hardware" _ is derived by :  SPT2CE-2504 - REQ-CP - CP HW-wise update of the CP SW according to redundancy principle of FS

SPT2CE-1978 - Fct-CP - Backup CP Software and CP Configuration

Create a backup of the current used CP software version and CP configuration version





- Safety: No
- Security: No

Allocated to	CP Admin CP software and configuration
Linked Work Items	has parent :  SPT2CE-2551 - SW handling for CP Software on CP Hardware _ is related to :  SPT2CE-2296 - Scenario "Update of the CP Software onto the CP Hardware" _ is derived by :  SPT2CE-2480 - REQ-CP - Create Backup of the current CP software version _ is derived by :  SPT2CE-2545 - REQ-CP - Create Backup of the current CP configuration version

SPT2CE-2328 - Fct-CP - Restore CP backup-version of the CP Software and CP Configuration

Restore a backup-version of the CP software version and CP configuration version

- Safety: No
- Security: No




Allocated to	CP Admin CP CP Software
Linked Work Items	has parent :  SPT2CE-2551 - SW handling for CP Software on CP Hardware _ is related to :  SPT2CE-2296 - Scenario "Update of the CP Software onto the CP Hardware" _ is derived by :  SPT2CE-2481 - REQ-CP - Restore a backup version of the CP software version _ is derived by :  SPT2CE-2546 - REQ-CP - Restore backup version of the CP configuration version

6.1.4 Handling of FS Comp SW to deploy and update SMI

SPT2CE-2512 - Fct-CP SMI - CP with SMI service to provide interface I1-SMI for FS Comp deployment


The CP management provides the functionality (e.g. update service) to provide the interface I1-SMI for the deployment of a new FS Comp.

- Safety: No
- Security: No

Allocated to	CP Management I1-SMI
Rationale	I1-SMI is needed to use Shared Service Update as basic service for transfer of BBCs to the CP.
Linked Work Items	has parent :  SPT2CE-2555 - Handling of FS Comp SW to deploy and update SMI _ is related to :  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP" _ is derived by :  SPT2CE-2514 - REQ-CP - SMI service for remote deployment of initial FS Comp





SPT2CE-1850 - Fct-CP SMI - Creation of the Initial FS Comp with BBC(InSW)

Creation of a new FS Comp with BBC(InSW)) as initial software.
 Transfer of the BBC(DR) via I1-Update (SMI) from Shared Services to the Computing Platform.

 SPT2CE-2492 - Open #SMI - deploy new FS - initiation by the admins ?


- Safety: No
- Security: No

Allocated to	FS Admin Shared Services CP BBC(InSW) via I1-Update (SMI)
--------------	--


Rationale	Initial FS Comp has to be created by the CP as preparation for update of the BBC(SW) into the Initial FS Comp.
Linked Work Items	has parent :  SPT2CE-2555 - Handling of FS Comp SW to deploy and update SMI _ is related to :  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP" _ is derived by :  SPT2CE-2363 - REQ-CP - SMI - Transfer the BBC(InSW) via I1-Update SMI from the Shared Services _ is derived by :  SPT2CE-2364 - REQ-CP - SMI - Create the Initial FS Compartment

SPT2CE-2002 - Fct-CP SMI - Shutdown a FS Comp

Shutdown of a FS Comp.

 SPT2CE-2557 - Open #SDI - Process and scenario for stop of a FS by Shared Services Diagnostics ?

- Safety: Yes context "split-brain" in case of handling of safety related FS Comps
- Security: No



Allocated to	CP Admin I1-ADM
Rationale	Necessary in case of re-allocation of a FS Comp onto another part of the CP.
Linked Work Items	has parent :  SPT2CE-2555 - Handling of FS Comp SW to deploy and update SMI

6.1.5 IT-Security SSI

SPT2CE-2325 - Fct-CP SSI - Provide access to HW-based security solution e.g. TPM

FS compartment needs access to the HW-based security solutions e.g. TPM of the used Computing Platform Hardware.

- Safety: No
- Security: Yes TPM is used as trust anchor and for required HW pinning.

Allocated to	CP FS Compartments I3-runtime
Rationale	IT security mechanism within the FS Compartment need the access to the HW-based security solutions e.g. TPM as trust anchor and in context of HW-pinning.
Linked Work Items	has parent :  SPT2CE-2554 - IT-Security SSI _ is derived by :  SPT2CE-2478 - REQ-CP - Provide accessibility to the TPM of the used CP hardware

SPT2CE-2449 - Fct-CP SSI - Restriction and protection of the device-internal communication

The ability to restrict the communication of an FS Compartment to other compartments running on the same Computing Platform Hardware. Only the compartment with security stack allowed to communicate

with FS compartments on other hardware.


- Safety: No
- Security: Yes

Allocated to	FS Comp CP I3
Rationale	To separate IT-security stack from the functional FS Comp.
Linked Work Items	has parent :  SPT2CE-2554 - IT-Security SSI _ is related to :  SPT2CE-2438 - Scenario "Running of FS Comps - IT-security related aspects" _ is derived by :  SPT2CE-2477 - REQ-CP - Restriction of the communication between FS compartments

SPT2CE-2562 - Fct-CP SSI - Provide I3 with interface for secure communication of the FS Comp

Provide I3 with interface for secure communication of the FS Comp.

- Safety: No
- Security: Yes


Allocated to	CP I3-CP
Rationale	For the architecture "IT security stack with in the CP"
Linked Work Items	has parent :  SPT2CE-2554 - IT-Security SSI _ is related to :  SPT2CE-2501 - Architecture: IT-security stack as part of the CP

SPT2CE-2563 - Fct-CP SSI - Provide I1-SSI by CP

The IT-security stack is provided by the CP among others:

- Time server
- Logging
- Certificate-handling

- Safety: No
- Security: Yes

Allocated to	CP I1-SSI
Rationale	For generic solution of IT security stack within the CP
Linked Work Items	has parent :  SPT2CE-2554 - IT-Security SSI _ is related to :  SPT2CE-2501 - Architecture: IT-security stack as part of the CP

6.1.6 Diagnostics SDI



SPT2CE-2431 - Fct-CP SDI - State monitoring of the CP hardware nodes

Monitoring of the states of the individual CP hardware nodes.

Note:

State is provided as diagnostic data via interface I1-Diagnostics to the Shared Service Diagnostics.

- Safety: No
- Security: No

Allocated to	CP Hardware CP Software CP HW state
Linked Work Items	has parent :  SPT2CE-2553 - Diagnostics SDI _ is related to :  SPT2CE-2401 - Scenario "HW failure within the CP"



SPT2CE-2433 - Fct-CP SDI - State monitoring of the network communication

Monitoring of the states of the network communication within the CP (communication between FS Comps running on CP).

Note:

State is provided as diagnostic data via interface I1-Diagnostics to the Shared Service Diagnostics.

- Safety: No
- Security: No

Allocated to	CP CP internal
Linked Work Items	has parent :  SPT2CE-2553 - Diagnostics SDI _ is related to :  SPT2CE-2437 - Scenario "Network failure within the CP"

SPT2CE-2323 - Fct-CP SDI - Process root cause analysis for FS Comp failures







In case of FS compartment failures caused by failures within the Computing Platform (e.g. failures in CP software, CP hardware, network) a root cause analysis is necessary to identify the concrete root cause.

Relevant diagnostic data:

- state of the individual FS compartment
- state of the CP software (relevant for the FS compartment)
- state of the CP hardware (which is relevant for the FS compartment)
- state of the communication network (which is relevant for the FS compartment)

- Safety: No
- Security: No

Allocated to	CP FS Compartments Diagnostic data of the FS Compartment SPT2CE-2593 - Open #SDI - Identification of FS Comp failure by CP ?
Rationale	For optimisation of the maintenance process in context of failures within the Computing Platform. FS itself is not able to identify to root cause for the failure of an individual FS compartment. Shared Service does not know details about the relationship between FS and used Computing Platform parts.






Linked Work Items	has parent :  SPT2CE-2553 - Diagnostics SDI _ is related to :  SPT2CE-2312 - Scenario "SW Failure within an individual FS Comp" _ is derived by :  SPT2CE-2375 - REQ-CP - SDI - Process root cause analysis for FS Comp runtime failures _ is related to :  SPT2CE-2397 - Scenario "SW Failure within the CP" _ is related to :  SPT2CE-2401 - Scenario "HW failure within the CP" _ is related to :  SPT2CE-2437 - Scenario "Network failure within the CP"
-------------------	---

SPT2CE-2322 - Fct-CP SDI - Provide CP diagnostic data according I1-Diag SDI

Computing platform provides the health state of itself:

- states of the individual CP Software instances (running on CP hardware nodes)
- states of the individual physical CP hardware nodes
- states of the network components (which are needed for communication between FS compartments)

- Safety: No
- Security: No





Allocated to	CP Shared Services Interface I1-Diag SDI* for CP diagnostics not yet defined, needs to be discussed.
Linked Work Items	has parent :  SPT2CE-2553 - Diagnostics SDI _ is derived by :  SPT2CE-2376 - REQ-CP - SDI - Provide FS Comp state via I1-SDI to Shared Services Diagnostics _ is related to :  SPT2CE-2397 - Scenario "SW Failure within the CP" _ is related to :  SPT2CE-2401 - Scenario "HW failure within the CP" _ is related to :  SPT2CE-2437 - Scenario "Network failure within the CP"

6.1.7 Recovery

SPT2CE-1848 - Fct-CP Rec - Automatic Restart of a existing FS Comp which has failed


Automated Restart of existing FS Compartment.

- Safety: No
- Security: No





Allocated to	CP CP internal
Rationale	This function is needed to repair a failed FS Comp which had not been able to repair itself automatically by self restart of the FS Comp.
Linked Work Items	has parent :  SPT2CE-2556 - Recovery _ is related to :  SPT2CE-2312 - Scenario "SW Failure within an individual FS Comp" _ is related to :  SPT2CE-2397 - Scenario "SW Failure within the CP" _ is derived by :  SPT2CE-2483 - REQ-CP - Automated restart of failed FS Compartment

SPT2CE-2527 - Fct-CP Rec - Automatic deployment of a failed FS Comp on another CP location

Automatic Deployment of a failed FS Comp on another CP location.

 SPT2CE-2528 - Open #CP #SMI - Automatic deployment of a failed FS Comp onto another CP location




- Safety: Yes SPT2CE-2500 - Open #CP - "Safe" deletion SIL4 FS Compartment
- Security: No

Allocated to	CP Admin CP
Rationale	reduce manual maintenance activities in case of failures which can not be recovered by SW itself.
Linked Work Items	has parent :  SPT2CE-2556 - Recovery _ is related to :  SPT2CE-2312 - Scenario "SW Failure within an individual FS Comp" _ is related to :  SPT2CE-2397 - Scenario "SW Failure within the CP" _ is related to :  SPT2CE-2401 - Scenario "HW failure within the CP"

SPT2CE-2398 - Fct-CP Rec - Repair of a SW failure within the CP software

Repair of a SW failure within the CP Software e.g., by restarting the CP SW on one PCE.


- Safety: No
- Security: No

Allocated to	CP Admin CP CP software and configuration
Linked Work Items	has parent :  SPT2CE-2556 - Recovery _ is related to :  SPT2CE-2397 - Scenario "SW Failure within the CP" _ is derived by :  SPT2CE-2482 - REQ-CP - Modular repair of SW failure within the CP

SPT2CE-2561 - Fct-CP Rec - Deletion of FS Comp

Deletion of a FS Comp.



