DEDICATED TO SOLUTIONS.

SBB-RCDC

**ESG Elektroniksystem-
und Logistik-GmbH**

Livry-Gargan-Straße 6
82256 Fürstenfeldbruck, Germany

Phone +49 89 9216-0
Fax +49 89 9216-2631

www.esg.de

Study

On Design, Introduction and Operation Of Safety-critical Applications in a Data Center In the Railway System of Schweizerische Bundesbahnen SBB

SBB has issued a contract to ESG to analyze and define the requirements on a future IT system to be used as an operational system for SBB under special consideration of the requirements imposed on systems to be used for the operation of a railway network. Of major importance is the fulfillment of the requirements which lead to a certification according to SIL 1-4.

Doc. No.: DokNr-1160
Issued: 14.06.2018
Issue No.: V3.1

Total pages:	117
thereof:	
open	
corporate confidential	117

Annex A: Comparison of requirements against properties of the three designs
Document 1160a Requirement Listing and Fulfillment V1.1 180425.pdf

Annex B: General statement on economic processes for data centers
Document 1161 Allgemeiner Überblick WiBe 5.0 V1.1 SOEM2180425.pdf

Annex C: General statement on requirements to commence with the way ahead
Document 1160b Notwendige Beistellungen durch SBB zur weiteren Bearbeitung des Themas

Doc No.:	DokNr-1160
Issued:	14.06.2018
Issue No.:	V3.1

Record of changes

Ausgabe- Nr., Änd.- Index	Ersetzt		Ergänzt	Gestrichen	Grund der Änderung	Bearbeitet: Datum, Name
	Alt	Neu				
V1.0					Ersterstellung	22.02.2018, E.Stöhr, M.Gangkofer C.Patzlaff A.Kister U. Beher
V2.0					Extension as planned after 2.Workshop with SBB	22.4.2018 E.Stöhr, M.Gangkofer C.Patzlaff A.Kister U. Beher Dr.M Stöhr
V3.0					Extension as planned after 3.Workshop with SBB	17.5.2018 E.Stöhr, A.Kister Dr.M Stöhr
V3.1					Clarification of wording in chapters 10.3 and 12.7 after request by SBB	14.6.2018 M.Gangkofer U. Beher E. Brämer

Table of Contents

Page

Table of Figures

Management Summary

Schweizerische Bundesbahnen SBB has awarded a contract to ESG GmbH to create a study for SmartRail 4.0 in respect to the design of a data center in the safety-critical environment, to operate the railway system of SBB.

SmartRail 4.0 is a program to newly define the systems that plan, operate, control and secure train movement and other movements on and in the vicinity of the tracks.

Deviating from today, the safety systems (such as interlockings) shall be designed as safety-critical applications with no direct dependency on special hardware. The applications shall be operated in a centralized data center on standardized HW, COTS ("Commercial off the Shelf") equipment, housed in a number of data centers. This data center solution shall be named "Rail Control Data Center" and will be abbreviated in the following as "RCDC".

Currently the systems deployed for railway use are dominated by special designs for the respective purpose. The fulfillment of industry requirements made it necessary to proceed in this way, as necessary stability, safety, lifespan und functionality were unique to the railway industry and could therefore not be interchanged by other technologies used elsewhere, for example in the industrial or automotive sectors.

Significant efforts and expenses were necessary to build and to maintain that principle for several decades. Therefore, at a first glance the currently used technology appears to be outdated. Spare parts are difficult and costly to obtain. Further developments to lower costs – especially life cycle costs – proved to be extremely difficult.

Therefore, SBB started a new approach based on data center technology. In the present study, the requirements – very much based on embedded technologies - have been formalized and interpreted and applied to a classical data center structure. For analysis purpose three sample designs for that data center based on avionic technology, automotive principles and COTS data center structures had been made and compared to the requirements.

The use of IMA (avionics) as embedded approach needs adaptation and further investigation on suitability. Economic factors speak against the currently available solutions as well as the limited market for such products. The properties of such existing systems deliver high performance in areas, which are not required in a data center, but lack features to use the advantages of modern data center in design, operation, maintenance and life cycle costs.

The automotive AUTOSAR approach proved not yet to be mature. Due to the fast development in this area and a growing market further observation is recommended. In the future, the currently available components with SIL4 certification may well be replaced by that approach. However, AUTOSAR is not applicable for high risk application, which discourages its use.

A classical data center built exclusively from COTS equipment will not fulfill the certification requirements. Using certified components instead would negate the intended savings in investment costs and LCC.

The best todays methodology to develop such a system will be a concept, which combines the advantages of the presented technologies with the requirements on system safety to a classical data center with special

features and structures. Basically, the advantages of both IT-worlds will be combined by a suitable system design. A divided structure with diverse COTS clusters and SIL4 clusters will be used.

As the gateway to the external systems SIL4 system and safety management computers shall be used. This approach separates resources running applications from resources managing the system and its overall safety. The main computational tasks will be provided by standard servers and other mass items of general use in data centers such as storage devices, networks etc. These COTS-products would require reduced or no SIL capability (depending on the certification approach). Management resources would be specific SIL4 devices with limited COTS percentage.

The achievable percentage of COTS equipment depends on the applied certification basis (EN5012X recommended as applicable for railways) and possible cross-standard-certification, as well as the level of diagnostic coverage of the COTS parts possible from remote or by attached watchdog-like diagnostic devices and required therefore a detailed design for calculation of investment and LCC.

Based on the finding of this study, the way ahead seems clear:

1. Early involvement of certification authorities is highly recommended as this design is a ground-breaking concept. The early inclusion of authorities will identify safety concerns which may have immediate impact on the system design.

2. The design of the RCDC has to be completed to a - by far higher! - detailed grade than today, considering also the surrounding elements, interfaces and the total environment of the RCDC..

3. The design shall be based on already qualified special server components with SIL4 capabilities for the safety critical functions and COTS-equipment for all other computing tasks under control of the SIL4 components.

4. The availability of equipment with SIL0 and SIL4, their maintainability and their safety and security features need to be combined in an optimized data center structure, following the principles outlined in this document.

5. The applications to be used need to be taken into consideration at that point in time, as there are interactions to the virtual layers, the used operating system(s), and the programming tools.

6. A LCC estimation is to be done in line with the definitions of SBB on the planned design and a competitive design completely made from SIL4 components to compare the cost impacts.

1. Introduction and Purpose of study

1.1 Overall Rationale and Task

Schweizerische Bundesbahnen SBB has awarded a contract to ESG GmbH to create a study for SmartRail 4.0 in respect to the design of a data center in the safety-critical environment, to operate the railway system of SBB.

SmartRail 4.0 is a program to newly define the systems that plan, operate, control and secure train movement and other movements on and in the vicinity of the tracks.

Deviating from today, the safety systems (such as interlockings) shall be designed as safety-critical applications with no direct dependency on special hardware. The applications shall be operated in a centralized data center on standardized HW, COTS ("Commercial off the Shelf") equipment, housed in a number of data centers. This data center solution shall be named "Rail Control Data Center" and will be abbreviated in the following as "RCDC".

The very basic railway safety requirement for the system is to comply with the rules applicable for railway signaling systems. Without further discussion, SIL4 according to CENELEC is assumed as today's only reasonable safety target.

This study shall define suitable solution concepts, examine them on their properties in respect to the given task and analyze to which extent the intended advantages will be achieved.

1.2 Scope of this Document

Currently the systems deployed for railway use are dominated by special designs for the respective purpose. The fulfillment of industry requirements made it necessary to proceed in this way, as necessary stability, safety, lifespan und functionality were unique to the railway industry and could therefore not be interchanged by other technologies used elsewhere, for example in the industrial or automotive sectors.

Significant efforts and expenses were necessary to build and to maintain that principle for several decades. Therefore, at a first glance the currently used technology appears to be outdated. Spare parts are difficult and costly to obtain. Further developments to lower costs – especially life cycle costs – proved to be extremely difficult.

Therefore, a new approach has been started. This document shall contribute to a qualified discussion on design criteria and to the identification and validation of potential solutions.

In preparation of this study, three potential solution fields were identified in the field of air transport, automotive and professional data centers including cloud operation. Of special importance are requirements imposed on the system to fulfill SIL4, the highest safety level defined for railway signaling systems.

None of these fields completely fit the requirements of the railway industry, as there is no such solution available in the market. Therefore, a four-stage approach has been identified to assess given technologies on their suitability and their shortfalls and provide a limited number of solutions for further examination.

These four stages consist of:

- Identification of requirements imposed on the systems from national and international rules and standards as well as requirements stemming from internal SBB documents on SmartRail4.0
- Identification and assessment of solution elements, which appear to be promising candidates, on their properties and their potential to achieve the project target, especially in respect to safety
- Design of a number of solutions using these elements to fulfill the overarching tasks as specified in the documents mentioned above
- Assessment of the suitability and properties of these solutions and definition of a fulfillment matrix as well as a matrix of shortfalls and problems for each solution.

It must be understood that such a centralized solution consists of numerous elements, which contribute not only to safety, but also to security. These elements themselves are not subject to SIL4, but provide the basis for the overall construction to be able to provide the necessary properties for such a system. As a logical consequence, these requirements and potential solutions are stated in this document.

Other elements may compensate the shortfalls of SIL elements in that just the combination of two or more elements can provide the necessary certification. Therefore, a full system design is required to organize the available elements depending on their properties in a way that is acceptable for SIL4. As a logical consequence, rough system designs of the data center also must be part of this document.

Therefore, the designed systems will deviate in the use of central elements and also in the processes of cooperation with other elements, several surrounding components may be similar although having a significant influence on safety. Subsequently a layered model on security and safety layers must be applied to fulfill the overall task, which is also part of this document.

1.3 Documents to be considered

1.3.1 Standards

As this data center will operate in a railway environment and use to a great extent telecommunication features, standards from both worlds are applicable. In the following, the respective EN standards are listed. Many design criteria have been published internationally by BITCOM and the German BSI. Additionally, several European standards shall be considered.

It is well understood, that, for example, BSI rules have no binding character in Switzerland. However, these documentations provide best practice information from practical experience. Therefore, it appears to be reasonable to take these rules as a non-binding recommendation in the absence of other information.

No.	Name	Document ID
1	RAILWAY APPLICATIONS - THE SPECIFICATION AND DEMONSTRATION OF RELIABILITY, AVAILABILITY, MAINTAINABILITY AND SAFETY (RAMS)	CENELEC EN50126
2	RAILWAY APPLICATIONS - COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS SOFTWARE FOR RAILWAY CONTROL AND PROTECTION SYSTEMS	CENELEC EN50128
3	RAILWAY APPLICATIONS - COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS - SAFETY-RELATED ELECTRONIC SYSTEMS FOR SIGNALLING	CENELEC EN50129
4	RAILWAY APPLICATIONS - COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS - SAFETY-RELATED COMMUNICATION IN TRANSMISSION SYSTEMS	CENELEC EN50159
5	INDUSTRIAL COMMUNICATION NETWORKS - NETWORK AND SYSTEM SECURITY - PART 3-3: SYSTEM SECURITY REQUIREMENTS AND SECURITY LEVELS	CSA IEC 62443
6	BSI Grundschutz Dokumentation	Baustein INF: Infrastruktur
7	BITCOM: Leitfaden Betriebssicheres Rechenzentrum,“	Version Dezember 2013
8	BITCOM: Planungshilfe für ein betriebssicheres RZ	Version Dezember 2013

Since the latest state of technology applies, the draft standard EN50129:2017 is used in this paper.

As a first approach stemming from the CENELEC standards, the system software shall have the safety integrity applicable for the most demanding safety functions to be implemented, namely interlocking functions, and shall therefore meet SIL4 requirements, unless independency from higher level software can be shown. (Source: Draft EN50128:2017 Table E.2)

The necessary safety integrity depends on the maximum damage that may be caused by failure of the system. Since SIL4 is the maximum integrity level defined in the railway domain, the system must be designed in such a way that SIL4 reduces the actual overall risks to an acceptable level. An obvious approach would be to build the system from individual SIL4 clusters distributed over the railway network under centralized control. The system must be structured in such a way that railway SIL4 capability is sufficient for the task, with the task probably being very different from the regionally limited tasks currently applicable for classic widely distributed railway signalling 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 possible victims than known with current systems.

1.3.2 SBB System Documentation

SBB has defined the intended overall process. The special requirements stemming from this process have been identified in some depth and provide a good understanding of the planned rules of operation. Also, the system boundaries and the integration of the data center in the overarching architecture have been well defined. These statements and findings have been summarized in the following documents.

No.	Name and Document ID	Originator
1	SR40_Programm_02-SysArchitecture_System_Architecture_Description.pdf	SBB, 12.1.2018
2	SR40_Programm_03-BizArchitecture_Quality_Attributes.pdf	SBB, 12.1.2018
3	Non- Functional Requirements: NFR Checkliste.xlsx	SBB, 12.1.2018
4	Kick-Off Studie sicherheitskritische Applikationen in Rechenzentrum 16_9.pptx	SBB,16.8.2017
5	000 Einstieg für Extern 20F.pptx	SBB, April 2017
6	Einladungsverfahren: ELV_Studie_Sicherheitskritische-Applikationen-In-Rechenzentrum.docx	SBB, 2017

2. Analysis of System Requirements and their Applicability

2.1 Borders and Interfaces of Study

The contract awarded to ESG limits the subject of the study to the data center (marked blue, in red frame). After careful consideration, ESG is of the opinion that, due to technical interdependencies, some surrounding elements must be taken into account as well.

Due to security issues und safety features which are strongly impacted by the interfaces and in particular the design of the bridge, the interfaces must be taken into account as well. Also, it cannot be the subject to the study at this time, some criteria for the following components will be given at the relevant locations of this document.

- Filter function und security activity of the bridge in respect to separation of the data center from the rest of the internal SBB network (in order to avoid the transfer of malware).

- Data transfer to/from the actuators via public and mobile networks and the inherent risks to be taken into account for a sound system design. (Communication through public space requires security measures and mobile data transfer requires special protocols.)

These areas are marked in broken lines in red.

