

System Concept including operational analysis


1 Content

1	Content	2
2	Introduction	4
3	Terminology	5
3.1	Abbreviations	5
3.2	Terms	6
4	Operational Context	8
4.1	Operational scenario overview	12
4.2	User classes and other involved personnel	13
4.2.1	Operational Actors/Entities	13
4.2.2	Interactions among user classes	14
5	Operational scenarios	14
5.1	Integration Scenarios	14
5.2	Deployment Scenarios	18
5.2.1	Install New Hardware	18
5.2.2	Deploy Functional System	22
5.2.3	Remove a productive Functional System	26
5.3	Update Scenarios	28
5.3.1	Update of the Compartment Execution Environment	28
5.3.1.1	Update the Physical Computing Element	28
5.3.1.2	Update of Virtualization Environment	29
5.3.1.2.1	Update of Compatible Virtualisation Environment	29
5.3.1.2.2	Update of Incompatible Virtualization Environment	31
5.3.2	Update Functional System	32
5.3.2.1	Update of compatible FS	32
5.3.2.2	Update of non-compatible FS	33
5.4	Recovery Scenarios	34
5.4.1	SW failures within the Functional System	35
5.4.1.1	Total SW Failure of one FS Compartment	35
5.4.1.2	Total SW Failure of all FS Compartments	37
5.4.2	SW failures within the Virtualization Environment	38
5.4.2.1	Individual SW failure of one Virtual Computing Element	38
5.4.2.2	SW Failure of one complete VE Instance	40
5.4.2.3	SW Failure of all VE Instances	41
5.4.3	SW Failures within the Firmware of the Hardware	43

5.4.4	Hardware failure	43
5.4.4.1	Individual HW failure within one physical computing element	43
5.4.4.2	Total HW failure of one complete physical computing element	44
5.4.4.3	Failure of all computing elements	46
5.4.5	Network communication failures	47
5.4.5.1	Failure of one external communication connection	47
5.4.5.2	Failure of all external communication channels	49
5.4.5.3	Failure of FS internal communication connections	50
6	Requirements	50
6.1	Hardware	51
6.2	Safety and Availability	51
6.3	Virtualization	53
7	Open Points	57
8	Conclusion and Future Work	57
9	Appendix	58
9.1	Referenced documents	58

2 Introduction

The System Pillar domain Computing Environment has the aim to perform an operational and system analysis related to computing environments in the further evolved rail operations system. A mid/long term goal is to specify well identified and reasoned interfaces, as far as possible. The term Computing Environment refers to an environment on which secure functional applications up to SIL4 can be executed. This covers software as well as hardware, as far as possible. It shall be noted that the domain covers all possible CCS applications including onboard and track-side, with a distinction in those cases where the respective requirements, business aspects, operational conditions or eventually potential solution strongly differ.








This second deliverable addresses an analysis of operation including operational scenarios, an operational context and a first set of operational requirements. Results from the first deliverable  [Recommendation on Interfaces to be standardised](#) are respected in the way, that a clear priority and focus is put to operational analysis concerning standardized I1, I2 and I3. Operational analysis taking into account details of I4/5 might be part of future versions of this document.

The document is structured in four main chapters: [3 - Terminology](#) , [4 - Operational Context](#) , [5 - Operational scenarios](#) , [6 - Requirements](#). Explanation of the purpose of the respective chapter can be found in the respective chapter introduction.

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 standardized 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 standardized interfaces).

3 Terminology

In the subsequent chapters, crucial aspects are highlighted with specific icons to enhance visibility and easy identification.

	Concept	Text marked with this icon relates to a concept
	Safety	Represents a rule that impact safety, e.g., it influences the Safety Layer of the Functional System.
	Availability	Represents a rule that is related to availability, e.g., it addresses needed SW mechanism to achieve highest availability of the Functional System.
	Virtualisation	Represents a rule that influences the Virtualisation Layer.
	Physical Hardware	Represents a rule that influences the physical hardware layer.
	Security	Represents a rule that influences security.
	Important	Text marked with this icon highlights an important aspect

3.1 Abbreviations

Term	Abbreviation	Referenced
Application Execution Environment	AEE	here...
Application Layer	AL	here...
Basic Integrity Platform Independence Interface	I4	here...
Compartment	CP	here...
Compartment Execution Environment	CEE	here...
External Diagnostic, Logging, Orchestration and IT Security Interface(s)	I1	here...
Functional Application	FA	here...
Functional Application Task	FAT	here...
Functional System	FS	here...
Functional System Deployment Rules	FSDR	here...
Hardware Abstraction Interface	I2	here...
Hardware Layer	HL	here...
Instance	INS	here...
Operational Interfaces	I0	here...
Orchestration Interface	OI	here...
Physical Computing Element	PCE	here...
Replica	REP	here...
Runtime Environment	RTE	here...
Runtime Layer	RL	here...
Safety Environment	SE	here...
Safety Environment Task	SET	here...
Safety Layer	SL	here...
Safety Platform Independence Interface	I5	here...
Virtual Computing Element	VCE	here...
Virtualisation Environment	VE	here...
Virtualisation Interface	I3	here...
Virtualisation Layer	VL	here...

3.2 Terms

For a generic glossary used in CE context refer to CE Glossary.

Term (Abbreviation)	
Description	Referenced
Application Execution Environment (AEE) The Application Execution Environment refers to the combination of Runtime Environment and Safety Environment.	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...
Compartment (CP) 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 Virtualization Environment.	here...
External Diagnostic, Logging, Orchestration and IT Security Interface(s) (I1) The External Diagnostic, Configuration & orchestration Interface I1 (Interface 1) comprises communication-based interfaces between rail systems and central infrastructure components 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...
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...

Term (Abbreviation)	
Description	Referenced
Hardware Abstraction Interface (I2) <p>The Hardware Abstraction Interface I2 (Interface 2) provides an abstraction of all technology layers above from the specific hardware used below, enabling easy replace ability of commercial of-the-shelf hardware procurable from a well-sized market of hardware vendors.</p> <p>Note: This is not really an interface, but rather a compatibility list of allowed hardware incl. CPU, memory, etc.</p>	here...
Hardware Layer (HL) <p>The Hardware Layer contains the actual Physical Computing Elements providing the compute resources to the platform.</p>	here...
Instance (INS) <p>An Instance is a specific realization of any entity.</p>	here...
Operational Interfaces (I0) <p>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). Exampls for these set of interfaces are the Eulynx Interfaces (SCI-xx) or interfaces like Euroradio or TSI-standardized interfaces.</p>	here...
Orchestration Interface (OI) <p>This interface is used to manage (monitor, control, diagnose, configure) the virtual computing environments. It only exists if a Virtualisation Interface is present. OI is part of I1.</p>	here...
Physical Computing Element (PCE) <p>The Physical Computing Element refers to the physical device providing compute resources.</p>	here...
Provide data for system identification <p>Provide data for system identification</p>	here...
Replica (REP) <p>A Replica is a specific realization 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.</p>	here...
Runtime Environment (RTE) <p>The Runtime Environment refers to the software needed to provide the services of the Runtime Layer in a single Compartment.</p>	here...
Runtime Layer (RL) <p>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.</p>	here...
Safety Environment (SE) <p>The Safety Environment refers to all Safety Environment Tasks needed for a Functional System.</p>	here...

Term (Abbreviation)	
Description	Referenced
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 generalized abstraction between the application logic and the system interfaces, will run unchanged on different platform implementations.	here...
Supplier The company or organization providing a component, product or system.	here...
Virtual Computing Element (VCE) The Virtual Computing Element refers to virtually provided compute resources with computing resource guarantees.	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 Virtualization Interface I3 (Interface 3) is used to provide a standardized 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...

4 Operational Context

All Operational Scenarios described in this document assume the conceptual Computing Environment structure as introduced in the previously published document titled [Recommendation on Interfaces to be standardised](#). While the detailed architecture of an actual Computing Environment will be discussed in later steps, such as System Analysis, Logical Architecture, and Physical Architecture, it is important to understand the general components, their high-level functions, and interactions in order to discuss Operational Scenarios within the context of a standardized Computing Environment.

The following diagram illustrates the essential elements within a Computing Environment, all of which are part of the domain-specific terminology used to describe the Operational Scenarios listed in the subsequent chapters of this document. For further clarification of the terms used, please consult the [Glossary](#). Please note that the depicted

MooN configurations provided are for illustrative purposes only.

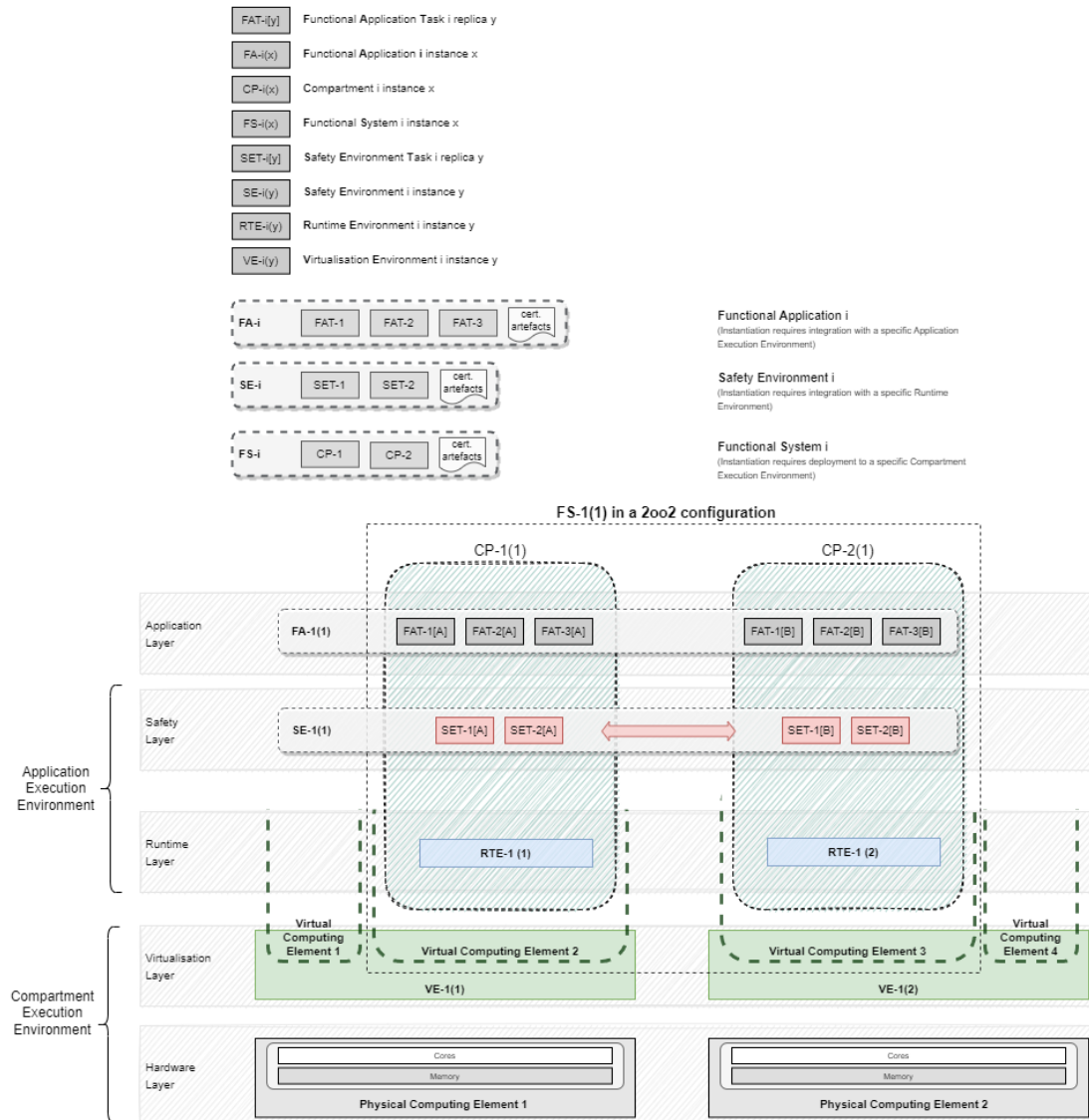


Figure 1 Conceptual Computing Environment architecture

Additionally, it is assumed that operational activities are focused on the granularity of the Functional System. While all internal components of Functional Systems are integral to the overall Computing Environment, they (and the interfaces between them) are currently regarded as specific to individual suppliers and thus deemed lower-priority candidates for standardisation (refer to [Recommendation on Interfaces to be standardised](#) chapter [Conclusion on the interfaces to be standardized](#)).

In summary, the main objective of standardising the Computing Environment is to enable the operation of Functional Systems from various suppliers on a shared pool of physical computing resources. Each individual Functional System operates independently within its own Virtual Computing Element(s). Depending on the specific characteristics of the Functional System, such as safety-criticality and safety principles, or availability, multiple Replicas are required to run on distinct Physical Computing Elements.

In the following a set of three Functional Systems is introduced. These Functional Systems are used in the discussion of the Operational Scenarios in the subsequent chapters of this document. Two Functional Systems, namely FS1 and

FS2, both responsible for safety-critical functions, are employed to illustrate Operational Scenarios. The assumption is made that Functional Systems FS1 and FS2 originate from different suppliers, and their communication is facilitated through a standardized interface called IO. A third Functional System FS3, responsible for non-safety critical functions, is provided by a third supplier.

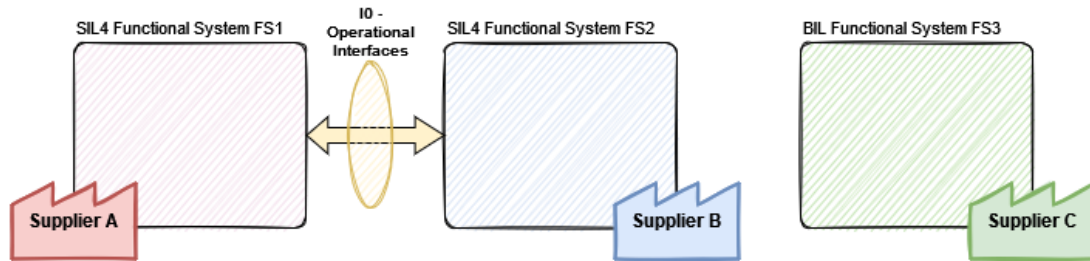


Figure 2 SIL4 Functional Systems FS1 and FS2 communicating using SCI-1 & BIL Functional System FS3

Furthermore, it is assumed that an integrated, tested and qualified Functional System comprises the following components:

- the FS Compartments,
- the FS Deployment Rules
- as well as all necessary Approval Documentation.