- Safety: Yes  SPT2CE-2500 - Open #CP - "Safe" deletion SIL4 FS Compartment
- Security: No

Allocated to	CP Admin CP I1-ADM
Rationale	Needed in context of recovery for the case that a restart of a failed FS compartment is not successfully possible. Before the failed FS compartment can be reinstalled on another place on the Computing Platform the existing FS Compartment needs to be deleted.
Linked Work Items	has parent :  SPT2CE-2556 - Recovery

SPT2CE-2402 - Fct-CP Rec - Deactivate an individual CP hardware node

Deactivation of an individual physical CP hardware node.


- Safety: Yes will be relevant to avoid "split-brain" in context of geographical redundant CPs.
- Security: No

Allocated to	CP Admin CP I1-ADM
Linked Work Items	has parent :  SPT2CE-2556 - Recovery _ is related to :  SPT2CE-2401 - Scenario "HW failure within the CP"

SPT2CE-2003 - Fct-CP Rec - Shutdown the total CP

Shutdown of the total CP, means stop all CP software running on any CP hardware.

- Safety: yes (context is to avoid split-brain in case of switch-over of the operation to another CP placed on another location)
- Security: No

Allocated to	CP Admin CP internal
Rationale	This shutdown is necessary in context of re-allocation of the running FS Comps onto another CP placed on another location in case of geographical redundancy.
Linked Work Items	has parent :  SPT2CE-2556 - Recovery






6.2 Functions of the FS Compartment (FS Comp)

SPT2CE-2329 - Fct-FS Comp - Provide FS Comp deployment rules BBC(DR)

The FS Comp related details in context of needed CP resources (CPU cores, memory, ...) are defined by FS Comp related deployment rules within BBC(DR).

- Safety: yes The aspect "distribution of FS compartments of a safe FS onto separate CP hardware" is safety related.
- Security: No



Allocated to	FS Compartment BBC(DR)
--------------	---------------------------

Linked Work Items	has parent :  SPT2CE-2324 - Functions of the FS Compartment (FS Comp) _ is related to :  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP" _ is related to :  SPT2CE-2303 - Scenario "Running of FS Comps of a SIL4 FS - safety related aspects" _ is related to :  SPT2CE-2307 - Scenario "Aggregation of different kinds of FS Comps on the same CP" _ is related to :  SPT2CE-2334 - Scenario "Network Communication of a running FS Comp"
-------------------	---

SPT2CE-2319 - Fct-FS Comp - Provide BBC(InSW) with SMI client functionality

The initial FS Comp contains the BBC(InSW) with SMI client functionality which supports the update of the BBCs via I1-SMI by Shared Services Update.




- Safety: No
- Security: No

Allocated to	Initial FS Compartment BBC(InSW)
Rationale	For remote update of BBCs into the Initial FS Compartment
Linked Work Items	has parent :  SPT2CE-2324 - Functions of the FS Compartment (FS Comp) _ is related to :  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP"

SPT2CE-1876 - Fct-FS Comp - automatic self-restart of the FS Comp for recovery

A FS compartment shall initiate a automated SW restart of failed SW components within the FS compartment to recover the FS Compartment SW failure automatically.





- Safety: No
- Security: No

Allocated to	FS Comp FS Comp internal
Rationale	This function is necessary to increase the availability of the FS compartment by automated self repair.
Linked Work Items	has parent :  SPT2CE-2324 - Functions of the FS Compartment (FS Comp) _ is related to :  SPT2CE-2312 - Scenario "SW Failure within an individual FS Comp" _ is derived by :  SPT2CE-2387 - REQ-FS - Self-repair of failed FS Compartment

SPT2CE-1904 - Fct-FS Comp - Process update BBC(SW) into existing FS Comp according I1-SMI

Deployment the update of new versions of the BBC(SW) into an existing FS Comp.

- Safety: For a safe FS the SW update of the operative FS Comp is safety related.
- Security: No



Allocated to	FS Compartment Shared Services I1-SMI
Rationale	Update of BBCs shall be processed by the FS Compartment itself without dependency to the CP.
Linked Work Items	has parent :  SPT2CE-2324 - Functions of the FS Compartment (FS Comp) _ is related to :  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP" _ is related to :  SPT2CE-2293 - Scenario "Update of FS software" _ is derived by :  SPT2CE-2388 - REQ-FS - FS Compartment-wise update of non-safe SW parts during operative mode

SPT2CE-2337 - Fct-FS Comp - Sync with neighbour FS Comp for safe update SMI

A FS compartment-wise update of the safe BBC shall be handled by the safety layer in a safe way, means the needed safe state of the FS has to be considered in context of involvement of the Safe Configuration Authority for update SMI.

Each safe FS compartment needs to consider the synchronisation with a neighbour-compartment before the safety related involvement of the SCA can be confirmed.

- Safety: Yes
- Security: No



Allocated to	FS compartments FS internal synchronisation of the safety layer
Linked Work Items	has parent :  SPT2CE-2324 - Functions of the FS Compartment (FS Comp) _ is related to :  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP"

SPT2CE-1930 - Fct-FS Comp - Provide FS Comp runtime state according SDI

Provide own health state of the FS compartment

- on running mode of the FS Compartment
- state of the synchronisation with the neighbour compartments.

- Safety: No
- Security: No







Allocated to	FS Compartment Shared Services CP I1-DIAG
Rationale	All diagnostic data shall be provided to the Shared Services as central data sink. CP needs FS compartment runtime state to decide about repair in context of recovery mechanism in case of failures.
Linked Work Items	has parent :  SPT2CE-2324 - Functions of the FS Compartment (FS Comp) _ is derived by :  SPT2CE-2390 - REQ-FS - Provide FS compartment state as diagnostic data via I1-diagnostics SDI

SPT2CE-2338 - Fct-FS Comp - Provide FS state according SDI

Provide the overall state of the FS according to interface I1-Diagnostics SDI

- Safety: No

- Security: No





Allocated to	FS Compartment Shared Services Diagnostics I1-SDI
Linked Work Items	has parent :  SPT2CE-2324 - Functions of the FS Compartment (FS Comp) _ is related to :  SPT2CE-2312 - Scenario "SW Failure within an individual FS Comp" _ is derived by :  SPT2CE-2389 - REQ-FS - Provide FS state as diagnostic data via I1-diagnostics SDI _ is related to :  SPT2CE-2397 - Scenario "SW Failure within the CP" _ is related to :  SPT2CE-2401 - Scenario "HW failure within the CP" _ is related to :  SPT2CE-2437 - Scenario "Network failure within the CP"

SPT2CE-2339 - Fct-FS Comp - Provide I1-SSI by FS Comp

The IT-security stack of the FS Comp is provided by the FS Comp, among others:

- Time server
- Logging
- Certificate-handling etc.

- Safety: No
- Security: Yes



Allocated to	FS Comp with IT-security stack Shared Services Cybersecurity I1-SSI
Linked Work Items	has parent :  SPT2CE-2324 - Functions of the FS Compartment (FS Comp) _ is derived by :  SPT2CE-2432 - REQ-FS - Separation of Safety Layer and IT-sec-mechanism _ is related to :  SPT2CE-2438 - Scenario "Running of FS Comps - IT-security related aspects" _ is derived by :  SPT2CE-2475 - REQ-FS - Provide interface I1 IT-security according SSI

SPT2CE-2539 - Fct-FS Comp - Provide I1-SSI by separate FS related FS-IT Comp

The IT-security stack of the FS Comp is provided by a separate FS related FS-IT Comp. This includes among others:

- Time server
- Logging
- Certificate-handling

- Safety: No
- Security: Yes




Allocated to	FS-IT Comp Shared Services Cybersecurity I1-SSI
Rationale	Separate IT-Security stack from the functional FS Comp
Linked Work Items	has parent :  SPT2CE-2324 - Functions of the FS Compartment (FS Comp) _ is related to :  SPT2CE-2438 - Scenario "Running of FS Comps - IT-security related aspects"

SPT2CE-2474 - Fct-FS Comp - Provide secure communication for I1 SDI,SMI and I0 SCI

Provide encrypted operative communication via the interfaces

- I1 - SDI Diagnostics
- I1 - SMI Update
- I0 - SCI operative communication

- Safety: No
- Security: Yes





Allocated to	FS-Comp I0 SCI
Linked Work Items	has parent :  SPT2CE-2324 - Functions of the FS Compartment (FS Comp) _ is related to :  SPT2CE-2438 - Scenario "Running of FS Comps - IT-security related aspects" _ is derived by :  SPT2CE-2476 - REQ-FS - Provide interface I0 SCI as secured communication

6.3 Functions of the Shared Services (SS)

SPT2CE-2508 - Fct-SS - SMI - Considering FS Comp related BBC structure for FS release management

The Shared Services for Update considers the correlation of the individual BBCs of the FS Comps and the correlation of the individual FS Comps of a FS in context of FS release management.




- Safety: Yes (specific process for update of SIL4 BBCs)
- Security: No

Allocated to	FS Shared Services Update BBCs of the FS
Linked Work Items	has parent :  SPT2CE-1838 - Functions of the Shared Services (SS) _ is related to :  SPT2CE-2054 - Deployment of the FS Software onto the CP _ is derived by :  SPT2CE-2509 - REQ-SS - SMI Release management with correlation of BBCs of a FS Comp _ is derived by :  SPT2CE-2510 - REQ-SS - SMI Release management with correlation of FS Comps of a FS

SPT2CE-2516 - Fct-SS - SMI - Initiate the first deployment of a new FS via interface I1-SMI onto the CP

The installation of a new FS onto the CP is initiated by the FS admin and the Shared Services Update processes this by load of the BBC(DR) and BBC(InSW) of the FS Comps via I1-SMI onto the CP.

- Safety: No
- Security: No

Allocated to	Shared Services CP Management I1-SMI Transfer of BBC(DR) and BBC(InSW)
Linked Work Items	has parent :  SPT2CE-1838 - Functions of the Shared Services (SS) _ is related to :  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP" _ is derived by :  SPT2CE-2515 - REQ-SS - SMI initiation to deploy Initial FS Comp onto the CP

SPT2CE-2335 - Fct-SS - SMI - Handling of FS Comp relationships for update of basic integrity BBCs





For FS which consist of several FS compartments with basic integrity BBCs it is necessary to handle the relationship of this BBCs in context of SW update SMI.

The basic integrity BBCs(SW-x)[1], [2], ...can be updated **step-wise "one after the other" during runtime of the FS.**

Note:

Due to the redundancy principle of a FS it's possible to update an individual basic integrity BBC of one FS Compartment during runtime, means without stopping of the FS. The FS keeps running with reduced availability (missing redundancy). After finishing of the update of FS Compartment [1] it's possible to do the update for FS Compartment [2].

- Safety: No
- Security: No

Allocated to	Shared Services FS Admin BBCs(SW)
Rationale	The Computing Platform shall provide a runtime environment for FS Compartments and shall not have specific functionalities in context of handling of relationships of FS Compartments for optimised automation of update scenarios.
Linked Work Items	has parent :  SPT2CE-1838 - Functions of the Shared Services (SS) _ is related to :  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP" _ is related to :  SPT2CE-2293 - Scenario "Update of FS software" _ is derived by :  SPT2CE-2377 - REQ-SS - SMI Update of basic integrity BBCs into FS Comps stepwise during FS operation

SPT2CE-2336 - Fct-SS - SMI - Handling of FS Comp relationships for update of safe BBCs

For FS which consist of several FS compartments with safe BBCs it's necessary to handle the relationship of this BBCs in context of SW update SMI.

