

# General Concept ETCS Interlocking Datacenter

## Document information

### Document Properties

Status:  **Published**

Version: 1

Owner: Kuster Michael (I-SR40-PMO-EXT)

Contributors: Grabowski David (I-AT-SAZ-SIH), Kuster Michael (I-SR40-PMO-EXT)

### Document history

Version (revision)	Changes	Document Owner	Approved	Signed
1		Kuster Michael (I-SR40-PMO-EXT)	Grabowski David (I-AT-SAZ-SIH)	



# 1 Content

Document history .....	1
1 Content .....	2
2 Glossary .....	3
3 Scope of the Document .....	3
4 Premises .....	4
4.1 Summary .....	4
4.2 EI Datacenter overview .....	4
4.3 Safe Datacenter Application Platform .....	5
4.4 Facility .....	6
4.5 Safety considerations .....	7
4.6 IT Security considerations .....	8
5 Requirements .....	8
5.1 List of system requirements (functional, non functional) .....	8
5.2 Standard derived requirements .....	10
5.2.1 Requirements derived from CENELEC Standards .....	11
5.2.2 Requirements derived from IEC61508 .....	13
6 System design concepts proposals .....	16
6.1 Safe Datacenter Application Platform .....	16
6.1.1 Approach 1 - Pre-certified safety .....	16
6.1.2 Approach 2 - Hardware-centered safety mechanisms .....	17
6.1.3 Approach 3 - Mixed safety mechanisms .....	18
6.1.4 Approach 4 - Software-centered safety mechanisms .....	19
6.2 Geo Redundancy / Regionalization .....	19

## 2 Glossary

Term	Abbrev.	Description
<b>Application Programming Interface</b>	API	A set of functions and procedures that allow the creation of applications which access the features or data of an operating system, application, or other service.
<b>Availability</b>		Ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval SOURCE: IEC 60050-821: CDV2015, 821-05-82, modified
<b>Commercial off-the-shelf</b>	COTS	Commercial items, including services, available in the commercial marketplace that can be bought and used, without the need to commission custom-made, or bespoke, solutions.
<b>Electronic interlocking</b>		Interlocking system realized by means of software logic running on special-purpose control hardware.
<b>European Train Control System</b>	ETCS	The <b>European Train Control System (ETCS)</b> is the <a href="#">signalling</a> and control component of the <a href="#">European Rail Traffic Management System (ERTMS)</a> . It is a replacement for legacy <a href="#">train protection systems</a> and designed to replace the many incompatible safety systems currently used by European railways. The standard was also adopted outside Europe and is an option for worldwide application.
<b>Infrastructure Manager</b>	IM	An authority responsible in particular for establishing, managing and maintaining railway infrastructure, including traffic management and control-command and signalling. (Oftentimes the owner of the railway infrastructure as well).
<b>Legacy Interlocking</b>	LI	Legacy interlocking system (e.g. relay and electronic interlocking) that shall be replaced by the ETCS Interlocking (EI).
<b>smartrail 4.0</b>	SR40	A program with disruptive innovations for the processes and systems of the railway production.

## 3 Scope of the Document

This document is a refinement to the  [SRP-2658 - Kerndokumente des Gesamtkonzeptes SR40](#) and describes the  [WI-3679 - ETCS Interlocking Datacenter](#) in a general way. Basic requirements, functionalities and concepts to fulfill these requirements are presented. This document shall furthermore define the projects premises, scope and boundaries.

The functionality of the "functional software applications" that will be hosted in the datacenter are not discussed here, but the applications common requirements yielding the datacenter obviously have to be considered here.

The document does not cover migration concepts nor financial aspects.

## 4 Premises

### 4.1 Summary

The [SRP-2738 - System Architecture Description](#) decomposes the functional logic of the [WI-2077 - smartrail 4.0](#) program into several applications, with some of them considered as safety critical.

The aim of the [WI-3679 - ETCS Interlocking Datacenter](#) project is to lay the fundament for the design of a reliable, safe and secure host for those safety critical applications.

Safety critical in this context means, that a [WI-1831 - Safety Integrity Level](#) (SIL) higher than zero, according to the CENELEC EN50128 standard, has been assigned to the application. Those fault-tolerant applications will, with minor exceptions (such as the [WI-1990 - Object Controller](#) firmware / software), all be deployed to a platform in the [WI-3679 - ETCS Interlocking Datacenter](#). That platform is referred as [SRP-4951 - Safe Data Center Application Platform](#) in [SRP-2738 - System Architecture Description](#) and relating documents.

To cope with the high demanding [WI-1018 - Availability](#) requirements more than just one datacenter at georedundant locations will likely be required. The rail network could be split into multiple regions represented by [WI-3265 - Topology](#) sections. Functionally and hardware independent instances of the [SRP-4951 - Safe Data Center Application Platform](#) would then control each section in order to minimize operational impact in case of a system failure of one instance.

### 4.2 EI Datacenter overview

The following figure shows a high level schematic representation of all elements forming the [WI-3679 - ETCS Interlocking Datacenter](#), to illustrate the scope of the project.

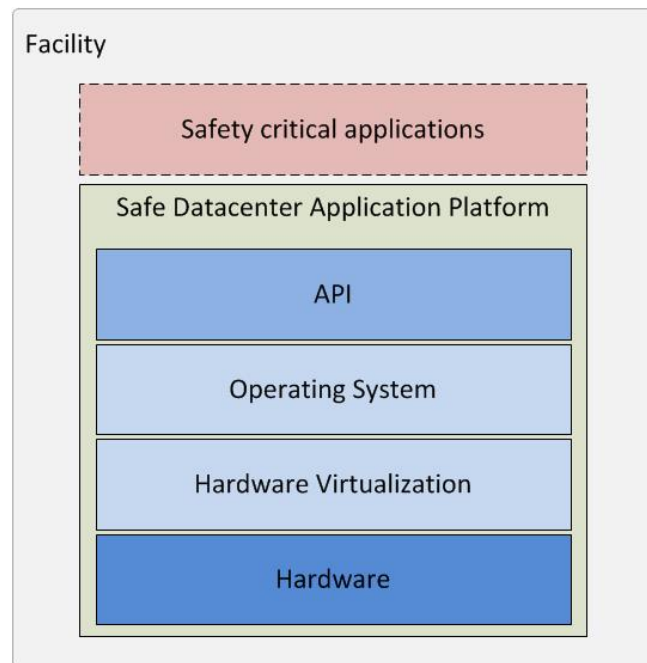


Figure 1 EI Datacenter Scope

The EI Datacenter consists of the following elements that will be explained more detailed in subsequent sections of this document:

- **Facility:** Building infrastructure that provides an optimal environment to the IT and telecom equipment by minimizing negative external influences such as power outages or temperature changes. Among others the

following factors have to be considered when designing the facility:

- **Power supply:** Engine generator supply, local utility power connection, UPS modules
- **Environmental control:** Cooling devices and fire suppression measures
- **Physical security:** Access control, Intrusion protection
- **Site Location / Architecture:** Building Characteristics, Compartmentalization, Cabeling
- **SRP-4951 - Safe Data Center Application Platform:** Runtime environment for the applications that provide the functional logic (business logic). The platform itself can be divided into the listed elements:
  - **Computing Hardware:** Hardware (including firmware) for data processing and storage, plus network infrastructure including IT security measure
  - **Hardware Virtualization:** WI-2088 - Hardware Abstraction Layer to abstract hardware from the rest of the platform.
  - **Operating system:** Operating systems(s)
  - **Middleware with generic WI-2989 - Application Programming Interface :** Abstraction layer to insulate the applications from the operating system, the virtualization layer and finally from the hardware. Provides the mechanisms to run the safety critical, functional applications in a fault-tolerant manner
- **Safety critical applications:** Applications providing the functional logic for different tasks in the SR40 landscape. The applications code shall only contain the pure functional logic. Mechanism to achive the high demanding SIL requirements regarding fault tolerance and availability are delegated to the platform, as stipulated by SRP-12686 - Portable to different Platforms. The safety critical functional software applications are not part of the EI Datacenter project.

### 4.3 Safe Datacenter Application Platform

The SRP-4951 - Safe Data Center Application Platform shall be designed as generic and scalable as possible. This shall ensure that safety critical applications that are not yet foreseeable can be implemented in future without altering the platform. It is even desired that the platform is designed in such way that applications in other fields than railway signaling become possible. Opening the platform to other markets might help to reduce LCC of the platform or it's components

The design must further allow different software and hardware life cycles thru rigorous insulation of hardware and application by means of hardware virtualization and a generic middleware and a defined WI-2989 - Application Programming Interface . This shall facilitate the individual exchange of components (software and hardware) and prevent from vendor lock in. Especially the life cycle of the applications containing the functional logic and the platform itself shall be decoupled.

Whenever possible and reasonably, [WI-2654 - Commercial off-the-shelf](#) parts shall be used to minimize lifecycle costs. This is true for hardware, as well as for software components such as operating systems. Different possible routes to achieve a safety certification for unsafe COTS hardware will be presented later in this document.

Beside the technical implementation, this requirement also presumes a certification strategy that supports that modularity. This means that the exchange of components (hardware / software) shall be possible without a complete recertification of the platform, or even worse the entire system including the functional applications.

It might turn out to be reasonable to have different implementations of the platform, since a single design will likely not be sufficiently scalable to meet the divergent needs of different [WI-2289 - Infrastructure Managers](#). Also during different life cycles of the [WI-2077 - smartrail 4.0](#) system (pilote phase, rollout, network wide implementation) platforms of vastly different scales seem likely.

As already introduced, the platform shall provide the runtime environment to the applications. It shall furthermore provide all mechanisms for a fault-tolerant operation, for application management and for persistence. An application model based on "state machine replication" is proposed in [SRP-12684 - Fault-Tolerant Portable SW-Application Architecture](#). A defined [WI-2989 - Application Programming Interface](#) between the functional applications and the platform itself ensures the portability of the applications to different platform implementations.

#### 4.4 Facility

The design of the facility has a great impact on the [WI-1018 - Availability](#) and reliability of the datacenter. The two key aspects are power supply and cooling capabilities. Even the most sophisticated platform will not be able to achieve its targeted availability, when power supply is running short, or the system overheats, due to a damaged cooling unit. There are two widely used standards for planning and designing datacenters with main focus on infrastructural aspects: The Uptime Institute's Tier Classification mainly focuses on power supply and cooling since these are the primary and most important factors of a datacenter.

The Telecommunications Industry Association's TIA-942 standard trace its origins also to the Uptime Institute's four tiered approach, which dates back to the 1990's. TIA no longer uses the term Tier in the recent version of TIA-942-B standard to avoid confusion with the Uptime Institute's classification system. The TIA standard is more comprehensive and also gives guidelines for environmental control (fire suppression), physical security, cabling, site location and more.

With the EN50600 series of standards, initially published only in 2015, there is now also a guideline available that is formally valid overall Europe.

It covers all the relevant parts and areas of a datacenter— from the building itself to the power supply and air conditioning, all the way to fire protection, and from the IT wiring itself to access controls.

Part two of the series defines four availability classes that are mostly congruent to the classes / ratings in the two other cited standards.

To scope with the availability requirements for the interlocking datacenter that will control the majority of the Swiss rail traffic a design with no single point of fault must be chosen. In all mentioned standards only the highest class Tier IV / Rate 4 fulfills that requirement.

A Rated-4 / Tier-4 datacenter has redundant capacity components and multiple independent distribution paths serving the computer equipment. Typically, only one distribution path serves the computer equipment at any time. The site is concurrently maintainable which means that each and every capacity component including elements which are part of the distribution path, can be removed/replaced/serviced on a planned basis without disrupting the capabilities of the safety critical applications. The datacenter allows concurrent maintainability plus one fault anywhere in the installation without causing downtime. It has protection against almost all physical events.

Alternatively an intelligently designed network of a multitude of Rated-3 / Tier-3 datacenter will also allow an overall

design with no single point of failure and allow concurrent maintenance.

It shall be noted that those high demands to the facility might not be necessary for a datacenter of a [WI-2289 - Infrastructure Manager](#) manager with limited regional network. The availability targets scale with the size and the importance of the controlled network. Same also applies for the pilote (field test) phase of the SR40 system where a breakdown or interruption in the execution of the centralized interlocking applications might be tolerable.

#### 4.5 Safety considerations

The following figure shows an extract of the [SRP-4680 - Deployment View](#), part of the [SRP-2738 - System Architecture Description](#). The applications inside the red frame are intended to be deployed to the [SRP-4951 - Safe Data Center Application Platform](#).