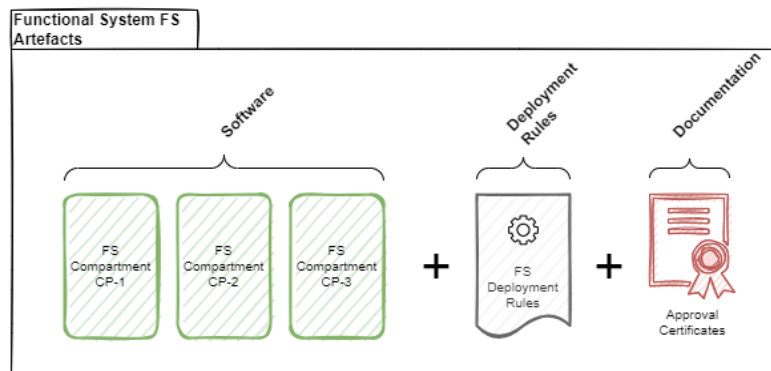


Figure 3 Functional System Artefacts

The FS Deployment Rules comprise all necessary information for deploying the respective Functional System to a qualified Compartment Execution Environment.

Functional System FS1 is configured in a 2oo3 MooN arrangement, consisting of three FS Compartments. All internal components within the compartments are supplier specific. FS1 communicates with FS2 using a standardised communication interface, IO, using a standardised safety protocol.

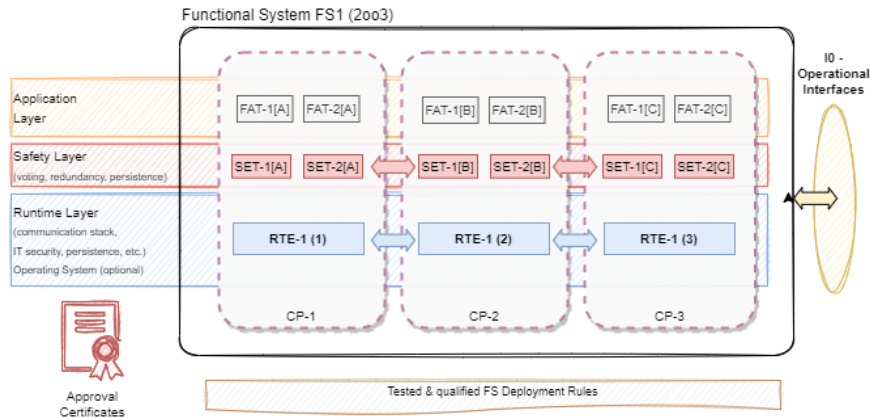


Figure 4 Tested & Qualified Functional System FS1

To visually represent the concept of a Functional System, the above diagram illustrates the typical internal elements of FS Compartments. These elements encompass a Runtime Environment, which may comprise an operating system and services for external communication, security, and persistence. Additionally, a Safety Environment is depicted, responsible for implementing safety and redundancy mechanisms crucial for safety-critical functions, along with a set of Functional Application Tasks dedicated to executing the specific function(s) of the Functional System.

Functional System FS2 adopts as well a 2oo3 MooN configuration, featuring three FS Compartments dedicated to safety-critical functions. Additionally, it includes an extra FS Compartment with Basic Integrity software, which is neither safety-critical nor influences the availability of FS2. Internals of all compartments are specific to the supplier. Furthermore, FS2 communicates with FS1 via a standardized communication interface, I0, utilizing a standardised safety protocol.

P.S: In case redundancy is required for Basic integrity software it could be extended. In the following example we have considered a case where redundancy is not required for basic integrity software.

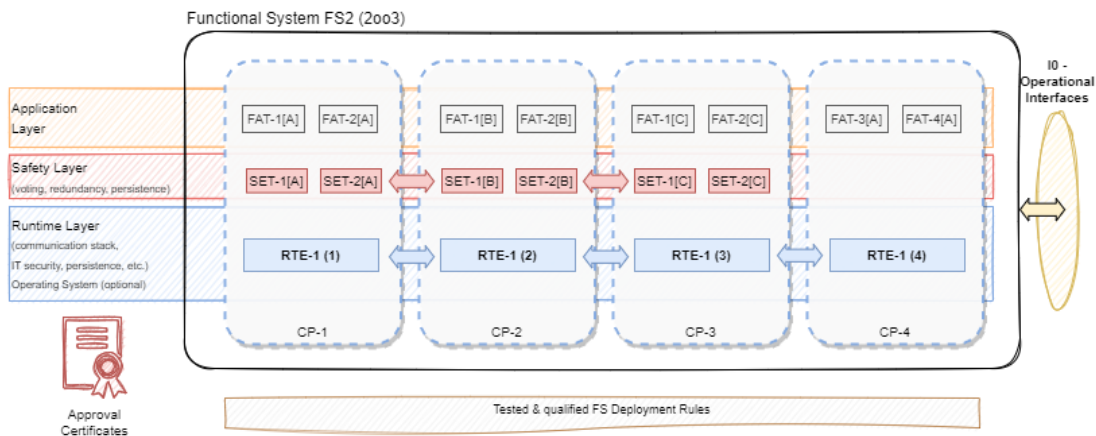


Figure 5 Tested & Qualified Functional System FS2

To visually represent the concept of a Functional System, the above diagram illustrates the typical internal elements of FS Compartments. These elements encompass a Runtime Environment, which may comprise an operating system and services for external communication, security, and persistence. Additionally, a Safety Environment is depicted, responsible for implementing vital safety and redundancy mechanisms crucial for safety-critical functions, along with a set of Functional Application Tasks dedicated to executing the specific function(s) of the Functional System

Functional System FS3 represents a basic integrity system, featuring two FS Compartments for availability reasons, dedicated to non-safe functions. Internals of all compartments are supplier specific.

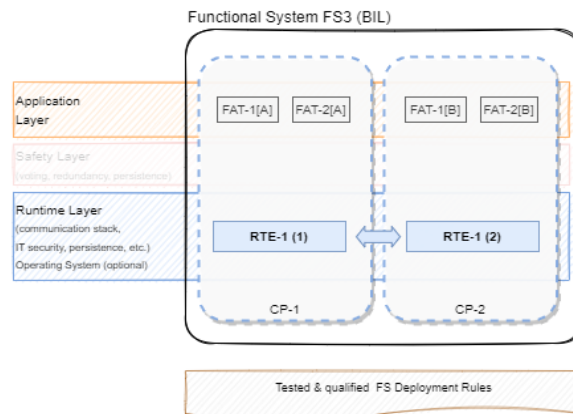






Figure 6 Tested & qualified Functional System FS3

To visually represent the concept of a Functional System, the above diagram illustrates the typical internal elements of FS Compartments. These elements encompass a Runtime Environment, which may comprise an operating system and services for external communication, security, and persistence along with a set of Functional Application Tasks dedicated to executing the specific BIL function(s) of the Functional System

4.1 Operational scenario overview

The below table lists all Operational Scenarios discussed in the following chapters of this document.








ID	Scenario
Integration	
SPT2CE-1411	Integration of Functional System FS2 beside Functional System FS1 on already existing physical Computing Element
SPT2CE-1406	Integration of Functional System FS2 with Functional System FS1, interacting with each other
SPT2CE-1405	Integration of Virtualisation Environment on a new version/type of a Physical Computing Element
Deployment	
SPT2CE-1420	Prepare Physical Computing Element(s)
SPT2CE-1421	Install Virtualisation Environment on Physical Computing Element(s)
SPT2CE-1428	Configure Virtual Computing Elements required for first Functional System
SPT2CE-1431	Deploy Functional System Compartments on Virtual Computing Elements
SPT2CE-1439	Uninstall Functional System deployed on Virtual Computing Element(s)
Update	
SPT2CE-1448	Replace physical computing element
SPT2CE-1446	Update Virtualization Environment while Functional System is Running (Compatible Update)
SPT2CE-1456	Update Functional System while it is Running (Compatible Update)
SPT2CE-1458	Update Functional System including Stopping of FS (Incompatible Update)
Recovery	
SPT2CE-1483	Total SW Failure of one FS Compartment
SPT2CE-1499	Failure of all external communication channels regarding IO
SPT2CE-1485	Total SW Failure of all FS Compartments
SPT2CE-1482	Individual SW failure of one virtual computing element
SPT2CE-1489	SW Failure of one complete VE Instance
SPT2CE-1487	SW Failure of all VE Instances

ID	Scenario
 SPT2CE-1496	Individual HW failure within one physical Computing Element
 SPT2CE-1490	Total HW failure of one complete physical computing element.
 SPT2CE-1492	Disaster scenario - failure of all computing elements
 SPT2CE-1501	Failure of one external communication channel regarding IO

4.2 User classes and other involved personnel

This chapter describes all relevant potential users from a common platforms point of view. The users are usually actors with a dedicated task/role/purpose in the Operational Scenario in chapter 6.

4.2.1 Operational Actors/Entities

ID	Actor/Entity	Description
 SPT2CE-1327	Functional System	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.
 SPT2CE-1064	Installation Team Member	Is able to deploy Functional Systems including: <ul style="list-style-type: none"> commissioning and configuring the Physical Computing Elements manual on-site installation and configuration of the Virtualisation Layer software remote installation of Functional System compartments
 SPT2CE-1204	Maintainer	Is able to diagnose and automatically or manually repair Functional Systems including: <ul style="list-style-type: none"> configuring the Physical Computing Elements manual on-site installation and configuration of the Virtualisation Layer software remote installation of Functional System compartments
 SPT2CE-1519	Operational Integrator	The entity/actor responsible for integration new artifacts of a system used for operation. This includes formal and technical activities. Detailed responsibilities are defined by the concrete operator.
 SPT2CE-1205	Operator	The operator use the functional system to achieve his tasks.
 SPT2CE-1169	Validator	
 SPT2CE-1325	Version Checker	The entity/actor verifying that the correct version of a deployable entity is being installed/updated/deleted etc.

4.2.2 Interactions among user classes

Operational relevant interactions between different users are described directly in the scenarios, if necessary.

5 Operational scenarios

5.1 Integration Scenarios

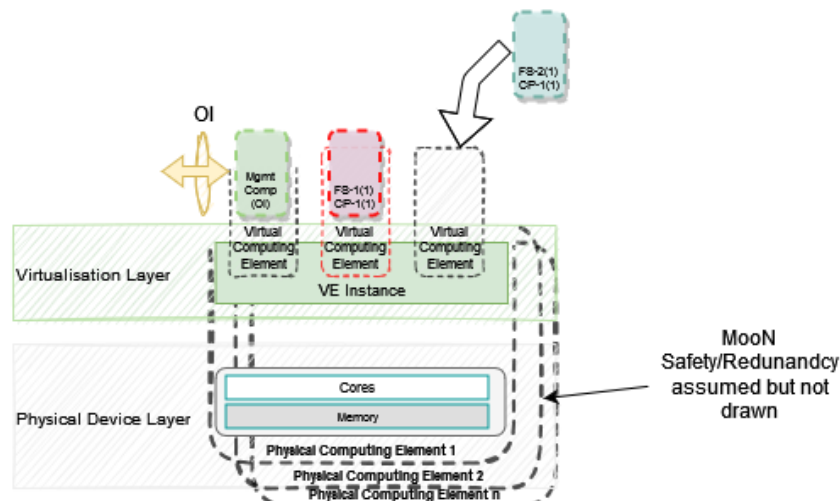
Integration means to bring a new item (FS, VE, ...) to the overall operational system. New means here either a new version of an already used item or a complete new type of an item. Integration is an activity which is usually done as a first step to assure, that the new (as defined above) fulfils all operational requirements and does not interfere with other, already existing operational systems. It depends on concrete operational rules, if an integration is done directly on the running operational system or on a so-called "shadow system" for de-risking. The scenarios are written to support both approaches.

Note: Integration is assumed to always consist of two levels:

1. The first level is done from the vendor, otherwise no assessment or acceptance would be possible. This is not scope of the document here.
2. The second level is done from the Operational Integrator. Here a tested and pre-integrated item "only" needs to be integrated into a concrete operational environment. This is an essential step, but it does not mean, that all functional capabilities need to be retested during that kind on integration.





SPT2CE-1411 - Integration of Functional System FS2 beside Functional System FS1 on already existing physical Computing Element


A new independent Functional System is integrated to an already existing hardware (with virtualization layer), hosting a functional system FS2.




Scenario:

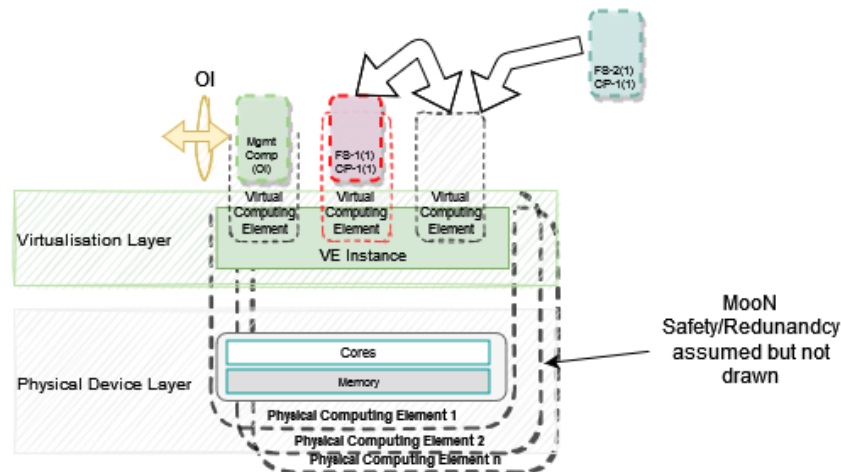
Step	Description	Involved Entity

Step	Description	Involved Entity
Check formal compliance	The compliance of the new FS against all required features, standards and norms needs to be checked. For this, a proper set of "FS documentation" needs to exist.	 SPT2CE-1519 - Operational Integrator
Checking of needed computing resources	It needs to be assured that the new FS can be integrated to the existing HW/virtualization. For this needed computing resources like memory, processing power, performance, network capabilities and HW separation necessities need to be assured. These needs are specified in the documentation of the FS.	 SPT2CE-1519 - Operational Integrator
Integration of the system	If the previous steps are done successfully, the new FS can now be installed onto the HW/virtualisation layer. It must follow the organization-specific operational integration process.	 SPT2CE-1519 - Operational Integrator
Test of Integration	The new FS must be tested against generic function and influence to neighbour system. Just if these tests are positive, the integration can be considered as successful.	 SPT2CE-1519 - Operational Integrator

Op.Entities	Operational Integrator
Op.Postcondition	
Op.Precondition	<ul style="list-style-type: none"> • FS with all certifications, assessments and validation proof • Agreed and understood operational process to perform concrete integration • HW/virtualization layer available to integrate FS • spatial resources availability, memory to contain and run FS • HW sharing and time repartition to contain and run FS1 and FS2
Op.Rationale	
Linked Work Items	has parent :  SPT2CE-1399 - Integration Scenarios

SPT2CE-1406 - Integration of Functional System FS2 with Functional System FS1, interacting with each other

A new Functional System is integrated to an already existing hardware (with virtualization layer), hosting a functional system FS1 in execution. FS2 needs to interact with FS1. Note that the individual integration of the two systems FS1 and FS2 falls under description of  SPT2CE-1411 Only "delta-steps" are described.