The safe BBCs [1], [2], .. need to be updated usually **in parallel for all FS Compartments of the FS.**

Note:





Due to the safety relevance of the BBCs it's usually not possible to update individual BBCs during runtime., means the update leads to a operative stop of the FS compartment.

In consequence the update of a safe BBC has to be done in parallel for all involved FS Compartments to keep the time duration of operative stop of the FS as short as possible.

A FS compartment-wise update of the safe BBC is handled by the safety layer in a safe way, means the needed safe state of the FS is considered in context of involvement of the Safe Configuration Authority. Each safe FS compartment needs to consider the synchronisation with a neighbour-compartment before the safety related involvement of the SCA can be confirmed.

- Safety: Yes
- Security: No

Allocated to	Shared Services FS Admin BBCs(SW)
Rationale	The Computing Platform shall provide a runtime environment for FS Compartments and shall not have specific functionalities in context of handling of relationships of FS Compartments for optimised automation of update scenarios.

Linked Work Items	has parent :  SPT2CE-1838 - Functions of the Shared Services (SS) _ is related to :  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP" _ is related to :  SPT2CE-2293 - Scenario "Update of FS software" _ is derived by :  SPT2CE-2378 - REQ-SS - SMI Update of safety related BBCs into FS Comps
-------------------	--




SPT2CE-2519 - Fct-SS - SMI - Automation of basic integrity updates for patching.

The Shared Services Update provides automation of basic integrity updates.

Note: Some functions could not be updated automatically and therefore need manual update.

- Safety: No
- Security: Yes




SPT2CE-2520 - Open #SMI - automated IT-sec patching ?

Allocated to	Shared Services Update FS Admin
Rationale	Reduce manual maintenance effort to minimum, especially for IT-security patching
Linked Work Items	has parent :  SPT2CE-1838 - Functions of the Shared Services (SS) _ is related to :  SPT2CE-2293 - Scenario "Update of FS software" _ is derived by :  SPT2CE-2518 - REQ-SS - SMI automate basic integrity updates for IT-Sec patching

SPT2CE-1843 - Fct-SS - SDI - Aggregate FS Comp runtime states to FS runtime state

Aggregation of the FS Comp related runtime states of the FS Comps of a FS to a FS runtime state.


- Safety: No
- Security: No









Allocated to	Shared Services Diagnostics internal
Rationale	The CP provides the FS Comp related runtime state with details in context of failures (e.g. FS Comp runtime failure due to CP hardware failure, ..). This states of the FS Comps need to be aggregated to a FS state.
Linked Work Items	has parent :  SPT2CE-1838 - Functions of the Shared Services (SS) _ is related to :  SPT2CE-2312 - Scenario "SW Failure within an individual FS Comp" _ is derived by :  SPT2CE-2406 - REQ-SS - Aggregate FS Compartment states to FS State

SPT2CE-1846 - Fct-SS - SDI - Provide root cause for SW failure in FS Comp

Evaluate all provided diagnostic data for FS Comps and FS and process a root cause for the FS failure.

- Safety: No
- Security: No


See  SPT2CE-2340 - Sources of diagnostic data:

Allocated to	Shared Services Diagnostics I1-SDI
Rationale	In the layered architecture with several parallel FS Comps and network communication in between, an individual failure leads to several diagnostic messages provided by the FS Comps and the CP. A FS Comp related root cause analysis is done by the CP, see  SPT2CE-2323 - Fct-CP SDI - Process root cause analysis for FS Comp failures The CP does not have an FS context, by this the CP is not able to evaluate a FS state.
Linked Work Items	has parent :  SPT2CE-1838 - Functions of the Shared Services (SS) _ is related to :  SPT2CE-2312 - Scenario "SW Failure within an individual FS Comp" _ is related to :  SPT2CE-2340 - Sources of diagnostic data: _ is related to :  SPT2CE-2397 - Scenario "SW Failure within the CP" _ is related to :  SPT2CE-2401 - Scenario "HW failure within the CP" _ is derived by :  SPT2CE-2407 - REQ-SS - Provide root cause for FS failures _ is related to :  SPT2CE-2437 - Scenario "Network failure within the CP"

SPT2CE-2558 - Fct-SS - SMI - Stop all FS Comps for FS Stop

For a stop of a FS the stop-command is generated for all FS Comps which belong to the FS.

- Safety: No
- Security: No

Allocated to	Shared Services Diagnostics FS Comp I1-SMI
Linked Work Items	has parent :  SPT2CE-1838 - Functions of the Shared Services (SS)

6.4 Function Overview

Function Overview




The following table shows the overview of the functionalities with relevance to the different scenarios categories.




















Run = Runtime






















Dep = Deployment








Up = Update

Rec =Recovery

Functions	Run	Dep	Up	Rec
CP as runtime environment for FS Comps				
 SPT2CE-2484 - Fct-CP Basic - CP as basic integrity standard solution for SW and HW	X			
 SPT2CE-1862 - Fct-CP Basic - Runtime environment for FS Comp	X			
 SPT2CE-2315 - Fct-CP Basic - Isolation of the resources mapped to different FS comps	X			

Functions	Run	Dep	Up	Rec
 SPT2CE-1901 - Fct-CP Basic - Provide steady clock from physical hardware of used CP HW node via I3-CP	X			
Configuration of the CP for usage by FS Comps				
 SPT2CE-2505 - Fct-CP Config - FS Comp mapping to CP HW according to FS redundancy principle		X		
 SPT2CE-1911 - Fct-CP Config - FS related CP configuration according to deployment rules		X		
 SPT2CE-2314 - Fct-CP Config - FS Comp related mapping of runtime resources	X	X		
 SPT2CE-2327 - Fct-CP Config - FS Comp related mapping of communication resources	X			
Handling of CP software on CP hardware				
 SPT2CE-1899 - Fct-CP - Deploy CP Software onto CP Hardware		X		
 SPT2CE-2503 - Fct-CP - Update CP software with compatibility for I3 and configuration			X	
 SPT2CE-1984 - Fct-CP - Update CP software HW-wise			X	
 SPT2CE-1978 - Fct-CP - Backup CP Software and CP Configuration			X	
 SPT2CE-2328 - Fct-CP - Restore CP backup-version of the CP Software and CP Configuration			X	
Handling of FS Comp software for deployment and update SMI				
 SPT2CE-2508 - Fct-SS - SMI - Considering FS Comp related BBC structure for FS release management		X		
 SPT2CE-2516 - Fct-SS - SMI - Initiate the first deployment of a new FS via interface I1-SMI onto the CP		X		
 SPT2CE-2329 - Fct-FS Comp - Provide FS Comp deployment rules BBC(DR)	X	X		
 SPT2CE-2512 - Fct-CP SMI - CP with SMI service to provide interface I1-SMI for FS Comp deployment		X		
 SPT2CE-2319 - Fct-FS Comp - Provide BBC(InSW) with SMI client functionality		X		
 SPT2CE-1850 - Fct-CP SMI - Creation of the Initial FS Comp with BBC(InSW)		X		
 SPT2CE-1904 - Fct-FS Comp - Process update BBC(SW) into existing FS Comp according I1-SMI			X	
 SPT2CE-2337 - Fct-FS Comp - Sync with neighbour FS Comp for safe update SMI			X	
 SPT2CE-2335 - Fct-SS - SMI - Handling of FS Comp relationships for update of basic integrity BBCs		X	X	

Functions	Run	Dep	Up	Rec
 SPT2CE-2336 - Fct-SS - SMI - Handling of FS Comp relationships for update of safe BBCs		X	X	
 SPT2CE-2519 - Fct-SS - SMI - Automation of basic integrity updates for patching.			X	
 SPT2CE-2002 - Fct-CP SMI - Shutdown a FS Comp				
Diagnostics SDI				
 SPT2CE-2431 - Fct-CP SDI - State monitoring of the CP hardware nodes				X
 SPT2CE-2433 - Fct-CP SDI - State monitoring of the network communication				X
 SPT2CE-1930 - Fct-FS Comp - Provide FS Comp runtime state according SDI				
 SPT2CE-2338 - Fct-FS Comp - Provide FS state according SDI				X
 SPT2CE-1843 - Fct-SS - SDI - Aggregate FS Comp runtime states to FS runtime state				
 SPT2CE-2323 - Fct-CP SDI - Process root cause analysis for FS Comp failures				X
 SPT2CE-2322 - Fct-CP SDI - Provide CP diagnostic data according I1-Diag SDI				X
 SPT2CE-1846 - Fct-SS - SDI - Provide root cause for SW failure in FS Comp				X
Recovery				
 SPT2CE-1876 - Fct-FS Comp - automatic self-restart of the FS Comp for recovery				X
 SPT2CE-1848 - Fct-CP Rec - Automatic Restart of a existing FS Comp which has failed				X
 SPT2CE-2527 - Fct-CP Rec - Automatic deployment of a failed FS Comp on another CP location				X
 SPT2CE-2398 - Fct-CP Rec - Repair of a SW failure within the CP software				X
 SPT2CE-2561 - Fct-CP Rec - Deletion of FS Comp				
 SPT2CE-2402 - Fct-CP Rec - Deactivate an individual CP hardware node				X
 SPT2CE-2003 - Fct-CP Rec - Shutdown the total CP				
A) IT Security Stack within the FS Comp				
 SPT2CE-2325 - Fct-CP SSI - Provide access to HW-based security solution e.g. TPM	X			
 SPT2CE-2339 - Fct-FS Comp - Provide I1-SSI by FS Comp	X			
 SPT2CE-2474 - Fct-FS Comp - Provide secure communication for I1 SDI, SMI and I0 SCI	X			

Functions	Run	Dep	Up	Rec
B) IT Security Stack as separate FS-IT Comp				
 SPT2CE-2325 - Fct-CP SSI - Provide access to HW-based security solution e.g. TPM				
 SPT2CE-2449 - Fct-CP SSI - Restriction and protection of the device-internal communication	X			
 SPT2CE-2539 - Fct-FS Comp - Provide I1-SSI by separate FS related FS-IT Comp	X			
 SPT2CE-2474 - Fct-FS Comp - Provide secure communication for I1 SDI, SMI and I0 SCI	X			
C) IT Security Stack within CP				
 SPT2CE-2449 - Fct-CP SSI - Restriction and protection of the device-internal communication	X			
 SPT2CE-2562 - Fct-CP SSI - Provide I3 with interface for secure communication of the FS Comp	X			
 SPT2CE-2563 - Fct-CP SSI - Provide I1-SSI by CP	X			

7 System requirements



The goal of this process is to prepare the formal outputs of the **System Analysis** phase.

PRAMS requirements to the Computing Environment are currently being written by PRAMS and not ready to be used.

7.1 Requirements for the Computing Platform

SPT2CE-2485 - REQ-CP - Use standard solutions for software and hardware



The Computing platform shall be a basic integrity solution and it is based on COTS components for software and hardware.

Linked Work Items	is derived from :  SPT2CE-2484 - Fct-CP Basic - CP as basic integrity standard solution for SW and HW has parent :  SPT2CE-2358 - Requirements for the Computing Platform
Requirement Type	Maintainability Requirement
Rationale	Usage of standard solutions for CP parts with short lifecycles avoids high effort in rail specific solutions.

7.1.1 Interface I3 and CP Configuration

SPT2CE-2479 - REQ-CP - Compatibility of I3 in context of CP SW update



The CP shall be compliant to the interface I3 specification in context of changes in the CP SW.

Linked Work Items	is derived from :  SPT2CE-2503 - Fct-CP - Update CP software with compatibility for I3 and configuration has parent :  SPT2CE-2544 - Interface I3 and CP Configuration
Requirement Type	Functional Requirement
Rationale	Compatibility at the I3 interface is essential to avoid impact onto already installed FS compartments.