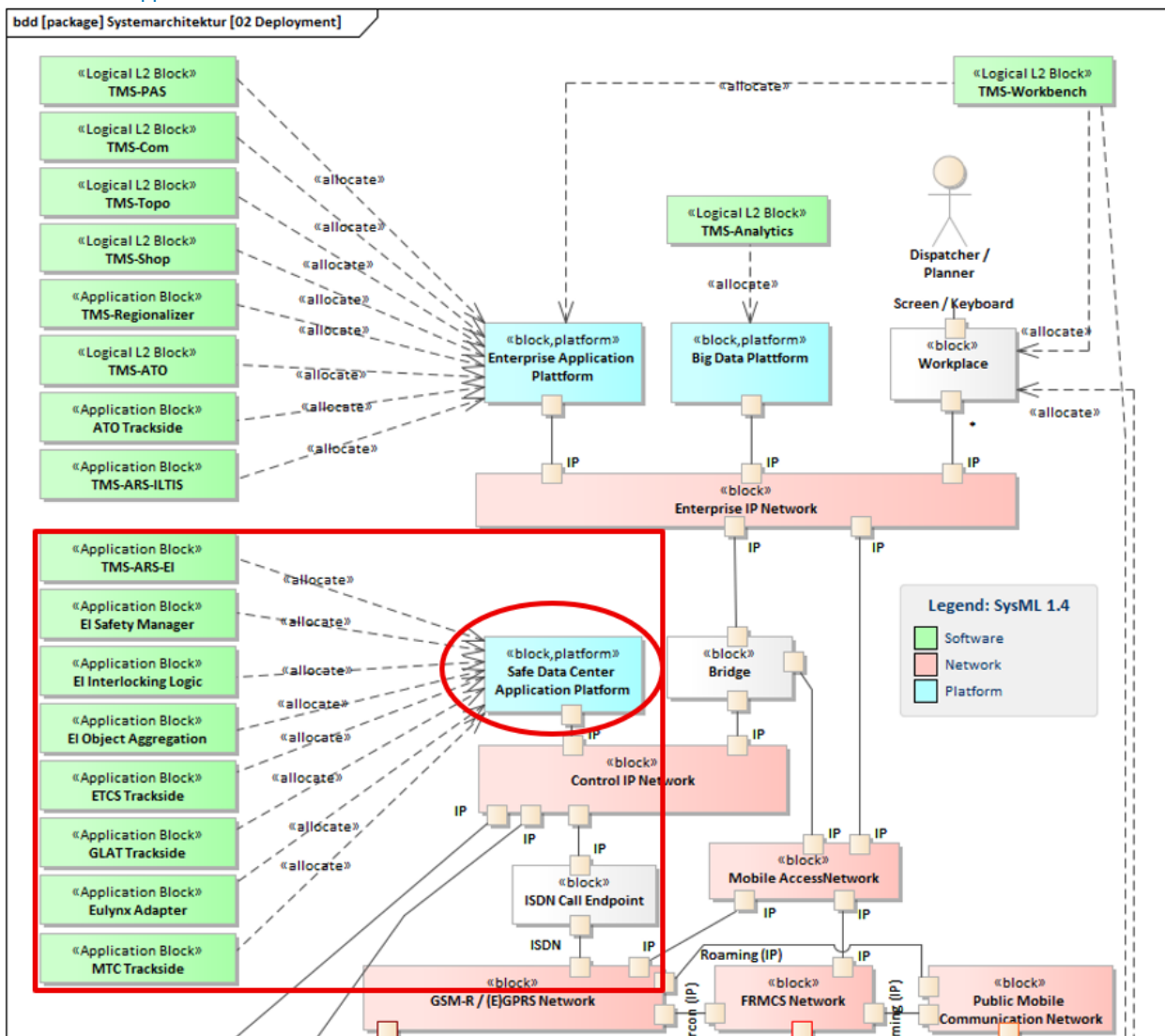


Figure 2 Deployment View

The [SRP-4951 - Safe Data Center Application Platform](#) will need to be certified to at least the same [WI-1831 - Safety Integrity Level](#) as the functional software application with the highest SIL deployed to it. Moreover mixed criticality shall be supported by the platform. This means that most likely applications with different SIL, or even no SIL demand will run on the same platform, which requires mechanisms to properly isolate those.

The necessary [WI-1832 - Safety Integrity](#) depends on the maximum damage that may be caused by failure of the system. SIL4 is the maximum integrity level defined by the relevant CENELEC standards. That demanding requirement is already mandatory for a nowadays, state of the art, regionally limited [WI-2578 - Electronic interlocking](#). Thus a SIL4

will be inevitable for the interlocking software application developed in the frame of SR40, and hence also for the platform hosting it. Still must the overall system be structured such that the SIL4 capability is sufficient for its task, with the task being much different from the regionally limited tasks currently applicable for classical distributed [WI-2523 - Legacy Interlocking](#) systems. The worst-case damage scenario caused by a system controlling all the rail traffic in Switzerland would include a large number of trains, and a much higher number of [WI-1029 - Fatalities](#) than known with current systems.

#### 4.6 IT Security considerations

The digital transformation and centralization of the interlocking systems is bringing substantial benefits in safety, operational efficiency and reliability. Yet, it also inevitably increases the vulnerability of the signaling infrastructure to cyber-threats. There is no doubt that the EI Datacenter, the host to signaling applications controlling the majority of the Swiss railway network will form major attack surface for cyber criminals.

The SR40 interlocking logic is purely based on software algorithms. If the system is compromised by an unwanted external or malware, the safety cannot be guaranteed anymore. Thus security gains a much more important level of attention.

Adequate measures to protect not only the datacenter, but also the communication network must be incorporated in the design. Obviously those measures must not compromise the availability and reliability targets by e.g. decreasing latency. An end-to-end protection of the entire signaling system is essential, thus the security measures taken for the datacenter must be seamlessly embedded in the SR40 security concept proposed in [SRP-10014 - Security study and preliminary concept](#).

## 5 Requirements

The following is a not exhaustive list of requirements for the [WI-3679 - ETCS Interlocking Datacenter](#) that mainly relate to the [SRP-4951 - Safe Data Center Application Platform](#) serving as working assumptions until the final binding requirements have been derived from the overarching system architecture and the business objectives.