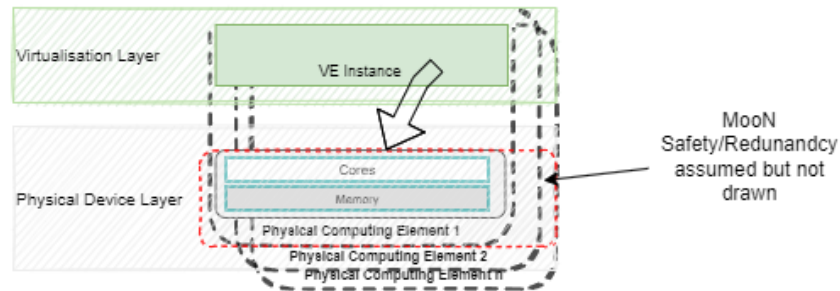
Scenario:

Step	Description	Involved Entity
Configuration changing FS1	If the steps of scenario SPT2CE-1411 are done successfully, the FS in execution need to be configured to communicate with FS2. This could be done stopping or not stopping the execution of FS1.	SPT2CE-1519 - Operational Integrator
FS2 Installation	If the previous steps are done successfully, the new FS can now be installed onto the HW/virtualisation layer. It must follow the organization-specific operational integration process.	SPT2CE-1519 - Operational Integrator

Op.Entities	Operational Integrator
Op.Postcondition	
Op.Precondition	<ul style="list-style-type: none"> FS with all certifications, assessments and validation proof Agreed and understood operational process to perform concrete integration HW/virtualization layer available to integrate FS: <ul style="list-style-type: none"> spatial resources availability, memory to contain and run FS HW sharing and time repartition to contain and run FS1 and FS2
Op.Rationale	
Linked Work Items	has parent : SPT2CE-1399 - Integration Scenarios

SPT2CE-1405 - Integration of Virtualisation Environment on a new version/type of a Physical Computing Element

A new version/type of a Physical Computing Element is added to the existing system. For this, preparation of the VE on the new PCE to integrate into the existing system is necessary.



Scenario:

Step	Description	Involved Entity
Check formal compliance	Compliance and necessities to integrate a VE on the new Physical Computing Element are checked to ensure allowance.	🧑 SPT2CE-1519 - Operational Integrator
Installation of VE on PCE	VE is installed on the PCE (see SPT2CE-1428).	🧑 SPT2CE-1519 - Operational Integrator
Integration tests	Computing Node is added to the operational network (productive or shadow) and integration is tested as operational procedures require.	🧑 SPT2CE-1519 - Operational Integrator
Integration Confirmation	A confirmation, as defined in the operational rules, is documented so that future installations can be done following the install/deploy scenarios (SPT2CE-1431) without additional tests.	

Op.Entities	Operational Integrator
Op.Postcondition	
Op.Precondition	<ul style="list-style-type: none"> • PCE is installed and powered up. • All necessary network cables are installed. • VE is available, pre integration on HW type was done by vendor.
Op.Rationale	
Linked Work Items	has parent : 📁 SPT2CE-1399 - Integration Scenarios

5.2 Deployment Scenarios

In the following it is assumed that Functional System 1 has already been deployed and Functional System 2 is being added. For a description of the two Functional Systems used in the description of the scenarios, please refer to chapter 4-2 - Introduction.

5.2.1 Install New Hardware

The hardware setup must align precisely with the tested and qualified FS Deployment Rules of the Functional System to be installed. The use of any alternative hardware configuration is strictly prohibited, as it may result in unforeseen availability issues.

SPT2CE-1420 - Prepare Physical Computing Element(s)

Functional System Compartments are deployed to Virtual Computing Elements that allow the execution of several Compartments on the same Physical Computing Element. The preparation of Physical Devices must adhere strictly to the tested and qualified FS Deployment Rules of the Functional System that is to be deployed. The correct number of Physical Computing Elements as per the FS Deployment Rules of the Functional System must be available.

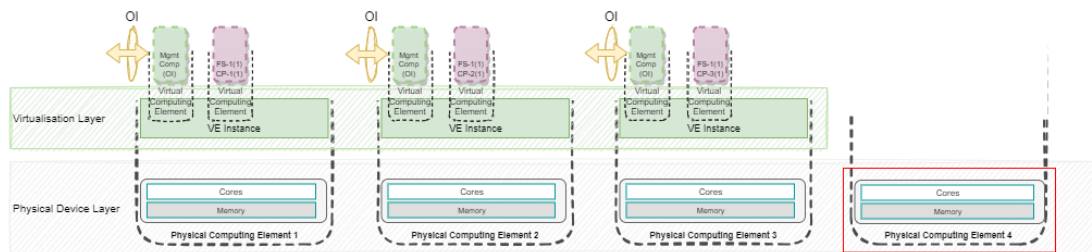










Figure 7 Preparation of Physical Computing Element

Scenario

Step	Description	Involved Entities
1	Verify that the Physical Computing Element(s) to be installed comply with the FS Deployment Rules of the Functional System(s) to be deployed.	SPT2CE-1 064 - Installation Team Member
2	Mechanical installation of additional Physical Computing Element(s) into their designated space.	SPT2CE-1 064 - Installation Team Member
3	Connect power and external communication network.	SPT2CE-1 064 - Installation Team Member

Step	Description	Involved Entities
4	Configure external communication network components for operation with newly added Physical Computing Element(s)	 SPT2CE-1064 - Installation Team Member
5	Verify proper installation.	 SPT2CE-1064 - Installation Team Member

Op.Entities	 SPT2CE-1064 - Installation Team Member
Op.Postcondition	<ul style="list-style-type: none"> Physical Computing Element(s) are installed in their designated location and connected to power and the communication network. Communication network components are configured for newly added Physical Computing Element(s)
Op.Precondition	<ul style="list-style-type: none"> Artefacts of Functional System(s) to be deployed are available - specifically the FS Deployment Rules. The  SPT2CE-1064 - Installation Team Member has to ensure that all conditions to install the new hardware are met e.g. space for the installation of the Physical Computing Element(s) is available, dedicated power for each Physical Computing Element is available, free communication network ports are available, etc. Physical Computing Element(s) are available All required/mandated certificates (cybersecurity) have been installed (e.g. in TPM) and are valid.
Op.Rationale	
Linked Work Items	<p>refers to :  SPT2CE-1234 - Physical Computing Element</p> <p>has parent :  SPT2CE-1408 - Install New Hardware</p> <p>_ is ruled by :  SPT2CE-1422 - While the actual Physical Computing Elements may vary in type and originate from...</p> <p>_ is ruled by :  SPT2CE-1418 - The hardware installation procedures shall not be standardized, as they heavily...</p>

SPT2CE-1418 -



The hardware installation procedures shall not be standardized, as they heavily depend on various factors such as the type of Physical Computing Elements being installed, the installation location (on-board, trackside, etc.), and operator-specific installation guidelines.

SPT2CE-1422 -



While the actual Physical Computing Elements may vary in type and originate from different suppliers, it is essential that they all adhere to a standardized set of hardware requirements.

SPT2CE-1421 - Install Virtualisation Environment on Physical Computing Element(s)

A Virtualisation Environment is used to offer Virtual Computing Elements for the deployment and operation of Functional Systems. The Virtualisation Environment deployed to the Physical Computing Element(s) must strictly

comply with the FS Deployment Rules of the Functional System to be deployed.

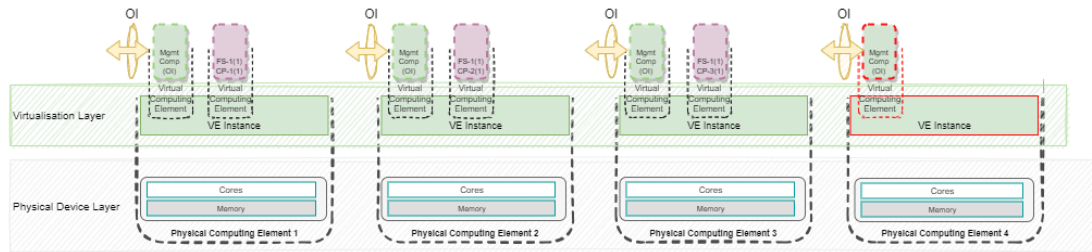












Figure 8 Installation of Virtualisation Layer instances on prepared Physical Computing Elements

During this step, an instance of the Virtualisation Environment is installed on each prepared Physical Computing Element. The initial parametrisation of the Virtualisation Environment enables the subsequent configuration of Virtual Computing Elements using an Orchestration Interface (OI).

Scenario

Step	Description	Involved Entities
1	Verify that the Virtualisation Environment Software complies with the FS Deployment Rules of the Functional System(s) to be deployed.	SPT2CE-1064 - Installation Team Member
2	Verify that the prepared Physical Computing Element(s) comply with the FS Deployment Rules of the Functional System(s) to be deployed.	SPT2CE-1064 - Installation Team Member
3	Install and configure on each Physical Computing Element the Virtualisation Environment as per the respective installation guide. The installation of the Virtualisation Environment includes the installation and configuration of the Orchestration Interface (OI) used for subsequent configuration of Virtual Computing Elements and the deployment of FS compartments.	SPT2CE-1064 - Installation Team Member
4	Verify for each installation the remote access via the Orchestration Interface (OI).	SPT2CE-1064 - Installation Team Member

Op.Entities	SPT2CE-1064 - Installation Team Member
Op.Postcondition	<ul style="list-style-type: none"> Virtualisation Layer Instance is installed and configured on the Physical Computing Element(s). Remote access via the Standard Orchestration Interface (OI) is up and running.

Op.Precondition	<ul style="list-style-type: none"> Physical Computing Element(s) have been prepared ( SPT2CE-1420 - Prepare Physical Computing Element(s)). The qualified Virtualisation Environment Software is available. The qualified Virtualisation Environment Software installation guide is available. Onsite access to the previously prepared Physical Computing Elements via out of band management network.
Op.Rationale	
Linked Work Items	<p>is derived from :  SPT2CE-19 - Aggregate multiple Functional Applications on the same Instance of a Computing Platform</p> <p>refers to :  SPT2CE-1574 - Orchestration Interface</p> <p>refers to :  SPT2CE-1235 - Instance</p> <p>refers to :  SPT2CE-1692 - Provide data for system identification</p> <p>has parent :  SPT2CE-1408 - Install New Hardware</p> <p>_ is ruled by :  SPT2CE-1417 - Preferably, an existing off-the-shelf Virtualisation Environment shall be used....</p> <p>_ is ruled by :  SPT2CE-1414 - From the perspective of the Entity in Charge of Maintenance, the Functional Syst...</p> <p>_ is ruled by :  SPT2CE-1416 - Different Virtualisation Environment implementations shall be allowed, as long a...</p> <p>_ is ruled by :  SPT2CE-1415 - The Virtualization Environment Instance installed on the available Physical Comp...</p>

SPT2CE-1415 -



The Virtualization Environment Instance installed on the available Physical Computing Elements must align with the requirements specified in the FS Deployment Rules of the intended Functional System.

Rationale: To warrant the availability of the intended Functional System, it is crucial that its deployment adheres precisely to the qualified FS Deployment Rules.

SPT2CE-1414 -



From the perspective of the Entity in Charge of Maintenance, the Functional System orchestration shall provide a standard set of functionalities.

Rationale: Having a common set of OI functionalities for operating all Functional System(s) simplifies the overall maintenance and reduces the cost.

SPT2CE-1417 -



Preferably, an existing off-the-shelf Virtualisation Environment shall be used.

Rationale: It does not make a lot of sense to develop a rail specific Virtualisation Environment.

SPT2CE-1416 -



Different Virtualisation Environment implementations shall be allowed, as long as an Orchestration Interface (OI) is provided, and the respective Virtualisation Environment has been qualified to be used with the functional system to be installed.

Rationale: This shall open the market for different Virtualisation Environment solutions, that can be used depending on the suppliers of the IM/RU's preferences.

SPT2CE-1562 -



The Orchestration Interface (OI) may either be an integral part of the Virtualisation Environment or being installed as an add-on, e.g., in from of a dedicated Management Compartment providing the OI.

Rationale: This helps to avoid rail specific implementation of the Virtualisation Environment. From an operational perspective it is irrelevant where and how the OI is implemented.

5.2.2 Deploy Functional System

SPT2CE-1428 - Configure Virtual Computing Elements required for first Functional System

During this step, the configuration involves setting up the number of required Virtual Computing Elements, adhering strictly to the qualified FS Deployment Rules of Functional System. This configuration encompasses, among others, spatial and temporal parameters as well as the network configuration.

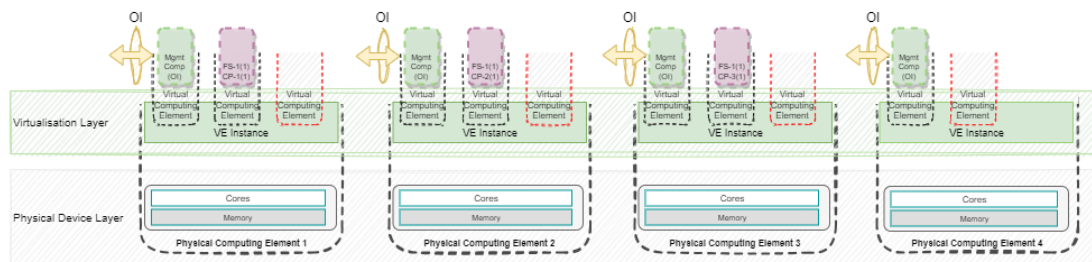











Figure 9 Configuration of Virtual Computing Elements

Scenario

Step	Description	Involved Entities
1	Verify via OI that the Virtualisation Environment of the designated Physical Computing Elements complies with the requirements as per the qualified FS Deployment Rules of the intended Functional System.	SPT2CE-1064 - Installation Team Member
2	Confirm via OI whether sufficient resources can be allocated on the designated Physical Computing Element(s) in accordance with the FS Deployment Rules of the intended Functional System.	SPT2CE-1064 - Installation Team Member
3	Create via OI all Virtual Computing Element(s) according to the FS Deployment Rules of the intended Functional System.	SPT2CE-1064 - Installation Team Member
4	Verify via OI that the correct Virtual Computing Element(s) have been created and that they are ready to for FS Compartment deployment.	SPT2CE-1064 - Installation Team Member

Op.Entities	SPT2CE-1064 - Installation Team Member
-------------	--

Op.Postcondition	<ul style="list-style-type: none"> • All Virtual Computing Element(s) required for the deployment of the FS Compartments of the intended Functional System have been created. • It has been verified that the Virtual Computing Elements(s) configuration comply with the FS Deployment Rules of the intended Functional System.
Op.Precondition	<ul style="list-style-type: none"> • Virtualisation Environment has been installed and configured on each Physical Computing Element • Physical Computing Element(s) are accessible via the OI. • FS Deployment Rules of intended Functional System are available.
Op.Rationale	
Linked Work Items	<p>is derived from :  SPT2CE-19 - Aggregate multiple Functional Applications on the same Instance of a Computing Platform</p> <p>is derived from :  SPT2CE-22 - Deploy Functional Applications through a harmonized approach</p> <p>is derived from :  SPT2CE-30 - System operation and update deployment without or with minimal on-site presence</p> <p>has parent :  SPT2CE-1429 - Deploy Functional System</p> <p>_ is ruled by :  SPT2CE-1432 - No Application Condition (safety and non-safety related) of a Functional System...</p> <p>_ is ruled by :  SPT2CE-1599 - Meticulous attention must be given to ensuring that the needed Virtual Computing...</p> <p>_ is ruled by :  SPT2CE-1433 - Importantly, configuring an additional Virtual Computing Element on the Virtuali...</p> <p>_ is ruled by :  SPT2CE-1427 - The configuration of Virtual Computing Elements shall be conducted remotely thro...</p> <p>_ is ruled by :  SPT2CE-1426 - The Virtualisation Environment Instances installed on the Physical Computing Ele...</p>

SPT2CE-1427 -



The configuration of Virtual Computing Elements shall be conducted remotely through the Orchestration Interface (OI).