SPT2CE-2394 - REQ-CP - Defined and stable user interfaces for CP configuration

The CP shall provide defined and stable user interfaces for the configuration of the CP usage by FS Comps.



A new version of the CP may not have any impact onto the existing CP configuration of the existing FS Comps.

Linked Work Items	is derived from :  SPT2CE-1911 - Fct-CP Config - FS related CP configuration according to deployment rules has parent :  SPT2CE-2544 - Interface I3 and CP Configuration
-------------------	---

Rationale	<p>Each change in the user interface for the CP configuration shall be compatible in such a way that existing CP configurations (of already running FS Comps) can be used furthermore.</p> <p>Rationale: The independency of CP configuration is essential for independent handling of individual FS running aggregated in parallel on same CP.</p>
-----------	---




SPT2CE-2391 - REQ-CP - Modularity of FS Comp related CP configuration

The individual configurations of FS Comps shall be modular and independent. Each FS Comp shall have its own configuration for the CP. Adding or deleting of FS Comps onto the CP must not have any impact on the CP configuration of the other FS Comps.

Linked Work Items	<p>is derived from :  SPT2CE-1911 - Fct-CP Config - FS related CP configuration according to deployment rules</p> <p>has parent :  SPT2CE-2544 - Interface I3 and CP Configuration</p>
Requirement Type	Functional Requirement
Rationale	The independency of FS Comp related CP configuration is essential for independent handling of individual FS Comps running aggregated in parallel on same CP hardware.

SPT2CE-2506 - REQ-CP - Mapping of FS Comps to CP hardware according to redundancy principle of the FS

The CP shall map the FS Comps to CP hardware nodes sorted according to the FS redundancy principle as defined in the FS Comp deployment rules BBC(DR).



Linked Work Items	<p>is derived from :  SPT2CE-2505 - Fct-CP Config - FS Comp mapping to CP HW according to FS redundancy principle</p> <p>has parent :  SPT2CE-2544 - Interface I3 and CP Configuration</p>
Requirement Type	Functional Requirement
Rationale	<p>Example: FS Comps of FS with 2oo3 shall be sorted together (can be installed in parallel on same CP hardware). FS Comps of FS with 2x2oo2 shall be sorted together (can be . FS Comps of FS with 2oo3 shall not be installed on same CP hardware as FS Comps with 2x2oo2.</p> <p>Such sorted mapping according to the redundancy principles for SW deploy allows later on the update of CP SW during operation, See  SPT2CE-2294 - Update of the CP Software onto the CP Hardware</p>

SPT2CE-2355 - REQ-CP - Configuration of the runtime resources for the AEE according BBC(DR)

The CP shall configure the runtime resources as



- CPU cores and
- memory

for the Application Execution Environment for a FS Comp according to the deployment rules as provided via the FS Comp related BBC(DR).

Linked Work Items	is derived from :  SPT2CE-1911 - Fct-CP Config - FS related CP configuration according to deployment rules has parent :  SPT2CE-2544 - Interface I3 and CP Configuration
Requirement Type	Functional Requirement

SPT2CE-2359 - REQ-CP - Configuration of the communication resources for the AEE according BBC(DR)

The CP shall configure the communication resources for the Application Execution Environment for a FS Comp according to the deployment rules as provided via the FS Comp related BBC(DR).



Linked Work Items	is derived from :  SPT2CE-1911 - Fct-CP Config - FS related CP configuration according to deployment rules has parent :  SPT2CE-2544 - Interface I3 and CP Configuration
Requirement Type	Functional Requirement

SPT2CE-2361 - REQ-CP - Configuration of communication connections for the AEE according BBC(DR)

The Computing Platform shall configure the communication connections for the Application Execution Environment for a FS Comp according to the deployment rules as provided via the BBC(DR).



This includes the communication connections

- to neighbour FS Comp(s) of the same FS which are allowed to run on the same physical computing element
- to neighbour FS Comp(s) of the same FS which are not allowed to run on the same physical computing element
- to any other FS Comp(s) which do not belong to the same FS

Linked Work Items	is derived from :  SPT2CE-1911 - Fct-CP Config - FS related CP configuration according to deployment rules has parent :  SPT2CE-2544 - Interface I3 and CP Configuration
Requirement Type	Functional Requirement



SPT2CE-2362 - REQ-CP - Consider HW distribution for safety related FS Comps

The CP shall consider the required distribution of safety related FS Comps onto different CP hardware nodes.

Linked Work Items	is derived from :  SPT2CE-1911 - Fct-CP Config - FS related CP configuration according to deployment rules has parent :  SPT2CE-2544 - Interface I3 and CP Configuration
Requirement Type	Raliability/Availability Req.
Rationale	Note: this criteria "distribution of safety related neighbour FS Comps on separate CP HW" is provided via the FS Comp related deployment rules. The fulfilment of the distribution is checked by the safety layer of the FS. A deployment failure would lead to reduced availability due to safe reaction of the safety layer.



SPT2CE-2366 - REQ-CP - Provide runtime environment for any compatible GuestOS based FS Compartments

The Computing Platform shall provide a runtime environment which is feasible to run any compatible Guest OS in FS Compartments.

Linked Work Items	is derived from :  SPT2CE-1862 - Fct-CP Basic - Runtime environment for FS Comp has parent :  SPT2CE-2544 - Interface I3 and CP Configuration
Requirement Type	Functional Requirement



SPT2CE-2372 - REQ-CP - Provide FS Comp related exclusive mapping of runtime resources

The CP shall provide FS Comp related exclusive mapping of runtime resources as needed CPU cores and memory.

Linked Work Items	is derived from :  SPT2CE-2314 - Fct-CP Config - FS Comp related mapping of runtime resources has parent :  SPT2CE-2544 - Interface I3 and CP Configuration
Requirement Type	Functional Requirement
Rationale	Such a FS Comp related exclusive resource mapping is essential to isolate the FS Comps in context of resource usage to achieve stable running FS Comps.



SPT2CE-2392 - REQ-CP - Guarantee for the CPU resources for each timepoint

The CPU performance provided by the mapped CPU resources must be guaranteed for every timepoint during the runtime of an FS Compartment.

Linked Work Items	is derived from :  SPT2CE-2314 - Fct-CP Config - FS Comp related mapping of runtime resources has parent :  SPT2CE-2544 - Interface I3 and CP Configuration
Requirement Type	Raliability/Availability Req.
Rationale	Variations or instabilities in the provided CPU performance will be identified by the safety layer within the FS and will directly lead to reduced availability as consequence of reactions by the safety layer. Example: If an individual application replica does not react in the required time then this will be evaluated as a misbehaviour of the application replica and this leads to reduced availability (as e.g. running mode reduced from 2oo3 to 2oo2; In case of a 2oo2 system, it will be stopped).

SPT2CE-2393 - REQ-CP - FS Comp independency of FS Comp related mapping of CPU resources



The installation of additional FS Comps (of other FS) on the same CP must not have any impact on the guaranteed CPU performance (cores) for running FS Compartments.

Linked Work Items	is derived from :  SPT2CE-2314 - Fct-CP Config - FS Comp related mapping of runtime resources has parent :  SPT2CE-2544 - Interface I3 and CP Configuration
-------------------	--

Requirement Type	Raliability/Availability Req.
Rationale	The independency of the configuration of FS Comp related mapping of CPU resources is essential for independent handling of individual FS Comps in context of SW deployment and maintenance.



SPT2CE-2373 - REQ-CP - Provide FS Comp related mapping of communication resources

The CP shall provide FS Comp related mapping of communication resources.
The resource mapping shall be done exclusively for each FS Comp.

Linked Work Items	is derived from :  SPT2CE-2327 - Fct-CP Config - FS Comp related mapping of communication resources has parent :  SPT2CE-2544 - Interface I3 and CP Configuration
Requirement Type	Functional Requirement
Rationale	For aggregation of several FS Comps on same CP hardware its essential that the CP provides for each FS Comp stable communication resources.



SPT2CE-2374 - REQ-CP - Provide FS Comp related mapping of network communication resources

The CP shall provide FS Comp related mapping of network communication resources.

Linked Work Items	is derived from :  SPT2CE-2327 - Fct-CP Config - FS Comp related mapping of communication resources has parent :  SPT2CE-2544 - Interface I3 and CP Configuration
Requirement Type	Functional Requirement
Rationale	For aggregation of several FS Comps on same CP hardware its essential that the CP provides for each FS Comp stable network communication resources.

SPT2CE-2371 - REQ-CP - Provide isolation of the mapped runtime resources



The CP shall provide a reliable resource isolation for the FS Comps.
Each FS Comp shall use its own mapped runtime resources and there shall be no kind of interference between the aggregated FS Comps in the resource availability.

Linked Work Items	is derived from :  SPT2CE-2315 - Fct-CP Basic - Isolation of the resources mapped to different FS comps has parent :  SPT2CE-2544 - Interface I3 and CP Configuration
Requirement Type	Raliability/Availability Req.
Rationale	The stability of the CPU resources is essential for independent handling of individual FS Compartments running aggregated in parallel on same CP hardware.

7.1.2 CP Release Management



SPT2CE-2480 - REQ-CP - Create Backup of the current CP software version

The CP shall support to create a backup of the current CP software version.

Linked Work Items	is derived from :  SPT2CE-1978 - Fct-CP - Backup CP Software and CP Configuration has parent :  SPT2CE-2548 - CP Release Management
Requirement Type	Functional Requirement



SPT2CE-2545 - REQ-CP - Create Backup of the current CP configuration version

The CP shall support to create a backup of the current CP configuration version.

Linked Work Items	is derived from :  SPT2CE-1978 - Fct-CP - Backup CP Software and CP Configuration has parent :  SPT2CE-2548 - CP Release Management
-------------------	--



SPT2CE-2481 - REQ-CP - Restore a backup version of the CP software version

The CP shall support to restore a backup version of the CP software version.

Linked Work Items	is derived from :  SPT2CE-2328 - Fct-CP - Restore CP backup-version of the CP Software and CP Configuration has parent :  SPT2CE-2548 - CP Release Management
Requirement Type	Functional Requirement

SPT2CE-2546 - REQ-CP - Restore backup version of the CP configuration version

The CP shall support to restore a backup version of the CP configuration version.



Linked Work Items	is derived from :  SPT2CE-2328 - Fct-CP - Restore CP backup-version of the CP Software and CP Configuration has parent :  SPT2CE-2548 - CP Release Management
Rationale	Load of a backup version of concretely the CP configuration is beneficial in case of "new CP software version installed" to avoid complete new configuration of the newly installed CP software.

7.1.3 Maintenance of the CP

SPT2CE-2482 - REQ-CP - Modular repair of SW failure within the CP

The CP shall support a modular repair of SW failures within the CP software.

Modular repair means a repair without touching unfailed subsystem such as AEE, FS or the HW of the CP.

Linked Work Items	is derived from :  SPT2CE-2398 - Fct-CP Rec - Repair of a SW failure within the CP software has parent :  SPT2CE-2547 - Maintenance of the CP
Requirement Type	Raliability/Availability Req.
Rationale	Modular repair is essential to avoid impact onto running FS compartments.




SPT2CE-2549 - REQ-CP - Modular replacement of CP hardware

The CP shall support a modular replacement of CP hardware.

Linked Work Items	has parent :  SPT2CE-2547 - Maintenance of the CP
-------------------	--

SPT2CE-2483 - REQ-CP - Automated restart of failed FS Compartment




The CP shall automatically restart a failed FS Compartment.