The requirements were either identified in the frame of the study "On Design, Introduction and Operation Of Safety-critical Applications in the Railway System of Schweizerische Bundesbahnen SBB" conducted by ESG Elektroniksystem und Logistik GmbH or extracted from overarching SR40 documents:

### 5.1 List of system requirements (functional, non functional)

HW Upgrade shall be possible without changing Application Software. [DC-203 ]

Data center shall be based on COTS Hardware. [DC-204 ]

Update of Operating System shall be possible without affecting the configuration status of application software. [DC-212 ]

Exchange of the Operating System shall be possible without affecting the configuration status of application software [DC-213 ]

The Data Centre may be based on standardized HW modules for both, processing and storage. [DC-208 ]

The data center shall have a "very high" availability analogue to RAM Targets for ETCS Level 2. The detailed RAM Targets will be determined as part of the RAM Project of smartrail 4.0. [DC-210 ]

The data center shall be able to recover within x(sec) from significant damage to its infrastructure (disaster recovery) [DC-209 ]

The data center shall implement a strict monitoring of its configuration status, any change shall be recognized and



reported. [DC-215 ]

The data center shall communicate with de-central object controllers [DC-214 ]

Data center management function (System Management) shall be separated from payload function. [DC-216 ]

Data center hardware and software shall be independent with regard to integration. [DC-217 ]

Data center hardware and software shall be independent with regard to certification. [DC-218 ]

Dependency on a single source for hardware components or a specific technology should be avoided. [DC-219 ]

The data center shall be built on COTS Hardware components (including SIL4 COTS Hardware if necessary). [DC-226 ]

The data center shall be built on COTS operating system components. [DC-221 ]

The data center shall host applications qualified as SIL4. [DC-220 ]

Applications of a lower SIL levels shall not affect the execution of an application of a higher SIL level. [DC-223 ]

It shall be possible to replace HW and SW components separately from each other. [DC-222 ]

HW components shall be qualified independently of application and operating system software. Application conditions may be used. [DC-229 ]

Operating system components shall be qualified independently of HW and application software components. Application conditions may be used. [DC-225 ]

Application software components shall be qualified independently of operating system and HW components. Application conditions may be used. [DC-224 ]

Mechanism to achieve fault-tolerance shall be separated from business logic/domain logic. [DC-228 ]

The data center shall be scalable with respect to its components, both resources and functions. [DC-227 ]

Data integrity shall be protected against unauthorized manipulation. [DC-233 ]

Data center shall protect availability of data. [DC-232 ]

Total end-to-end processing time for "inner loop" functions in the data center shall be  $O(100 \text{ ms})$ . [DC-235 ]

$O(1000)$  Messages per second is the expected throughput. [DC-234 ]

Total latency of the data center, which is defined as the time between an incoming message until the responding outgoing message leaves the data center, shall be  $O(100 \text{ ms})$ . [DC-231 ]

Total processing time budget for the outer control loop, which is defined by complete set of trains that are under control of the data center, is  $O(1 \text{ seconds})$ . [DC-230 ]

The system shall be regionally distributed for availability and for damage limitation [DC-271 ]

The system shall consist of server, storage, controller and maintenance subsystems [DC-274 ]

The controllers shall provide hypervisor functions to dynamically invoke servers and storages [DC-269 ]

The controllers shall support virtualization functions to dislocate execution of functions [DC-268 ]

The controllers shall manage redundancies and stand-by operations of servers and storages [DC-264 ]

The controllers shall vote hypervised server or storage outputs with  $HFT > 2$  [DC-263 ]

The controllers shall supervise unused software, firmware or configuration data within COTS devices [DC-267 ]

The controllers shall provide black-channel communication services [DC-266 ]

The servers shall provide encapsulation of application functions and OS [DC-272 ]


The servers shall provide virtualization of resources for execution of application functions and OS [DC-270 ]

To further reduce LCC, the system shall make use of hardware components with a low probability of failure per hour (PFH). [DC-340 ]


To minimize channel (item) PFH targets (to approx. E-4/h in the first approach), and to consequently reduce LCC, the system should have a HFT (hardware fault tolerance) of 2 or higher. [DC-338 ]

With respect to safety the required system availability is determined by the most demanding safety function. Near real-time control functions may need higher availability than functions with longer repetition time intervals. As a reference for the „real-time“ class of functions, ETCS specification according to SBB sets a maximum of 0.0014/a inactivity of more than 1min, but relates to a single train only. [DC-334 ]

## 5.2 Standard derived requirements

These requirements have been derived from the relevant CENELEC railway standards. Where CENELEC lacks of detailed information, such as on the use of  [WI-2654 - Commercial off-the-shelf](#) , the IEC61508, cross industry functional safety standard has been considered:

Name	Standard Number	Applicable to
RAILWAY APPLICATIONS - THE SPECIFICATION AND DEMONSTRATION OF RELIABILITY, AVAILABILITY, MAINTAINABILITY AND SAFETY (RAMS)	CENELEC SN EN50126	RAILWAY SYSTEM
RAILWAY APPLICATIONS - COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS SOFTWARE FOR RAILWAY CONTROL AND PROTECTION SYSTEMS	CENELEC SN EN50128	SOFTWARE
RAILWAY APPLICATIONS - COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS - SAFETY-RELATED ELECTRONIC SYSTEMS FOR SIGNALLING	CENELEC SN EN50129	SIGNALLING SYSTEMS
RAILWAY APPLICATIONS - COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS - SAFETY-RELATED COMMUNICATION IN TRANSMISSION SYSTEMS	CENELEC SN EN50159	TRANSMISSION SYSTEMS
FUNCTIONAL SAFETY OF ELECTRICAL / ELECTRONIC / PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS	IEC61508	SAFETY SYSTEMS

The applicable version of the above standards is referenced in  [SRP-1716 - Zusammenhang der Normen und anzuwendende Versionen](#) .

The following figure illustrates the interrelation of the different standards and the field of application of said:

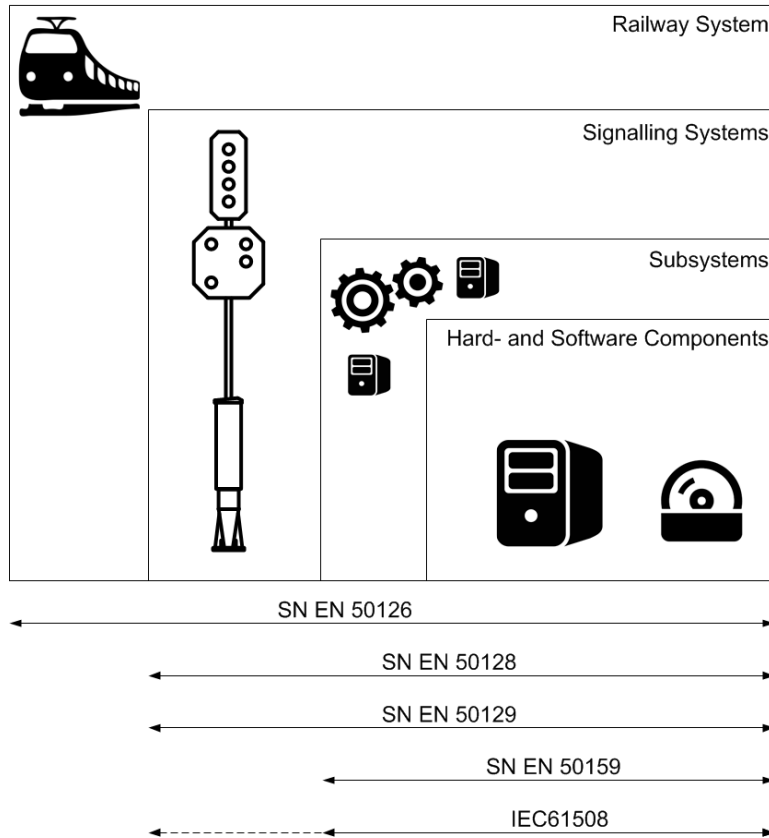


Figure 3 Standards Field of Application

**5.2.1 Requirements derived from CENELEC Standards**

For SIL4 capability, the total system must have the capability of a tolerable functional unsafe failure rate  $TFFR < E-8$  and safety-related system functions must meet their individual  $TFFR < E-8$  for random faults

Tolerierbare Gefährdungsrate THR pro Stunde und pro Funktion	Sicherheitsanforderungsstufe
$10^{-8} \leq THR < 10^{-9}$	4
$10^{-7} \leq THR < 10^{-8}$	3
$10^{-6} \leq THR < 10^{-7}$	2
$10^{-5} \leq THR < 10^{-6}$	1

[DC-307 ]

The system shall provide safe, secure and available communication means and methods, to exchange information within applications, in-between applications, and with system-external instances. [DC-308 ]

The system shall provide independency of safety-related and non-safety-related functions. Functions not safety-related shall have no influence on safety-related functions. This requirement may be satisfied by separated hardware or by dedicated SIL4 separation software, e.g. respective software encapsulation layers [DC-304 ]

The system shall be operator and maintainer friendly. The system needs protection against operating or maintenance errors. The system shall need limited human intervention. [DC-303 ]

Complete pre-existing systems may be used that perform one or more safety-related functions, and were developed according to other safety standards. It is expected that potential deficiencies are mostly formal and identifying and managing possible gaps is deemed feasible. [DC-306 ]

Pre-existing equipment may be used that performs only part of a safety-related function, and missing properties are supported by the remaining part of the function. [DC-305 ]

Use of COTS may be accepted if there are no valid alternatives or development would be too expensive or solutions are ineffective to defend against systematic faults due to the limited railway market or solutions are impossible to get due to highly advanced technology required. [DC-311 ]

Supervised COTS components require available information on functionality, interfaces, hardware and/or software constraints, failure rate, environmental conditions, conditions of use. [DC-309 ]

Supervised COTS components must be identified, included in the overall system definition and put under configuration control. [DC-315 ]

Supervised COTS components require interface hazard analysis or FMEA to identify hazardous failure modes on the boundary of the equipment, and SIL classification. [DC-314 ]

For each supervised COTS equipment's boundary failure mode, it must be demonstrated that it cannot occur due to the internal architecture or data structure or the part must be re-qualified according to the required SIL or there must be external supervising instances negating the failure and establishing a safe state within the safety target. [DC-317 ]

For supervised COTS equipment's boundary failure modes not traceable to the root cause, the full failure rate of the equipment shall be assigned unless it is possible to identify and exclude parts not able to contribute to the hazard. This failure rate shall be demonstrated to be compatible with the TFFR required for the complete function. [DC-316 ]

Supervised COTS equipment must be included in all system design, verification and validation activities as a black box. Functional and non-functional requirements must be assigned, and fulfillment verified and validated). [DC-313 ]

For supervised COTS equipment, a strategy shall be defined to manage the possible effects of product changes (e.g. disable automatic software updates) [DC-312 ]

Embedded COTS software developed according to EN50128 is to be preferred wherever possible [DC-323 ]

Embedded COTS software requires traceability to be established after implementation, but prior to verification/validation. It shall be shown that verification/validation is as effective as it would have been with traceability across all phases [DC-326 ]

Embedded COTS software requires

- documentation of the requirements that the pre-existing software is intended to fulfill
- documentation of the assumptions about the environment of the pre-existing software
- documentation of the interfaces with other parts of the software
- inclusion in the validation process of the whole software
- for SIL3/4 analysis of possible failures of the pre-existing software
- for SIL3/4 analysis of failure consequences on the whole software
- for SIL3/4 a strategy to detect failures of pre-existing software and to protect the system from these
- for SIL3/4 verification and validation of allocated requirements, failure detection and protection of the system from these failures
- SIL3/4 verification and validation of assumptions on the environment of the pre-existing software

[DC-324 ]

Embedded COTS software shall have a sufficiently precise (e.g. limited to the used functions) and complete description (i.e. functions, constraints and evidence), including hardware and/or software constraints for integration and application, description of what the software was designed for, its properties, behavior and characteristics. [DC-333 ]

Embedded COTS software shall, before delivering a software release, be included in a traceable software baseline under configuration control. [DC-343 ]

Upon configuration changes relating to embedded COTS software, the software shall be interface tested, including

- all interface variables at their extreme positions
- all interface variables individually at their extreme values with other interface variables at normal values
- all values of the domain of each interface variable with other interface variables at normal values
- all values of all variables in combination (this may only be feasible for small interfaces)
- the specified test conditions relevant to each call of each subroutin

[DC-349 ]

The system has no hazardous single random hardware component failure [DC-336 ]

Simultaneous faults in two items shall be non-hazardous [DC-341 ]

The system must check all inputs (value ranges, electrical characteristics, time, consistency) [DC-350 ]

The system detects and negotiates single faults before another such fault in a second channel occurs [DC-347 ]

The system detects dormant faults by periodical monitoring Periodic tests (meaning tests under the necessary conditions for the fault) shall be implemented for all hazardous faults, using (at least) the DC fault model, and shall show results within the failure detection time SDT. [DC-351 ]

The SDT for hazardous double faults shall be less than 2 / sum of the individual failure rates [DC-346 ]

The system's components shall have CPU fault detection covering DC faults of registers, internal RAM, program counters, stack pointers, reset generators [DC-345 ]

The system's components shall have power supply fault detection for supply of integrated circuits [DC-344 ]

The system shall have independent power supplies for the channels / cross-channel comparison [DC-337 ]

The system shall apply sequence monitoring including program sequence monitoring and temporal monitoring by a separate time base. The system monitors behavior and plausibility of the program sequence. The system monitors triggering points correctly placed in the program sequence. The system has logical monitoring of the correct sequence of individual program sections (by software or external watchdog) [DC-339 ]

The system has voltage monitoring functions. It includes measures against voltage breakdown, voltage variations, overvoltage, and low voltage. It detects overvoltage or under voltage early enough to store internal state (if necessary). It sets outputs to safe state upon over voltage or under voltage, or switches over to a second power unit. [DC-348 ]

The system has monitoring and measures on operating temperature outside of specified range [DC-342 ]

### 5.2.2 Requirements derived from IEC61508

If COTS components from other industries may be used to build the system, in a first approach, the requirements transform into a simple requirement for the reliability of the system hardware, namely a **probability of dangerous failure** per hour (PFH) of less than E-8/h according to the general industry safety standard IEC61508.