Rationale: *To avoid on-site presence of maintenance personnel.*

SPT2CE-1426 -



The Virtualisation Environment Instances installed on the Physical Computing Elements must comply with the requirements specified in the FS Deployment Rules of the intended Functional System

Rationale: *It is essential that the used Virtualisation Environment Instance complies to the qualified Virtualisation Environment.*

SPT2CE-1433 -



Importantly, configuring an additional Virtual Computing Element on the Virtualization Layer Instance of a Physical Computing Element shall not impact the operation of any other Virtual Computing Element already running on the same Physical Computing Element

Rationale: *Otherwise, all Functional Systems running FS Compartments in Virtual Computing Element(s) residing on the same Physical Computing Element would have to be stopped.*

SPT2CE-1432 -



No Application Condition (safety and non-safety related) of a Functional System shall prevent the concurrent operation of FS Compartments from different suppliers on the same Physical Computing Element, provided that temporal and spatial separation is maintained at all times in accordance with CENELEC EN 5012x.

***Rationale:** This is essential in order to be able to aggregate Functional Systems of various suppliers on the same Physical Computing Element(s)*

SPT2CE-1599 -



Meticulous attention must be given to ensuring that the needed Virtual Computing Elements are accurately mapped to the correct number of distinct Physical Computing Elements

***Rationale:** Wrong mapping of Virtual Computing Elements will eventually be detected by the Safety Layer of the deployed FS and hence have no safety impact, but it will affect the FS availability.*

SPT2CE-1713 -



The OI interface shall be standardised by the SP TCCS domain through configuration management/update. The SP CE domain will provide the requirements for the FS deployment and update.

SPT2CE-1431 - Deploy Functional System Compartments on Virtual Computing Elements

In this step, all FS Compartment Instances are deployed to their respective Virtual Computing Elements. Upon the successful deployment of all compartments, the Functional System can be activated and put into operation.

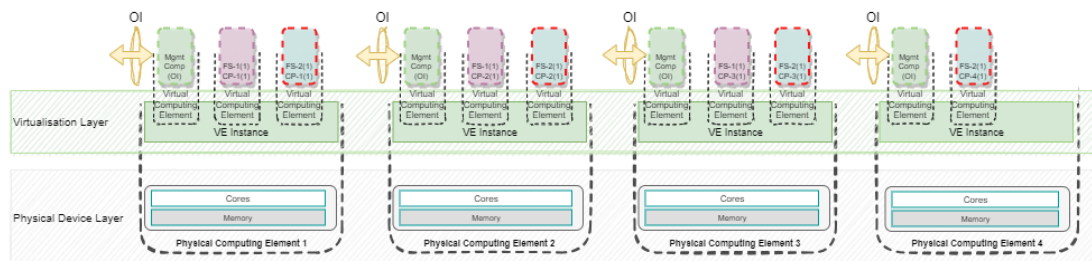










Figure 10 Distribution and installation of FS Compartments

Scenario

Step	Description	Involved Entities
1	Ensure that the correct version of the Functional System is used for deployment.	SPT2CE-1325 - Version Checker
2	For each Virtual Computing Element foreseen for the installation of a FS Compartment check whether it complies with the FS Deployment Rules of the intended Functional System.	SPT2CE-1064 - Installation Team Member
3	Using the OI, install each FS Compartment onto its corresponding Virtual Computing Element as per the FS Deployment Rules of the intended Functional System.	SPT2CE-1064 - Installation Team Member

Step	Description	Involved Entities
4	Verify via OI the correct mapping of FS Compartment and Virtual Computing Element.	 SPT2CE-1064 - Installation Team Member
5	Start Functional System via OI	 SPT2CE-1064 - Installation Team Member
6	Functional System checks at start-up if it has been deployed correctly according to the qualified and qualified FS Deployment Rules. In case the check fails, the system must not go into service.	 SPT2CE-1327 - Functional System
7	Verify proper operation	 SPT2CE-1064 - Installation Team Member

Op.Entities	SPT2CE-1064 - Installation Team Member
Op.Postcondition	* The Functional System is installed on the Virtual Computing Elements. * The Functional System is up and running
Op.Precondition	<ul style="list-style-type: none"> Virtual Computing Element(s) for the installation of the FS Compartment(S) have been created and configured. Virtual Computing Element(s) are accessible via OI FS Compartments, FS Deployment Rules and installation manuals of the intended Functional System are available.
Op.Rationale	
Linked Work Items	<p>has parent :  SPT2CE-1429 - Deploy Functional System</p> <p>_ is ruled by :  SPT2CE-1430 - The distribution to and installation of FS Compartment instances on their respec...</p> <p>_ is ruled by :  SPT2CE-1425 - Mechanisms need to be in place for the safe distribution, installation and activ...</p> <p>_ is ruled by :  SPT2CE-1424 - The safety layer must be adept at recognizing scenarios where the safety-critica...</p>

SPT2CE-1430 -



The distribution to and installation of FS Compartment instances on their respective Virtual Computing Elements shall be conducted remotely through the Orchestration Interface (OI)

Rationale: *To minimize on-site presence of maintenance personnel.*

SPT2CE-1425 -



Mechanisms need to be in place for the safe distribution, installation and activation of the FS Compartments.

Rationale: In order to be able to deploy a Functional System remotely via the OI requires mechanisms that guarantee that the deployed Functional System exactly complies with its certification and deployment rules.

SPT2CE-1424 -



The safety layer must be adept at recognizing scenarios where the safety-critical instances of the FS Compartments are wrongly deployed onto Virtual Computing Elements not residing on distinct Physical Computing Elements as required by the safety case.

Rationale: It is imperative that safety-critical functions employing composite safety, such as replication and voting, are executed on distinct hardware devices.

5.2.3 Remove a productive Functional System

SPT2CE-1439 - Uninstall Functional System deployed on Virtual Computing Element(s)

This scenario describes the steps to uninstall a productive Functional System.

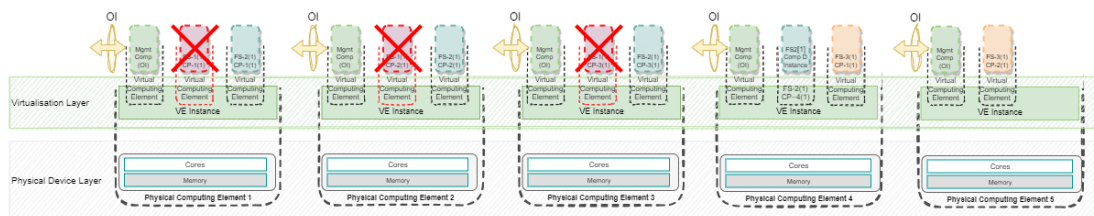


Figure 11 Uninstall Functional System FS1

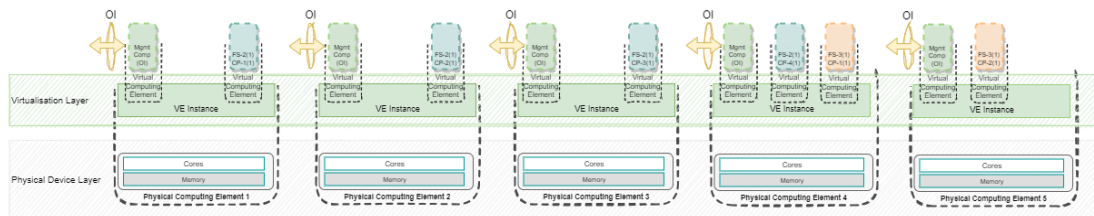










Figure 12 Situation after removal of Functional System FS1

Scenario

Step	Description	Involved Entities
1	Backup Data and Configuration - this ensures that you can restore the system if needed.	SPT2CE-1064 - Installation Team Member
2	Inform all relevant stakeholders about the upcoming uninstallation process	SPT2CE-1064 - Installation Team Member
3	Safely shut down the Functional System and associated Virtual Computing Elements	SPT2CE-1064 - Installation Team Member

Step	Description	Involved Entities
4	Remove Network configuration(s) associated with the intended Functional System	 SPT2CE-1064 - Installation Team Member
5	Follow the Functional System's documentation to uninstall the respective FS Compartment(s)	 SPT2CE-1064 - Installation Team Member
6	Remove Virtual Computing Element(s) e.g., free allocated spatial & temporal resources	 SPT2CE-1064 - Installation Team Member
7	Update overall system documentation to reflect the changes made during the uninstallation process	 SPT2CE-1064 - Installation Team Member
8	Implement any necessary security measures to ensure that the system or any residual data is not accessible by unauthorized individuals	 SPT2CE-1064 - Installation Team Member
9	Conduct a final round of testing to ensure that the system is no longer operational and that there are no unexpected side effects from the uninstallation process	 SPT2CE-1064 - Installation Team Member

Op.Entities	
Op.Postcondition	
Op.Precondition	<ul style="list-style-type: none"> Functional System is up and running on Virtual Computing Element(s) Remote access via OI to respective Virtual Computing Element(s) Functional System documentation is available Access to overall system documentation
Op.Rationale	
Linked Work Items	<p>has parent :  SPT2CE-1443 - Remove a productive Functional System</p> <p>_ is ruled by :  SPT2CE-1438 - Uninstalling Functional System Compartments deployed to Virtual Computing Elemen...</p>

SPT2CE-1438 -



Uninstalling Functional System Compartments deployed to Virtual Computing Elements shall be possible without affecting any other Functional System Compartment running on the same Physical Computing Element. Specifically, there shall be no need to shutdown and/or restart the respective Physical Computing Elements.

Rationale: *To warrant the safety and availability of other Functional Systems.*

5.3 Update Scenarios

5.3.1 Update of the Compartment Execution Environment

The new compartment execution environment must be qualified before the replacement. The compartment execution environment must be integrated, tested and qualified with specific FS to be deployed before the replacement. The use of non-qualified compartment execution environment is strictly prohibited as this may result in unforeseen reliability, availability, maintainability and safety issues.

5.3.1.1 Update the Physical Computing Element

The new physical computing element must be qualified before the replacement. The hardware must be tested with the specific hardware configuration such as processing power (CPUs), memory capacity (volatile/non-volatile), hardware accelerators, firmware versions etc. before the update. The use of hardware that does not comply with deployment rules is strictly prohibited as this may result in unforeseen reliability, availability, maintainability issues.

SPT2CE-1448 - Replace physical computing element

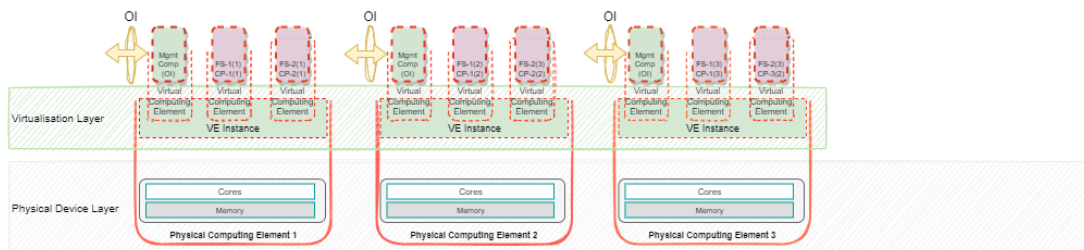


Figure 13 replacing Physical Computing Element

Scenario

Step	Description	Involved Entities
1	Inform all relevant stakeholders about the upcoming upgrade/replacement of physical computing element.	👤 SPT2CE-1064 - Installation Team Member
2	Shut down all FS compartments running on the physical computing element. If necessary, backup the state of compartments.	👤 SPT2CE-1064 - Installation Team Member
3	Shut down the virtualisation environment instance.	👤 SPT2CE-1064 - Installation Team Member
4	Shut down the physical computing element.	👤 SPT2CE-1064 - Installation Team Member
5	Remove the physical computing element.	👤 SPT2CE-1064 - Installation Team Member
6	Install the new hardware according to scenario SPT2CE-1420 - Prepare Physical Computing Element(s)	👤 SPT2CE-1064 - Installation Team Member
7	Install the virtualisation environment according to scenario SPT2CE-1421 - Install Virtualisation Environment on Physical Computing Element(s)	👤 SPT2CE-1064 - Installation Team Member

Step	Description	Involved Entities
8	Install all FS compartments that shall run on the physical computing element according to scenario SPT2CE-1431 - Deploy Functional System Compartments on Virtual Computing Elements If necessary, restore the state that was backed up before.	SPT2CE-1064 - Installation Team Member
9	Test all functional system compartments running on the physical computing element are up and running.	SPT2CE-1064 - Installation Team Member

Op.Entities	
Op.Postcondition	<ul style="list-style-type: none"> The upgraded system is up and running
Op.Precondition	<ul style="list-style-type: none"> Replacement of physical computing element is qualified, planned and communicated Qualified physical computing element is available for replacement The new hardware is compatible with FS Deployment Rules as well as all necessary Approval Documentation.
Op.Rationale	
Linked Work Items	<p>has parent : SPT2CE-1445 - Update the Physical Computing Element</p> <p>_ is ruled by : SPT2CE-1556 - To replace defective HW it is essential that the safety environment shall support FS compartment management</p>

5.3.1.2 Update of Virtualization Environment

The new VE must be qualified before the replacement. The VE must be integrated, tested and qualified before the replacement. The use of non-qualified VE is strictly prohibited as this may result in unforeseen reliability, availability, maintainability and safety issues.