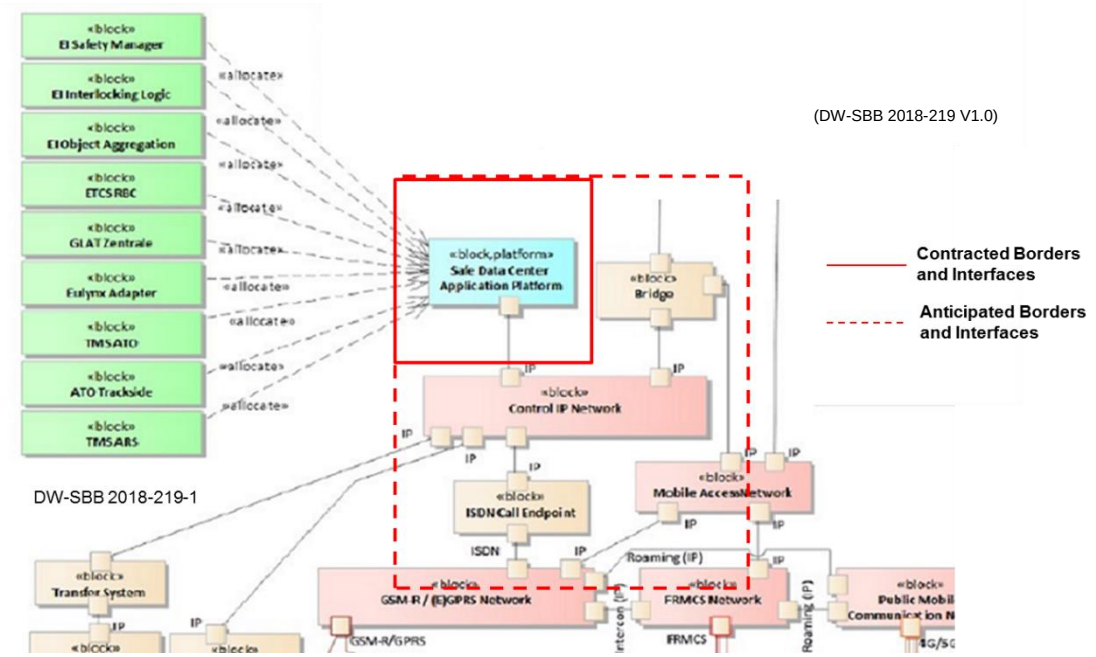


Figure 1: Borders and interfaces of the study for the future data system

Thus, the interaction between the different elements of the system outside of the data center can be described as follows:

Figure 2: Data flow and interaction

In detail the elements depicted above have the following functions:

The **Traffic Management System** is responsible for analyzing the state of the SBB rail system and to provide planning relative to existing schedules, which shall be used by the rail control functions, which are centralized in the data center to steer the elements of the SBB rail system.

The **SBB Rail Control (Data) Center** (RCDC) holds the up-to-date state of the SBB rail system and is responsible for the safe evolution of this state in accordance with the planning provided by the Traffic Management System. It has to detect and avoid unsafe states, which may be caused by undetected conflicts in the TMS planning or may be caused by external events or conflicts. The functions of this data center are classified to the highest security category SIL4. the implementation of the functions needs to be fail-safe, which

means that loss of the data center functions will lead to a stable and safe state. However, safety reactions must remain executable at any time. Nevertheless, for economic reasons, the availability of the SBB Rail Control Center must be very high.

The **Distributed Object Controllers** represent the physical elements of the SBB rail system: This includes trains, vehicles, tracks, switches, crossings, etc. Each of these elements is operated by a controller, which communicates with the SBB RCDC. It provides the state of the associated objects and receives commands which are valid for a limited period of time to project this state into the future. If communication with the data center fails or if it is unavailable, the object controller ensures that its associated objects fall back into a safe and stable state. For example, if the train stops, the crossing will be closed etc.

The **TMS Bridge** has the task of securing the communication between the Traffic Management System and the SBB Rail Control Centre. In particular, it has to detect and prevent any cyber-attack on the SBB Rail Control Centre, as an attack has the potential of causing catastrophic evolution of the rail system´s state.

The **OC Bridge** has the same responsibility for the communication of the SBB Rail Control Centre with the object controllers. In addition, it has the task of ensuring safe transmission. Within the fail-safe design philosophy of the complete system, it is not necessary to control either the delivery of communication or any time constraints, but only that the delivered contents are correct.

In the following, several sets of requirements are listed and discussed. Please note that several requirements are mentioned in more than one requirement set, as the sources of these requirements are different, although they have the same goal. Therefore, duplications cannot be avoided.

The requirements are tagged by source, which can be identified by the first digit (e.g. TL-**1**xx):

- 0: Technical requirements from SBB and ESG. These requirements are attached as Annex 1.
- 1: Requirements directly derived from standard documents
- 2: Functional requirements from SBB and ESG centered around SIL4

2.2 Requirements from Safety Standards

Based on the documentation list, the following analysis provides a number of critical key requirements to achieve the safety level SIL4. Mainly these are formulated in EN50129 and relate to the overall railway SIL4 capability, under special consideration of lifecycle cost requirements and use of COTS components, system availability, system architecture, and detailed requirements on safety characteristics of the subsystems and components used. This chapter is intended to provide a general overview of requirements imposed, and the likely consequences for the system design.

These requirements will be used to assess the capabilities of the three distinct designs on their level of fulfillment.

It shall be noted that the specification is very HW-dominated and suits mainly embedded solutions. If used in a data center, for example, environmental concerns are no longer applicable due to defined environmental conditions of operation. Therefore, the intended properties may be achieved with an appropriate system design rather than with technical features of single units.

Also, architectural requirements such as SW architecture requirements are given with mainly embedded systems in mind. In classic data centers, a similar feature is achieved with an appropriate system design and multiplication of functional blocks.

2.2.1 Overall Railway SIL4 Capability

As a very basic requirement to allow application of the CENELEC SIL4 design rules, the system's functions must have a **tolerable hazard rate** (THR) within the range given for SIL4, therefore less than E-8/h/function:

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

Figure 3: Tolerable hazard rate requirement according to EN50129

TL101: For SIL4 capability, the total system must have the capability of a **tolerable functional unsafe failure rate** TFFR<E-8 (Source: Draft EN50129:2007 Table A.1) and safety-related system functions must meet their individual TFFR<E-8 for random faults (Source: Draft EN50129:2007 B.3.1).

TL102: Bearing in mind that COTS components from other industries may be used to build the system, in a first approach, the above 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^{-1}] (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 $< 10^{-5}$

Figure 4: Reliability requirement according to IEC61508-1

ESG appraisal: While the quantitative targets seem identical, there are additional requirements from IEC61508 compared to EN50129, e.g. on diagnostic coverage (DC) or common cause failures (CCF). In general, the industry standard gives a more conservative classification than the railway standard. It is recommended to not only rely on the "relaxed" Cenelec requirements but to consider other safety standards as far as possible, to allow use of industry COTS components, and to avoid a mismatch with the state-of-the-art, which in any case must be followed in accordance with product law.

The SIL4 requirement applies to both hardware and software (Source: Draft EN50129:2017 Introduction).

ESG appraisal: It is presumed in this paper that only adequately qualified system and application software will be used, meaning SIL4 qualified software throughout the system (while individual application software may have less integrity when separated by SIL4 layers). The same applies to firmware embedded within the hardware platform, e.g. within COTS components. Also, the data used by applications, and the infrastructure dealing with the data, need the SIL4 capability, leading to the following derived requirement:

TL103: The system shall provide SIL4 compliant data storage services to the applications, to safely and securely capture, conserve, retrieve, and communicate data. The services shall be hosted by a pre-certified or trusted subsystem (called **storage subsystem** in the following). (Source: ESG, derived, and from discussion with SBB).

TL104: The system shall **capture the overall status** of the railway system as a consistent set of data, including consistency in the time domain, and provide the information consistently to the applications (Source: ESG, from discussion with SBB).

ESG appraisal: There are various solutions that fulfill this requirement. The degree of sequential versus parallel processing, and the necessary repetition rates for execution of the applications need consideration. This requirement also touches the problem of keeping large computer systems synchronous. From a user's point of view, the system shall at all times provide a consistent image of the modelled railway system to the applications using the system, e.g. by means of a respective generic and managed interface layer or API. Read access to the status data would yield the values captured at a certain time point, and write access would either immediately change the status (allowing locally sequential processing) or "wait" until the program cycle is finished. The application software would have to consider this timely behavior. From a system's point of view, the much simpler approach of asynchronous access would be preferred, with the applications required to manage time dependencies on their own behalf. A global optimum will likely be a mixture of both technical approaches. From a safety and complexity point of view, the synchronous approach would be preferred. In all cases, there is a significant impact on the application software and the interface to the system.

TL105: The system shall provide safe, secure and available **communication means** and methods to exchange information within applications, between applications, and with system-external instances (Source: ESG; to be refined).

*ESG appraisal: It is assumed here that communication will follow the black channel principle, with end-to-end protection measures and EN50159 applied. It is recommended to include a respective generic **communication management layer** into the system to keep the application software simple, e.g. by means of an open standard API for the applications.*

TL106: The system shall provide **independency of safety-related and non-safety-related functions**. Non-safety-related functions 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** (Source: Draft EN50129:2017 Table E.2).

ESG appraisal: While software encapsulation is recommended in general, the solution depends on the concept for inter-application communication (asynchronous "app-to-app" versus synchronous "via-global-storage" communication).

Regarding costs, the system's **regional distribution** over the Swiss railway network shall induce minimum lifecycle costs (LLC), while meeting the SIL targets. It is assumed here that a SIL4 software based solution for the separation requirement has minimum LCC. The system shall have software to safely separate non-safe from safe functions. (Source: ESG w/ LCC requirement from SBB)

TL107: The system shall be operator and maintainer-friendly. The system needs protection against operating or maintenance errors. The system shall need limited human intervention (Source: Draft EN50129:2007 Table E.3).

*ESG appraisal: Requirements on manual operations and related functions are to be specified and include system administration, system housekeeping, operational modes, degraded modes. It is recommended to carefully separate between system-related human action and railway operations related manual interaction. Actions of the latter kind shall not be supported in the computer center. It is recommended to have such functions concentrated in a dedicated **maintenance subsystem**.*

2.2.2 Use of COTS Components

TL108: The system shall make use of **COTS hardware and software** as far as reasonably possible, resulting in reduced LCC. It is assumed that COTS IT components have less LCC than railway-specific COTS components, which have less LCC than non-COTS (specifically developed) components. This applies for computing (processing) subsystems and for storage subsystems (Source: SBB w/ assumptions from ESG).

ESG appraisal: There are foreseeable constraints from existing applications and legacy implementations. The decision will, at the end, depend on individual and in-depth assessment of the impact on LCC, including cost of certification. It is recommended to focus the investigation for COTS on the elements of the architecture that will have the highest number of line replaceable instances. Most likely, this could be servers and/or storage devices.

The system shall therefore include COTS IT hardware and software components as far as reasonably possible, resulting in low LCC. Where IT components cannot fulfill requirements, railway standard COTS components shall be used as far as reasonably possible, resulting in reduced LCC (e.g. MEN components). Only where unavoidable shall the system rely on to-be-developed dedicated computing or storage subsystems.
(Source: ESG w/ LCC requirement from SBB)

To evaluate the possibilities for COTS deployment, the following chapters deal with requirements on COTS components.

2.2.2.1 General Requirements related to COTS

TL109: For use of COTS components, the **EN50129 Draft** standard shall primarily apply (Source: ESG, derived).

ESG appraisal: There are various known safe railway systems certified according to EN50129 and including COTS components (e.g. Siemens SIMIS PC based applications). The COTS approach therefore seems feasible in general. The following requirements draft the possible solutions opened by EN50129.

TL110: 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 (Source: EN50129-2016-Draft 6.2).

*ESG appraisal: While IT servers ("IT COTS") today do not NOT comply with other safety standards, the above requirement opens up the possibility to make use of "specific COTS" computers certified for dedicated markets and therefore compliant with safety standards like IEC61508 (general industrial applications), IEC61511 (process industry), or ARP/RTCA (avionics). Nevertheless, the market for safety-certified equipment is still much smaller than the market for general IT applications, thus limiting the possible and intended reduction in lifecycle costs. Application of specific COTS requires **cross certification** from other industries to railway signaling applications. EN50129 expects the gaps to be "mostly formal" and the approach therefore seems applicable in general. Therefore, requirements on COTS from other standards are discussed further in this paper. Note that EN50129 is the only standard addressing "complete" COTS systems and "equipment" within safety applications, obviously meaning and including subsystems like servers. Nevertheless, today there are obviously no "big servers" with any kind of safety certificate available from the market, but the cumulated market of components with multiple derived certifications may be attractive for potential hardware partners.*

TL110: 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 (Source: EN50129-2016-Draft 6.2).

*ESG appraisal: There is no obvious reason to limit COTS to "parts of safety functions". The wording seems to address the obvious necessity to "make the COTS parts safe" by means of other parts of the system providing the capabilities probably missing with typical COTS. An example would be to provide a managed operating temperature for COTS parts that have only a limited temperature profile, by adding non-COTS functionality to control the temperature, with reliability adequate to the SIL of the safety function. As a result, the system, when using COTS, must provide adequate functions to compensate missing properties of COTS components. Note that the term "properties" likely refers to the very detailed requirements set by EN50129 and referenced standards applicable for newly developed systems, resulting in the need for deep-digging technical measures to supervise the actual characteristics and performance of the COTS components. Feasibility of this approach needs further discussion. Such compensation may need hardware and/or software, and is named "**COTS supervision layer**" in this paper. Consequently, the COTS parts managed by the layer are called "Supervised COTS" within the following discussion of more detailed requirements.*

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

(Source: EN50129-2016-Draft 6.2 and Note and 6.2.3)

ESG appraisal: The main argument for use of COTS is the server-like high computer performance required to provide the safety functions for all the SBB operational network from only a few computer centers. Development of respective computers according to EN50129 seems feasible in principle, but would require very high effort.

Nevertheless, related to the foreseeable worst-case damage of a SIL4 railway signaling system, development costs or even the reduced lifecycle costs would be no compelling reason, accepted by society, to force a COTS-based solution.

Therefore, the use of COTS equipment is acceptable, as there is no valid alternative (to work in a data center environment) available and such development would be extremely expensive.

TL111: Supervised COTS components require available information on functionality, interfaces, hardware and/or software constraints, failure rate, environmental conditions, conditions of use (EN50129-2016-Draft 6.2.3.1).

ESG appraisal: Most IT server components fulfill this requirement. Nevertheless, the validity of determination of the failure rate might need individual assessment.

TL112: Supervised COTS components must be identified, included in the overall system definition and put under configuration control (EN50129-2016-Draft 6.2.3.2).

ESG appraisal: This requirement is no problem because the COTS components are in any case covered by the system development safety processes.

TL113: Supervised COTS components require interface hazard analysis or FMEA to identify hazardous failure modes on the boundary of the equipment, and SIL classification. (EN50129-2016-Draft 6.2.3.3)

ESG appraisal: The requirement explicitly allows the COTS equipment to be treated as a "black box", with the hazard analysis reduced to the boundaries of the COTS parts. For the servers, the significant boundary failure mode is foreseeably a "faulty result of a calculation", on a safety integrity level dependent on the overall system architecture that integrates the respective COTS component.