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h <sup>-1</sup> ] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

[DC-310 ]

Use of COTS equipment requires evidence of

- clearly restricted and specified functionality
- probability of dangerous systematic faults meeting SIL requirement
- analysis of operational experience of a specific configuration
- suitability analysis and testing regarding performance in the target application
- prior analysis and testing
- known functional behavior and behavior with faults
- known accuracy, time response and response to overload

- known usability, human error impact, maintainability

[DC-331 ]

Use of COTS components requires analytical evidence of

- similar conditions of use
- similar operational profile covering all factors enabling system faults
- similar applicational environment
- similar modes of use and functions performed
- similar configuration and interfaces to other systems
- similar operating system and translator/compiler
- similar human factors
- that the dangerous failure rate has not been exceeded in previous use
- that an effective system for reporting failures has been used

[DC-330 ]

Use of COTS components requires

- impact analysis on any differences (analytics and testing)
- demonstration that quantitative SIL targets given by the using system are met
- that unused functions cannot affect the required integrity of used functions
- that unused functions are physically or electrically disabled
- or that related software is excluded from the configuration

[DC-328 ]

Use of COTS components, including use after any modification of COTS parts, requires justification of proven-in-use characteristics including

- suitability analysis and testing for the intended application
- demonstration of equivalence between the intended and the previous operation
- impact analysis on any differences
- statistical evidence from prior use

[DC-321 ]

Use of COTS components, including use after any modification of COTS parts, requires, for documentation, analysis and justification, a degree of coverage and detail reflecting

- the complexity of the element
- the systematic capability required for the element
- the novelty of the design

[DC-320 ]

For the software or firmware embedded in COTS components, e.g. drivers or operations systems software, the Embedded COTS software use requires either

- development compliant to IEC61508 (Route 1) (*relates here to EN50128*)
- a proven-in-use argument (Route 2 for software, as for system or hardware), or
- probabilistic assessment (Route 3 applied for software)

and

- a safety manual with a precise and complete description adequate for an assessment
- supplier's documentation and records of the development process
- and/or additional qualification activities
- and in some cases, reverse engineering
- creation of adequate specification or design documentation
- consideration of legal conditions (e.g. intellectual property rights)
- early justification of the element (e.g. during safety planning)

[DC-332 ]

Configurable COTS software use requires

- application software reflecting configurability versus existing functionality and complexity
- fault prevention during design, production, loading and modification of configuration data
- data structures consistent with the functional system requirements and application data
- data structures complete, self-consistent, protected against alteration or corruption
- a well-documented configuration process

[DC-355 ]

When justifying COTS software use by quantification of operational experience (proven-in-use argument, Route 2 for software), the following is required:

- the software or data version used shall be identical to the one used previously to gain experience
- the operational profile of the input space shall be unchanged
- an effective system for reporting and documenting failures shall have been in place
- mechanisms shall have been in place to detect any failures which may occur (on-line monitoring)
- test data distribution shall be equal to distribution for demands during previous operation
- test runs shall be statistically independent from each other, with respect to the cause of a failure
- the number of test cases shall be  $n > 100$
- there shall have been no failure identified during the  $n$  test cases
- operational experience shall exceed  $5E9$  hours for SIL4 (equaling 571000 years cumulated)

[DC-357 ]

COTS software use may be justified by assessment of the non-compliant development (Route 3). The assessment requires

an IEC61508 compliant software safety requirements specification for the new application (refer to IEC61508-2010-3 Table A.1, here superseded by requirements from EN50128)

- the justification that the IEC61508 requirements and guidance for software have been considered (here superseded by requirements from EN50128)
- design documentation sufficient to argue compliance with the requirements specification
- design documentation sufficient to argue the required systematic capability
- design documentation covering the software's integration with the hardware
- systematic verification and validation with documented testing and review of design and code
- positive operational experience may replace some black-box or probabilistic testing
- evidence that unwanted functions will not prevent the system from its safety requirements
- removing unwanted functions from the build, or disabling unwanted functions

- architectural measures (e.g. partitioning, wrappers, diversity, checking the credibility of outputs)
- extensive testing
- identified failure mechanisms of the software element
- mitigation measures implemented (e.g. exception handling)
- planning for use of the COTS embedded software elements
- planned configuration of software element, and run-time environment, compiler/linker, etc.

[DC-356 ]

## 6 System design concepts proposals

### 6.1 Safe Datacenter Application Platform

A market research conducted by ESG Elektroniksystem und Logistik GmbH confirms the lack of [WI-2654 - Commercial off-the-shelf](#) (COTS) servers or high performance computers with SIL4 capabilities. Yet SIL4 pre-certified hardware is available as embedded systems. In the railway field those embedded computer are mainly used for onboard applications such as [WI-2292 - ETCS - On Board Unit](#). Components pre-certified to EN 50129 are therefore designed for the operation in harsh environments. These supplementary requirements, yielding the operation in harsh conditions are not needed for the targeted application in the datacenter and imply therefore only an unjustifiably cost factor.

Moreover the embedded solutions, provided by different vendors are all based on dated CPU architectures and must often be operated in restricted conditions to fulfill the SIL4 demands. Typically the boards are operated in lockstep mode, where the clocks of two CPU are synchronized and the safety function is processed in parallel and validated with a 2oo2 voting.

Thus the potential of modern day multicore CPUs cannot be exploited in such a setup. That performance is highly desired to design a performant [SRP-4951 - Safe Data Center Application Platform](#).

To overcome this dilemma new innovative architectures for the [SRP-4951 - Safe Data Center Application Platform](#) are proposed in this section. Some of them are based on disruptive principles, and can therefore most likely not be certified by strictly following the routes denoted in the CENELEC standards. Thus the proposed designs must be evaluated against there ability to being certified. This has to be done in close collaboration with the certification authorities, namely the [WI-2171 - Federal Office of Transport](#) (BAV).