5.3.1.2.1 Update of Compatible Virtualisation Environment

SPT2CE-1446 - Update Virtualization Environment while Functional System is Running (Compatible Update)

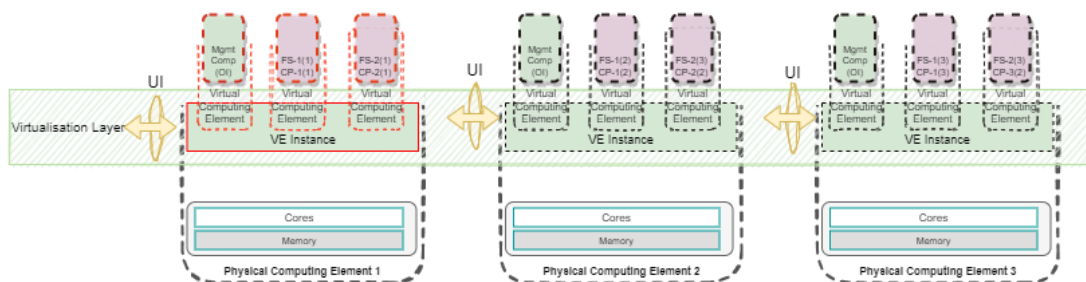







Figure 14 replacing Virtualisation Environment

Scenario

Step	Description	Involved Entities
------	-------------	-------------------

Step	Description	Involved Entities
1	Inform all relevant stakeholders about the upcoming virtualisation environment upgrade/replacement.	👤 SPT2CE-1064 - Installation Team Member
2	Shut down all FS compartments running on the virtualisation environment instance. If necessary, backup the state of compartments.	👤 SPT2CE-1064 - Installation Team Member
3	Shut down the virtualisation environment instance.	👤 SPT2CE-1064 - Installation Team Member
4	Install the new virtualisation environment instance according to scenario  SPT2CE-1421 - Install Virtualisation Environment on Physical Computing Element(s)	👤 SPT2CE-1064 - Installation Team Member
5	Install all FS compartments that shall run on the virtualisation environment instance according to scenario  SPT2CE-1431 - Deploy Functional System Compartments on Virtual Computing Elements If necessary, restore the state that was backed up before.	👤 SPT2CE-1064 - Installation Team Member
6	Test all functional system compartments running on the virtualisation environment instance are up and running.	👤 SPT2CE-1064 - Installation Team Member

Op.Entities	
Op.Postcondition	<ul style="list-style-type: none"> The upgraded system is up and running
Op.Precondition	<ul style="list-style-type: none"> Upgrade of the virtualisation environment is qualified, planned and communicated Qualified virtualisation environment is available for the upgrade The new virtualisation environment is compatible with FS Deployment Rules as well as all necessary Approval Documentation.
Op.Rationale	
Linked Work Items	<p>references in description :  SPT2CE-1026 - Install Virtualisation Environment on Physical Computing Element(s)</p> <p>references in description :  SPT2CE-1050 - Deploy Functional System Compartments on Virtual Computing Elements</p> <p>has parent :  SPT2CE-1447 - Update of Compatible Virtualisation Environment</p>

SPT2CE-1564 -



The Virtualisation Environment shall provide a full HW abstraction, the adaptation of the virtualisation for running of different types of hardware must not have any impact onto the Functional Systems running above.

Rationale: HW specific drivers shall not impact the Functional Systems running above I3

SPT2CE-1566 -



Updating the virtualization environment shall have no impact on the FS configuration and deployment rules.

Rationale: It is essential that new version of VE shall not impact the FS running above I3

5.3.1.2.2 Update of Incompatible Virtualization Environment

SPT2CE-1602 - Update Virtualization Environment including Stopping of FS (Incompatible Update)

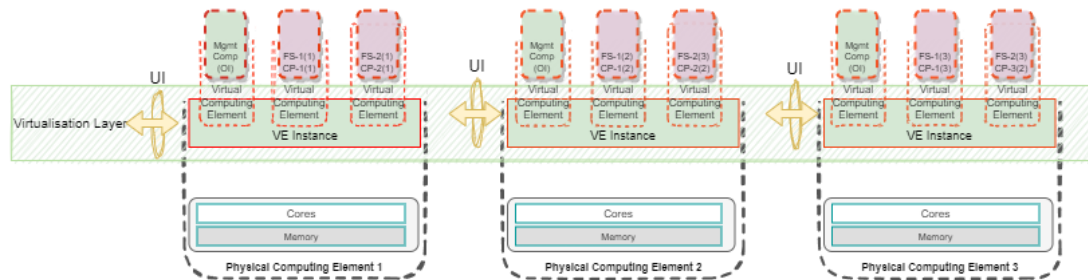


Figure 15 replacing Incompatible virtualisation environment

Scenario

Step	Description	Involved Entities
1	Inform all relevant stakeholders about the upcoming virtualisation environment upgrade/replacement.	🧑 SPT2CE-1064 - Installation Team Member
2	Shut down all Virtualization environment instances and all FS compartments running on those virtualisation environment instances. If necessary, backup the state of compartments.	🧑 SPT2CE-1064 - Installation Team Member
3	Shut down all the virtualisation environment instances.	🧑 SPT2CE-1064 - Installation Team Member
4	Install the new virtualisation environment instance according to scenario SPT2CE-1421 - Install Virtualisation Environment on Physical Computing Element(s)	🧑 SPT2CE-1064 - Installation Team Member
5	Install all FS compartments that shall run on the virtualisation environment instances according to scenario SPT2CE-1431 - Deploy Functional System Compartments on Virtual Computing Elements If necessary, restore the state that was backed up before.	🧑 SPT2CE-1064 - Installation Team Member
6	Test all functional system compartments running on the virtualisation environment instances are up and running.	🧑 SPT2CE-1064 - Installation Team Member

Op.Entities	
Op.Postcondition	The upgraded system is up and running
Op.Precondition	<ul style="list-style-type: none"> Upgrade of the virtualisation environment is qualified, planned and communicated Qualified virtualisation environment is available for the upgrade The new virtualisation environment is compatible with FS Deployment Rules as well as all necessary Approval Documentation.
Op.Rationale	
Linked Work Items	has parent : SPT2CE-1601 - Update of Incompatible Virtualization Environment

5.3.2 Update Functional System

The new FS must be qualified before the replacement. The FS must be integrated, tested and qualified with the specific compartment execution environment to be deployed before the replacement. The use of non-qualified FS is strictly prohibited as this may result in unforeseen reliability, availability, maintainability and safety issues.

5.3.2.1 Update of compatible FS

SPT2CE-1456 - Update Functional System while it is Running (Compatible Update)

Update of the running Functional System with a new version, where the new FS compartments are compatible with the previous FS compartments.

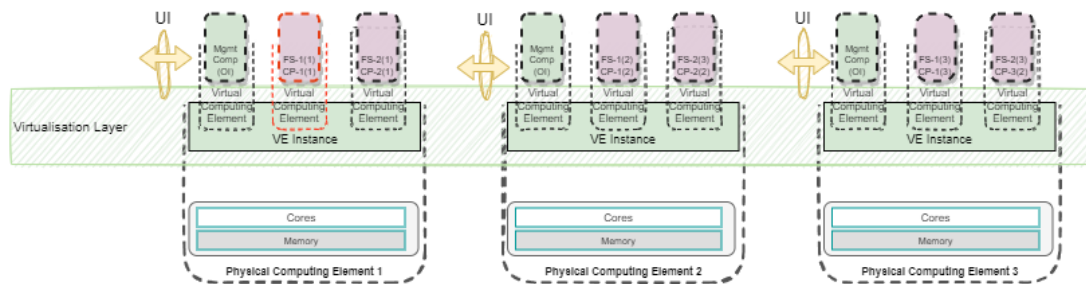


Figure 16 replacing Compatible Functional System

Scenario

Step	Description	Involved Entities
1	Inform all relevant stakeholders about the upcoming FS upgrade.	👤 SPT2CE-1064 - Installation Team Member
2	Shut down the first FS compartment.	👤 SPT2CE-1064 - Installation Team Member
3	Uninstall the first FS compartment.	👤 SPT2CE-1064 - Installation Team Member
4	Install the new version of the first FS compartment according to the FS Deployment Rules.	👤 SPT2CE-1064 - Installation Team Member
5	Start the new version of the first FS compartment.	👤 SPT2CE-1064 - Installation Team Member
6	Verify that the FS is running and the new version of the first FS compartment is running synchronised with the other compartments of the FS.	👤 SPT2CE-1064 - Installation Team Member
7	Repeat steps 2 to 6 for each remaining FS compartment.	👤 SPT2CE-1064 - Installation Team Member
8	Verify that all FS compartments are updated to the new version and are running synchronised.	👤 SPT2CE-1064 - Installation Team Member

Op.Entities	
Op.Postcondition	The updated functional system is up and running

Op.Precondition	<ul style="list-style-type: none"> • Upgrade of the FS is qualified, planned and communicated. • Pre-qualified and qualified FS is available for the upgrade. • The computing environment is compatible with the FS Deployment Rules of the new version of the FS. • The new version of the FS compartments is compatible with the previous version of the FS compartments.
Op.Rationale	
Linked Work Items	has parent : SPT2CE-1457 - Update of compatible FS

SPT2CE-1559 -



After the update of compatible FS compartment to a new version, it must be synchronized with other running FS compartments.

Rationale: In order to have a fully functional Moon configuration of the respective Functional System

SPT2CE-1565 -



The update of the FS compartment must not impact other running FS compartments onto the same physical computing element.

Rationale: The virtual computing elements onto the same physical computing element may not interfere with each other and can be independently managed.

5.3.2.2 Update of non-compatible FS

SPT2CE-1458 - Update Functional System including Stopping of FS (Incompatible Update)

Update of the Functional System with new version, where the new FS compartments are incompatible with the previous FS compartments. Therefore, the FS has to be stopped for the update.

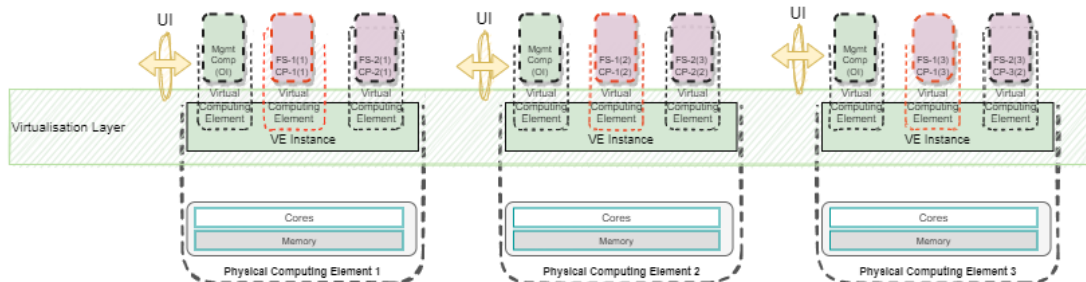










Figure 17 replacing Incompatible Functional System

Step	Description	Involved Entities
1	Inform all relevant stakeholders about the upcoming FS upgrade.	SPT2CE-1064 - Installation Team Member
2	Shut down the FS. If necessary, backup state of the FS.	SPT2CE-1064 - Installation Team Member
3	Uninstall all FS compartments.	SPT2CE-1064 - Installation Team Member

Step	Description	Involved Entities
4	If necessary, update the configuration of the Virtual Computing Elements according to scenario  SPT2CE-1428 - Configure Virtual Computing Elements required for first Functional System .	 SPT2CE-1064 - Installation Team Member
5	Install the new FS according to scenario  SPT2CE-1431 - Deploy Functional System Compartments on Virtual Computing Elements . If necessary, restore the FS state from backup.	 SPT2CE-1064 - Installation Team Member
6	Start the new FS.	 SPT2CE-1064 - Installation Team Member
7	Verify that the upgraded FS is up and running.	 SPT2CE-1064 - Installation Team Member

Op.Entities	
Op.Postcondition	<ul style="list-style-type: none"> The updated functional system is up and running
Op.Precondition	<ul style="list-style-type: none"> Upgrade of the FS is qualified, planned and communicated Pre-qualified and qualified FS is available for the upgrade The computing environment is compatible with the FS Deployment Rules of the new version of the FS.
Op.Rationale	
Linked Work Items	<p>references in description :  SPT2CE-1050 - Deploy Functional System Compartments on Virtual Computing Elements</p> <p>has parent :  SPT2CE-1459 - Update of non-compatible FS</p>

SPT2CE-1563 -



The Virtualisation Environment shall support the remote deletion of a compartment without any impact to already installed and running other compartments on the same computing element.

Rationale: *The deletion of compartments must not have any impact to other compartments running on the same computing element.*

5.4 Recovery Scenarios

The recovery scenarios below describe all the scenarios in which a failure occurs during the operation and how to manage it until a full recovery of the Functional System is achieved. Three main actors are involved in these scenarios: the functional system, the **operator** and the **maintainer** .

The functional system is involved when an automatic recovery is possible. The operator could see the effects of the failure, possibly could initiate the maintainer to restart the functional system and validate the recovery. The maintainer has all the tools to monitor, diagnose, recover the system (e.g. restart SW) and validate the recovery.

In the scenarios below, the figures show the **origin of the failure in red** and, **the collateral effects**, if any, **on other components in orange**. In terms of failures, it is clear that recovery scenarios are only relevant if a clear failure is detected by other components. So, a failure in the running system that does not affect any of the components would not be detected.

The scenarios below consider a SIL4 system with exemplary 2oo3 principle. Other architectures exist such as 1oo2 or 2oo2; however, it is not considered necessary to evaluate every MooN architecture.

The impact on functional systems will vary depending on the number of components still available; if below M, the

functional system fails. This case is treated as a total failure in the following scenarios. For other configurations, a failure leads to different impacts and recovery steps.

For the goal “highest availability of functional systems” it’s recommended to implement dedicated redundancy and repair-mechanisms within the different SW layers of the RTE to handle failures of HW, SW and network in best available and automated way - avoiding manual maintenance activities as good as possible.

5.4.1 SW failures within the Functional System

5.4.1.1 Total SW Failure of one FS Compartment

SPT2CE-1483 - Total SW Failure of one FS Compartment

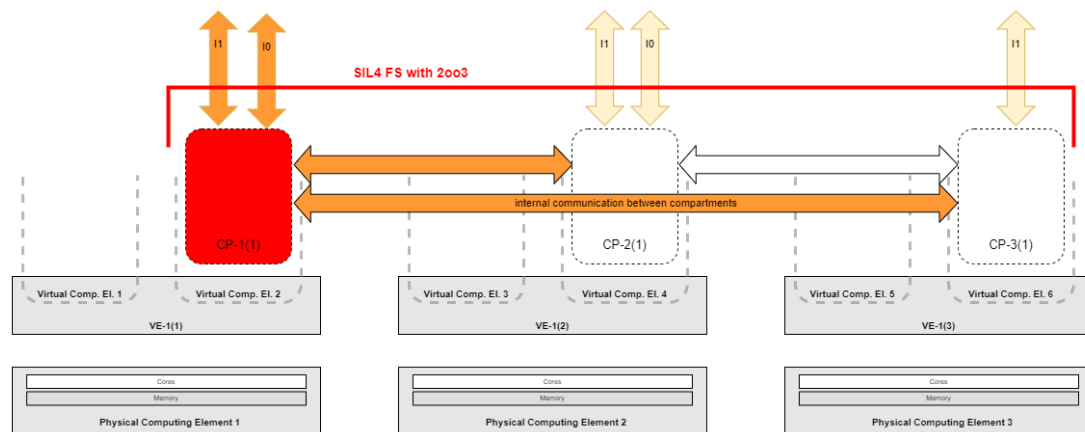





Figure 18 Total SW failure of one FS compartment

Scenario

Step	Description	Involved Entities
1a	<p>Failure:</p> <p>The total software within compartment 1 of a FS fails</p> <p>This failure can occur within SIL or BIL Functional System.</p> <p>This doesn't have to mean that the SW within the compartment 1 has completely (100%) failed. But so much has failed that the SW within the compartment can no longer work operationally and is considered "down" from a FS availability perspective.</p>	internal
1b	<p>Impact on FS:</p> <ul style="list-style-type: none"> FS SW instance within compartment 1 stops working, but FS keeps running with reduced availability: SIL4 FS running as 2oo2. BIL FS running as 1oo1. External communication connections of the affected compartment 1 break down. This leads to reduced availability in communication: only single communication channel instead of redundant channels. 	internal

Step	Description	Involved Entities
2	Failure identification: <ul style="list-style-type: none"> by the dedicated RTE monitoring task within the compartment 1, it provides diagnosis message via I1 by the other compartments 2 and 3, they provide diagnosis message via I1 	I1 - diagnosis
3	Recovery: For the recovery it's necessary to restart the failed compartment 1.	internal
3a	The RTE monitoring task of the compartment 1 automatically restarts the failed SW component(s) of the compartment 1.	automated restart by RTE
3b	If such a automated restart is not possible - e.g., if monitoring task itself is failed or restarting of failed tasks not successful - the restart has to be initiated by a maintainer remotely. It depends on the details of the SW failure if the failed compartment can be restarted automatically or has to be restarted by the maintainer	 SPT2CE-1204 - Maintainer via I1
4	Compartment 1 starts up and synchronizes with each other compartment 2 and 3 automatically Failed communication connection channels are build up automatically by the compartment 1.	internal
5	Failure clearing: <ul style="list-style-type: none"> Diagnosis message of RTE informs that the failure is cleared, and the functional system is fully operational. 	I1 (to diagnosis)

Op.Entities	 SPT2CE-1204 - Maintainer (step 3b if a manual recovery is needed)
Op.Postcondition	<ul style="list-style-type: none"> FS is running without any failure
Op.Precondition	<ul style="list-style-type: none"> FS is running without any failure
Op.Rationale	
Linked Work Items	has parent :  SPT2CE-1484 - Total SW Failure of one FS Compartment

SPT2CE-1558 -



For the recovery of FS compartment in case the automatic recovery process fails, the remote maintainer may be able to manually restart the FS compartments.