TL114: 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 (EN50129-2016-Draft 6.2.3.4.1), OR the part must be re-qualified according to the required SIL (EN50129-2016-Draft 6.2.3.4.2), OR there must be external supervising instances negating the failure and establishing a safe state within the safety target. (EN50129-2016-Draft 6.2.3.4.3)

ESG appraisal: Since the terms "external" and "failure" are used here, versus e.g. "diagnostics" and "fault", the significant failure of COTS servers used would be "calculation of a safety function failed", implying that diagnosis of the failure is only possible by comparison to the results of a similar function. This matches with the above-mentioned black box approach. As a result, mutual comparison or voting between several similar units seems adequate, and in-depth diagnostics may not be required in the first approach.

TL115: 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. (EN50129-2016-Draft 6.2.3.5)

ESG appraisal: The significant failure mode "bad calculation" of a COTS server must be considered to occur at least once within the normally well-known MTBF time interval based on simple "parts count". Vice versa, as a first approach, for a SIL4 reliability requirement of PFH<E-8/h (10FIT), the MTBF requirement of a server system would be an overall 1/PFH, before architectural measures that may easily reduce by factor 1000. With

HFT=2 for example, the required MTBF would reduce to, say, 10 years, which is very reasonable for mainstream IT servers. Therefore, use of high-quality COTS servers, with known MTBF figures, for composite safety seems feasible.

TL116: 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. (EN50129-2016-Draft 6.2.3.6 and 6.2.3.7). For supervised COTS equipment, a strategy shall be defined to manage the possible effects of product changes (e.g. disable automatic software updates) (EN50129-2016-Draft 6.2.3.8).

ESG appraisal: These requirements relate to the system development process and can therefore be fulfilled.

Since both EN50129 and EN50126 have no further details on the use of COTS, since the above requirements are somewhat inconsistent regarding the required depth of supervision of the COTS parts, and because cross-certification from other industries might be an option, the following requirements on the use of COTS at the system and hardware level have been extracted from the most significant safety standards from various industries, as a reference for further consideration.

For COTS components, the **IEC61508**-2010-2 (2nd edition) standard is without doubt a reference, as state-of-the-art for safety-critical systems and hardware in general, including detailed requirements on COTS. Since this is the standard from which the Cenelec standards have been derived for railway applications, IEC61508 must be considered whenever the railway standards don't offer a more detailed or specific view. Cross-certification from this standard to railway signaling applications seems reasonably possible.

TL117: Use of COTS equipment requires evidence of

1. clearly restricted and specified functionality
2. probability of dangerous systematic faults meeting SIL requirement
3. analysis of operational experience of a specific configuration
4. suitability analysis and testing regarding performance in the target application
5. prior analysis and testing
6. known functional behavior and behavior with faults
7. known accuracy, time response and response to overload
8. known usability, human error impact, maintainability

(Source: IEC61508-2010-2-7.4.10.1)

ESG appraisal:

1. *The functionality of a COTS server is unfortunately not clearly restricted and specified. While the basic function is to "calculate something", the variance of possible calculations seems extremely wide. Obviously, the COTS approach with IEC61508 is intended for subsystems of limited complexity. Nevertheless, the reason for the requirement seems to allow a complete specification of functions and test cases. Since the complexity of a server is mainly defined by its integrated circuits, especially CPU devices, which again are a kind of COTS, it makes sense to try to apply requirements intended for complex circuits (to be detailed).*

2. *COTS servers normally come with MTBF figures which can be used to conservatively calculate the PFH.*

3. *COTS servers normally don't allow for many configurations, and they are typically operated with lots of diagnostic functions continuously logged. There is therefore likely to be sufficient operational experience data available for dedicated devices and configurations. Nevertheless, such data will not necessarily cover calculation faults in detail. Only some configurations with applied voting will probably uncover calculation faults and provide sound data for the required analysis.*

4. *Suitability analysis and performance testing in the target application seems clearly feasible.*

5. *Optional requirement intentionally left open.*

6. *The functional behavior of servers, regarding the main function of providing calculation results, is trivial, as is the behavior upon calculation faults.*

7. *The accuracy, time response and response to overload of servers heavily depends on firmware, operational system and other hardware-related software layers used. It is assumed that the requirement is covered when applying the requirements to COTS software.*

8. *COTS servers are mainstream parts widely used, therefore normally with well-known operational and maintenance characteristics.*

Summary: COTS hardware can reasonably fulfill the requirements, given that the complexity can be covered by dedicated measures. It is recommended to apply the IEC61508 rules for complex devices (to be detailed).

Use of COTS components requires analytical evidence of

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

(Source: IEC61508-2010-2-7.4.10.2)

ESG appraisal: COTS servers and storage devices run within computer clusters, built into racks, and operated within server rooms in defined conditions, under managed continuous load, in an undisturbed environment, with standard interfaces used, with extensive logging of faults and failures, as far as detected, and with the same human factors applying in operation and maintenance. Nevertheless, different operating systems or configurations and different low-level software will likely be used for the railway application. Also, there is normally little evidence of critical faults actually happening, because respective logging data will not necessarily cover processing faults in detail. Only some configurations with applied voting will probably uncover calculation faults and provide sound data for the required similarity argument. Therefore, COTS servers can probably fulfill this requirement only partly. Mitigation measures may include extensive testing efforts plus extensive software-based fault detection mechanisms within the COTS supervision layer.

Use of COTS components requires

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

(Source: IEC61508-2010-2-7.4.10.3 and IEC61508-2010-2-7.4.10.6)

ESG appraisal: COTS servers and storage subsystems will include numerous functions in addition to the safety functions. In fact, such parts sell, among others, by the quantity and convenience of their built-in features, including network or even internet related features and functions, such as remote firmware updates via the internet. Most of these functions may be considered as health monitoring or diagnostic functions reasonably contributing to the overall robustness of the solution.

Nevertheless, other functions, being no integral part of the safety functions, must be identified by documentation, analytics or reverse engineering, and disabled by configuration. In addition, the disabling function must be sufficiently reliable, e.g. adequately diagnosed or supervised, and it must be shown that the disabled features remain without possible impact on safety functions. Functions providing connectivity not immediately required by the safety functions must be reliably disabled. In particular any features relating to open networks, e.g. the internet, must remain without possible impact.

Since most of the features and disabling functions relate to software, e.g. firmware, it is necessary for the use of COTS parts, to consider the safety standards on COTS software. Respective analysis has therefore been added later on in this paper. Note that the above requirements are independent of the system architecture, especially independent of any voting mechanisms applied at the system level. In other words, and trivial, multi-channel voting is no replacement for reliable processing within the individual system channels. Nevertheless, some unwanted features and functions may become sufficiently reliable when closely supervised by a COTS supervision layer.

TL118: Use of COTS components, including use after any modification of COTS parts, requires justification of proven-in-use characteristics including

1. suitability analysis and testing for the intended application
2. demonstration of equivalence between the intended and the previous operation
3. impact analysis on any differences
4. statistical evidence from prior use

(Source: IEC61508-2010-2-7.4.10.4 and IEC61508-2010-2-7.4.10.7)

TL119: 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

1. the complexity of the element
2. the systematic capability required for the element
3. the novelty of the design

(Source: IEC61508-2010-2-7.4.10.5 and IEC61508-2010-2-7.4.10.7)

ESG appraisal: COTS servers and storage subsystems are obviously complex, need at least SIL3 capability (as shown later), and must be considered as new designs due to their very nature as continuously evolving and broadly used commodity parts. Therefore, in-depth analysis, comprehensive testing and sound justification for use within a safety system is absolutely necessary. Since these efforts come up with each and every change of the COTS parts (and there are many changes with COTS), there is a significant impact on the lifecycle costs of the system.

The above requirements from IEC61508 seem much more restrictive than the few requirements on COTS components given by EN50129. As a verification of the applicable state-of-the-art, the following requirements have been extracted from the automotive industry's standard ISO26262 (the current draft issue used), considered to be relatively "progressive" due to the very nature of the highly dynamic automotive market.

TL120 Use of COTS components requires available safety architectural constraints from the design of the parts, or estimation from basic data such as failure rate, failure modes, failure rate distribution per failure modes, built-in diagnostics, etc.; Use of COTS components requires safety analyses involving the supplier of the parts, with defined scope split between parties, agreement on procedures and methods applied, exchange of information/documentation or confirmation of assumptions, and agreed procedures for verification (e.g. joint reviews) (Source: **ISO26262-2016-Draft**-4 7.4.4.6 NOTE 1 and ISO26262-2016-Draft-6 E.2.3).

ESG appraisal: Sufficient knowledge of functions, features and reliability characteristics is necessary to allow analysis and justification. It is required to only use COTS parts from suppliers willing to very closely cooperate with the system designer on a technically detailed level over the complete parts' lifecycles, and ready to contract for this.

TL121 Use of COTS components requires qualification of hardware elements through a combination of test, analysis, and argumentation that the risk of a safety goal or safety requirement violation is sufficiently low. This requires detailed knowledge of implementation and development and production processes (ISO26262-2016-8-Draft 13.2 and 13.4.1.1 class III).

ESG appraisal: This requirement adds the necessity to include the supplier's development and production processes into the overall qualification tests, analysis and safety argumentation. An example would be detailed technical safety audits performed at the supplier's development and production sites. Note that this means recurrent effort with each and every change of the COTS part or its production, rollout and delivery processes, with significant impact on lifecycle costs of the system. A reasonable alternative may be pre-qualified COTS from a supplier with continuously third-party-certified safety processes.

TL122: Use of COTS components can be justified by demonstration of sufficient confidence from prior use, called "proven-in-use argument", with the following detailed requirements:

1. the candidate COTS product must be very similar in definition to the released COTS product used to gain the confidence from prior use (called "reference product" later on in this paper)
2. the conditions of use of the candidate COTS product must be very similar to the reference product
3. appropriate documentation *of both products* must be available
4. configuration and change management records must be available *for both products*
5. there must be field data available on safety-related incidents related to the reference product
6. the field data must be sufficiently relevant
7. the field data must address both systematic and random failures of the candidate

8. the changes to the reference product during prior use must be known and considered
9. the proven-in-use credit must be planned and described in the safety plan of the system
10. the system safety case must include data and work products resulting from the proven-in-use argument
11. the data and work products from the proven-in-use argument must be subject to confirmation measures
12. missing field data may be substituted by available data from the development phases of the candidate

(Source: ISO26262-2016-8-Draft-8 14)

ESG appraisal: While most of the requirements can be fulfilled with significant justification efforts, provided the field data is sound and available, field data on safety-related incidents will NOT be available. The intention of this requirement is that the COTS parts can only be considered as proven-in-use if the intended safety function has been proven-in-use before. Since for COTS servers and storage devices the safety functions are "process data" and "store and retrieve data", there is an abstract argument that the safety functions were observed in prior use, provided the functions were closely monitored in prior operations. Nevertheless, it is hard to prove that the monitoring and fault detection applied were sufficiently "deep" and actually capable of detecting any processing or storage faults.

As another verification of the applicable state-of-the-art, the following requirements have been extracted from avionics standards, considered to be relatively conservative due to the very nature of possible aviation accidents. Note that use of COTS components with the DO-254 standard relates both to components (such as resistors, integrated circuits) and complete LRUs (line replaceable units) which are typically available as a catalog item. The latter seem applicable for the kind of safety system considered here.

TL123: Use of COTS parts shall be managed by a supporting process associated with hardware development. COTS components shall have configuration management established before they are used in a baseline (Source: DO-254-11.2.1 and **DO-254**-7.2.1).

ESG appraisal: This shall be considered in the system development process.

TL124: Changes to COTS equipment, including requirement changes, changes upon detection of errors, changes due to hardware or technology enhancements or procurement difficulties, shall be assessed before modification, regarding the system safety assessment results, and the impact and consequences of the change. Changes to COTS equipment may result in a re-verification effort involving more than the area changed. This area may be determined by signal flow analysis, functional analysis, timing analysis, traceability analysis, etc. (Source: DO-254-11.1)

ESG appraisal: This requires the same detailed information on the COTS parts' design, and the same process of close cooperation with the COTS product suppliers as requested by ISO26262 mentioned earlier in this paper. Management of changes to COTS equipment is obviously a crucial part of the state-of-the-art.

TL125: COTS certification credit is given by a track record *on the system development side* for

1. COTS product's production *process* of high quality
2. COTS product manufacturer with established quality control procedures
3. COTS product operational service experience
4. COTS product qualified by the manufacturer or by additional testing regarding reliability
5. COTS products selected based on technical suitability to the intended application, such as temperature range, power or voltage rating, or additional testing or other means to verify this suitability

6. COTS product's performance and reliability monitored on a continuous basis, with feedback to the product manufacturers

(Source: DO-254-11.2.1)

ESG appraisal: The requirements can be considered in the system development process and are similar to the requirements found in other standards.

TL126: COTS component procurement concerns include the actual availability of the COTS design assurance data, variations in component parameters identified, evolving aspects of electronic component technology, and COTS components which become non-procurable (Source: DO-254-11.2.2).

ESG appraisal: The intention seems to prefer long-term procurable COTS products to avoid inherent safety risks from frequent change of products.

TL127: Use of COTS components can be justified by sufficient confidence from prior use, provided that

1. the product has been widely and successfully used in service
2. there is available evidence of design maturity
3. there is evidence that the COTS product is free of errors
4. there is demonstrated manufacturing quality

(Source: DO-254-11.3 Note)

Justification of confidence from prior use of COTS requires

1. similarity of usage with respect to application, function, environment and DAL *("SIL")*
2. the item being based on the proposed configuration
3. evidence of design errors found, assessed, eliminated, mitigated, or without impact

(Source: DO-254-11.3.1)

ESG appraisal: Again, prior use within a safety function requiring the same rigor of design (design assurance level DAL, in this aspect similar to the safety integrity level SIL) is necessary for justification of use of COTS components. Normal COTS IT products will NOT have track records fulfilling this requirement. Nevertheless, a COTS product will always have a first application on the required level. A possibly acceptable approach would be to accumulate hours of prior use within less demanding applications, and, gradually over time, "upgrade" to higher level applications. In this case the requested "similarity" could be justified. The following requirement may relax stringency by requesting only the data used should be adequate to the target integrity level:

Justification of use of COTS components by confidence from prior use requires justification for the adequacy of the service experience data relative to the intended use and required design assurance level (Source: DO-254-11.3.3-3).

Justification of use of COTS components by confidence from prior use requires hazard analysis considering the actual (*not only* calculated) failure rates (Source: DO-254-11.3.1-4 Note).

Justification of use of COTS components by confidence from prior use requires assessment, based on engineering analysis, of

1. substantial available service data
2. relevance of the previous applications, installations and environments to the target application
3. relevant sources (specs, data sheets, application notes, service bulletins, user correspondence, errata notices)
4. the intended usage, to identify impacts on the necessary system safety assessment
5. actual mitigation of the effects of design errors identified by the used data
6. any available statistics on design errors and their impact on the system safety assessment
7. available problem reports, with respect to available improvements in the current configuration
8. problems not yet fixed, for mitigation by architectural means or additional verification.

