I3-Virtualisation Interface Specification

Abstract	This document is System Interface Specification of I3-virtualisation interface
Config Item	System Interface Description
Document ID	30 Deliverables/I3 Interface Specification#907312 I3 Interface Specification
Classification	Public
Status	Open
Version	1.0
Revision	907312
Last Change Date	2026-06-05

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

INFO: History table is not displayed, because this document is in status **doc_open**.

RULE: History table is not displayed, in statuses: { draft doc_open doc_inprogress doc_contentApproval doc_contentDecision }

CONTACT: For more information contact Administrator

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

Type of Approval	Document Review
Comments	
Approvals	
Attachments	

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

Type of Approval	Document Approval
Comments	
Approvals	
Attachments	

Table of contents

1 Preamble

1.1 Purpose

SPT2CE-3335 - Purpose

This document describes the **I3 virtualisation interface**, which provides a standardised interface between the Computing Platform (CP) and the Functional System (FS) and enables the Functional System to be independent of a specific implementation of the computing platform hardware.

The I3-interface specification is derived from the System Concept including operational analysis , System Analysis and System Architecture .

1.2 Intended Audience

SPT2CE-3513 - Intended Audience

This document is intended for the key players shaping the future of rail, specifically **Infrastructure Managers**, **Railway Undertakings**, **CCS Suppliers**, and **Sector Organisations**. It should be noted, however, that **this list is not limited to the mentioned audience**; the content serves as a valuable resource for any professional, regulator, or partner working within the broader rail and transport ecosystem.

1.2.1 Document Context

SPT2CE-3519 - Document Context

This document defines the technical specifications CPSW designed to be used in the datacenters to host safe and non-safe applications

Scope: This document is part of the CONEMP specification (comprising System Architecture, I2, I3 and Glossary)

1.3 Glossary

Term (Abbreviation) **Description**	**Referenced**
building block configuration identification (bbcid) building block configuration identification as defined in the CONEMP System Pillar	here...
building block identification (bbid) building block identification as defined in the CONEMP System Pillar	here...
Commercial-of-the Shelf (COTS) Components available for public purchase without modification, listed in manufacturer's standard catalog (Hardware/Software)	here...
Compartment (Comp) A Compartment is a consistent, integrated entity which is part of a FS. It can be deployed on either a Physical or a Virtual Computing Element.	here...
Computing Environment (CEnv) A computing environment encompasses the hardware, software, network resources, and services that enable the deployment, operation, and management of applications or services. Computing environment includes the application execution environment and the computing platform.	here...
Computing Platform (CP) The Computing Platform provides and manages computing resources and communication resources for functional systems (specialised IO are not included). It contains CP hardware (physical computing element(s) and communication hardware) and CP software (virtualisation environment and platform management). Note: The CP shows an abstract view and may contains several Physical Computing Elements (PCE)s.	here...
Computing Platform Hardware (CPHW) Physical Computing Elements and network hardware.	here...
Computing Platform Software (CPSW) Provides platform-level services (e.g., resource allocation, compartment execution environment, and platform management).	here...

Term (Abbreviation) **Description**	**Referenced**
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...
Native Hardware Access (NHA) Specific software component(s) providing the additional functions needed by the Functional Systems (especially the Safety Layer) that are not available in COTS solutions.	here...
Physical Computing Element (PCE) The Physical Computing Element refers to the physical device providing compute resources.	here...
Service Function Configuration (SFC) The Service Function Configuration (SFC) is the implementation of the Configuration Management System. The SFC is a central location technical system that is responsible for managing the BuildingBlock Configurations. Each BuildingBlock deployment is managed by exactly one SFC.	here...
Service Function Diagnostic (SFD) A standardized OPC UA-based interface framework for the integration of diagnostic, condition monitoring, and asset-related data across different subsystems and suppliers.	here...
Virtual Computing Element (VCE) The Virtual Computing Element refers to virtually provided compute resources with computing resource guarantees.	here...

Term (Abbreviation) **Description**	**Referenced**
Virtualisation Interface (I3) The Virtualisation Interface I3 (Interface 3) is used to provide a standardised interface above the virtualisation layer so that applications or higher platform layers are independent of a specific implementation of the computing hardware.	here...

2 Interface I3 overview

SPT2CE-3279 - I3-Virtualisation Interface

The I3 virtualisation interface is between the compartments of the Functional System (FS Comp) and the Computing Platform, as shown in Figure 1. The I3 interface provides virtual computing resources from the subsystem Computing Platform to the Functional System. The Functional System Compartments are hosted in VCEs. The interface has five parts:

- the hardware abstraction (I3-VCE) ,
- the data exchange needed between FS and CP to implement a safety layer as part of a Functional System (FS) (I3-NHA),
- the communication interfaces (I3-Communication),
- the diagnostic interface (I3-Diagnostic),
- the security interface (I3-Security).