Rationale: *It is essential that FS compartments are up and running as soon as possible.*

SPT2CE-1567 -



The periodic diagnosis messages provide the health status of the FS compartments.

Rationale: *It is essential to have updated health message of the FS compartment to detect faults and failures on time.*

5.4.1.2 Total SW Failure of all FS Compartments

SPT2CE-1485 - Total SW Failure of all FS Compartments

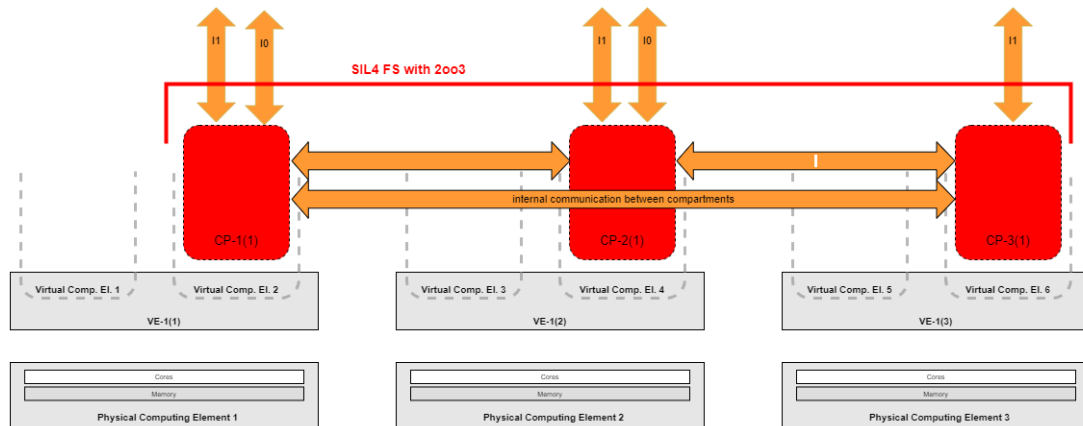


Figure 19 Total SW failure of all FS compartments

Scenario

Step	Description	Involved Entities
1	Failure: All compartments of a FS instance fail at same time point (e.g. due to same SW bug within the SW in all FS compartments)	internal
	Impact on FS: <ul style="list-style-type: none"> FS instance stops operational working All operative communication connections to other systems fail 	internal
2	Failure Identification: <ul style="list-style-type: none"> by the dedicated RTE monitoring task within the compartments, it provides diagnosis message via I1 by the other FS which are connected to the FS, they provide diagnosis message via I1 Operator identifies the total failure 	I1 (to diagnosis) 🧑 SPT2CE-1205 - Operator
3	Recovery: For the recovery it's necessary to restart the failed FS compartments 1,2 and 3 in parallel.	-
3a	The RTE monitoring task within the compartments 1,2 and 3 automatically restarts the failed SW task(s) within the FS compartments.	automated restart by RTE monitoring component

Step	Description	Involved Entities
3b	If such an automated restart is not possible - e.g., if monitoring task itself is failed or restarting of failed tasks not successful - the restart has to be initiated by a maintainer remotely or a manual reboot of the platform directly by the operator. It depends on the details of the SW failure if the failed compartments can be restarted automatically or has to be restarted by the maintainer	<p>🧑 SPT2CE-1204 - Maintainer via I1 / I3</p> <p>🧑 SPT2CE-1205 - Operator</p>
4	All compartments 1,2 and 3 start up and synchronize with each other automatically Communication connections are built up automatically by the compartments.	internal
5	Failure clearing: <ul style="list-style-type: none"> Diagnosis message of RTE informs that the failure is cleared, and the functional system is fully operational. 	I1 (to diagnosis)
6	Operation: Operator has to handle the re-start of the FS instance (e.g. in use case IXL the track detection has to be handled after IXL restart).	🧑 SPT2CE-1205 - Operator

Op.Entities	<p>🧑 SPT2CE-1204 - Maintainer (step 3b if a manual recovery is needed)</p> <p>🧑 SPT2CE-1205 - Operator</p>
Op.Postcondition	<ul style="list-style-type: none"> FS is working without any failure.
Op.Precondition	<ul style="list-style-type: none"> FS is working without any failure.
Op.Rationale	
Linked Work Items	has parent : 📁 SPT2CE-1486 - Total SW Failure of all FS Compartments

5.4.2 SW failures within the Virtualization Environment

5.4.2.1 Individual SW failure of one Virtual Computing Element

SPT2CE-1482 - Individual SW failure of one virtual computing element

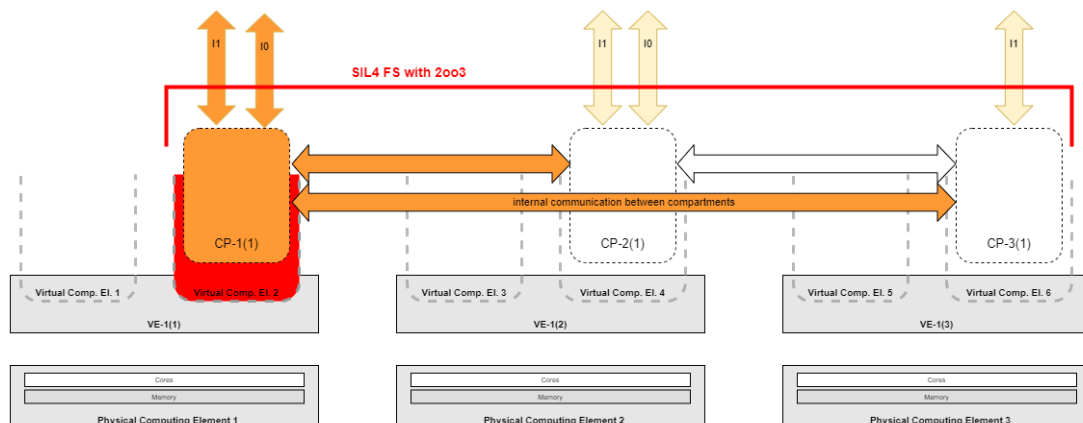





Figure 20 Individual SW failure of one virtual computing element

Scenario

Step	Description	Involved Entities
1	Failure: One virtual computing element of a FS fails.	internal
	Impact on FS: <ul style="list-style-type: none"> • Compartment 1 stops working • FS availability reduced: SIL4 FS running as 2oo2. BIL FS running as 1oo1. • Belonging external comm connections fail and lead to a single channel communication (without redundancy) 	internal
2	Failure Identification: <ul style="list-style-type: none"> • by the other compartment(s), they provide diagnosis message via I1 • by the other systems which are connected to the FS, they provide diagnosis message via I1 • by the Virtualization Environment via OI 	I1 (to diagnosis) OI
3	Recovery: Failed virtual computing element has to be repaired by maintainer A deployment of a new VM and compartment is necessary, and the compartment has to be started.	automated or  SPT2CE-1204 - Maintainer via OI and I1
4	Compartment 1 starts up and synchronizes with other compartments automatically. Failed communication connection channels are build up automatically by the compartment 1.	internal
5	Failure clearing: <ul style="list-style-type: none"> • Diagnosis message of RTE informs that the failure is cleared, and the functional system is fully operational. 	I1 - diagnosis

Op.Entities	 SPT2CE-1204 - Maintainer (step 3 if manual recovery is needed)
Op.Postcondition	<ul style="list-style-type: none"> • FS is running without any failure.
Op.Precondition	<ul style="list-style-type: none"> • FS is running without any failure.
Op.Rationale	
Linked Work Items	has parent :  SPT2CE-1479 - Individual SW failure of one Virtual Computing Element

5.4.2.2 SW Failure of one complete VE Instance

SPT2CE-1489 - SW Failure of one complete VE Instance

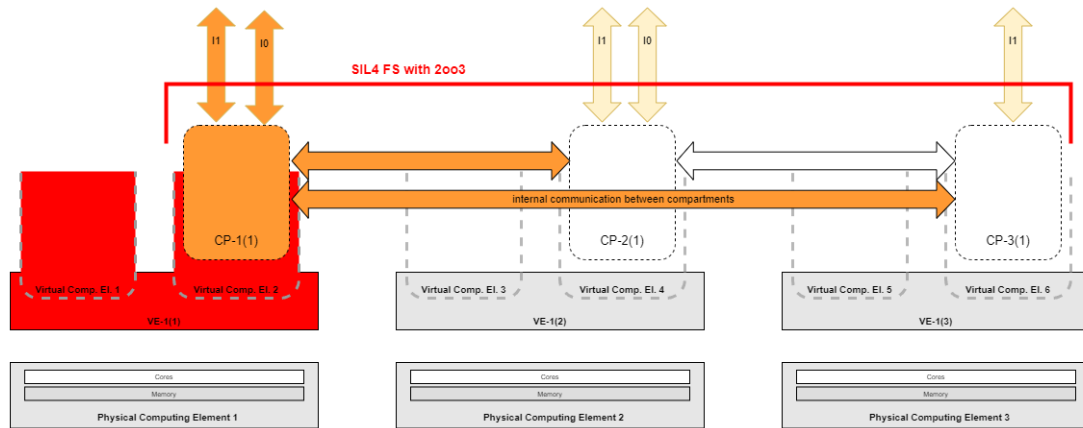




Figure 21 Failure of one complete VE Instance

Scenario

Step	Description	Involved Entities
1	Failure: One complete VE instance fails.	internal
	Impact on FS: <ul style="list-style-type: none"> Compartment 1 stops working FS availability reduced: SIL4 FS running as 2oo2. BIL FS running as 1oo1. Belonging external communication connections fail and lead to single channel communication (without redundancy) 	internal
2	Failure Identification: <ul style="list-style-type: none"> by the other compartment(s), they provide diagnosis message via I1 by the other systems which are connected to the FS, they provide diagnosis message via I1 by Orchestration tool behind OI 	I1 (to diagnosis) OI
3a	Recovery: Failed VE instance has to be repaired by maintainer Deployment of a new VMs and affected compartments is necessary and the compartments has to be started.	automated or SPT2CE-12 04 - Maintainer via I1
4	Compartment starts up and synchronizes with other compartments automatically. Failed communication connection channels are build up automatically by the compartment 1.	

Step	Description	Involved Entities
5	Failure clearing: <ul style="list-style-type: none"> Diagnosis message of RTE informs that the failure is cleared, and the functional system is fully operational 	I1 - diagnosis

Op.Entities	 SPT2CE-1204 - Maintainer (step 3 if manual recovery is needed)
Op.Postcondition	<ul style="list-style-type: none"> FS is running without any failure.
Op.Precondition	<ul style="list-style-type: none"> FS is running without any failure.
Op.Rationale	
Linked Work Items	has parent :  SPT2CE-1481 - SW Failure of one complete VE Instance

5.4.2.3 SW Failure of all VE Instances

SPT2CE-1487 - SW Failure of all VE Instances

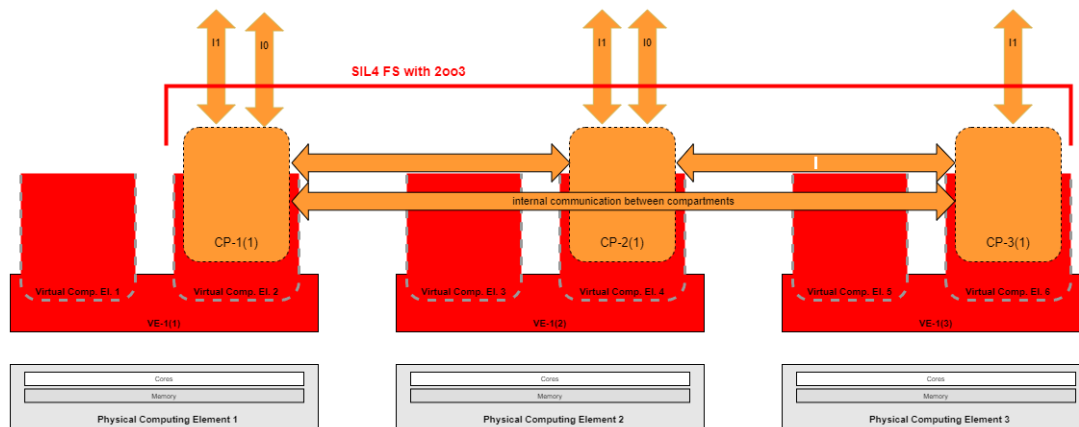








Figure 22 SW Failure of all VE Instances

Scenario

Step	Description	Involved Entities
1	Failure: All VE on all Computing Elements fail. Such a failure may be caused by a systematic error within the virtualisation environment which leads to parallel stop of all VE at (nearly) same time point. One of the potential reasons of such systematic error could be by a cyber-attack.	internal

Step	Description	Involved Entities
	Impact on FS: <ul style="list-style-type: none"> • All compartments stop working • All operative communication connections to other systems fail 	internal
2	Failure Identification: <ul style="list-style-type: none"> • by the other systems which are connected to the FS, they provide diagnosis message via I1 • Operator identifies the total failure • Central diagnosis may identify this total failure. 	I1 (to diagnosis)  SPT2CE-1205 - Operator
3	Recovery: For the recovery it's necessary to repair and restart all VE Instances on all Computing Elements. Via management interface (out of band interface) on maybe prepared machines. Deployment of a new VMs and affected compartments is necessary and the compartments has to be started.	 SPT2CE-1204 - Maintainer via OI
4	All FS compartments start up and synchronize with each other automatically Communication connections are built up automatically by the FS.	internal
5	Failure clearing: <ul style="list-style-type: none"> • Diagnosis message of RTE informs that the failure is cleared, and the functional system is fully operational 	I1 (to diagnosis)
6	Operation: Operator has to handle the re-start of the FS instance (e.g. in use case IXL the track detection has to be handled after IXL restart).	 SPT2CE-1205 - Operator

Op.Entities	 SPT2CE-1205 - Operator  SPT2CE-1204 - Maintainer
Op.Postcondition	<ul style="list-style-type: none"> • FS is running without any failure
Op.Precondition	<ul style="list-style-type: none"> • FS is running without any failure
Op.Rationale	
Linked Work Items	has parent :  SPT2CE-1488 - SW Failure of all VE Instances

5.4.3 SW Failures within the Firmware of the Hardware

A Firmware failure could be managed as a Hardware failure described in the chapters below.