Qualitative assessment is acceptable if statistics are not available.
(Source: DO-254-11.3.2 and DO-254-11.3.2-3)

Confidence from prior use requires data including identification of the component, its intended function in the system and the design assurance level. For Level A and B functions, a description of additional means of assurance for the component, such as architectural means and additional or advanced verification strategies, is required (Source: DO-254-11.3.3-1).

Confidence from prior use requires a description of the service experience data collection and assessment process, including criteria for determining the adequacy and validity of the data (Source: DO-254-11.3.3-2).

Confidence from prior use requires detailed description of the service information considered, change history, assumptions used to analyze the data, and a summary of the analysis results (Source: DO-254-11.3.3-3).

ESG appraisal: The avionics requirements are similar to those in other industries.

2.2.2.2 Requirements related to COTS-Embedded Software

Use of COTS servers or storage subsystems preferably will not only use “naked” hardware, but include some embedded lower-level firmware or configuration data. Therefore, this chapter will discuss the software-related requirements to be considered both from the EN50128 standard on software referenced by EN50129, and from other safety standards from different industries building the state-of-the-art for reuse of existing software. The railway standard EN50129 refers in any case to the more generic safety standard IEC61508 to provide the necessary details. The first following requirements stem from EN50128 applicable for railway signaling software, firmware and data.

Embedded COTS software developed according to EN50128 is to be preferred wherever possible (EN50128-2011-7.3.4.8).

ESG appraisal: The railway industry clearly prefers railway certified COTS products unless there are very good reasons convincing the certifying party. It is recommended to team up early with certifiers to build confidence in the use of COTS from other industries.

TL128: 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 (EN50128-2011-6.5.4.16).

ESG appraisal: Since verification and validation refer to requirements, and the original requirements of the COTS parts may be unavailable or targeting other applications, the only way to fulfill this requirement is to develop system requirements and assign them formally to the COTS parts of the system. Verification and validation efforts will then trace to these requirements. It is therefore NOT sufficient to simply make use of existing COTS servers or storage subsystems. The functions and characteristics of embedded software, firmware and configuration data must be specified by derivation from system requirements, and verified and validated at COTS part level and at system level after integration. While this seems feasible in principle, there is obviously a significant effort for specification and test of the COTS parts' software.

TL129: Embedded COTS software requires

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

(Source: EN50128-2011-7.3.4.7)

ESG appraisal: The SIL3/4 requirements assume failure detection functions within the COTS parts, or in a COTS supervision layer on system level, and protection of the system from those failures. Since all failure modes relating to functions or characteristics of the embedded software shall be covered, all software hidden in the COTS parts must be well-known and capable of being supervised or diagnosed by an external COTS supervision layer.

TL130: 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 (Source: EN50128-2011-7.3.4.7).

TL131: Embedded COTS software shall, before delivering a software release, be included in a traceable software baseline under configuration control (Source: EN50128-2011-9.1.4.2).

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

1. all interface variables at their extreme positions
2. all interface variables individually at their extreme values with other interface variables at normal values
3. all values of the domain of each interface variable with other interface variables at normal values
4. all values of all variables in combination (this may only be feasible for small interfaces)
5. the specified test conditions relevant to each call of each subroutine

(Source: EN50128-2011-D.34)

ESG appraisal: As required with COTS in general, it is also necessary to team up with the manufacturers of any software, firmware or data hidden in the COTS component to be used, and to establish a sound lifecycle support covering changes and verification/validation of changes.

As a verification of the above requirements from the railway standard versus the state-of-the-art, and because EN50129 refers to IEC61508 for details, the following requirements have been extracted from there.

TL132: For the software or firmware embedded in COTS components, e.g. drivers or operations systems software, the **IEC61508**-2010-3 (2nd edition) standard may be a reference, as state-of-the-art for safety-critical systems software, including detailed requirements on COTS. Cross-certification from general industry to railway signaling applications seems possible (details to be added).

Embedded COTS software use requires either

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

and

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

(Source: IEC61508-2010-3-7.4.2.12)

ESG appraisal: Software embedded in a COTS component may be developed from scratch or claimed to be proven-in-use, or assessed in detail. Or vice versa: Software embedded in a COTS component shall be claimed proven-in-use, if necessary including re-engineering, or, whenever a proof is not possible, assessed in detail, or, if this is not possible, developed from scratch. In all cases, a close cooperation with the manufacturer of the hardware is unavoidable, for proven-in-use also with the manufacturer of the software or firmware or data. The embedded software must be completely specified, verified and validated. In the following, the term "trusted" is used for components qualified by one of these certification approaches.

TL133: Configurable COTS software use requires

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

(Source: IEC61508-2010-3-7.4.2.14)

ESG appraisal: The configuration data used in COTS servers or storage subsystems needs adequate specification of the given data structures, and system level management processes to prevent faults during design of the data, production, download, modification, etc. Again, this requires close cooperation with the manufacturers.

TL134: When justifying COTS software use by quantification of operational experience (proven-in-use argument, Route 2 for software), the following is required:

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

(Source: IEC61508-2010-7-Annex_D and IEC61508-2010-7-D.2.1.1 and IEC61508-2010-7-Table_D.1)

ESG appraisal: For servers or data storage subsystems, with managed firmware and configuration data, stable operational profile, effective and exhaustive health monitoring and diagnostics, requirements 1 to 4 can reasonably be fulfilled in cooperation with the manufacturer.

The distribution of demands, failure-related planning of tests, and statistical relevance related to any safety functions, meaning requirements 6 to 8, will NOT be available from previous non-railway use of the COTS embedded software. Therefore, according to IEC61508, the number of hours required to claim operational experience, as given with requirement 9, canNOT be fulfilled. Therefore, operational experience canNOT be claimed for the embedded software, firmware or configuration data coming with the COTS equipment.

TL135: COTS software use may be justified by assessment of the non-compliant development (Route 3). The assessment requires

1. 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)
2. the justification that the IEC61508 requirements and guidance for software have been considered (here superseded by requirements from EN50128)
3. design documentation sufficient to argue compliance with the requirements specification
4. design documentation sufficient to argue the required systematic capability
5. design documentation covering the software's integration with the hardware
6. systematic verification and validation with documented testing and review of design and code
10. positive operational experience may replace some black-box or probabilistic testing
11. evidence that unwanted functions will not prevent the system from its safety requirements
12. removing unwanted functions from the build, or disabling unwanted functions
13. architectural measures (e.g. partitioning, wrappers, diversity, checking the credibility of outputs)
14. extensive testing
15. identified failure mechanisms of the software element

16. mitigation measures implemented (e.g. exception handling)
17. planning for use of the COTS embedded software elements
18. planned configuration of software element, and run-time environment, compiler/linker, etc.

(Source: IEC61508-2010-3-7.4.2.13)

ESG appraisal: To avoid new development of COTS embedded software, firmware or data, according to the state-of-the-art, in-depth assessment is an option. The assessment must "post-mortem" prove SIL4 capability of the software elements in this rail application scenario, which is unlikely to be confirmed for most of the software provided with standard COTS IT servers or storage devices, since this was never a requirement during the development and requirements are stringent.

In addition, the assessment is very detailed and may cause changes or add-ons to the software, so full authority on the COTS product is required. Again, this does not seem feasible without close teaming with the manufacturers, who most likely have no experience or processes related to functional safety. Extensive testing remains necessary to complement the assessment.

Summing this up, the assessment-based path of certifying the software-based parts of the COTS equipment is NOT a preferred approach. It is recommended to team up with the hardware provider, and to develop the required hardware support package software from scratch according to SIL4 rules, and therefore sufficiently without systematic faults.

For verification of the state-of-the-art, the following requirements applicable to COTS embedded software have been identified in automotive or avionics safety standards.

TL136: Use of COTS equipment requires embedded software or firmware to be qualified based on its specification, evidence of compliance to the applicable safety standard, evidence of suitability for the intended use elaborated, and evidence of its development process' compliance to an adequate safety standard. This may require some re-engineering (Source: **ISO26262**-2016-6-Draft 12.4.1 and Note).

ESG appraisal: The automotive standard also calls for application-specific qualification of the software, including assessment of the development processes, as does the IEC61508 standard.

TL137: Embedded COTS software must conform to the standard. If deficiencies exist in the software lifecycle data, the data should be augmented to satisfy the objectives of the standard ("upgrade of the development baseline"). Embedded COTS software may be re-engineered to regenerate software lifecycle data. (Source: **DO-178C**-2011-2.5.3 and DO-178C-2011-12.1.4)

ESG appraisal: The avionics approach also comprises assessment and, if necessary, some re-engineering.

TL138: Embedded COTS certification should be based on the failure conditions and DAL *("SIL")* as determined by the system safety assessment. Comparison to failure conditions of the previous application will determine areas that may need to be upgraded (Source: DO-178C-2011-12.1.4).

ESG appraisal: While FMEAs might be available in some quality (likely not based on the railway failure conditions from EN50129), the SIL classification will not. As a result, a proper failure analysis and SIL classification must be performed. Also, functional enhancements may be necessary to implement necessary measures. Teaming with the COTS hardware and firmware suppliers and full change authority is necessary.

Embedded COTS software lifecycle data from previous development should be evaluated to ensure that the software verification process objectives of the software level are satisfied for the new application to the necessary level of rigor and independence (Source: DO-178C-2011-12.1.4).

Confidence from prior use of embedded COTS software may have credit from applied configuration management, problem reporting, stability and maturity, relevance of product service history environment, length of the product service history, actual error rates in the product service history, impact of modifications. Credit depends on sufficiency, relevance, and types of problems occurring during the service history period (Source: DO-178C-2011-12.3.4).

Confidence from prior use of embedded COTS software requires the use, conditions of use, and results of software service history to be defined, assessed within the system development and assessment processes (Source: DO-178C-2011-12.3.4).

Confidence from prior use of embedded COTS software requires the service history to be defined and reflecting intended operations of the system. The applicant should have been under configuration management. The service period and/or number of demands must be sufficiently accurate and complete, and account for any changes in software, system configuration, operational mode or state, operating environment, software configuration, etc. An impact analysis should be conducted upon such changes (Source: DO-178C-2011-12.3.4.1).

Confidence from prior use of embedded COTS software requires that software capabilities to be used are exercised in all operational modes, with input data executed in all relevant permutations (Source: DO-178C-2011-12.3.4.1)

Confidence from prior use of embedded COTS software requires assessment of the operating environment to show relevance to the intended use in the proposed application, and relation between the service history environment and the intended environment. Additional verification in the target environment may be required (Source: DO-178C-2011-12.3.4.1).

Confidence from prior use of embedded COTS software requires assessment of impact of any hardware modifications during the service history period (Source: DO-178C-2011-12.3.4.1).

Confidence from prior use of embedded COTS software requires analysis to show that any code that was deactivated during the period of service history is not activated in the new environment. Additional verification may be necessary (Source: DO-178C-2011-12.3.4.1).

Confidence from prior use of embedded COTS software requires an adequate amount of service history, depending on the system safety objectives and required safety level, the differences to the intended system operational environment, the applicable objectives of the DO-178C standard, other available evidence addressing those objectives (Source: DO-178C-2011-12.3.4.2).

Confidence from prior use of embedded COTS software requires the service history including systematic and complete collection, reporting, retrieval and analysis of problems found in service. For each recorded problem, this includes the hardware/software configuration, the operating environment, the operating mode or state, the application-specific information needed for problem assessment, classification of the problem with respect to severity, safety and significance, and whether the problem was the result of a change in the software configuration (Source: DO-178C-2011-12.3.4.3).

Confidence from prior use of embedded COTS software requires assessment of the service history whether the individual problem was reproducible, recoverable, related to previously reported problems, including common causes. The chronological trend shall be evaluated with any increasing trend explained. Problems indicating process or safety insufficiencies shall be separated and corrections confirmed (Source: DO-178C-2011-12.3.4.3).

ESG appraisal: Requirements from avionics are similar, somewhat more stringent, and underpin the appraisal given above, that certification of pre-existing software, firmware or configuration data embedded in COTS parts is NOT recommended on the basis of confidence from prior use.

2.2.2.3 Architectural Hardware Requirements related to COTS

It is assumed here, that the EN50129 concept of inherent fail-safety is not suitable for complex subsystems as required to build the system. It is further assumed here, that the LCC of components heavily loaded with diagnostic functions to realize reactive fail-safety is high in comparison to simple parts. Therefore, the system shall not rely on inherent or reactive fail-safety principles. (Source: ESG w/ LCC requirement from SBB)

TL139: As a result, the system shall be composed from **multiple system channels** (called “items” in EN50129) with fail-safe comparison (meaning voting of results). (Source: Draft EN50129:2017 B.3.1);

TL140: To further reduce LCC, the system shall make use of hardware components with a low **probability of failure** per hour (PFH). It is assumed here that low failure probability means high LCC. (Source: ESG w/ LCC requirement from SBB)

TL141: To minimize channel (item) PFH targets (to approx. E-4/h in the first approach), and to consequently reduce LCC, the system shall have a HFT (**hardware fault tolerance**) of 2 or higher. *Note that IEC61508 gives no credit for systems with HFT>2, but justification seems reasonable.* (Source: IEC61508-2 and good engineering practice regarding PFH quantification)

TL142: It is assumed here, that less integrated **fault control** (including safe failure fraction SFF and diagnostic coverage DC) results in less LCC. The system shall therefore not rely on components with a high level of integrated fault control. (Source: ESG w/ LCC requirement from SBB)

Consequently, the system shall again have a HFT (hardware fault tolerance) of 2 or higher to minimize the necessary channel (item) fault control efforts. A second fault shall not be hazardous. (Source: Draft EN50129:2017 Figure B.2)

The system shall have a HFT (hardware fault tolerance) of 2 or higher to minimize the necessary channel (item) fault control efforts, especially the necessary safe failure fraction SFF and diagnostic coverage DC. A second fault shall not be hazardous. (Source: IEC61508-2 7.4.4+5 and Table 4)

It is assumed here, that certification by proof of sufficient confidence from prior use in similar applications may reduce LCC despite the fact that the safety argument is difficult to prove. It might be beneficial to use hardware channels (items) w/ **safe failure fraction** SFF as low as possible between 60% and 99%, to allow safety proof by confidence from prior use according to IEC61508-2. (Source: IEC61508-2 w/ LCC requirement from SBB)

ESG appraisal: Obviously, the main question on the architecture of the system is how much diagnostic coverage (DC) can reasonably be provided from the COTS supervision layer.

2.2.2.4 Diagnostic Coverage (DC) Considerations

This inserted ESG appraisal is to further discuss the diagnostic coverage (DC) identified before as being a key requirement for the system architecture and certification.