I3 Hardware abstraction can be Commercial-of-the-Shelf (COTS) and could be realised through Hypervisor technology.

SPT2CE-3333 - Virtualisation interface overview diagram

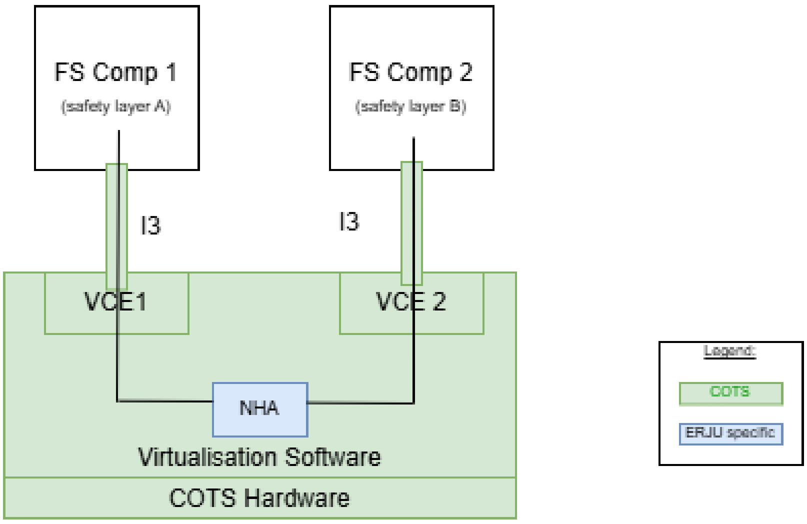

Figure 1 I3- Virtualisation interface overview diagram

3 Interface Functional Description

SPT2CE-3337 - Interface I3

This chapter describes the functions required by the FS to run on the Computing Platform.

3.1 Hardware Abstraction- Virtualised Computing Resources (I3-VCE)

SPT2CE-3336 - Interface I3-VCE

I3-VCE interface provides the virtualised computing resources to the FS based on the Functional System Deployment Rules (FSDR).

SPT2CE-3284 - VCE Resource service

The CP ensures the correct mapping of runtime resources for each compartment according to the FS compartment related deployment rules provided by the FS.

Interface I3-VCE provides the access of FS to the allocated resources of a compartment.

The resources include:

- CPUs
- Memory
- IOMMU

All interfaces to these functions can be realised through COTS components.

SPT2CE-3332 - VCE Virtualisation

VCEs are to be virtualised using hardware assisted virtualisation relying on virtualisation extensions provided by I2 (such as VT or AMD-V, see SPT2CE-2629 - CPU aided virtualization).

3.1.1 I3 Virtualised I/O resources

SPT2CE-3338 - Virtualised I/O

Interface I3 provides I/O channels e.g. for the exchange of hardware information, but also for persistence or external communications, etc. While these resources are provided through the virtualisation software into the VCE, in order to use them, the compartment must use specific dev ice drivers.

SPT2CE-3310 - I3 I/O resource mapping

Interface I3 provides virtualised I/O resources to the FS based on the FSDR as part of I3-VCE.

The resources include:

- virtual disk
- virtual network interfaces
- virtual I/O devices (e.g. Watchdog, RTC, Timers, TPM)
- virtual boot environment including secure boot

SPT2CE-3311 - I3 I/O resource device drivers

Interface I3-VCE uses devices complying to the OASIS VIRTIO standard allowing for them to be used with virtio drivers by the FS compartment.

SPT2CE-3339 - I3 virtual sockets

Interface I3-VCE offer virtual sockets for communication between the host-system of the virtualisation environment and its hosted compartments (e.g. Linux socket address family AF_VSOCK).

3.2 Hardware Information (I3-NHA)

SPT2CE-3334 - I3-NHA

I3-NHA provides a transport-channel to be able to transfer HW related information from the CP SW into the FS. This information is important to implement the safety function.

There are multiple options to implement interface I3-NHA and they are related to the available technologies, for example:

- virtual sockets
- direct memory transfer
- standard IP protocol

The hardware information required to implement the safety layer is specific to each Functional System supplier. The table below summarizes commonly used hardware data elements gathered from multiple FS suppliers:

SPT2CE-3281 - Native Hardware Access data

The following information is provided to the FS from the native hardware components to operate:

Information element	Generated by	Consumed by
Hardware IDs	Generated from computing platform hardware (possibly through TPM)	Functional system safety layer to ensure that the compartments are deployed on distinct physical computing elements, in accordance with the Functional Systems deployment rule.
System Clock	Generated by the computing platform hardware	Functional system safety layer to implement safe time
Temperature (Optional)	Generated by the computing platform hardware sensor	Functional system safety layer to ensure operational environmental conditions
Voltage (Optional)	Generated by the computing platform hardware sensor	Functional system safety layer to ensure the operational environment conditions

Note: Native Hardware Access data is presented as possible available data from CP HW. FS safety concept will define which data is necessary from CP in order to satisfy its safety case. In the end, NHA data is a compatibility feature between the FS safety concept and the CP HW (to be further evaluated when the domains safety requirements and application conditions are defined).