Linked Work Items	is derived from :  SPT2CE-1848 - Fct-CP Rec - Automatic Restart of a existing FS Comp which has failed has parent :  SPT2CE-2547 - Maintenance of the CP
Requirement Type	Raliability/Availability Req.
Rationale	It may happen that a FS Comp fails and is not able to restart itself automatically. By this an additional mechanism in the CP shall support the automated repair of a failed FS Comp.  SPT2CE-2526 - Open #13 - restart of failed FS Comp by CP - how to automate ?

7.1.4 Deploy and Update SMI



SPT2CE-2514 - REQ-CP - SMI service for remote deployment of initial FS Comp

The Computing Platform shall contain a SMI service to process the interface I1-SMI for remote deployment of a new FS Comp.

Linked Work Items	is derived from :  SPT2CE-2512 - Fct-CP SMI - CP with SMI service to provide interface I1-SMI for FS Comp deployment has parent :  SPT2CE-2540 - Deploy and Update SMI
Requirement Type	Functional Requirement
Rationale	Note: Shared Services Update initiates the transfer of the BBCs to the CP. See  SPT2CE-2515 - REQ-SS - SMI initiation to deploy Initial FS Comp onto the CP Rationale: The SMI service is needed for transfer of the BBC(DR) and BBC(InSW) from Shared Services Update via I1-SMI to the Computing Platform.

SPT2CE-2360 - REQ-CP - SMI - Receive the BBC(DR) via I1-Update SMI from the Shared Services



The Computing Platform shall receive the Deployment Rules provided as BBC(DR) from the Shared Services via the I1-Update SMI interface.

Linked Work Items	is derived from :  SPT2CE-1911 - Fct-CP Config - FS related CP configuration according to deployment rules has parent :  SPT2CE-2540 - Deploy and Update SMI
-------------------	---

Requirement Type	Functional Requirement
------------------	------------------------



SPT2CE-2363 - REQ-CP - SMI - Transfer the BBC(InSW) via I1-Update SMI from the Shared Services

Initial FS Comp software provided as BBC(InSW) shall be transferred from the Shared Services via the I1-Update SMI interface.

Linked Work Items	is derived from :  SPT2CE-1850 - Fct-CP SMI - Creation of the Initial FS Comp with BBC(InSW) has parent :  SPT2CE-2540 - Deploy and Update SMI
Requirement Type	Functional Requirement



SPT2CE-2364 - REQ-CP - SMI - Create the Initial FS Compartment

The CP shall create and start the Initial FS Comp with the BBC(InSW).

Linked Work Items	is derived from :  SPT2CE-1850 - Fct-CP SMI - Creation of the Initial FS Comp with BBC(InSW) has parent :  SPT2CE-2540 - Deploy and Update SMI
Requirement Type	Functional Requirement

SPT2CE-2504 - REQ-CP - CP HW-wise update of the CP SW according to redundancy principle of FS



The CP shall support the CP hardware wise update of the CP SW according to the redundancy principle of the installed FS.

Linked Work Items	is derived from :  SPT2CE-1984 - Fct-CP - Update CP software HW-wise has parent :  SPT2CE-2540 - Deploy and Update SMI
Requirement Type	Functional Requirement

7.1.5 Diagnostics SDI

SPT2CE-2375 - REQ-CP - SDI - Process root cause analysis for FS Comp runtime failures



The CP shall process a root cause analysis for FS Comp runtime failures.

Linked Work Items	is derived from :  SPT2CE-2323 - Fct-CP SDI - Process root cause analysis for FS Comp failures has parent :  SPT2CE-2543 - Diagnostics SDI
Requirement Type	Functional Requirement

Rationale	<p>Relevant diagnostic data:</p> <ul style="list-style-type: none"> - runtime state of the FS Comp - state of the Computing Platform Software - state of the Computing Platform Hardware - state of the communication network <p>Rationale: Logical failures (as e.g. corrupted data messages) are not visible for the CP, such failures are handled within the FS Comps. In context of "running state of the FS Comp" different failures may lead to the stop of a FS Comp (see above) and only the CP is able to analyse the situation "what has happened and what needs to be repaired".</p>
-----------	---

SPT2CE-2376 - REQ-CP - SDI - Provide FS Comp state via I1-SDI to Shared Services Diagnostics



The Computing Platform shall provide the FS Compartment state via the interface I1-Diagnostics SDI to the Shared Services.

Linked Work Items	is derived from :  SPT2CE-2322 - Fct-CP SDI - Provide CP diagnostic data according I1-Diag SDI has parent :  SPT2CE-2543 - Diagnostics SDI
Requirement Type	Functional Requirement

7.1.6 IT-Security SSI




SPT2CE-2478 - REQ-CP - Provide accessibility to the TPM of the used CP hardware

The CP shall provide the access to the TPM of the used CP hardware.

Linked Work Items	is derived from :  SPT2CE-2325 - Fct-CP SSI - Provide access to HW-based security solution e.g. TPM has parent :  SPT2CE-2542 - IT-Security SSI
Requirement Type	Security Requirement

SPT2CE-2477 - REQ-CP - Restriction of the communication between FS compartments



The CP shall restrict the unauthorised communication of an FS Compartment to other compartments running on the same Computing Platform Hardware.

Linked Work Items	is derived from :  SPT2CE-2449 - Fct-CP SSI - Restriction and protection of the device-internal communication has parent :  SPT2CE-2542 - IT-Security SSI
Requirement Type	Security Requirement
Rationale	<p> SPT2CE-2495 - Open #SSI - CP protection for internal communication - what exactly ?</p> <p>Rationale: The CP supports different security and communication architecture.</p>

7.1.7 Hardware related requirements

SPT2CE-2403 - REQ-CP - HW abstraction



The Computing Platform Software shall support HW abstraction in such a quality that the usage of changed Computing Platform Hardware does not have any impact onto the FS compartments.

Linked Work Items	is derived from :  SPT2CE-1899 - Fct-CP - Deploy CP Software onto CP Hardware has parent :  SPT2CE-2541 - Hardware related requirements
Requirement Type	Functional Requirement
Rationale	Ordering of the same hardware does not guarantee that the exact same hardware is delivered with 100% compatibility to the software. HW internal changes of details are possible

SPT2CE-2368 - REQ-CP - NHA - Provide unique identification of the used CP hardware to the FS Comps



The CP shall provide a unique identification of the used CP hardware to the FS Comps (which are running on this CP hardware).

This identification shall be always the identification of the currently used CP hardware.

Linked Work Items	is derived from :  SPT2CE-2592 - Fct-CP Basic - Provide ID of the used physical CP HW node via I3-CP has parent :  SPT2CE-2541 - Hardware related requirements
Requirement Type	Safety Requirement
Rationale	The CP shall ensure that this HW identification cannot be influenced / falsified in such systematic way that FS Comps can run on same CP hardware nodes and are getting different HW identifications.



SPT2CE-2369 - REQ-CP - NHA - Provide steady system clock from physical hardware to FS Compartments

The CP shall provide a steady clock value from the physical CP hardware to the FS Comps (which are running on this CP hardware).

Linked Work Items	is derived from :  SPT2CE-1901 - Fct-CP Basic - Provide steady clock from physical hardware of used CP HW node via I3-CP has parent :  SPT2CE-2541 - Hardware related requirements
Requirement Type	Safety Requirement
Rationale	<p>The CP shall ensure that this steady clock value cannot be influenced / falsified in such systematic way that FS Comps running on different CP hardware nodes get the steady clock value from the same CP hardware node.</p> <p>Note: The safety layer needs independent steady clock sources provided by independent CP hardware nodes to create a "safe" system clock. In a 2oo3 system each of the three FS Comps needs an own steady clock source of the used CP hardware: Two sources for safety, an additional third source for availability.</p>

SPT2CE-2404 - REQ-CP - Mixture of HW variants



The CP shall support the usage of different variants of hardware – provided by different vendors – in parallel at the same time.
 Needed adaptations within the CP for usage of a new hardware variant may not have any impact on the AEE with already running FS compartments.

Linked Work Items	is derived from :  SPT2CE-1899 - Fct-CP - Deploy CP Software onto CP Hardware has parent :  SPT2CE-2541 - Hardware related requirements
Requirement Type	Functional Requirement
Rationale	Due to short lifecycle of COTS hardware it's essential for efficient handling of COTS hardware to avoid impact on already running FS Compartments.

7.2 Requirements for the FS Compartment


SPT2CE-2382 - REQ-FS - Safety concept for usage of basic integrity CP

Each solution of a safety critical FS shall use a safety concept in a way which allows the usage of a basic integrity CP (means COTS software running on COTS hardware).

Linked Work Items	is derived from :  SPT2CE-1862 - Fct-CP Basic - Runtime environment for FS Comp has parent :  SPT2CE-1634 - Requirements for the FS Compartment
Requirement Type	Safety Requirement
Rationale	<p><i>For aggregation of several FS compartments on a common basic integrity Computing Platform it's essential that the VE shall not have any dependency to safety. The safety layer itself must identify if the safety related parts of the FS are not running in the required time range or performance.</i></p> <p>Each miss-behaviour of the CP as e.g. wrong scheduling of the individual FS compartments may not have any impact onto the safety of the FS.</p> <p><i>The safety layer of the FS can't rely on the behaviour of the CP, means the safety layer must identify each misbehaviour of the Computing Platform and react safely.</i></p> <p>Information about misbehaviour of the CP must be provided as diagnostic data by FS.</p>

SPT2CE-2383 - REQ-FS - Safety concept independent from the CPU instruction set



The safety concept of the safety layer shall be basically independent from the processor instruction set to be able to change the CPU architecture of the COTS hardware without impact to the safety concept.

Linked Work Items	has parent :  SPT2CE-1634 - Requirements for the FS Compartment
-------------------	--

Requirement Type	Safety Requirement
Rationale	For future proofness in context of usage of COTS hardware it's essential to be able to change the processor instruction set without impact onto the basic safety concept.



SPT2CE-2385 - REQ-FS - Safety check of correct SW deployment on different physical computing elements

The safety layer of the FS shall ensure that the FS compartments are deployed in correct way running on different physical computing elements. In case of a false deployment (FS compartments running on the same physical computing element) the safety layer shall identify the failure and react in a safe way.

Linked Work Items	is derived from :  SPT2CE-1862 - Fct-CP Basic - Runtime environment for FS Comp has parent :  SPT2CE-1634 - Requirements for the FS Compartment
Requirement Type	Safety Requirement
Rationale	To guarantee the safety while using a Basic Integrity CP, safety layer shall check the correct distribution on different physical computing elements.



SPT2CE-2386 - REQ-FS - Consistency check of safety related software parts

The safety layer of the FS shall realise safety mechanism to ensure the consistency of the safety related SW parts of a Safety related FS.

Linked Work Items	is derived from :  SPT2CE-1862 - Fct-CP Basic - Runtime environment for FS Comp has parent :  SPT2CE-1634 - Requirements for the FS Compartment
Requirement Type	Safety Requirement
Rationale	By usage of basic integrity CP it's not guaranteed that stopping, deleting and starting of safety related software parts is successful. By this the safety layer has to ensure the consistency.



SPT2CE-2387 - REQ-FS - Self-repair of failed FS Compartment

The FS shall support to repair a failed FS compartment during the operational phase of the FS. The synchronisation of the repaired FS compartment with the running FS compartments shall be done automatically by the FS to achieve full redundancy again.