The IEC61508 industry standard considers a single channel decomposed from a more complex safety architecture as another safety (sub)system, with the related design rules to be applied "again". The standard's rules include requirements on the diagnostic coverage (DC), addressing possible faults within the hardware of the subsystem. It requires possible faults to be identified in the design phase, by means of both top-down and bottom-up methods (e.g. fault tree analysis and failure mode analysis). The latter method implies that both analysis and failure detection shall work down to component level.

The EN50129 railway standard has been derived from IEC61508 with the intention to tailor the requirements for railway applications. It can be assumed that IEC61508 requirements not explicitly modified, or missing, in EN50129 remain applicable and unchanged, unless there is sufficient justification. This "legal" interpretation would require the servers to be devices with a high degree of "detailed" diagnostic coverage. This coverage may be implemented as "inherent", basically meaning servers specifically designed for safety, which is in contradiction to SBB's COTS requirements, or "reactive", meaning that some diagnostic functions would work from outside the core server devices and cover a sufficient percentage of the possible low-level faults.

The "reactive" approach basically means diagnostic functions reside in independent devices closely "attached" to the servers (in practice probably: additionally, inserted into the server racks), and/or within an instance on the next higher level of the architecture (e.g. within the voting device). One possible approach for justification may come from EN50129's requirements on diagnostic functions to detect faults in integrated circuits, considering them applicable to servers as another species of "parts" with complexity too high to evaluate in all detail. The requirements may be interpreted as follows (refer to Table B.1 of prEN50129):

Considering a server as a "big CPU", failure modes (including static, dynamic and transient faults) of registers and internal RAM, instruction decoding and execution, program counter, stack pointer, etc., shall be covered by sufficiently fast and independent hardware comparison or mutual software comparison or voting between the servers. Considering today's performance of both servers and communication network, this seems feasible by kind of a lock-step-like operation of the servers. This can be implemented by introduction of numerous synchronization gates into the flow of calculations, therefore by software.

Considering a server as a "big CPU", the device's clock frequency and period shall be diagnosed by comparison and monitoring by a fail-safe independent item. Obviously, this is very close to hardware. Nevertheless, modification to servers to allow access to clock signals from outside may be a feasible approach, using "server-attached" dedicated hardware with external watchdog functionality.

Considering a server as a "big CPU", the hardware circuits intended to initialize a reset of the server shall be diagnosed. Sources of reset may be software (e.g. "traps" set on CPU level) and/or hardware (e.g. a hardware watchdog within the server, for example triggered by a circuit to measure the local temperature). It can be assumed that only minor modification would be necessary to extract or replace the required information from the hardware boards of a server. It should also be possible to initialize and hold the safe state of the server,

which is "no communication", from and by an "attached" external circuit, e.g. including a safety relay to cut communications.

Considering a server as a "big CPU", the power supplies shall be diagnosed with respect to voltage/current specifications and oscillation. While supervision of the main supplies for the servers will be straight forward from outside the servers, diagnosis of the server-internal supplies with the required reliability may again require small modifications to access the respective signals on the PCBs of the server.

Considering a server as a "big CPU", ROM and RAM shall be diagnosed by respective CRC, replication, RAM tests, etc., including coverage of soft-errors. Since independence is not required, standard low-level server software will do.

Summing up, smaller modifications to the servers, and "attachment" of dedicated diagnostic devices to the servers, seem a valid approach to consider servers as "big CPUs". One of the system design approaches detailed in this paper therefore includes such additional plug-on diagnostic devices to increase diagnostic coverage of the servers.

2.2.3 System Availability

TL143: 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.

ESG appraisal: The requirement needs additional quantification from operational point of view for the complete railway system to be covered. The system shall have a basic architecture similar to proven IT computer center architectures, with managed redundancy on various levels, since such centers satisfy similar demanding availability requirements.

Nevertheless, high availability basically means that the system continues seamless safe operation despite of faults. On overall system level, therefore the system will consist of at least two independent **locally diverse** centers. (Source: SBB)

Known buzzwords in the context of high availability are fail-operational characteristics, graceful degradation, self-healing capabilities. (Source: SBB w/ ESG interpretation)

Known **fail-operational** system architectures include the following MooN structures (M channels out of N channels are required to control the system into the safe state): 2oo3, 2oo4, 3oo4, 2*1oo2, and others. The requirement basically means a hardware fault tolerance of HFT>0. It is superseded by HFT=2 or higher requirements in this specification. (Source: SBB w/ interpretation from ESG)

Another requirement related to availability is **graceful degradation**. It basically means that multiple faults do not violate the safety targets. This can be by hardware fault tolerance HFT>2 and/or gradually reduced safety targets (e.g. by limitation of the operational envelope). The latter solution seems contradictious to the intention of the given fail-operational requirement. (Source: SBB w/ heavy interpretation from ESG)

It is assumed, that (only) some of the intended functions benefit from graceful degradation. Therefore, the system shall have HFT>2, and this shall (only) be a capability for individual functions. Note that independence is a resulting requirement and may be difficult to achieve. (To be refined. Source: ESG)

The system shall have **self-healing** capabilities. Self-healing basically means that the system activates the safe state of failed elements, and invokes spare resources (standby resources) with the same capabilities instead. The failed units will then be replaced and/or repaired while operation continues without degradation. The principle can be applied from overall system level down to the smallest line replaceable unit (LRU). (Source: ESG)

To support availability, the system shall include **standby subsystems**. The requirement includes the necessary failure detection and wake-up functions to invoke the standby subsystems. Hot standby and plug-and-play capabilities may be beneficial. (To be refined. Source: ESG)

2.2.4 System Architecture

TL144: Resulting from HFT=2 or higher, the system needs more than three **independent voted channels** (items). Possible accepted fail-operational architectures include 2*1oo2, 2oo4, 2*1oo3, 4oo6, and others. The system shall have at least four independent voted channels. (Source: Other requirements and Draft EN50129:2007 B.3.1)

Two **traditional architectural options** are at hand: The system, if with classical 2oo4 architecture, shall use COTS hardware channels w/ SFF>=90% for SIL4 capability (IEC61508-2).

The system, if with 2*1oo2 hierarchically structured architecture, shall use COTS hardware channels w/ SFF>=60% for SIL3 capability. It shall use individual voted channels with at least SIL3 capabilities (IEC61508-2 7.4.3.2-4).

Individual system channels (called items with EN50129) must have a failure rate of <2E-4/h (which is a level below SIL1), or detection of triple faults (Source: Draft EN50129:2007 B.9, B.3.5.2). System failure rates must consider the component's stress profile dependent on environmental conditions and the application (Source: Draft EN50129:2007 B.3.5.2).

The **voting** functions may be either hardware or software-based. Nevertheless, as a first approach for a possible solution, the system may have Railway-COTS SIL4 voting and hypervisor unit(s) (to be refined; ESG).

*Note that a **disruptive safety approach** is probably worth consideration, relying on a very high number of processing or storage instances working independently in parallel, with the majority of these many instances deciding on the results. The approach lacks known mechanisms to quantify influences from common causes (CCF). Nevertheless, the approach may be worth further investigation (Source: ESG).*

The system design avoids unnecessary complexity (Source: Draft EN50129:2007 Table E.3). *Since complexity mainly comes from diagnostic mechanisms, and not from an increased number of identical instances, this requirement calls for emphasis on multi-channel designs versus designs with high diagnostic coverage integrated (Source: ESG).*

The system's required hardware fault tolerance (minimum HFT=2) implies dedicated measures against **common cause faults** (CCF) (Source: Draft EN50129:2007 B.3.1, IEC61508-2 7.4.3.4). No multiple faults shall result from a common cause (Source: Draft EN50129:2007 B.3.5.1).

TL145: To reduce CCF, the system shall have technically diverse components or parts (Source: Draft EN50129:2007 B.3.1 1). **Diversity** may reduce the efforts to prove sufficiently small CCF (Source: ESG).

The absolute target quantity figure for CCF depends on the system architecture, and therefore on the specific design of the system. Nevertheless, with COTS in mind, only a small number of measures against CCF can be assumed, resulting in a low beta factor score according to IEC61508-6 Table D.1. Assuming a score of less than 45 for the logic solver, a 5% beta int factor seems reasonable. Applying IEC61508-6 Table D.5 gives initial targets for different multi-channel system architectures:

MooN		N			
		2	3	4	5
M	1	β_{int}	0,5 β_{int}	0,3 β_{int}	0,2 β_{int}
	2	-	1,5 β_{int}	0,6 β_{int}	0,4 β_{int}
	3	-	-	1,75 β_{int}	0,8 β_{int}
	4	-	-	-	2 β_{int}

Figure 5: CCF-Targets for Multichannel Systems IEC61508-6

For system implementations with a 2oo4 architecture, a beta factor of 0.6 times beta int can be assumed. The initial approach for 2*1oo2 would be the same, in both cases resulting in about 2.5% overall CCF as a reasonable target.

TL146: The system must be **fail-safe** upon single and multiple faults, within the specified safety target (Source: Draft EN50129:2007 B.3.4, B.3.5.1, Table E.2). The probability of further faults in other channels may be considered (Source: Draft EN50129:2007 B.3.5.2).

TL147: Detection time plus negation time shall be within the specified **safety target**. (Source: Draft EN50129:2007 B.3.4, Fig. B.4, B.5, Table E.2)

TL148: Further faults during permissible delay times to repair shall not cancel the **safe state** (Source: Draft EN50129:2007 B.3.4). Cancellation of a restrictive safe state shall be controlled by corrective procedure. (Source: Draft EN50129:2007 B.3.4)

*Note that the above requirements do not necessarily mean a requirement for a safe state for the components or channels the system is composed from, for example COTS components, if CCF are sufficiently covered. With the proposed 2*1oo2 architecture for example, the requirement may only apply for the root stage of the logic, with unsafe states of individual channels being masked by the voting mechanism (Source: ESG).*

2.2.5 Faults and Failures

TL149: The system has no hazardous single random hardware component failure (Source: Draft EN50129:2007 B.3.1). *Note that with multi-channel voted systems, only CCF are addressed here, and covered by other requirements (Source: ESG).*

TL150: Simultaneous faults in two items shall be non-hazardous (Source: Draft EN50129:2007 B.3.5.2). *This is trivial with HFT>1 and no CCF (Source: ESG)*

TL151: The top-down and bottom-up **failure analysis** of the system must make use of the dedicated failure modes from Annex C (Source: Draft EN50129:2007 B.3.1). *With non-railway COTS components, such analysis must be performed post-mortem, or another method argued (Source: ESG).*

TL152: The system must check all inputs (value ranges, electrical characteristics, time, consistency) (Source: Draft EN50129:2007 Table E.3).

*ESG appraisal: Since the data center's inputs are foreseeable all communication based, with protocols and black channel mechanisms applied, this requirement reduces to software functional checks (e.g. plausibility or range checks) on each and every information received from the communication system, and used for the respective safety functions. It is recommended to concentrate communication-related safety and security-for-safety measures in a dedicated **communication management layer**, and provide a generic respective API. Only application-related non-standard or additional measures shall reside within individual applications.*

TL153: The system detects and negotiates **single faults** before another such fault in a second channel occurs (Source: Draft EN50129:2007 B.3.1 1). *Note that "second channel" is meant literally, if the second fault is masked by a voting mechanism (Source: ESG).* The system detects and negotiates single faults within TFFR (Source: Draft EN50129:2007 B.3.1 1).

TL154: The system detects **dormant faults** (causing failure only conditionally) by periodical monitoring (Source: Draft EN50129:2007 B.3.1 1). 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 (Source: Draft EN50129:2007 B.3.5.2).

TL155: The SDT for hazardous **double faults** shall be less than 2 / sum of the individual failure rates (Source: Draft EN50129:2007 B.3.5.2). *This means the mean value of the two failures (Source: ESG).*

TL156: Detection of faults in integrated circuits compliant with Table B.1, using DC fault model (Source: Draft EN50129:2007 B.3.5.2). *Note: This relates to very common measures to cover CPU registers, internal RAM, instruction decoding, program counter, stack pointer, clock, reset, invariable memory, variable memory, and power supply. It is to be investigated how far typical IT COTS components adopt such measures, therefore detailed requirements follow below (Source: ESG).*

TL157: The system's components shall have CPU fault detection covering DC faults of registers, internal RAM, program counters, stack pointers, reset generators (Source: Draft EN50129:2007 B.1)

TL158: The system's components shall have memory fault detection for invariables (minimum 16bit CRC or block replication) and variables (Source: Draft EN50129:2007 B.1)

TL159: The system's components shall have power supply fault detection for supply of integrated circuits (Source: Draft EN50129:2007 B.1)

TL160: The system shall have **independent power supplies** for the channels (Source: ESG) w/ cross-channel comparison (Source: Draft EN50129:2007 B.1)

TL161: 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) (Source: Draft EN50129:2007 Table E.3).

TL162: 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. (Source: Draft EN50129:2007 Table E.3)

TL163: The system has monitoring and measures on **operating temperature** outside of specified range (Source: Draft EN50129:2007 Table E.3)

The system has protection measures on internal failures potentially leading to local temperature increase. It should have negotiation measures on such failures. (Source: Draft EN50129:2007 Table E.3). *Note that with safety hardware, temperature flow simulations are state-of- the-art. It is to be investigated if COTS components have similar design assurance measures (Source: ESG).*

2.2.6 Summary of Recommendations

The following condensed high-level requirements have been derived from the appraisals, to describe the very basic system characteristics, as a starting point for system architecture design:

- **TL201:** The system shall be regionally distributed for availability and for damage limitation
- **TL202:** The system shall consist of **server**, **storage**, **controller** and maintenance subsystems
- **TL203:** The subsystems shall include **software**, firmware and configuration data compliant to SIL4
- **TL204:** The servers shall be clusters of COTS IT servers trusted SIL3 (IEC61508)
- **TL205:** The storages shall be clusters of COTS IT storages trusted SIL3 (IEC61508)
- **TL206:** The maintenance subsystems shall be COTS IT terminal systems trusted SIL3 (IEC61508)
- **TL207:** The controllers shall be (clusters of) pre-certified railway COTS SIL4 systems (EN5012x)
- **TL208:** The controllers shall provide **hypervisor** functions to dynamically invoke servers and storages
- **TL209:** The controllers shall support **virtualization** functions to dislocate execution of functions
- **TL210:** The controllers shall manage **redundancies** and stand-by operations of servers and storages
- **TL211:** The controllers shall **vote** hypervised server or storage outputs with HFT>2
- **TL212:** The controllers shall vote intermediate results of server calculations with HFT>2
- **TL213:** The controllers shall **supervise** servers and storages with diagnostic coverage for SIL3 (IEC61508)
- **TL214:** The controllers shall provide watchdog supervision of servers, storages and environment
- **TL215:** The controllers shall supervise unused software, firmware or configuration data within COTS devices
- **TL216:** The controllers shall provide black-channel **communication** services
- **TL217:** The servers shall provide **encapsulation** of application functions and OS
- **TL218:** The servers shall provide **virtualization** of resources for execution of application functions and OS

2.3 Certification Process

2.3.1 Railway versus other Industries

As shown in preceding chapters of this document, the most demanding aspects of certifying the system to SIL4 relate to COTS subsystems and components.