5.4.4 Hardware failure

5.4.4.1 Individual HW failure within one physical computing element

SPT2CE-1496 - Individual HW failure within one physical Computing Element

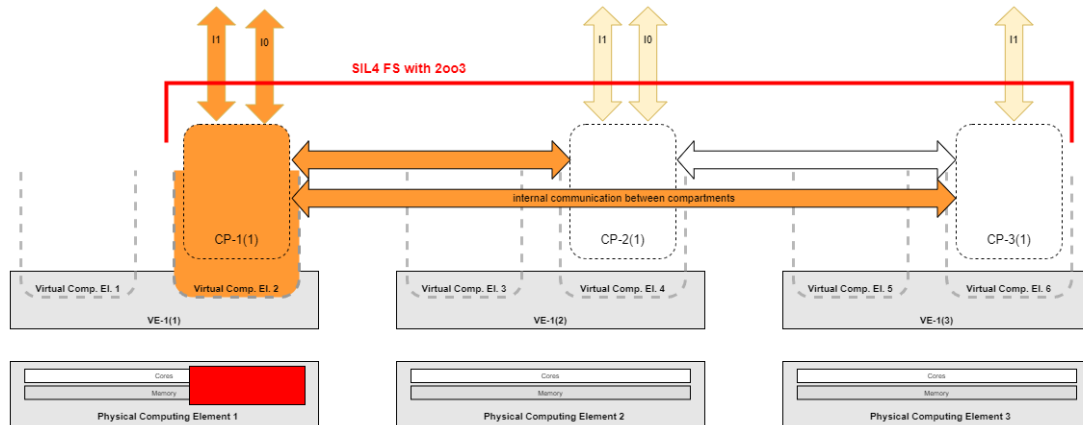


Figure 23 Individual HW failure within one physical Computing Element

Scenario

Step	Description	Involved Entities
1	Failure: An individual Hardware failure happens in such a way that one virtual computing element fails, e.g. failure of one CPU core.	internal
	Impact on FS: <ul style="list-style-type: none"> Virtual Computing Element stops -> Compartment fails FS availability reduced: SIL4 FS running as 2oo2. BIL FS running as 1oo1. FS internal communication connections to other compartments fail. This leads to reduced system availability, e.g. SIL4 FS is running as 2oo2, BIL FS is running as 1oo1. Belonging external communication connections fail and lead to single channel communication (without redundancy) 	internal
2	Failure Identification: <ul style="list-style-type: none"> by the other compartments 2 and 3, they provide diagnosis message via I1 by the other systems which are connected to the FS, they provide diagnosis message via I1 By the monitoring functionality for this physical computing element. 	I1 (to diagnosis) OI

Step	Description	Involved Entities
3	Recovery: Defect Hardware has to be repaired or replaced, see SPT2CE-1490 - Total HW failure of one complete physical computing element . Or: Re-allocation of the affected compartment by the maintainer onto another virtual computing element. Deployment of a new VE and affected compartment is necessary and the compartments has to be started.	SPT2CE-1204 - Maintainer via OI and I1
4	FS SW instance within the compartment 1 starts up and synchronizes with each other FS SW instances within compartments 2, 3 automatically. Failed communication connection channels are build up automatically by the FS compartment.	internal
5	Failure clearing: <ul style="list-style-type: none"> Diagnosis message of RTE informs that the failure is cleared, and the functional system is fully operational 	I1 (to diagnosis)

Op.Entities	SPT2CE-1204 - Maintainer
Op.Postcondition	<ul style="list-style-type: none"> FS is running without any failure.
Op.Precondition	<ul style="list-style-type: none"> FS is running without any failure.
Op.Rationale	
Linked Work Items	has parent : SPT2CE-1497 - Individual HW failure within one physical computing element

5.4.4.2 Total HW failure of one complete physical computing element

SPT2CE-1490 - Total HW failure of one complete physical computing element.

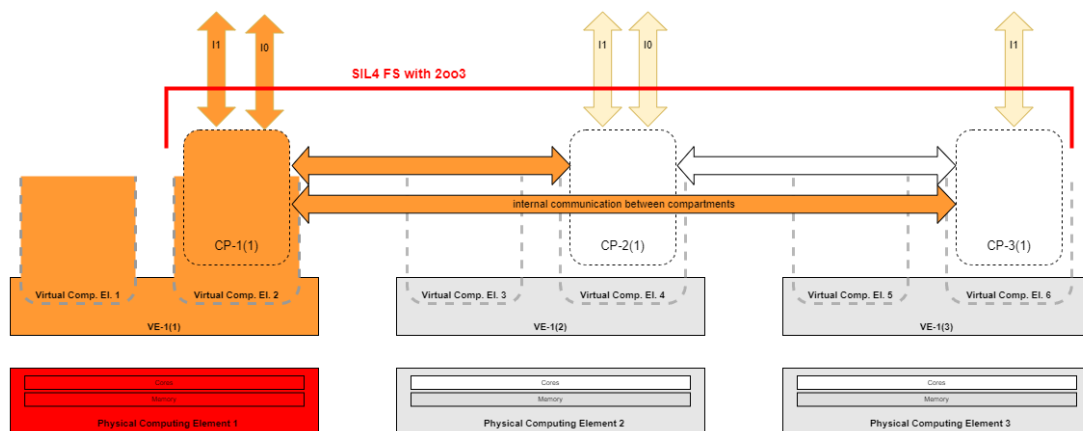





Figure 24 HW failure of a complete physical computing element

Scenario

Step	Description	Involved Entities
1	Failure: A total HW failure of a complete physical computing element happens.	internal
	Impact on FS: <ul style="list-style-type: none"> • VE Instance stops • Compartments of the VE stops. • FS availability reduced: SIL4 FS running as 2oo2. BIL FS running as 1oo1. • FS internal communication connections to other FS SW instances fail. This leads to reduced system availability, e.g. system is running as 2oo2. • Belonging external comm connections fail and lead to single channel communication (without redundancy) 	internal
2	Failure Identification: <ul style="list-style-type: none"> • by the other compartments 2 and 3, they provide diagnosis message via I1 • by the other systems which are connected to the FS, they provide diagnosis message via I1 • by the virtualization management behind OI 	I1 (to diagnosis)
3a	Recovery: Defect Hardware has to be repaired or replaced. Or: Re-allocation of the affected compartment by the maintainer onto another virtual computing element. Deployment of a new VE and affected compartment is necessary and the compartment has to be started. The detailed procedure for exchange of the hardware depends on the use case e.g. if onboard system (without prepared spare hardware) or trackside data center (with prepared spare hardware).	 SPT2CE-12 04 - Maintainer
4	Compartment 1 starts up and synchronizes with each other compartments 2 and 3 automatically. Failed communication connection channels are build up automatically by the compartment.	internal
5	Failure clearing: <ul style="list-style-type: none"> • Diagnosis message of RTE informs that the failure is cleared, and the functional system is fully operational 	I1 (to diagnosis)

Op.Entities	 SPT2CE-1204 - Maintainer
Op.Postcondition	<ul style="list-style-type: none"> • FS is running without any failure.
Op.Precondition	<ul style="list-style-type: none"> • FS is running without any failure.
Op.Rationale	
Linked Work Items	has parent :  SPT2CE-1491 - Total HW failure of one complete physical computing element

SPT2CE-1568 -



Periodic diagnosis messages provide the health status of the physical computing element.

Rationale: It is essential to have updated health message of the physical computing element to detect faults and failures on time.

5.4.4.3 Failure of all computing elements

SPT2CE-1492 - Disaster scenario - failure of all computing elements

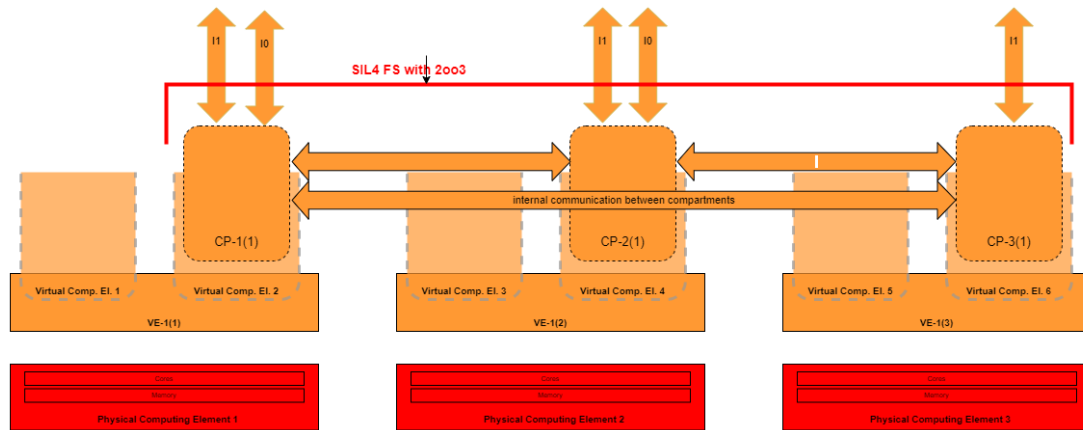







Figure 25 All computing elements fail

Scenario

Step	Description	Involved Entities
1	Failure: Disaster scenario: all computing elements fail, caused by blackout, flood, fire, earthquake,...	internal
	Impact on FS: <ul style="list-style-type: none"> All compartments stop operation 	internal
2	Failure Identification: <ul style="list-style-type: none"> Connected other systems identify the failure Operator identifies the total failure. Central diagnosis may identify this total failure. 	I1 (to diagnosis) SPT2CE-1 205 - Operator
3	Recovery: If a restart of the failed component is not possible manually (hardware damaged), the deployment scenarios have to be considered: hardware setup, virtualisation environment configuration and functional system deployment and startup.	SPT2CE-12 04 - Maintainer SPT2CE-1 205 - Operator

Step	Description	Involved Entities
4	Failure clearing: <ul style="list-style-type: none"> Diagnosis message of RTE informs that the failure is cleared, and the functional system is fully operational 	I1 (to diagnosis)
5	Operation: Operator has to handle the re-start of the FS instance (e.g. in use case IXL the track detection has to be handled after IXL restart).	 SPT2CE-1205 - Operator

Op.Entities	 SPT2CE-1204 - Maintainer  SPT2CE-1205 - Operator
Op.Postcondition	<ul style="list-style-type: none"> FS running without any failure.
Op.Precondition	<ul style="list-style-type: none"> FS running without any failure.
Op.Rationale	
Linked Work Items	is derived from :  SPT2CE-24 - Planned movement/relocation of Functional Applications from one instance of a Computing Platform to another has parent :  SPT2CE-1493 - Failure of all computing elements

5.4.5 Network communication failures

External communication to external systems

- operative communication to rail systems (= I0)
- communication to infrastructure elements as Diagnosis, IT-Security,... (= I1)

Redundant communication = parallel communication with 2 communication channels over 2 networks.

Internal communication between the compartments of a functional system

5.4.5.1 Failure of one external communication connection

SPT2CE-1501 - Failure of one external communication channel regarding I0

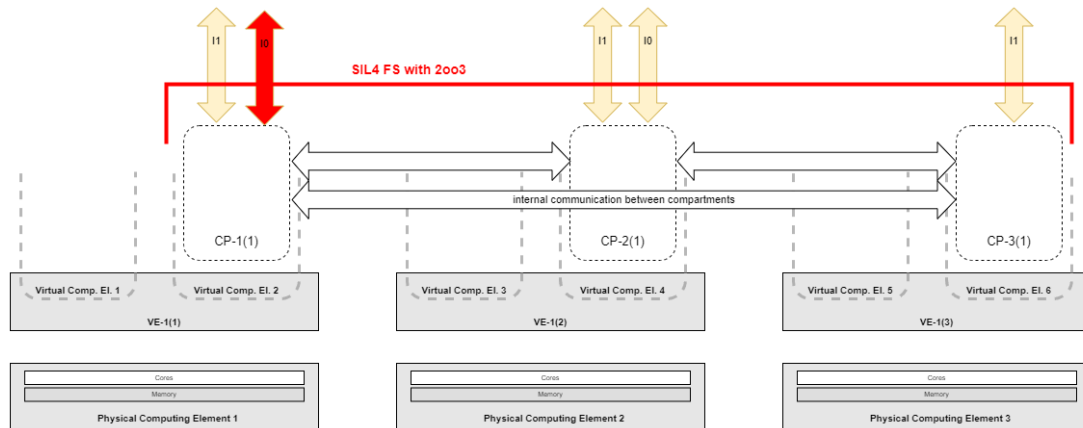


Figure 26 Failure of one external operative communication connection

Scenario

Step	Description	Involved Entities
1	Failure: One external operative communication connection (I0) fails, failure is in the network (switch, cable,...)	internal
	Impact on FS: <ul style="list-style-type: none"> FS is running without redundancy in the affected communication. For the affected communication connection(s) only compartment 2 has active communication channel. 	internal
2	Failure Identification: <ul style="list-style-type: none"> FS provides diagnosis message via I1 Connected other system(s) provides diagnosis message via I1 By the network monitoring functionalities 	I1 (to diagnosis)
3	Recovery: <ul style="list-style-type: none"> Failure has to be repaired (cable, switch...) FS shall automatically build up the communication channel. FS shall try to restore the failed communication continuously until communication is successful. 	SPT2CE-1204 - Maintainer
4	Failure clearing: <ul style="list-style-type: none"> Diagnosis message of RTE informs that the failure is cleared, and the functional system is fully operational. Connected other system(s) provide message that failure is cleared. 	I1 (to diagnosis)

Op.Entities	SPT2CE-1204 - Maintainer
Op.Postcondition	<ul style="list-style-type: none"> FS is running without any failure.

Op.Precondition	<ul style="list-style-type: none"> FS is running without any failure.
Op.Rationale	
Linked Work Items	has parent : SPT2CE-1502 - Failure of one external communication connection

SPT2CE-1560 -



Wherever possible redundant communication channels shall be implemented.

Rationale: It is essential to minimize communication failures and maximize availability.