Linked Work Items	is derived from :  SPT2CE-1876 - Fct-FS Comp - automatic self-restart of the FS Comp for recovery has parent :  SPT2CE-1634 - Requirements for the FS Compartment
Requirement Type	Reliability/Availability Req.
Rationale	Highest FS availability in context of SW maintenance: avoid stopping of the FS due to repair of an individual failure.



SPT2CE-2432 - REQ-FS - Separation of Safety Layer and IT-sec-mechanism

The FS shall separate the safety layer from the IT-sec mechanism according to the different lifecycles.

Linked Work Items	is derived from :  SPT2CE-2339 - Fct-FS Comp - Provide I1-SSI by FS Comp has parent :  SPT2CE-1634 - Requirements for the FS Compartment
Requirement Type	Security Requirement
Rationale	Replacing IT-security mechanism for IT-sec patches without impact to the safety related FS parts.



SPT2CE-2388 - REQ-FS - FS Compartment-wise update of non-safe SW parts during operative mode

The FS shall allow to update non-safe SW parts as e.g. the IT security mechanism individually FS compartment-wise “one after the other” during operational phase of the FS.

Linked Work Items	is derived from :  SPT2CE-1904 - Fct-FS Comp - Process update BBC(SW) into existing FS Comp according I1-SMI has parent :  SPT2CE-1634 - Requirements for the FS Compartment
Requirement Type	Raliability/Availability Req.
Rationale	Highest FS availability in context of SW maintenance: avoid stopping of the FS due to installation of an IT-security patch



SPT2CE-2390 - REQ-FS - Provide FS compartment state as diagnostic data via I1-diagnostics SDI

The FS compartment shall provide the FS compartment state as diagnostic data via the interface I1-Diagnostics SDI.

Linked Work Items	is derived from :  SPT2CE-1930 - Fct-FS Comp - Provide FS Comp runtime state according SDI has parent :  SPT2CE-1634 - Requirements for the FS Compartment
Requirement Type	Functional Requirement
Rationale	Shared Services for diagnostics are data sink for all kind of diagnostic data



SPT2CE-2389 - REQ-FS - Provide FS state as diagnostic data via I1-diagnostics SDI

Each FS compartment shall provide diagnostic data about the logical FS state via the interface I1-Diagnostics SDI.

Linked Work Items	is derived from :  SPT2CE-2338 - Fct-FS Comp - Provide FS state according SDI has parent :  SPT2CE-1634 - Requirements for the FS Compartment
Requirement Type	Functional Requirement
Rationale	Shared Services for diagnostics are data sink for all kind of diagnostic data



SPT2CE-2475 - REQ-FS - Provide interface I1 IT-security according SSI

The FS compartment shall provide the interface I1 IT-security according SSI.

Linked Work Items	is derived from :  SPT2CE-2339 - Fct-FS Comp - Provide I1-SSI by FS Comp has parent :  SPT2CE-1634 - Requirements for the FS Compartment
-------------------	---

SPT2CE-2476 - REQ-FS - Provide interface I0 SCI as secured communication

The FS compartment shall provide the interface I0 SCI as secured communication according to secure communication specification.

Linked Work Items	is derived from :  SPT2CE-2474 - Fct-FS Comp - Provide secure communication for I1 SDI, SMI and I0 SCI has parent :  SPT2CE-1634 - Requirements for the FS Compartment
Rationale	Source: Secure Communication Specification accessible via ERJU website

7.3 Requirements for the Shared Services

7.3.1 Update SMI

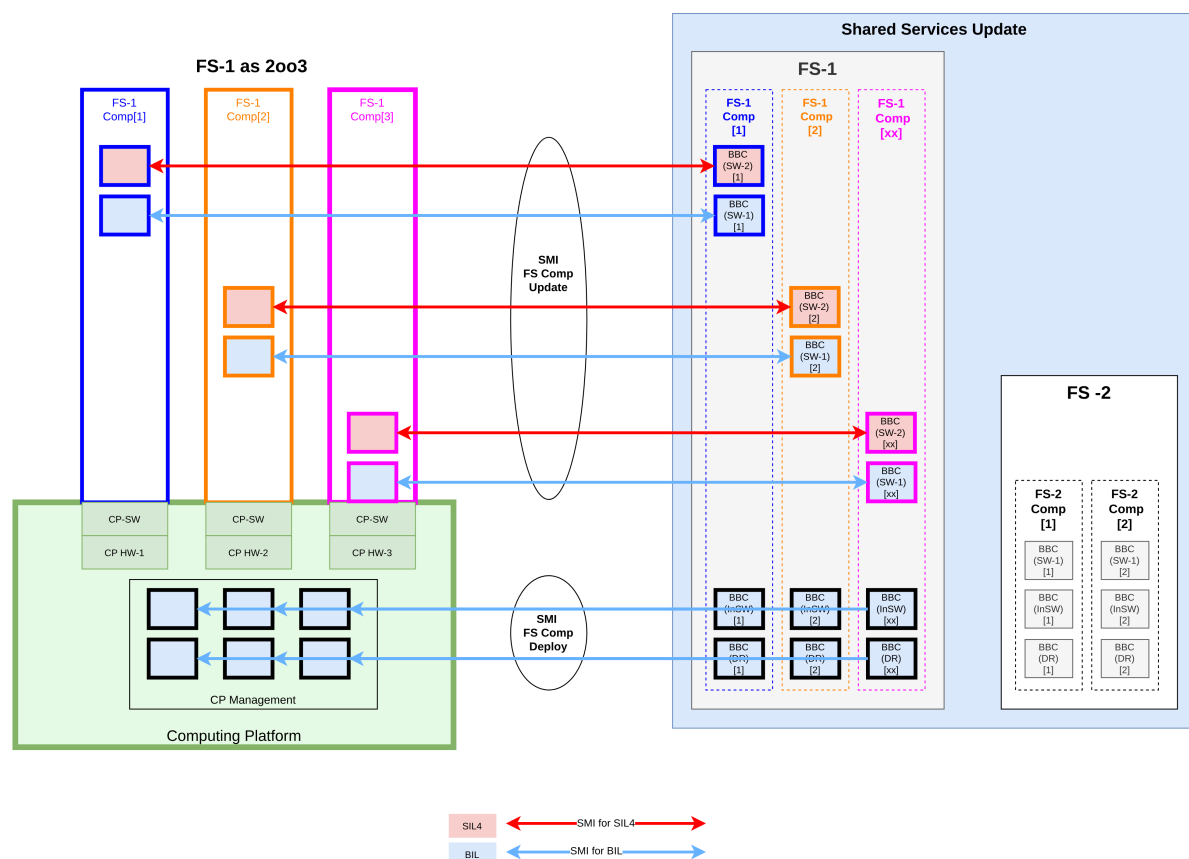






Figure 20 Correlations of BBCs of FS Comps of FS for exemplary SIL4 FS-1 with 3 FS Comps (2oo3 principle)




SPT2CE-2509 - REQ-SS - SMI Release management with correlation of BBCs of a FS Comp

The Shared Services Update shall consider the correlation of the BBCs of a FS Comp for the release management of a FS Comp.

Linked Work Items	is derived from :  SPT2CE-2508 - Fct-SS - SMI - Considering FS Comp related BBC structure for FS release management has parent :  SPT2CE-2511 - Update SMI
Requirement Type	Functional Requirement
Rationale	<p>Each FS Comp consists of several BBCs:</p> <ul style="list-style-type: none"> • BBC(DR) = deployment rules • BBC(InSW) = software of the Initial FS Comp (as initial software to provide bootloading and remote update SMI) • BBC(SW-1..x) = software of the functional FS Comp <p>The detailed amount of BBC(SW-x) depends on the concrete solution of the FS Comp. The safety relevance of individual BBC(SW-x) depends on the concrete solution of the FS Comp.</p> <p>See  SPT2CE-1992 - Overall Context "Deployment and Update of FS" See  SPT2CE-2513 - Correlations of BBCs of FS Comps of FS</p>



SPT2CE-2510 - REQ-SS - SMI Release management with correlation of FS Comps of a FS



The Shared Services Update shall consider the correlation of the FS Comps for the release management of a FS.

Linked Work Items	is derived from :  SPT2CE-2508 - Fct-SS - SMI - Considering FS Comp related BBC structure for FS release management has parent :  SPT2CE-2511 - Update SMI
Requirement Type	Functional Requirement
Rationale	<p>Each FS consists of several FS Comps. The detailed amount of FS Comps depends on the concrete solution of the FS.</p> <p><u>Examples:</u> A FS with 2oo3 principle consists of 3 FS Comps. A FS with 2x2oo2 principle consists of 4 FS Comps A FS with 2oo2 principle consists of 2 FS Comps</p> <p>See  SPT2CE-1992 - Overall Context "Deployment and Update of FS"</p>

SPT2CE-2515 - REQ-SS - SMI initiation to deploy Initial FS Comp onto the CP



The Shared Services Update shall provide the initiation of the deployment of the Initial FS Comp of a new FS onto the CP.

Linked Work Items	is derived from :  SPT2CE-2516 - Fct-SS - SMI - Initiate the first deployment of a new FS via interface I1-SMI onto the CP has parent :  SPT2CE-2511 - Update SMI
Requirement Type	Functional Requirement

Rationale	<p>For the deployment it is necessary to transfer the following:</p> <ul style="list-style-type: none"> - BBC(DR) = deployment rules - BBC(InSw) = the Initial FS Comp software (with bootloader functionality) via the interface I1-SMI onto the CP. <p>Note: CP Management contains a SMI client to receive the BBCs and process the deployment. See  SPT2CE-2514 - REQ-CP - SMI service for remote deployment of initial FS Comp</p> <p>Rational: All BBCs of an FS are handled on side of the Shared Services. By this, even the deployment-relevant BBC(DR) and BBC(InSW) shall be transferred via same I1-SMI.</p> <p> SPT2CE-2492 - Open #SMI - deploy new FS - initiation by the admins ?</p>
-----------	---



SPT2CE-2377 - REQ-SS - SMI Update of basic integrity BBCs into FS Comps stepwise during FS operation

The Shared Services Update shall consider the redundancy principle of the FS in context of update of basic integrity BBCs to provide basic integrity update during operation.

Linked Work Items	is derived from :  SPT2CE-2335 - Fct-SS - SMI - Handling of FS Comp relationships for update of basic integrity BBCs has parent :  SPT2CE-2511 - Update SMI
Requirement Type	Functional Requirement
Rationale	<p>For the update during FS operation the update shall be done step-wise "one FS Comp after the other" to avoid a simultaneous stop of all FS Comps at the same time-point.</p> <p><u>Example:</u> FS with three FS Comps (as e.g. FS with 2oo3 principle) During the update of FS Comp[1] the FS Comp[1] is stopped but the FS keeps running with FS Comp[2] and FS Comp[3] in 2oo2 mode with reduced availability (missing redundancy). After finishing of the update of FS Comp[1] and successful startup and synchronisation of FS Comp[1] the FS is running in 2oo3 mode with full availability. Now it's possible to do the update for the FS Comp[2]. After finishing of the update of FS Comp[2] it's possible to do the update of FS Comp[3].</p>

SPT2CE-2378 - REQ-SS - SMI Update of safety related BBCs into FS Comps




The Shared Services Update shall process the update of safety related BBC(SW-x) for FS Comps as defined in the data preparation phase.