The railway industry prefers “trusted” long-term procurable parts already used in very similar applications. As a result, certification would focus on availability and/or accessibility of reference applications and justified MTBF quantitative figures derived. Certification would require significant analytical and reverse engineering efforts, and use in a configuration already known as sufficiently robust. Provision of the necessary evidence would require in-depth insight into manufacturer’s processes and technical concepts applied, thus making close cooperation with the respective manufacturers a must.

The railway industry clearly prefers multi-channel architectures with adequate diversity applied to counter common cause failure effects. Limitation to “trusted” parts will limit the possible LCC-savings intended through re-use of COTS components.

Railway certification means close co-operation with certifying authorities, notified bodies, etc., from the beginning.

Since COTS parts in similar applications are hard to find, and due to the limited LCC savings expected, it is worth considering a different certification approach:

The general automation industries prefer "intelligent" parts, with a high level of diagnostic coverage. This may mean increased initial effort but nevertheless reduced LCC. This approach is especially visible with automotive industry products, which share this approach for parts-cost reasons. As a result, these applications require parts with high safe failure fraction (SFF) and integrated diagnostic coverage (DC). Nevertheless, safety assessment requires close insight into the equipment, and therefore close cooperation with the respective manufacturers.

General industry certification does not require any involvement of authorities, and the manufacturer remains self-responsible for product safety. Nevertheless, certification with regard to a certain safety standard, e.g. IEC61508, is common, and some certified SIL3 capable products exist. For general industry safety applications, SIL4 composition from SIL3 certified parts is common, possible and defined, resulting in a number of available products being in principle capable of SIL4 in composite architectures. It is possible, while not yet very common, to cross-certify such industry products for railway applications.

The IT industry has obviously adopted "the best of" both approaches: Data centers are highly redundant and have a very high degree of inherent diagnostics to keep the system available without service interruption. Therefore, the existence of components with very high diagnostic coverage is a fact, and the use of such components for certification seems very promising.

As an alternative or addition to integrated diagnostics, addition of non-COTS diagnostic hardware and software is possible to run diagnostic functions from outside the COTS parts used. Although already far advanced and common standard in COTS-components for the data center industry, not all parts necessarily provide the high

level of “remote” diagnostic capabilities necessary. Again, close co-operation with manufacturers is unavoidable and should be started early.

The resulting certification strategy therefore includes early involvement of both certification authorities, preferably with known capability for cross-certification, and manufacturers of widely used IT COTS parts.

2.3.2 Layered Safety Approach

Considering LCC, the use of COTS parts is most efficient for elements of the system architecture which are present in larger numbers within the computer center, namely servers and storage devices. Such parts shall be COTS, pre- or cross-certified for railway use either SIL0 (if the railway based certification approach is used) or SIL3 (if the recommended layered hardware architecture and industry based certification approach is used). As the RCDC is purely a railway data center, the use of the railway is recommended and thus the use of SIL0 equipment encouraged.

For parts used less numerously within the system, e.g. for the safety layer, supervisor, hypervisor, and health monitoring functions, LCC allows use of semi-COTS SIL4 units, providing the major part of the required diagnostic coverage. To provide the remaining necessary diagnostic coverage for the COTS parts, non-COTS diagnostic add-on devices may be necessary, depending on the certification approach and available COTS parts, attached to servers and storages. Nevertheless, some modification to COTS servers or storages may be required.

The resulting certification strategy therefore includes early pre-certification (modular certification) of servers and storage devices, to determine the possible certifiable diagnostic coverage provided from the safety layer and/or attached diagnostic devices.

2.3.3 Software Certification

The second certification step would address the software and firmware layers needed on SIL4 software safety integrity level, including RTOS and safe separation/virtualization. Cross-certification from IEC61508 may be an option. The SIL4 supervisor, hypervisor, health monitor, etc. software will need newly developed software, which can be designed for modular certification from the beginning. Since this software makes up most of the safety mechanisms found in the overall system, it is recommended to start early with development and certification. Note that parts of the SIL4 qualified software or firmware resides on the COTS parts, and must therefore also be developed specific to the selected devices, and most likely new from scratch. Again, modular certification should be feasible.

The already existing various applications will remain on the respective given SIL, managed and separated by the SIL4 layer. Nevertheless, some porting efforts, and respective re-certification will be necessary. The porting efforts heavily depend on the fundamental approaches selected for, or with impact on, safety, e.g. sequential versus parallel computing, stepwise synchronous mutual diagnostic comparison, asynchronous app-to-app versus synchronous inter-application communication, etc.; it is therefore recommended to early decide on those mechanisms. Also, early effort should go into software architecture, for example building on standard interfaces for basic services like

- Predictable, deterministic and timely transport of messages
- fault-tolerant clock synchronization
- strong fault isolation
- consistent detection of failing nodes, etc.,

and, based on these basic services, high-level services like

- encapsulation service
- virtual network service
- hidden gateway service
- fault tolerance service
- diagnostic services, etc.;

2.3.4 System Validation

A main problem of safety certification for software is providing verification and validation evidence. The process of building evidence involves much effort in testing, especially if path coverage or decision coverage is mandated by the certification authorities.

In case of the SBB Rail Control Centre there is an existing reference system, which is able to provide reference data for verification, it also provides a reference behavior, that allows to compare calculated results with an actual behavior that is qualified as safe.

This reference system, can be used in a transition phase, e.g. in the process, while the infrastructure related to the SBB Rail Control Centre is being built, to test parts of the application software, such as safety monitors or even the actual functions.

2.3.5 Incremental Certification

In avionics there is a guideline for incremental certification, which is RTCA DO-297. This guideline is based on the independence of hardware and software development, which is a main characteristic of an IMA architecture as well as of a data center architecture. A main problem of safety certification for software is providing certification evidence. The process of building certification evidence involves much effort in testing, especially if path coverage or decision coverage is mandated by the certification authorities.

In case of the SBB Rail Control Centre there is an existing reference system, which is able to provide reference data for verification, it also provides a reference behavior, that allows to compare calculated results with an actual behavior that is qualified as safe.

This reference system, can be used in a transition phase, e.g. in the process, while the infrastructure related to the SBB Rail Control Centre is being built, to test parts of the application software, such as safety monitors or even the actual functions.

2.4 The Need for a Certification higher than SIL 4

Depending on the final design of the RCDC Network, a safety breach may have significant impacts on the overall SBB-rail system. The damage will be maximized, if the total system would be controlled from one or two centers only and be diminished by the use of more locations and separation of the whole network into substructures.

The safety aspects of a breakdown of a complete (countrywide) network is out of scope of all current specifications. SIL4 does not cover such a scenario in any way, proposing the introduction of higher levels of certifications. Similar (initial) considerations exist for nuclear power plants, but are not far developed.

At this point no specification of this kind is in existence or in preparation, although some discussions have been started. Therefore, a consideration of a higher level than SIL4 is nor possible neither recommended for the foreseeable future.

2.5 Overall Characterization of the System to be built

Following its description in the preceding section, the SBB Rail Control Centre (RCDC) can be characterized as follows:

- It provides a scalable processing platform,
- it hosts virtualized applications, i.e. applications which are separated from hardware in a way that makes the individual software components independent of individual software components,
- it provides scalable storage resources for holding the state of the SBB Rail System and other application data,
- it provides an interface to the SBB Traffic Management System,
- it provides an interface to all the Object Controllers, which are available for executing control over the SBB Rail System,
- processing provides safety guarantees in accordance with SIL4 requirements,
- storage of data provides safety guarantees in accordance withSIL4 requirements, and
- very high availability of Rail Control function.

In addition to these characteristics SBB has a number of targets it intends to accomplish with the SBB Rail Control Centre:

- The top aim of building a SBB Rail Control center are cost savings by rationalizing the LCC-costs of the SBB Rail System
- centralized operation: distributed devices of the rail system shall be centralized into a single (logical) platform
- integrated function: distributed functions shall be integrated into a common function,
- scalability: the SBB Rail Control Centre shall provide the capability of scaling processing and storage resources in accordance with actual needs.
- upgradability: due to the different life periods of hardware and software assets, they shall provide a degree of independence that allows hardware or software components to be exchanges independently from each other. The term “Technology Transparency” addresses the same intent of saving long-term investment, while following the demands of technological evolution.
- modularity is a consequence of scalability and upgradability,

- V&V support: as the biggest expected effort is providing evidence for safety, built in support for V&V is of paramount importance for the success of this effort,
- independent certification of components is required for the operation of such a data center,
- parallel operation at different safety levels is a useful feature.

3. Safety and Security: Definitions and Overarching Properties defining the Architecture

3.1 Overview and Terminology

The project will have to be built in an environment which is currently dominated by specially developed and built systems. Current safety systems are mainly built as embedded systems in all industries including avionics and the automotive sector. The systems of the “embedded world” use several terms in a different way than they are used in the “data center world”.

There is a generally different philosophy to be observed in these two worlds. While in the embedded world the functions are concentrated in one block, regarding HW and SW as a combined functional unit, the data center world considers HW, FW and the SW to operate this combination only as a platform and resource, which is to execute the application in the anticipated way and can therefore be exchanged as seen fit.

This philosophy has been generally adopted as “Virtualization” and is today’s basis for every professional data center. The concentration on the software and many security and operational aspects have also promoted another architectural step – to virtualize the storage as well, storing besides RAM no data on the processors/servers, which are not necessary for the current process step.

Therefore, the nomenclature varies significantly and leads to continuous misunderstandings, if not defined in the beginning in a generally accepted manner. If possible, the understanding of the railway industry is used throughout this study, however several terms of the data center terminology have no equivalent in the “embedded world” and must therefore be understood in the correct way.

Additionally, the design methodologies - and thus the architecture of a data center or embedded device - differ significantly. Based on the properties of embedded systems, the functionality must be implemented under certain constraints, like limited power and space requirements, high reliability, low weight, high data processing rate, and directly linked into the system design of the respective vehicle or machine. This causes an engineering process to optimize the unit according to these constraints.

Data centers have other priorities. Power and space requirements are of secondary importance. Reliability is achieved by the installation of several hot standby components, which can be immediately activated when the need arises. Parallel processing and virtualization are used to achieve high processing speed. As most data centers have direct contact to other networks, security aspects are of the greatest importance, as well as the validity of all data, which is multiply stored in numerous devices and other data centers. Ciphering of data also guarantees the validity thereof.

3.2 Requirements on Availability and Time-to-Repair (TTR)

Availability is a percentage figure to describe the availability of the service. In order to achieve high availability a high tier-level of 3, or better 4, is a necessary basis alongside virtualization, as any interruption of service – planned or unplanned – reduces the availability, which is usually guaranteed to the customer of the data center. In the table below this percentage value is transferred in hours/minutes of maximum guaranteed downtime.

Availability (in %)	Minimum expected operating time (hours per year)	Maximum permitted downtime (hours per year)	Maximum permitted downtime (hours per month)	Maximum permitted downtime (minutes per year)	Maximum permitted downtime (minutes pro month)
100,0000	8760,00				
99,9900	8759,12	0,88	0,07	52,56	4,38
99,9500	8755,62	3,50	0,29	210,24	17,52
99,9000	8751,24	4,38	0,37	262,80	21,90
99,7000	8733,72	17,52	1,46	1051,20	87,60
99,5000	8716,20	17,52	1,46	1051,20	87,60
99,0000	8672,40	43,80	3,65	2628,00	219,00

Figure 6: Availability to permitted downtime in a data center (Samples)

In virtualized data centers, a HW fault is corrected immediately by transferring the task to a spare resource. As this consumes resources out of the pool, a repair or replacement service is required. Therefore, the MTTR remains important as it restitutes the original condition of the spare pool of resources.

Mean Time to Repair (MTTR) is a basic measure of the maintainability of repairable items. It represents the average time required to repair a failed component or device. From a logical point of view this repair is complete if the component is active and the pool brought back to its original capabilities. Therefore, in data centers no differentiation is made between MMR and the Meantime to Return Service (MTRS).

Expressed mathematically, it is the total corrective maintenance time for failures divided by the total number of corrective maintenance actions for failures during a given period of time. It generally does not include lead time for parts not readily available or other Administrative or Logistic Downtime (ALDT).

In fault-tolerant design, MTTR is usually considered to also include the time the fault is latent (the time from when the failure occurs until it is detected). If a latent fault goes undetected until an independent failure occurs, the system may not be able to recover.

3.3 Multichannel Architecture with Voting

To achieve the target figures for SIL4, a multichannel architecture with voting is necessary.

Several processors (embedded world) or SW stacks (data center world) receive the same input data and process it in parallel. The expected results should be identical. A further, independent processor with the classification SIL4 compares the results.

If the results are identical, the output data is true. If the results are not identical, there is a decision necessary, whether output data

- is classified false, with repetition of the process step considered necessary (data center world)
- is classified false, with a safe state of the respective server necessary (embedded world)
- is the result of the majority and therefore true (data centers typically use 4 channels to vote)

Details on possible voting models and decision principles are depicted in chapter 6.

3.4 Use of the Terms „Security and Safety"

These terms are used in a completely different way in the embedded ("railway") world and in the data center context.