#### 6.1.1 Approach 1 - Pre-certified safety



Figure 4 Moon Architecture with Safety COTS

The approach with expected the lowest certification hurdles, is based on safety pre-certified hardware and software. This means only hardware specially designed and pre-certified to CENELEC EN 50129 will be used. Such safety pre-certified embedded CPU boards are commercially available, mostly in combination with a board support package (BSP), a safety real time operating system (RTOS) and a certification package. The certification package contains certification artifacts, such as the safety case, the safety manual and typically the assessment report from the certification authority or notified body. These artifacts can be used for the system-level certification. Thus, an important part of the certification effort has already been conducted by the supplier.

This significantly lowers the certification risks and results in more predictable certification costs.



It must be noted that the artifacts are only beneficial for system level certification if the hardware is used in the exact same combination with the BSP and RTOS as the vendor intends.

The drawback of this approach is clearly the strong dependency of hardware and software. The dependence on a single hardware supplier during the whole life cycle of the platform once a particular supplier has been chosen is another negative aspect.

A further technical shortcoming of this approach is, as already mentioned in the introduction, the lack of available state-of-the-art pre-certified hardware.

Thus, parallelization of hardware might be inevitable to provide the necessary processing power.

It might furthermore not be possible to benefit from all advantages of modern day virtualization solutions applied in classical datacenters, such as virtual infrastructure with automated load balancing and fail over clustering with the advantage of managing pooled resources across the datacenter. Commercially available solutions with those functionalities simply don't comply with the certification packages provided with the pre-certified hardware.

Considering the described drawbacks, the pre-certified safety approach seems not to be ideal concept for a future proved platform. Nevertheless, it presents a respectable fallback option in case that the more disruptive approaches fail or as intermediate solution until other concepts are mature enough to be implemented.

### 6.1.2 Approach 2 - Hardware-centered safety mechanisms

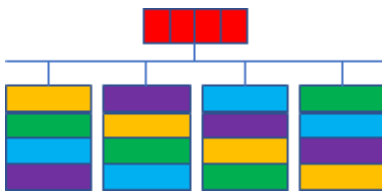



Figure 5 Moon Architecture with diverse COTS channels

The architectural design that lays behind this approach shall act as door opener for the use of  [WI-2654 - Commercial off-the-shelf \(COTS\) data center servers in the safe environment](#). The platform shall be composed of a multichannel architecture with Moon voting. The individual channels are built from diverse COTS components (Hard- and Software). This means that each channel uses a different hardware architecture from a different server vendor. Same is true for the operating system and any firmware or middleware. This is the key to prevent from hazards induced by common cause failures of the channels.

Only the voting and the supervision of the COTS servers is performed on pre-certified SIL4 hardware.

This vastly reduces the amount of pre-certified SIL4 components (Hard- and Software) in the system configuration.

Operations that require high processing power will be executed on the COTS equipment. The less resources demanding voting process will rely on Safety COTS.

State of the art IT hardware equipment (server) can be used for the processing intense tasks. Furthermore, modern day virtualization and clustering solutions can be applied without modifications. This results in a high available datacenter design, close to the days state of the art.

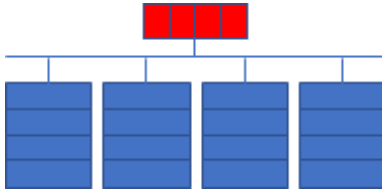
The drawback of this approach is undoubtedly the high effort required to prove and trace the diversity of the channels. Diversity is mandatory to avoid common cause failures. An examination of server hardware design down to component level might be required. This is only possible in close collaboration with the hardware manufacturer and depends on his willingness to disclose his designs. Since the design is the main intellectual property of a server manufacturer there is a least a doubt that this will be possible.

The use of diverse hard- and software also increases the maintenance and configurations effort.


Obsolescence management must be carried out for different hardware, supplied by different vendors which increases the effort. The comprehensive common cause analyses, will have to be reconducted every time a component has to be replaced because of obsolescence of said.

The general maintenance and operation cost are also likely to be higher with a heterogenic server portfolio.

### 6.1.3 Approach 3 - Mixed safety mechanisms



The main goal of this approach is to get rid of the heterogenic hardware and software portfolio that is needed to achieve diversity in the hardware centered approach.

The required diversity, diagnostic coverage and independence of the channels shall be achieved by means of software mechanisms. The precondition is that the error detection probability of the mechanism is independent of the actually used  WI-2654 - Commercial off-the-shelf hardware.

A known mechanism to detect malfunction of the hardware channels is the use of arithmetic codes. AN encoding is often referred in literature and seems to be the most applied encoding mechanism: Simplified spoken: The information in all variables and all instructions are multiplied with a constant A. Now only multiples of A are valid codewords. Soft errors causing alteration of the codeword such as bitflips in memory can be detected.

Before every new operation the variables are checked by computing the modulus with A. If the result is 0 then the codeword is valid and can be further processed.

More sophisticated implementation of AN encoding can furthermore detect control flow errors. AN encoding provides, with other words the standard demanded diagnostic coverage.

An further improvement of this approach is called diversified AN encoding in which multiple encoded replicas based on code with different encoding constants are used to achieve diversity. This allows a supplementary voting of the result of the replicas including one replica based on the native source code.


The safety standard IEC 61508 lists coded processing in volume 2 in A.4 as method to detect execution errors. For SIL4, the IEC 61508 additionally demands hardware redundancy. One might interpret the standard that encoding is a method allowed to increase diagnostic coverage but not to increase the hardware fault tolerance.

Therefore, a multilayered approach is chosen, the system channels will still be voted by a voter implemented on pre-certified SIL4 hardware as described in Approach 2, but each channel of the platform will be built out of multiple AN encoded sub channels (with or without diversity). The sub channels can run on identical COTS hardware or even on the same machine. This will basically increase the diagnostic coverage of each system channel and help to detect hardware failures at runtime. With this approach a channel built out of COTS hard- and software can be increased from no SIL to at least a SIL2.

There are only a few companies like Silistra GmbH in Germany with products on the market that offer compile time encoding as ready to use solution. These products are relatively new on the market and there is a lack of reference applications and certification in the railway signaling domain.

### 6.1.4 Approach 4 - Software-centered safety mechanisms



The software centered safety approach requires, contrary to the other presented approaches, no pre-certified SIL4 hardware. The whole platform shall be built out of  [WI-2654 - Commercial off-the-shelf server](#).