Linked Work Items	is derived from :  SPT2CE-2336 - Fct-SS - SMI - Handling of FS Comp relationships for update of safe BBCs has parent :  SPT2CE-2511 - Update SMI
Requirement Type	Functional Requirement

Rationale	<p>Rationale: The update of a safe BBC(SW) in one individual FS Comp may lead to inconsistency in the safety layer of the FS and by this the updated FS Comp is not able to synchronise successfully with the other FS Comps. This means in that case, for update of all FS Comps an interruption of the FS operation is not avoidable.</p> <p>Example: If a safety related FS is running as 2oo3 this means that three safe BBCs(SW) need to be updated: BBC(SW-x)[1] for FS Comp[1]. BBC(SW-x)[2] for FS Comp[2]. BBC(SW-x)[3] for FS Comp[3].</p> <p>The involvement of the Safe Configuration Authority SCA has to be done for each BBC(SW-x)[1]/[2]/[3] update into the belonging FS Comp[1]/[2]/[3] individually. The Safety Layer of the FS ensures that the safe process for this is done in context of a safe FS running mode, means at least as 2oo2.</p>
-----------	---

SPT2CE-2518 - REQ-SS - SMI automate basic integrity updates for IT-Sec patching



The Shared Services Update shall support the automation updates for IT-security patching with out affecting the BIL or SIL FAs.

Linked Work Items	is derived from :  SPT2CE-2519 - Fct-SS - SMI - Automation of basic integrity updates for patching. has parent :  SPT2CE-2511 - Update SMI
Requirement Type	Functional Requirement
Rationale	<p>For each FS the update shall be done FS Comp-wise "one after the other" during operation, see  SPT2CE-2377 - REQ-SS - SMI Update of basic integrity BBCs into FS Comps stepwise during FS operation</p> <p>FS Comps of different FS can be updated in parallel but should be scheduled with time delay in-between to avoid extremely high network traffic accumulation due to parallel FS Comp synchronisation between the FS Comps on different CP hardware.</p>

7.3.2 Diagnostics SDI



SPT2CE-2406 - REQ-SS - Aggregate FS Compartment states to FS State

The Shared Services Diagnostics shall aggregate the FS compartment related diagnostic data (as provided via I1-Diagnostics SDI) to an overall state of the FS.

Linked Work Items	is derived from :  SPT2CE-1843 - Fct-SS - SDI - Aggregate FS Comp runtime states to FS runtime state has parent :  SPT2CE-2517 - Diagnostics SDI
Requirement Type	Functional Requirement















SPT2CE-2407 - REQ-SS - Provide root cause for FS failures























The Shared Services Diagnostics shall process a root cause for FS failures.

Linked Work Items	is derived from :  SPT2CE-1846 - Fct-SS - SDI - Provide root cause for SW failure in FS Comp has parent :  SPT2CE-2517 - Diagnostics SDI
Rationale	<p>For this the following diagnostic states shall be considered:</p> <ol style="list-style-type: none"> 1. states of the FS Compartments 2. states of the used physical computing elements 3. states of the used AEEs 4. states of the used network communications <p>The amount of belonging FS Compartments depends on the concrete solution of the FS.</p>

7.4 Requirements Overview












Requirements for the Computing Platform

ID	Title
 SPT2CE-2483	REQ-CP - Automated restart of failed FS Compartment
 SPT2CE-2479	REQ-CP - Compatibility of I3 in context of CP SW update
 SPT2CE-2361	REQ-CP - Configuration of communication connections for the AEE according BBC(DR)
 SPT2CE-2359	REQ-CP - Configuration of the communication resources for the AEE according BBC(DR)
 SPT2CE-2355	REQ-CP - Configuration of the runtime resources for the AEE according BBC(DR)
 SPT2CE-2362	REQ-CP - Consider HW distribution for safety related FS Comps
 SPT2CE-2504	REQ-CP - CP HW-wise update of the CP SW according to redundancy principle of FS
 SPT2CE-2545	REQ-CP - Create Backup of the current CP configuration version
 SPT2CE-2480	REQ-CP - Create Backup of the current CP software version
 SPT2CE-2394	REQ-CP - Defined and stable user interfaces for CP configuration
 SPT2CE-2393	REQ-CP - FS Comp independency of FS Comp related mapping of CPU resources
 SPT2CE-2392	REQ-CP - Guarantee for the CPU resources for each timepoint
 SPT2CE-2403	REQ-CP - HW abstraction
 SPT2CE-2506	REQ-CP - Mapping of FS Comps to CP hardware according to redundancy principle of the FS

ID	Title
 SPT2CE-2404	REQ-CP - Mixture of HW variants
 SPT2CE-2482	REQ-CP - Modular repair of SW failure within the CP
 SPT2CE-2549	REQ-CP - Modular replacement of CP hardware
 SPT2CE-2391	REQ-CP - Modularity of FS Comp related CP configuration
 SPT2CE-2369	REQ-CP - NHA - Provide steady system clock from physical hardware to FS Compartments
 SPT2CE-2368	REQ-CP - NHA - Provide unique identification of the used CP hardware to the FS Comps
 SPT2CE-2478	REQ-CP - Provide accessibility to the TPM of the used CP hardware
 SPT2CE-2372	REQ-CP - Provide FS Comp related exclusive mapping of runtime resources
 SPT2CE-2373	REQ-CP - Provide FS Comp related mapping of communication resources
 SPT2CE-2374	REQ-CP - Provide FS Comp related mapping of network communication resources
 SPT2CE-2371	REQ-CP - Provide isolation of the mapped runtime resources
 SPT2CE-2366	REQ-CP - Provide runtime environment for any compatible GuestOS based FS Compartments
 SPT2CE-2481	REQ-CP - Restore a backup version of the CP software version
 SPT2CE-2546	REQ-CP - Restore backup version of the CP configuration version
 SPT2CE-2477	REQ-CP - Restriction of the communication between FS compartments
 SPT2CE-2375	REQ-CP - SDI - Process root cause analysis for FS Comp runtime failures
 SPT2CE-2376	REQ-CP - SDI - Provide FS Comp state via I1-SDI to Shared Services Diagnostics
 SPT2CE-2364	REQ-CP - SMI - Create the Initial FS Compartment
 SPT2CE-2360	REQ-CP - SMI - Receive the BBC(DR) via I1-Update SMI from the Shared Services
 SPT2CE-2363	REQ-CP - SMI - Transfer the BBC(InSW) via I1-Update SMI from the Shared Services
 SPT2CE-2514	REQ-CP - SMI service for remote deployment of initial FS Comp
 SPT2CE-2485	REQ-CP - Use standard solutions for software and hardware









36 items found 

Requirements for the FS Compartment

ID	Title
 SPT2CE-2386	REQ-FS - Consistency check of safety related software parts
 SPT2CE-2388	REQ-FS - FS Compartment-wise update of non-safe SW parts during operative mode
 SPT2CE-2390	REQ-FS - Provide FS compartment state as diagnostic data via I1-diagnostics SDI
 SPT2CE-2389	REQ-FS - Provide FS state as diagnostic data via I1-diagnostics SDI
 SPT2CE-2476	REQ-FS - Provide interface I0 SCI as secured communication
 SPT2CE-2475	REQ-FS - Provide interface I1 IT-security according SSI
 SPT2CE-2385	REQ-FS - Safety check of correct SW deployment on different physical computing elements
 SPT2CE-2382	REQ-FS - Safety concept for usage of basic integrity CP
 SPT2CE-2383	REQ-FS - Safety concept independent from the CPU instruction set
 SPT2CE-2387	REQ-FS - Self-repair of failed FS Compartment
 SPT2CE-2432	REQ-FS - Separation of Safety Layer and IT-sec-mechanism

[11 items found](#) 

Requirements for the Shared Services

ID	Title
 SPT2CE-2406	REQ-SS - Aggregate FS Compartment states to FS State
 SPT2CE-2407	REQ-SS - Provide root cause for FS failures
 SPT2CE-2518	REQ-SS - SMI automate basic integrity updates for IT-Sec patching
 SPT2CE-2515	REQ-SS - SMI initiation to deploy Initial FS Comp onto the CP
 SPT2CE-2509	REQ-SS - SMI Release management with correlation of BBCs of a FS Comp
 SPT2CE-2510	REQ-SS - SMI Release management with correlation of FS Comps of a FS
 SPT2CE-2377	REQ-SS - SMI Update of basic integrity BBCs into FS Comps stepwise during FS operation
 SPT2CE-2378	REQ-SS - SMI Update of safety related BBCs into FS Comps

[8 items found](#) 

Unassigned Requirements

0 items found 

8 Open Points


8.1 Update SMI

SPT2CE-2492 - Open #SMI - deploy new FS - initiation by the admins ?

What is initiated by whom (FS Admin / CP Admin) in context of deployment of a new FS onto the CP

See  SPT2CE-1992 - Overall Context "Deployment and Update of FS"

See  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP"

See  SPT2CE-1850 - Fct-CP SMI - Creation of the Initial FS Comp with BBC(InSW)

Result of discussion with Transversal: The decision to deploy the new FS should be initiated by the FS administrator. This is not part of the SMI process but rather configuration management process.

SPT2CE-2571 - Open #SMI - handling of default data for initial FS Compartment ?


How to handle the default data which is necessary within the initial FS Compartment to be ready to process I1 - SMI ?

What exactly is needed as default data ?

IP-addresses, .. ??

Is it possible to standardise this data ?

Perhaps separate generic BBC(InSW) and default data as own BBC ?

 SPT2CE-1992 - Overall Context "Deployment and Update of FS"

Result of discussion with Transversal: The default data should be provided by the integrator and is transparent to SMI. The default data may include OS and software for SMI end points e.g. OPC UA server endpoint which could be standardised. In addition vendor specific FS configuration will be needed for specific FS installation.

SPT2CE-2497 - Open #SMI - How to handle dependencies?

What happens in the case "pre-load fails" ?

- Preloading of some BBCs required the activation of other BBCs such as BBC(SW-1) need activation of BBC(InSW) before their activation.
- Confirmation requires activation of all safe BBCs.

See  SPT2CE-2291 - Scenario "Deployment of FS Software onto the CP"

Result of discussion with Transversal: This function has to be included in the SMI specifications.

SPT2CE-2520 - Open #SMI - automated IT-sec patching ?

How is the involvement of the FS Admin and CP admin in context of automated update for IT-sec-patching?


 SPT2CE-2519 - Fct-SS - SMI - Automation of basic integrity updates for patching.

Result of discussion with Transversal: This is part of the data preparation phase as such the operator of railway system (FS Admin) is responsible.

SPT2CE-2499 - Open #SMI - Re-install failed FS Compartment on another CP hardware ?

How to handle a failed FS Compartment which cannot be repaired by SW restart.

Re-installation of the FS Compartment on another place of the CP ?

See  SPT2CE-2312 - Scenario "SW Failure within an individual FS Comp"

Result of discussion with Transversal: This process has to be defined partially by platform management together with SMI to repair the compartment.


SPT2CE-2528 - Open #CP #SMI - Automatic deployment of a failed FS Comp onto another CP location


How can the process for "repair of a failed FS Comp by deploying onto another CP location" (e.g. another

CP hardware) be automated ?


How is the involvement of the CP Admin ?

What is the impact to the Shared Services Update SMI and FS Admin ?

 SPT2CE-2527 - Fct-CP Rec - Automatic deployment of a failed FS Comp on another CP location

 SPT2CE-2312 - Scenario "SW Failure within an individual FS Comp"

 SPT2CE-2397 - Scenario "SW Failure within the CP"


 SPT2CE-2401 - Scenario "HW failure within the CP"

Result of discussion with Transversal: This process has to be defined partially by platform management together with SMI to repair the compartment.

SPT2CE-2500 - Open #CP - "Safe" deletion SIL4 FS Compartment

How to ensure that the deletion of a safety critical FS Compartment is successful ?

From view of safety it has to be ensured that the deletion is successful to avoid a "split-brain" safely.