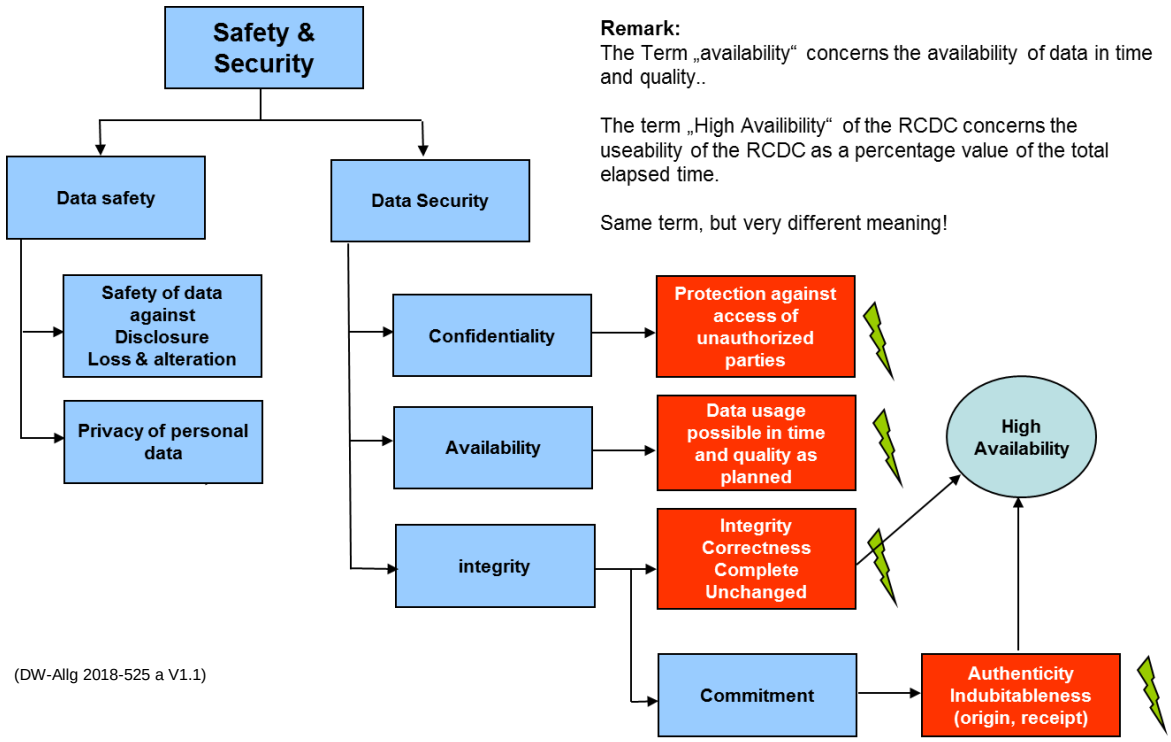


Figure 7: Data Safety and security according to BSI-Standards

Therefore, the understanding in the different worlds is as follows:

Railway: *Safety* is used to describe the absence of potentially dangerous faults or failures. Safe equipment is expected to do exactly what it is intended to, guarantee the quality of the results via various methods and checks and will not deliver a corrupted or wrong output or command which may create any danger for the user or the controlled equipment.

Data Center: Data *safety* means that the data processed is not falsified and will not be altered or lost during the process or in other way abused by unauthorized parties.

Railway: *Security* is seen in the immediate context of safety ("security for safety"), often reduced to physical security such as unauthorized access.

Data Center: Data *Security* is the overarching task in all IT processes. It consists of

- Data confidentiality/privacy

- Data availability
- Data integrity
- Data commitment

Therefore, any activity which may have an impact on these tasks are security issues, such as, but not limited to, hacker attacks, introduction of malware and viruses, data theft and identity theft.

In the case of the RCDC any (data center world) security issue may cause an immediate safety issue in the railway understanding of safety. Therefore, considerable efforts are necessary to protect the data center against such attacks. This is further discussed in this document.

3.5 Use of the Term „Architecture"

This term is used in a completely different way in the embedded ("railway") world and in the data center context. The reason for that discrepancy is the completely different structure and deviating strategies in the two worlds to achieve similar targets.

In the embedded world "architecture" applies to the hierarchical structure of the system, hardware down to function blocks, and software down to modules. The typical embedded architecture does not show any additional layered logical structure but few enabling basic functions to support applications, which may work in parallel to process data. Therefore, the architecture describes HW and SW up to the application layer and their interaction.

Subsequently the target of the "embedded" architectural process will be to create a SW structure on a (given) HW to fit the requirements. Broadening the basis into an overall system design with several HW systems is possible and is normally achieved by distributing tasks on different platforms. Although not impossible, clustering several units into a virtual system pool is not very common.

If HW faults occur, if not simply switching off, the usual method to compensate this fault is to activate a (hot) standby unit to take over the task of the faulty item.

In data centers the term "IT architecture" refers to all static and dynamic aspects of IT in an organization.

These include infrastructure (hardware, locations, networks), software (applications), technologies, interfaces, IT-supported functions and processes, and the associated architecture management (configuration and capacity planning, load balancing, data backup, availability, resilience, disaster planning, etc.).

Typically, HW and SW are decoupled via a virtual layer. All or groups of HW form pools of resources, controlled by a hypervisor. These resources are dedicated to SW stacks of the applications. Parallel processing is the standard procedure. If further processing power is needed, further virtual SW stacks will be activated, if necessary supported by widening the resource pool usage.

If HW faults occur, the usual method to compensate this fault is to move the application stacks from the faulty resource to another virtual resource without delay, usually without loss of data and in very short time.

The IT architecture of a data center describes IT in an organization on two levels: it defines the basic structures and sets rules that coordinate the dynamic interaction of all components, whereas components are understood to be independent complete units, consisting of HW and SW.

Both architectural approaches have pros and cons for the intended task. In the following chapters in this document their usage in the RCDC will be discussed. The terms applicable for the data center world will be used.

4. General Security and Safety architecture: A layered approach

Data centers concentrate the technical systems in a few places with high functionality. While this is very advantageous from a technical point of view and also provides other advantages like cost reductions, the security of the system provides a significant impact on the system. Flaws or compromised security have an immediate impact on the safety of the system. This also holds true for the fact, such undistributed locations will become prime targets for external attacks, be it physically or on the cyber level. Technical faults will cause much higher damage and compromise security, if not countered by a structure's design and respective countermeasures.

Therefore, considerable efforts have to be undertaken in order to reduce these impacts. A generally accepted principle is the Shell Model.

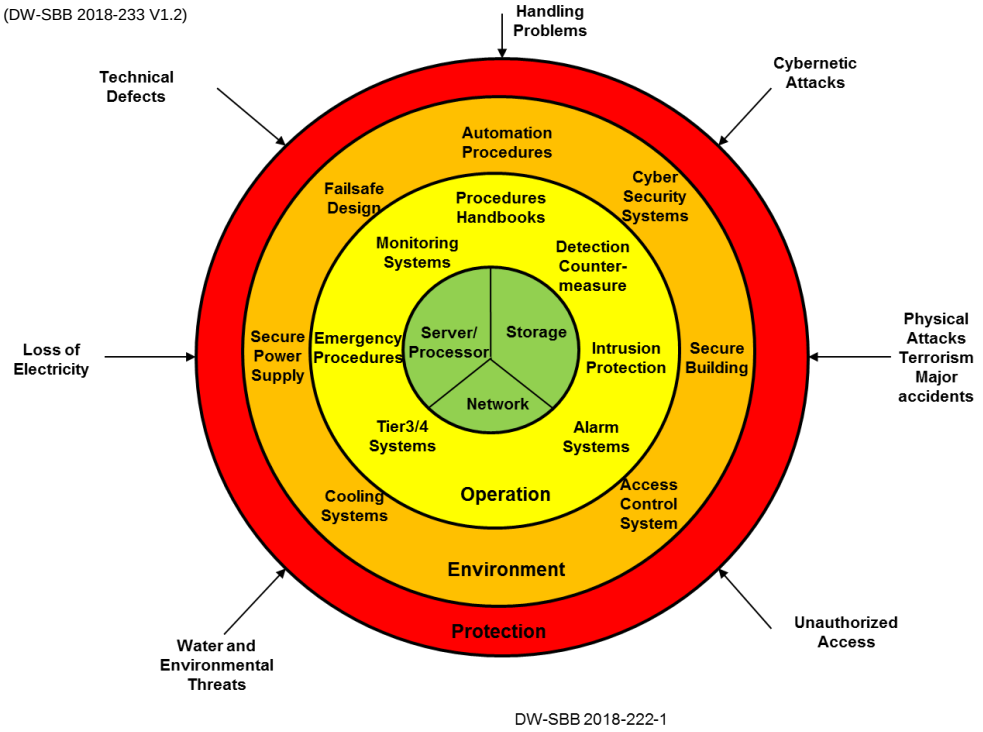


Figure 8: The shell model of a data center

As it is easy to understand, the outer shells protect the inner core. Data processing is only carried out in the inner core. All remaining activities support and protect the inner core. As a failure of these services has a direct impact on the functionality they contribute to the safety of the overall system, if designed in the right way.

Even the international standards state clearly that it is impossible to separate these functionalities completely. Therefore, highly in-depth checks and permanent tests compensate for shortfalls of elements in the inner core, which may have a limited reliability.

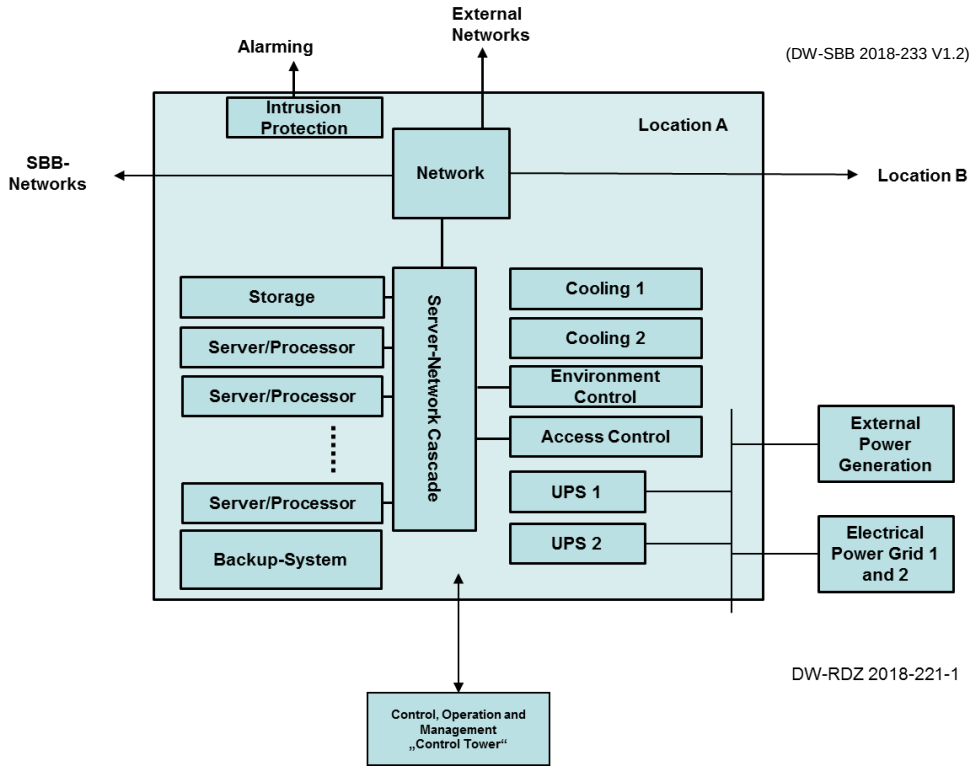


Figure 9: Physical Infrastructure for a safety critical datacenter

4.1 The Classification (Tier-) System of Data Centers

The infrastructure of data centers is classified by a 4 Stage System originally derived from TIA, better known as Tier 1 to Tier 4 systems. It follows the philosophy to increase system safety by the use of multiple systems of similar functionality but lower reliability to provide highest availability and stability. In simple terms this leads to structures with systems on standby to be activated in the case of need or to operate in parallel with enough capacity for every system to compensate failures in the parallel system.

Every system therefore provides the full capacity to operate the data center and can cope with complete failure of the parallel system components. It is applied to the physical infrastructure as well as for IT hardware in the data center.

Besides higher safety and stability this also allows maintenance of system components during operation without the need of deactivation of the system.

The different Tier grades differ in the amount of paralleling functions.

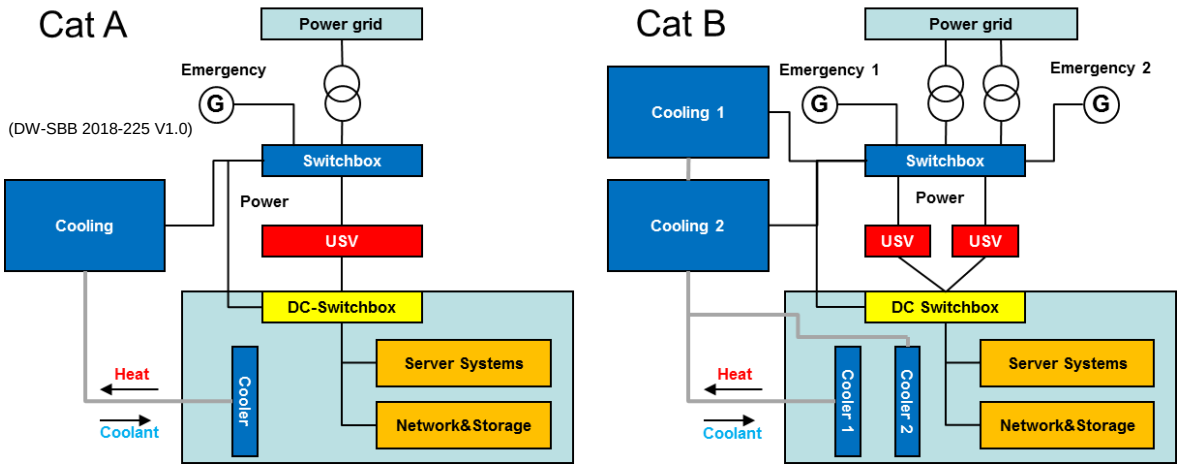
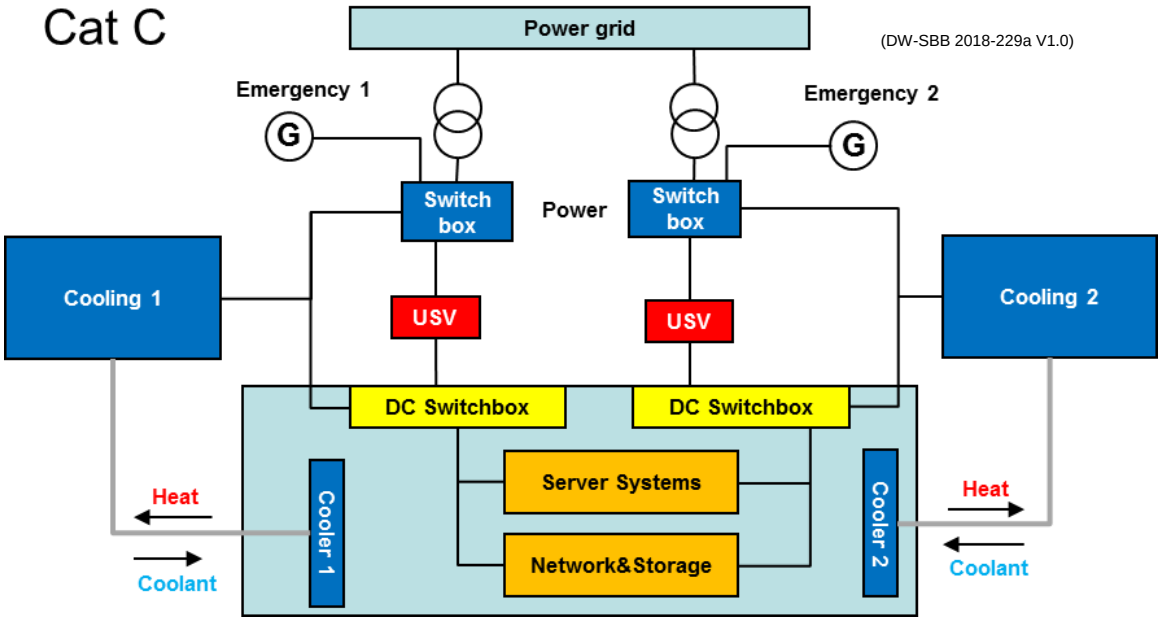


Figure 10: Physical Infrastructure Tier1 (Class A) and Tier 2 (Class B

These low Tier classes are not suitable for data centers requiring highest reliability and/or safety critical functions.