3.3 Network Segmentation (I3-Communication)

SPT2CE-3295 - Communication Network

Each FS compartment runs in an own VCE and communicates to other communication partners with the following communication types:

Communication Type	Description
FS Private	FS internal communication between the individual FS compartments of the same FS
Operational	Operational Communication between FS (e.g. SCI) - within same control area (as e.g. communication between interlocking and object controller) - between different control areas (as e.g. communication between two interlockings) - between trackside system and onboard system
Configuration	Communication to Service Function Configuration (SFC)
Diagnostic	Communication to Service Function Diagnostic (SFD)
Cybersecurity	Communication to Shared Cybersecurity Services

An individual FS compartment does not know details about the physical location of the communication partners and the network in between.
The following physical locations of communication partners are possible:

- in a neighbour-VCE running on the same PCE
- on another PCE in the same server rack
- in another rack in the same data centre
- in another data centre
- in the field or on-board.

Each FS compartment provides its own deployment rules which consider the details regarding the communication channels for the communication to other communication partners.
Per communication channel this includes the following details:

- the logical communication partner and belonging communication type
- the required network bandwidth and max. latency
- QoS requirements
- redundancy relationships between communication channels

The CP configuration (configuration of VLANs according to the FS deployment rules and the network architecture of the CP) must be defined for each CP individually, considering the security architecture of the CP as needed.

I3-Comm interface provides virtual network interfaces to the FS compartment.
The mapping of virtual network interfaces to physical network interface cards, VLANs and/or virtual switches is done by the computing platform and not visible within the FS compartment. Depending on the FSDR and security requirements different implementation mechanisms could be adapted such as priority based or separate virtual network interface for each type of communication.

3.4 I3 Diagnostic data (I3-Diagnostic)

.

.

:.

3.4.1 FS-Comp Health Status Monitoring

SPT2CE-3316 - FS-Comp Operational Health Status
FS-Comp provides an operational health status towards the CP. One possible implementation of the FS-Comp health status monitoring by CP is via a (virtual) watchdog in the VCE. This functionality is mandatory in order to implement the recovery scenarios defined in CP System Architecture.
As each FS-Comp has a specific implementation of health status monitoring, VCE requires to provide a (virtual) watchdog function with configurable parameters. The parameters of FS-Comp health status for VCE (virtual) watchdog implementation are defined in the FS Deployment Rules

(FSDR).

SPT2CE-3329 - Virtual Watchdog

To provide a (virtual) watchdog usually a standard COTS virtual watchdog device is used. For a more high level health monitoring, standard TCP/IP (or even HTTP/IP) is used between a service in the FS-Comp and a monitoring application in the CP (which then can also execute more complex rules depending on the health state).

4 Non-functional characteristics

4.1 Security

SPT2CE-3320 - Security Overview

Security includes the following topics:

Related to I3-VCE

- Secure boot and root of trust
- Secure keys storage (e.g. vTPM and/or TPM pass through)
- Secure storing of data (e.g. data in use in memory, data at rest in disk images)

Related to I3-Comm

- Secure separation of virtual networks for different communication type
- Support of different security architectures

SPT2CE-3322 - Security for I3-VCE

The mechanisms used are COTS.

SPT2CE-3321 - Security for I3-Comm

The Computing Platform supports security architectures which for example use a security gateway compartment that is independent from the FS compartments executing the railway function. To achieve this, a secure separation of networks is necessary, so that only the assigned compartments can communicate on each (virtual) network.

The mechanisms used are COTS.

4.2 Safety

SPT2CE-3340 - Safety for I3

The safety of the system is realised in the safety layer inside of the Functional Systems.
As the interface I3-NHA provides hardware related information to the safety layer, it has to be considered in the safety case of the Functional System.
All other interfaces are COTS and have no relevance for safety.

4.3 Performance

SPT2CE-3341 - Performance for I3

The needed performance is determined by the Functional System and specified in the FSDR.
The Computing Platform has to provide the requested performance as defined in FSDR (e.g. CP must be able to wake up processes within 40ms in 99,99999% of runtime).

SPT2CE-3486 - Core Pinning

The virtualisation software shall support core pinning in order to increase determinism in VCE execution time to ensure availability.

4.4 Diagnostics

SPT2CE-3487 - Hardware diagnostics support

The virtualisation software shall support reading diagnostics data from dedicated diagnostics interfaces provided by the CP hardware, such as an Intelligent Platform Management Interface (IPMI).

5 Reference

SPT2CE-3405 - References

No	Title	Status
1	System Architecture	In Review System Architecture

No	Title	Status
2	I2 - Hardware Abstraction Interface Specification	In Review I2-Hardware Abstraction Interface Specification
3	System Analysis	Released https://rail-research.europa.eu/v1-release/