The fault tolerance is solely guaranteed by software mechanism. As in approach 3 described, diversified source code encoding shall be applied. Multiple different replicas that cross-vote their results shall guarantee fault tolerance.



The safety certification of the safety layer of the platform could, in the best-case scenario, be totally uncoupled from the hardware. In a less optimistic scenario the certification demands some minimal application conditions to be fulfilled by the hardware.

In both scenarios, a hardware change during the life cycle of the platform would be possible without or only with a minimal obligation for recertification.

So far, no commercial and certified implementation of solely software based safety is known. Also do the relevant safety and railway standards not cover such a scenario.

There is doubt that products based on this mechanisms are already mature enough to be applied in such an extent. Extensive supplementary fundamental research to prove that a SIL4 can be achieved with such a design is to be expected.

### 6.2 Geo Redundancy / Regionalization

To fulfill the demanding  [WI-1018 - Availability](#) requirements yielding the control instances of the swiss rail network, said shall be split into multiple regions. A number of ten segments are considered for the SBB network, other  [WI-2289 - Infrastructure Manager](#) may have additional segments, leading to a total of ten to twenty regions in Switzerland.

All safety critical applications necessary to control a region or segment, shall be hosted in a cluster of two logical datacenters (DCn and DCn'). The cluster partners must be located geo redundant to prevent from a system breakdown in case of a major event such as a natural disaster or terrorist attacks. Each of the two datacenters must be able to control its dedicated region alone, without restriction, in the event that its cluster partner fails.

A short fail over interruption in operation while transferring services from the failing to the healthy partner might be tolerable. Yet fault tolerant system without fail over time is preferable.

Software or telecommunication issues happening in a region shall not affect other regions as each region is hardware and logically built as independent as possible.

Software or firmware updates can separately be deployed to the regions.

Since the construction and operation of 20 plus datacenter facilities seems not cost effective and contradictive to the SR40 centralization goals, the logical datacenters shall be co-hosted at two facilities (A and B).

The concept is illustrated in the figure below:

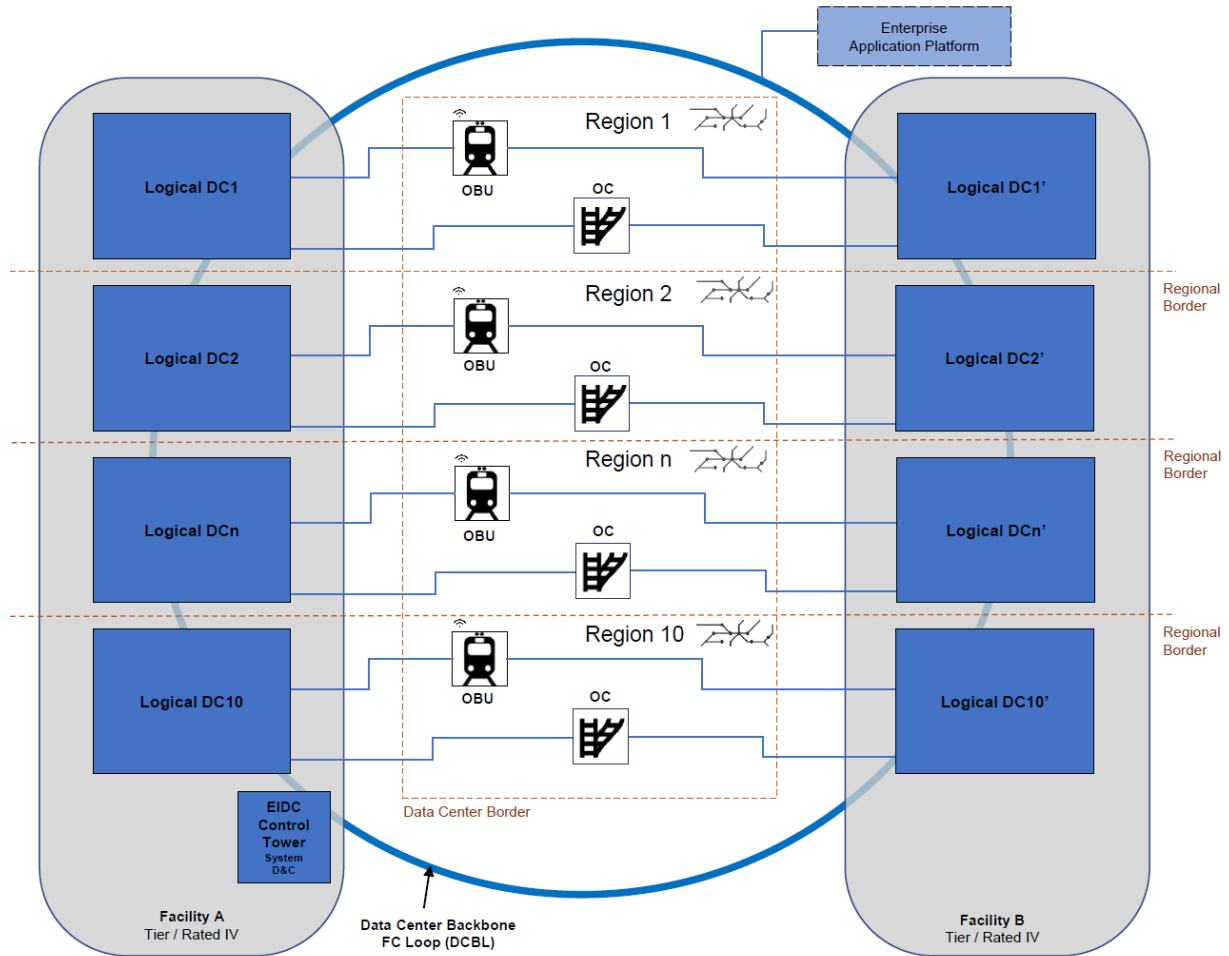


Figure 6 Regionalization

Each [WI-2164 - Trackside Asset](#)'s OC is redundantly connected to both cluster partner of its region. A possibility for a redundant connection to the [WI-2292 - ETCS - On Board Unit](#) has to be investigated in the frame of [WI-2115 - Technical specifications for interoperability](#).

The datacenter backbone loop serves as connection between the individual datacenters.

A train handover between regions is executed via the backbone loop. Diagnosis is carried out over all DC and clusters and centralized. The backbone loop also serves as connection to the DC that will host the enterprise application platform.

Datacenter of adjacent [WI-2289 - Infrastructure Manager](#) can also be connected via the backbone loop.