 SPT2CE-2326

Result of discussion with Transversal: This is part of the SMIv3 deactivation process- by deleting the operational token.

SPT2CE-2727 - How to handle changed Deployment Rules for new version of the FS

How to handle changed Deployment Rules for new version of the FS ? In this case the running FS has to be removed and the Computing Platform has to configure newly for new version of the BBC(DR).

Result of discussion with Transversal: The changed deployment rules are handled through dependency tree which is created in the data preparation phase.

SPT2CE-2751 - Common maintenance and diagnostic interface for FS and CP


The same interface for maintenance and diagnostic could be used for FS and CP? Or can we have a COTS interfaces for the CP? If yes then isn't contradict with the current approach where hardware and software used the same maintenance and diagnostic interfaces.

8.2 IT-Security SSI

SPT2CE-2529 - Open #SSI - Secure device with frequent software and configuration


The SW running on a CP hardware is not "static", it changes in context of SW deployment and perhaps even in case of recovery activities by re-allocation of FS Comps onto another CP hardware.

How to handle such "frequent changes" from view of IT security certification ?

 SPT2CE-2341 - Secure Device

SPT2CE-2530 - Open #SSI - FS Comp - which part of SSI provided by the functional FS Comp


Which part of the IT security stack has to be provided by the functional FS Comp ?


 SPT2CE-2438 - Scenario "Running of FS Comps - IT-security related aspects"

SPT2CE-2493 - Open #SSI - IT-Security stack as own FS-IT-Comp ?

Is it possible to standardise the FS-IT compartment / interface to FS-IT comp ? Should be evaluated from technical view, integration view and certification view.


Should be evaluated from technical view, integration view and certification view.


 SPT2CE-2487 - Architecture: IT-Security stack as separate FS related FS-IT Comp

 SPT2CE-2538 - Architecture: IT-Security stack as separate generic (standardised) FS-IT Comp

SPT2CE-2494 - Open #SSI - FS-IT-Comp latencies


The impact onto latency times in the communication via FS-IT compartment needs to be evaluated.


 SPT2CE-2487 - Architecture: IT-Security stack as separate FS related FS-IT Comp

 SPT2CE-2501 - Architecture: IT-security stack as part of the CP

SPT2CE-2564 - Open #SSI - CP Standardisation I3-SSI ?

Standardisation of the I3-SSI interface between FS Comp and the IT-Sec Stack.

 SPT2CE-2501 - Architecture: IT-security stack as part of the CP






 SPT2CE-2538 - Architecture: IT-Security stack as separate generic (standardised) FS-IT Comp

SPT2CE-2495 - Open #SSI - CP protection for internal communication - what exactly ?

What are the requirements for the CP to protect / restrict the communication within the secure device ?

The security mechanism of CP for protection of the functional FS Compartment (without own security


mechanism) must be evaluated from technical view and certification view.

-  SPT2CE-2487 - Architecture: IT-Security stack as separate FS related FS-IT Comp
-  SPT2CE-2538 - Architecture: IT-Security stack as separate generic (standardised) FS-IT Comp
-  SPT2CE-2501 - Architecture: IT-security stack as part of the CP
-  SPT2CE-1911 - Fct-CP Config - FS related CP configuration according to deployment rules
-  SPT2CE-2438 - Scenario "Running of FS Comps - IT-security related aspects"

SPT2CE-2537 - Open #SSI - IT-Security stack within the CP with standardised I3 to FS Comps ?

Is it possible to realise the IT-security stack as generic solution within the CP with standardised interface I3 to the FS Comps ?

How to handle the certification ?

-  SPT2CE-2501 - Architecture: IT-security stack as part of the CP


SPT2CE-2523 - Open #SSI - Access to TPM


Usage of TPM as trust anchor and topic of "HW pinning" in a data centre needs to be clarified with System Pillar IT-Sec

What does "virtual TPM" mean for IT-sec certification ?

The reliability/quality of the access to the TPM of the CP hardware, aspect "virtual TPM" needs to be clarified.


What are the requirements to the CP ?

See  SPT2CE-2325 - Fct-CP SSI - Provide access to HW-based security solution e.g. TPM

See  SPT2CE-2478 - REQ-CP - Provide accessibility to the TPM of the used CP hardware

SPT2CE-2570 - Open #SSI - Usage of vTPM (virtual TPM)

What does it mean for a platform solution with virtualisation that the IT-security stack (running within a virtual machine) does not have direct access to the physical TPM but is accessing a vTPM (virtual TPM) ?

-  SPT2CE-2486 - Architecture: each FS Compartment contains its own IT security stack and provides the interface...

SPT2CE-2591 - Open #SSI - Isolation of TPM content for content with access by different FS Comp ?

Is a "isolation" necessary in context of the TPM content with access by several different FS Comps ?

SPT2CE-2721 - Open #SSI - IT security of the COTS based CP

How does the IT security architecture and mechanisms of a COTS based CP itself fit into the overall architecture defined by the ERJU ?

How to achieve a IT security certification according to the rail standards for a COTS based CP ?

-  SPT2CE-1995 - Overall Context "IT-Security"

8.3 Diagnostics SDI

SPT2CE-2557 - Open #SDI - Process and scenario for stop of a FS by Shared Services Diagnostics ?

What is the exact process to deactivate a FS by the Shared Services Diagnostics ?

Which part processes the FS Comp stop - the FS Comp itself or the CP ?

What is the scenario behind this FS stop ? Switch over from CP-1 to CP-2 in context of geographical redundancy ?

-  SPT2CE-2002 - Fct-CP SMI - Shutdown a FS Comp


Result of discussion with Transversal: SMI will provide the functions and SDI does not support the start/stop functions

SPT2CE-2593 - Open #SDI - Identification of FS Comp failure by CP ?

How can CP identify if FS Comp is running or failed ?

FS Comp can provide the "running state" via SDI ?


Is this standardisable ?

-  SPT2CE-2323 - Fct-CP SDI - Process root cause analysis for FS Comp failures

Result of discussion with Transversal: This should be included in the diagnostic model of the CP.

SPT2CE-2744 - Open #SDI-Allocation of aggregation of diagnostic data for FS

The aggregation happens in the FS, platform management or in shared services?


 SPT2CE-2406 - REQ-SS - Aggregate FS Compartment states to FS State

Result of discussion with Transversal: Where to aggregate the data has to be discussed in the diagnostic model in the next remit.

8.4 Access to CP Hardware

SPT2CE-2521 - Open #NHA - HW identification standardisable ?


Is it possible to standardise the information provided via I3?

 SPT2CE-2592 - Fct-CP Basic - Provide ID of the used physical CP HW node via I3-CP

SPT2CE-2522 - Open #NHA - Access physical hardware- how ?

Is a direct access from the FS Comp to the quartz of the used physical hardware technically possible ?

I3 a function call possible or message based interface ?

 SPT2CE-1901 - Fct-CP Basic - Provide steady clock from physical hardware of used CP HW node via I3-CP

SPT2CE-2526 - Open #I3 - restart of failed FS Comp by CP - how to automate ?

How can the CP SW automatically restart a failed FS Comp p?

Does this affect I3 ?

How can CP identify that a restart is necessary ?

How to do the restart ?

See  SPT2CE-2483 - REQ-CP - Automated restart of failed FS Compartment


SPT2CE-2496 - Open #NHA - additional HW related information

Additional HW related information as CPU temperature, voltage information, core pinning Needs to be clarified and specified in detail.

See  SPT2CE-2303 - Scenario "Running of FS Comps of a SIL4 FS - safety related aspects"

SPT2CE-2728 - Open#guestOS/container

Do we allow the use of containers instead of VM for non-safety-related applications.

See  SPT2CE-1862 - Fct-CP Basic - Runtime environment for FS Comp

8.5 RAM and Safety

SPT2CE-2565 - PRAMS Requirements

PRAMS requirements to the Computing Environment (Computing Platform, FS compartments and Shared Services) are currently being written by the PRAMS team. They will be analysed in a future version of this document.


SPT2CE-2502 - Open #SIL1/2


Consideration SIL1/2 is outstanding.

Currently the Computing Environment emphasises on the requirement to use COTS hardware (that is also used in the non-safe IT environment) and as much as possible COTS software.

In this case, there is no SIL 1/2 certification available for the PCE or the VE.

The mechanisms defined to achieve safe operations in the safety environment are currently only described for "composite fail-safety with fail-safe comparison", which always need at least 2 compartments running on separate hardware's.

 SPPRAMSS-14420 - Computing Environment Strategies

 SPT2CE-2303 - Scenario "Running of FS Comps of a SIL4 FS - safety related aspects"

8.6 Realtime

SPT2CE-2572 - Realtime support for FS

Support for Realtime operating system for functional system might be required for some on-board functions. Details depends on the detailed architecture of on-board system.

8.7 Onboard Communication Protocols

SPT2CE-2812 - Open #Onboard Communication protocols

For onboard applications, the use of the Shared Services (SMI / SDI / SCI) defined by Transversal CCS for the update and diagnostics of virtualised building blocks and Computing Platform Software is not compatible. This topic needs to be worked out together with TrainCS and the Transversal domain and addressed in the future deliverable of CE.

9 Summary and Future Work

Analysis presented in this document describes the potential logical architecture of Computing Environment (CE) including its interfaces and identifies major stakeholders and actors for it. It also defines the scope of the system for initial deployment and configuration to run the target Functional System (FS). For analysis, a constraints from several inputs has been taken in to the account including design concept defined by Transversal group and standard interfaces defined by System Pillar.

In relation to major objectives the analysis defines Computing Platform based on COTS functional systems and technologies from different suppliers, scalable and manageable remotely by manual and automated procedures and functions within orchestration tools and standardised interfaces. However, the scope of CEnv has been limited to hardware and software needed to launch compartment for specific FS. Its operational functions including the Safety need to be analysed separately and it is out of scope of this deliverable. This analysis describes CEnv configuration management, diagnostic and security context and defines general requirements for:

- Computing Platform including hardware and communication interfaces to set up the Computing Environment,
- FS Compartment for Safety, consistency and operation (incl. diagnostic) context,
- Shared Services to define the scope of its interoperability with CEnv.

During the analysis, several open points related to Updating SMI, IT-Security SSI, Diagnostics SDI, Access to CP hardware, RAM, Safety, and Real-Time have been identified. These will provide CEnv input for the specification of SMI, SDI, and SSI specifications. Further collaboration with SP domains, including Transversal, Security, TrainCS, Traffic CS, PRAMS and ARCH, is planned.

Furthermore, the SP CEnv domain is now further working on the specifications of I2-Hardware Abstraction and I3-Virtualisation interfaces, in addition to collaborating on I1 interfaces with the Transversal and Security domains.

10 Reference

Reference No.	Dated (release date)	Title	link (informative)
1	September 2023	Recommendation on Interfaces to be standardised	accessible via ERJU website
2	Planned October 2025	Configuration Logical Concept	accessible via ERJU website

Reference No.	Dated (release date)	Title	link (informative)
3			
4			

11 Annex

11.1 Figures

Figure 1. Overall context "Update of the Computing Platform using the Shared services"

Figure 2. Scenario "Running of FS Comps of a SIL4 FS - safety related aspects"

Figure 3. Scenario "Running of FS Comps - IT-security related aspects"

Figure 5. Scenario "Deployment of FS Software onto the CP"

Figure 6. Scenario "Update of the CP Software onto the CP hardware"

Figure 7. Scenario "Update of the FS software"

Figure 8. Scenario "SW Failure within an individual FS Compartment"

Figure 9. Scenario "SW Failure within the CP"