5.4.5.2 Failure of all external communication channels

SPT2CE-1499 - Failure of all external communication channels regarding I/O

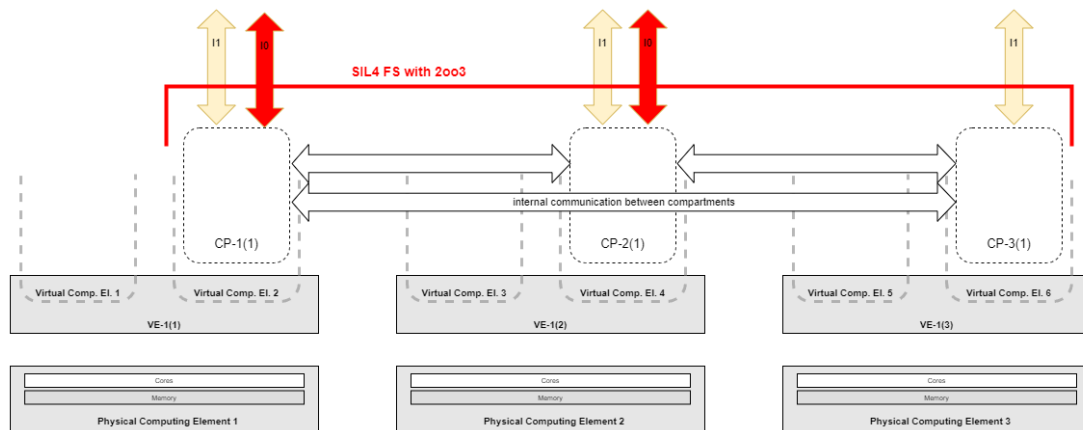







Figure 27 Failure of all external communication channels of I/O

Scenario

Step	Description	Involved Entities
1	Failure: Both external operative communication connection (I0) channels fail, failure is in the network (switch, cable,...)	internal
	Impact on FS: <ul style="list-style-type: none"> FS is running without operative communication. FS system is processing safe reaction if needed (e.g. if communication connection between interlocking and object controller fails). 	internal
2	Failure Identification: <ul style="list-style-type: none"> Operator identifies the communication failure. Connected other system(s) provides diagnosis message via I1 By the network monitoring functionalities 	SPT2CE-1205 - Operator I1 (to diagnosis)

Step	Description	Involved Entities
3	Recovery: <ul style="list-style-type: none"> Failure has to be repaired (cable, switch,...) FS shall automatically build up the communication channels. FS shall try to restore the failed communication continuously until the communication is successful. 	 SPT2CE-1204 - Maintainer
4	Failure clearing: <ul style="list-style-type: none"> Diagnosis message of RTE informs that the failure is cleared, and the functional system is fully operational. Connected other system(s) provide message that failure is cleared. 	I1 (to diagnosis)
5	Operation: <ul style="list-style-type: none"> Depending on the communication connection operator has to handle this buildup (e.g. if connection between interlocking and axle counter was failed the track detection has to be handled.) 	 SPT2CE-1205 - Operator

Op.Entities	 SPT2CE-1205 - Operator  SPT2CE-1204 - Maintainer
Op.Postcondition	<ul style="list-style-type: none"> FS is running without any failure.
Op.Precondition	<ul style="list-style-type: none"> FS is running without any failure.
Op.Rationale	
Linked Work Items	has parent :  SPT2CE-1500 - Failure of all external communication channels

5.4.5.3 Failure of FS internal communication connections

For the FS internal communication between the FS compartments, it depends on the detailed solution and detailed failure, in which way a failure is identified, handled and repaired.

6 Requirements

This chapter describes requirements which are derived from the operational rules from chapter 6. Here the scope of the requirements is at the operational scenarios and analysis level and therefore further, requirements will be covered at the system and sub-system level in the specification deliverable.




6.1 Hardware

This sub chapters describes the requirements related to the hardware.

SPT2CE-1505 - Installation procedure

The physical computing element hardware installation procedure shall not be standardised.




Rationale: As the Physical Computing Element hardware installation process can vary depending on factors such as the type of the Physical Computing Elements, the installation location (on-board, trackside, etc.), and supplier/operator-specific installation guidelines, therefore, the standardization may not be feasible. However, there are standard procedures and best practices that are commonly followed in the industry that could be useful.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1522 - Hardware _ is ruled by :  SPT2CE-1418 - The hardware installation procedures shall not be standardized, as they heavily...

SPT2CE-1520 - COTS components

The Physical Computing Element shall be based on COTS components.

Rationale: Leveraging COTS hardware provides several benefits, including cost-effectiveness, readily available components, and ease of integration.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1522 - Hardware _ is ruled by :  SPT2CE-1422 - While the actual Physical Computing Elements may vary in type and originate from...




6.2 Safety and Availability

This sub chapters describes the requirements related to the safety and availability

SPT2CE-1524 - Use of shared hardware resources

The Application conditions (safety and non-safety related) of the FS shall not limit the use of shared hardware resources.

Rationale: To maximize the efficiency and flexibility of hardware usage it is essential to be able to aggregate Functional Systems of various suppliers on the same Physical Computing Element(s)




Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1523 - Safety and Availability _ is ruled by :  SPT2CE-1432 - No Application Condition (safety and non-safety related) of a Functional System...

SPT2CE-1533 - Identification of incorrect FS Compartment deployment

The safety environment shall identify incorrect deployment of safety critical FS compartment.

Rationale: It is imperative that safety-critical functions employing composite safety, such as replication and voting,




are executed on distinct hardware devices.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1523 - Safety and Availability _ is ruled by :  SPT2CE-1424 - The safety layer must be adept at recognizing scenarios where the safety-critica...

SPT2CE-1529 - Allow mixed criticality on same physical computing element

The safety environment shall not restrict mixed criticality on physical computing element.




Rationale: To enable the wide range of applications with different critical levels to coexists and to attain resource efficiency, flexibility, improved system utilization, optimized performance, and scalability.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1523 - Safety and Availability _ is ruled by :  SPT2CE-1432 - No Application Condition (safety and non-safety related) of a Functional System...

SPT2CE-1528 - Allow for creation/initialization of new compartments during operations

The safety environment shall not restrict the creation/initialization of compartments of other FSs during operations.




Rationale: To support dynamic configuration the system shall support the aggregation/deployment of FS during operations.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1523 - Safety and Availability _ is ruled by :  SPT2CE-1433 - Importantly, configuring an additional Virtual Computing Element on the Virtuali...

SPT2CE-1534 - Allow for starting/stopping FS compartments on different physical computing element

The safety environment shall support start/stop of FS compartments on another physical computing element during runtime.

Rationale: To replace defective HW it is essential that the safety environment shall support FS compartment management



Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1523 - Safety and Availability _ is ruled by :  SPT2CE-1556 - To replace defective HW it is essential that the safety environment shall support FS compartment management

SPT2CE-1546 - Management of VCEs

The Virtual Environment shall provide the management of VCEs during operations

Rationale: This will allow to automate the recovery of FS during operations.




Status	 Content to be approved
--------	--

Linked Work Items	has parent :  SPT2CE-1523 - Safety and Availability _ is ruled by :  SPT2CE-1558 - For the recovery of FS compartment in case the automatic recovery process fails,...
-------------------	---

SPT2CE-1549 - Synchronization of restarted/updated compartment

The safety environment shall support the synchronization of restarted/updated compartment.




Rationale: To synchronize the safe applications replica with other running replicas after update/recovery.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1523 - Safety and Availability _ is ruled by :  SPT2CE-1559 - After the update of compatible FS compartment to a new version, it must be synch...

SPT2CE-1550 - Redundant communication channels

The compartment execution environment shall provide redundant communication channels.

Rationale: In order to achieve a high system availability and/or the safety requirements the FS system shall have redundant and independent communication channels based on Moon configuration.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1523 - Safety and Availability _ is ruled by :  SPT2CE-1560 - Wherever possible redundant communication channels shall be implemented. Rationa...




6.3 Virtualization

This sub chapters describes the requirements related to Virtualization

SPT2CE-1531 - APIs and tools to orchestrate the FS Compartments

The OI shall provide APIs and tools to orchestrate the FS Compartments.




Rationale: To facilitate the remote deployment of FS it is essential to implement mechanisms that automate, manage, and co-ordinate Functional System complies with its certification requirements.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1425 - Mechanisms need to be in place for the safe distribution, installation and activ...

SPT2CE-1553 - Guarantee assigned CPU resources

The virtualisation environment shall guarantee the assigned CPU resources (cores, memory, memory bandwidth, network bandwidth, network latency) for a FS continuously (7 days /24 hours / 60 minutes / 60 seconds) without any influence or dependency to existence and behaviour of other FS aggregated on same computing element.




Rationale: The VE must provide the committed resources to all FS compartments and ensures no interference between the virtual computing elements on same physical computing element.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1433 - Importantly, configuring an additional Virtual Computing Element on the Virtuali...

SPT2CE-1530 - Comply with the FS deployment rules

The configuration of the virtualization environment shall comply with the FS deployment rules.




Rationale: To ensures the function and availability of the intended FS, it is crucial to adhere to its deployment rules.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1426 - The Virtualisation Environment Instances installed on the Physical Computing Ele... _ is ruled by :  SPT2CE-1415 - The Virtualization Environment Instance installed on the available Physical Comp...

SPT2CE-1540 - Standard OI functionalities

The virtualization environment shall provide standard OI functionalities.




Rationale: Having a common set of OI functionalities for operating all Functional System(s) offers benefits such as resource optimization, scalability, high availability, automation, and cost efficiency.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1414 - From the perspective of the Entity in Charge of Maintenance, the Functional Syst...

SPT2CE-1542 - Based on COTS solutions.

The virtualization environment shall be based on COTS solutions.




Rationale: As there are already wide range of COTS virtualization solution available therefore developing a new for railways will not be a wise giving the complexity and cost.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1417 - Preferably, an existing off-the-shelf Virtualisation Environment shall be used....

SPT2CE-1541 - Allow for different virtualisation environment solutions

Different virtualisation environment solutions shall be allowed.




Rationale: There are several types of virtualisation environment solutions available in different domains, each with its own benefit. Therefore, the virtualisation solution could allow different implementation approaches as long as an standard Orchestration Interface (OI) is provided.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1416 - Different Virtualisation Environment implementations shall be allowed, as long a...

SPT2CE-1536 - Remote orchestration

The Virtualization environment shall provide remote orchestration.




Rationale: To enable the efficient management, scalability, cost reduction, it is essential to have a centralised FS management.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1427 - The configuration of Virtual Computing Elements shall be conducted remotely thro...

SPT2CE-1545 - Allow for uninstallation of individual Functional System Compartments

The Virtual Environment shall allow uninstallation of individual compartment deployed on a virtual computing element without interrupting neighboring compartments on the same physical hardware.




Rationale: To ensure the safety and availability of other Functional system compartments running on the same physical computing element.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1438 - Uninstalling Functional System Compartments deployed to Virtual Computing Elemen...

SPT2CE-1544 - Allow for remote creation of Virtual Computing Elements

The Virtualization Environment shall support remote creation of virtual computing element without interfering with already running virtual computing element on the shared physical hardware.




Rationale: To enable remote dynamic configuration of virtual computing elements.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1433 - Importantly, configuring an additional Virtual Computing Element on the Virtuali...

SPT2CE-1543 - Allow for remote deletion of Virtual Computing Elements

The Virtualization Environment shall support remote deletion of virtual computing element without impacting other running virtual computing element on the shared physical hardware.




Rationale: To enable remote dynamic configuration of virtual computing elements.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1563 - The Virtualisation Environment shall support the remote deletion of a compartmen...

SPT2CE-1535 - Provide hardware abstraction

The Virtualization Environment shall provide hardware abstraction. Changes in the underlying COTS HW (within the same HW architecture) may not have any impact to the FS running on the virtualisation environment.




Rationale: Virtualization Environment shall support different hardware architectures such as x86, ARM, PowerPC, and others to support seamless integration of FS.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1564 - The Virtualisation Environment shall provide a full HW abstraction, the adaptati...

SPT2CE-1551 - Allow for updates of the Virtualisation Environement

The Virtualization Environment shall support to do updates of the virtualisation environment computing-element-wise "one after the other" without affecting the virtualisation environment on the other virtual computing elements.




Rationale: This is necessary to update the virtualisation environment (e.g. due to IT-sec patches) during runtime of the FS.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1565 - The update of the FS compartment must not impact other running FS compartments o...

SPT2CE-1552 - Maintain backward compatibility at the Configuration Interface

The Virtualization Environment shall provide compatibility at the configuration interface.




Rationale: A new version of the virtualisation environment shall not have any impact on the FS related configuration data

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1566 - Updating the virtualization environment shall have no impact on the FS configura...

SPT2CE-1547 - Provide diagnostic interface

The Virtualization Environment shall provide the diagnostic interface to monitor the virtual computing element.




Rationale: The diagnostic information provided by the interface may be used to monitor the health of virtual computing element and to detect SW crashes and to enable automatic recovery.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1567 - The periodic diagnosis messages provide the health status of the FS compartments...

SPT2CE-1554 - Provide detailed health information of the Physical Computing Elements

The Virtualization Environment shall provide the health monitoring of the physical computing element(s).




Rationale: The health monitoring can be used for the predictive maintenance of the physical computing element and to detect HW faults as soon as possible.

Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1568 - Periodic diagnosis messages provide the health status of the physical computing...

SPT2CE-1548 - Mechanism to ensures correct FS compartment deployment

The Virtual Environment shall provide mechanism to ensures the correct deployment of FS compartments.

Rationale: To ensure the safety requirements such as to run each replica of FS compartment on distinct physical computing element.


Status	 Content to be approved
Linked Work Items	has parent :  SPT2CE-1526 - Virtualization _ is ruled by :  SPT2CE-1599 - Meticulous attention must be given to ensuring that the needed Virtual Computing...

7 Open Points

The following open points have been identified that will be covered in the future work:

- The details of the FSDR have intentionally not been defined at this stage. The FSDR will be defined in the upcoming domain work.

8 Conclusion and Future Work

This document provides a detailed operational analysis by describing the operational context, needs and expectation of the user of the standardised computing environment. The operational analysis is built based on the conceptual architecture proposed in the SP CE domain's previous deliverable  [Recommendation on Interfaces to be standardised](#). The operational analysis mainly focuses on the interfaces that's agreed to be specified by the domain namely, I1-External Diagnostic, Logging, Orchestration and IT Security Interface(s), I2-Hardware abstraction interface and I3-Virtualisation interface.

The operational analysis first enriched the layered CE architecture to understand the components' behaviour, functions, and interactions, which helped to develop the operational scenarios. Four categories of operational

scenarios are described, namely integration, deployment, update, and recovery, to enable the operation of the FS from different suppliers onto a standardised computing element. Furthermore, the operational requirements are derived from the operational scenarios that captures the intended platform usage, its functions, performance and constraint in the operational context.

Following the operational analysis, the next critical step is the system analysis. This phase, detailed in the next deliverable, is pivotal in defining the system definition, functions, and system capabilities. It will also outline the system definition and system requirements, paving the way for the logical and physical architecture of the standardized computing environment.

9 Appendix

9.1 Referenced documents

Reference No.	Dated (release date)	Title	link (informative)
1	September2023	Recommendation on Interfaces to be standardised	SharePoint Link
2			
3			
4			