..

Figure 11: Physical Infrastructure Tier3 (Class C)

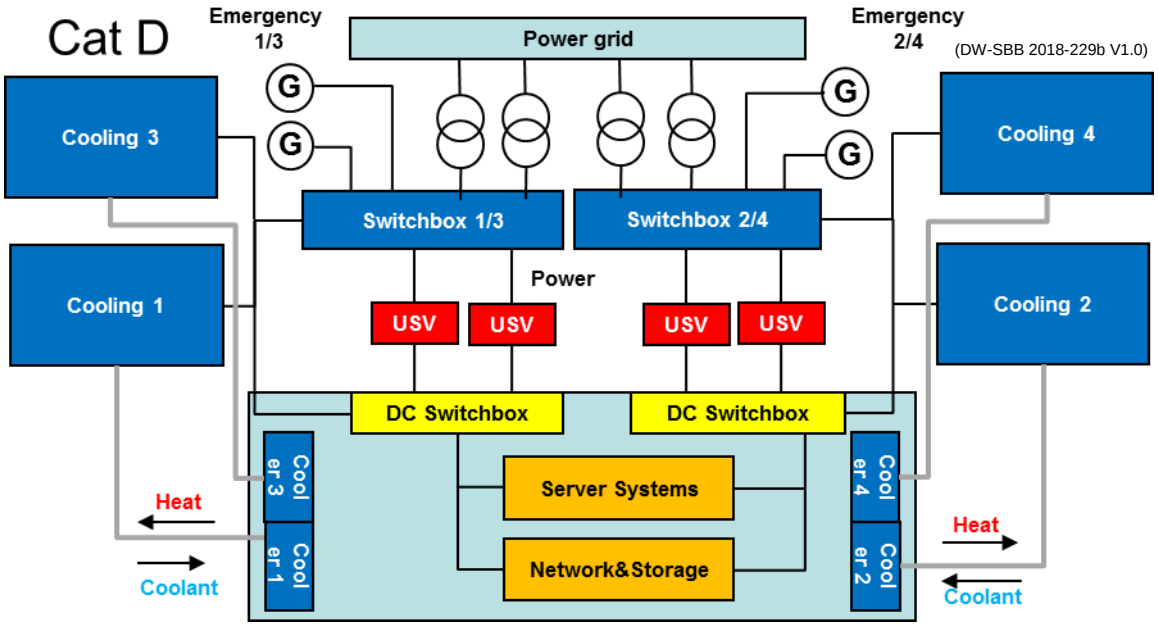


Figure 12: Physical Infrastructure Tier 4 (Class D

Only Class C and D provide no single Points of Fault. Therefore, this requires the data centers to be built in that way to cope with SBB's reliability requirements.

4.2 Control and Monitoring

The requirements for reliable data centers make it mandatory that all functions are permanently checked and tested and in the case of malfunction, countermeasures are immediately activated to compensate for the malfunction. Additionally, numerous parameters have to be checked permanently to recognize developing problems prior to the occurrence of real malfunctions.

This system is not limited to the physical infrastructure, but applies in a similar way to all IT equipment, like servers, switches, firewalls, storage systems, networks etc. They are checked permanently on their performance, network traffic etc. to create alarms, to activate countermeasures and to create operational data to operate the data center in the best possible way. All data is stored in logs to be used at a later date for evaluation.

As a minimum, the following features are necessary:

- Automatic monitoring of all essential parameters of power supply and cooling and the respective devices
- Status messages about temperature, humidity and correct double power supply at each rack
- Status messages on emergency power supply, tank contents and "Ready" messages
- Intrusion detection in the event of unauthorized entry or opening of doors, video systems for monitoring server rooms

- Fire protection systems

Furthermore, IT systems are often built at remote locations on the factory premises. This means that they must be able to be monitored and controlled from a security center or an IT control station 24 hour a day.

All these functions are concentrated in a “Data Center Control Tower” which automatically monitors all functions of the RCDC and creates responses and countermeasures. They may be:

- Automatically activated countermeasures without human interaction. Examples for such an activity may be to activate a hot spare unit as replacement for a unit which developed problems or the use of resources of the virtual pool to satisfy the actual demands.
- Creation of alarms to alert security personnel in the case of functional or security issues to proceed in accordance with a predefined process
- Create a master alarm to inform IT personnel about problems which need immediate action
- Start an immediate predefined action in the case of safety issues
- Deactivate the RCDC in the case of catastrophic failures to avoid any further damage.

An extensive system of that kind creates a significant impact onto the SIL capability of such a data center, since it compensates for shortfalls in single components.

4.3 Building and Access

The building or container offers protection and demarcation. An appropriate structure reduces the impact of interference and even physical attack.

As a minimum, the following features are necessary:

- A suitable location in the company, without public traffic and with as few impact hazards as possible, e.g. by moving trucks
- A suitable external wall against environmental impact, but also against bombardment and explosions
- An electronically controlled access system,
- A subdivision of the rooms according to tasks: Server room, telecommunications, physical infrastructure, battery compartment
- A suitable door with a burglar alarm system to prevent unauthorized intrusion
- No windows to prevent intrusion, and avoid the entry of dust, dirt and water

Generally applicable processes, procedures and specifications contribute significantly to reliability. As a minimum the following rules are mandatory:

- Any change in the IT system is subject to a change process with approval procedures.
- Access is limited to the absolutely necessary level and is recorded.
- Regular inspections and maintenance are carried out and recorded.

- External employees only enter IT areas under supervision.
- The IT system is documented, changes are immediately updated.
- Fixed requirements for the use of IT are available and proactively enforced.

4.4 Electric Supply

Even short-term power outages do not only lead to operating failures, but can also result in destruction of data and destruction of data bases.

Therefore, significant efforts must be invested into a safe and secure as well as a stable power supply. As a minimum the following features are mandatory:

- Own and several directly routed power supply lines directly from the main distributor with independent switching and protecting measures.
- Power filtering against electrical noise, ideally by using UPS systems.
- A further independent power supply, e.g. from an emergency generator with automatic activation in case of failure of the first power supply or a second electricity provider.
- Buffering of the power supply with battery-based UPS systems for a minimum operating life of 15-30 min.
- Double cable routing for every rack to be connected to the main distribution systems.
- At least doubled power supplies for every unit.

4.5 Cooling

IT systems transform practically all the supplied electrical power in heat. As a result, the components heat up quickly and need to be cooled externally. Failure to meet this requirement leads at least to the self-shutdown of the components, but can also lead to their destruction.

Therefore, cooling is of the same immediate importance to a data center as the electrical energy supply. As a minimum the following features are mandatory:

- Doubled coolant generation with heat exchanger outside the building
- Heat exchangers in the racks, arranged in such a way that heat nests are safely avoided
- A suitable concept for air guidance for ventilation of all heat-producing systems
- Temperature, humidity sensors and control systems, automatic coolant monitoring
- Sufficient power to completely shut down individual components of the refrigeration generation for maintenance purposes and remove them from the system
- Appropriate design is mandatory. Oversizing may lead to high temperature fluctuations in the coolant network

5. Overall Design of a Data Center

Based on the documentation listed in chapter 1, a rough design of the data center structure is now possible. Based on the BSI- recommendations, the safety requirements and all infrastructural und security considerations, a minimum of two independent centers in a georedundant setup are required. To avoid damages in the case of catastrophic accidents and occurrences, a minimum distance of 5-7 km between the two locations is recommended. To be able to synchronize data within a reasonable latency, a maximum of 60 - 100 km (length of interlinking cables) must not be exceeded. In the following, the two locations are identified by location A and B.

Assuming two locations, a well-developed cluster fulfills at least the following requirements:

- At least two sites have the same complete data base
- All necessary applications are available at both locations
- Doubled network spaces switch the connections between the sites and the users as needed,
- Virtual techniques simplify operation, increase safety and reduce costs

Georedundancy is a very effective element of security, but also the most expensive. Detailed planning of the functions and their distribution is required.

Under the given constraints, the use of multiple sub centers dislocated within Switzerland does not show advantages, but complicates data transfers and synchronization. It may be worthwhile to establish sub centers to maintain operation in geographically limited regions.

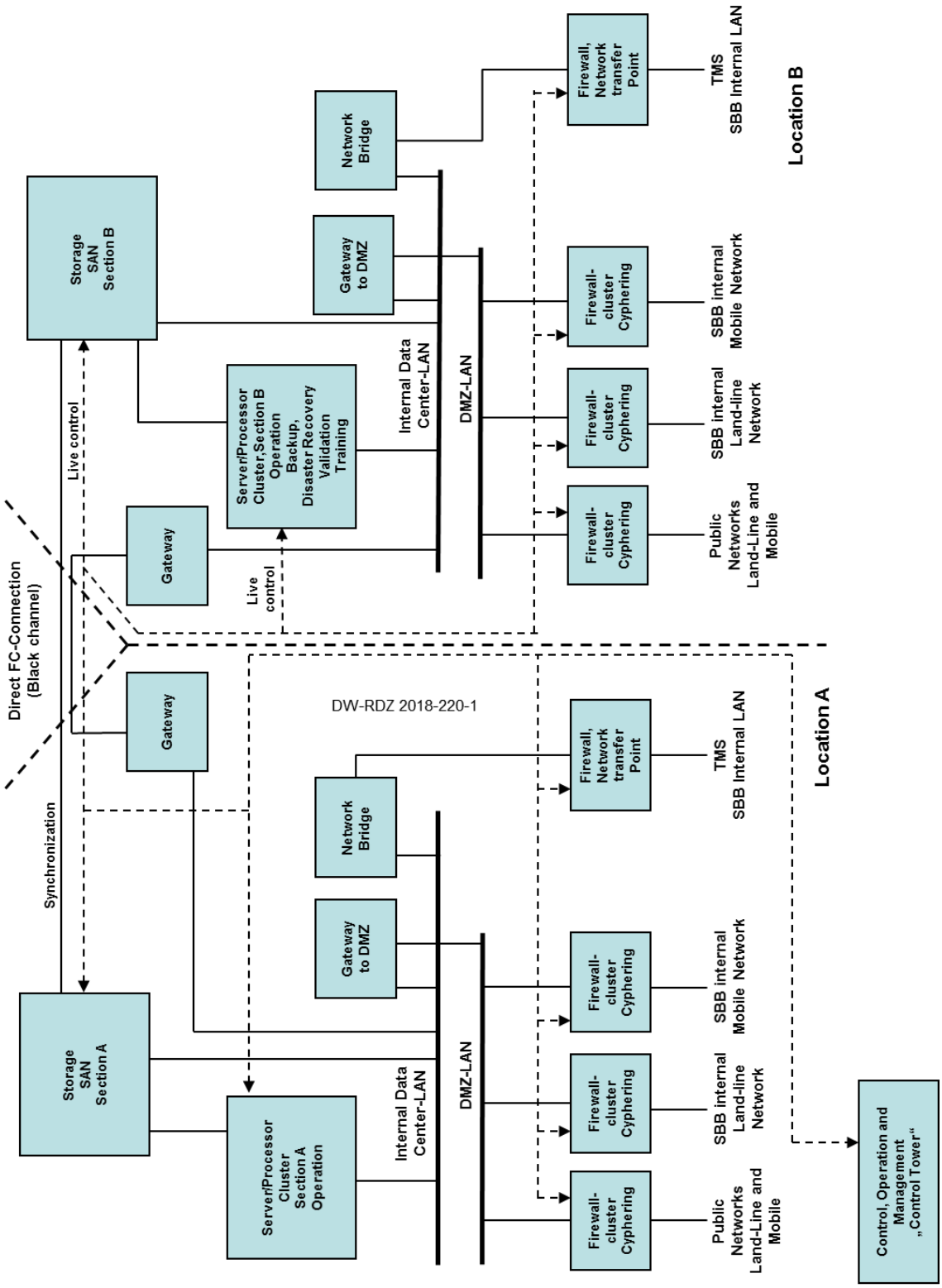


Figure 13: Rough Design for a data center Network

5.1 The System Components

The HW to be selected, such as server systems, mainframes or embedded system clusters, will not have any impact on this rough design as this design does not yet distinguish between different technologies or products, but lists only functional components.

As shown above, there are several components of the system that work together to fulfill the expected task.

No	Name	Comments and Function
1	Storage system	Dislocated between at least two geographical locations Stores all data in at least duplication, stores all applications, executes backup
2	Server/Processor Cluster	Processes all data with respective applications, by means of virtualization, embedded systems etc.
3	Gateways	Interconnects networks at one or more locations with limited filter functions
4	Network bridge	Router functionality to interconnect only defined systems within SBB with each other
5	DMZ	Interconnects networks with strict filter functions and cybernetic protection against viruses and other attack from public networks
6	Firewall Cluster	Interconnects the system with external components (actuators) with the use of tunnels and cyphering to avoid introduction of falsification of data and attacks from public networks
7	Control Tower	Manages, controls and checks permanently all components of the system, including the status of compromitation
8	Network	Interlinks via numerous virtual networks the different components of the system in a hierarchical manner under full control of the Control Tower

5.2 The Role of an Independent Storage System

To achieve the target to have no any dependency from HW, all data must be removed from the processing components. Data should be securely stored in an external Storage system. Only data necessary for the current task is stored in the processing function and returns the data into the main storage system. This has numerous advantages:

- The raw data is available at any time for processing at any processor resource. Therefore, processors can be used to the best extend at any time.
- Results of a process step are stored and can be used at any time for parallel processing or voting.
- XooU can easily be conducted by numerous processors processing the same raw data independently as basis for the voting process
- Should one processor become faulty, the process step can be reexecuted by another processor based on the same raw data
- Applications have always the latest status in the storage system and as the processors download their application from that source, the processing will always be executed with the current application version.
- Fault analysis is easily possible, as this principle allows an offline step-by-step analysis

However, this imposes on the Storage system very high requirements in respect to data validity, reliability and automatic fault correction and fault tolerance.

Modern storage systems are multiple redundant:

- As highest level such storage system work georedundant via at least two independent locations
- All processors, switches and data carrier are for themselves at least in RAID5 configuration redundant und allow hot swap for all components

The attached drawing shows as a sample a MetroCluster structure of Netapp-system. However, all similar products like EVA and Digital Domain work according to the same principles. So, this drawing illustrates only the numerous redundancies provided by such systems.

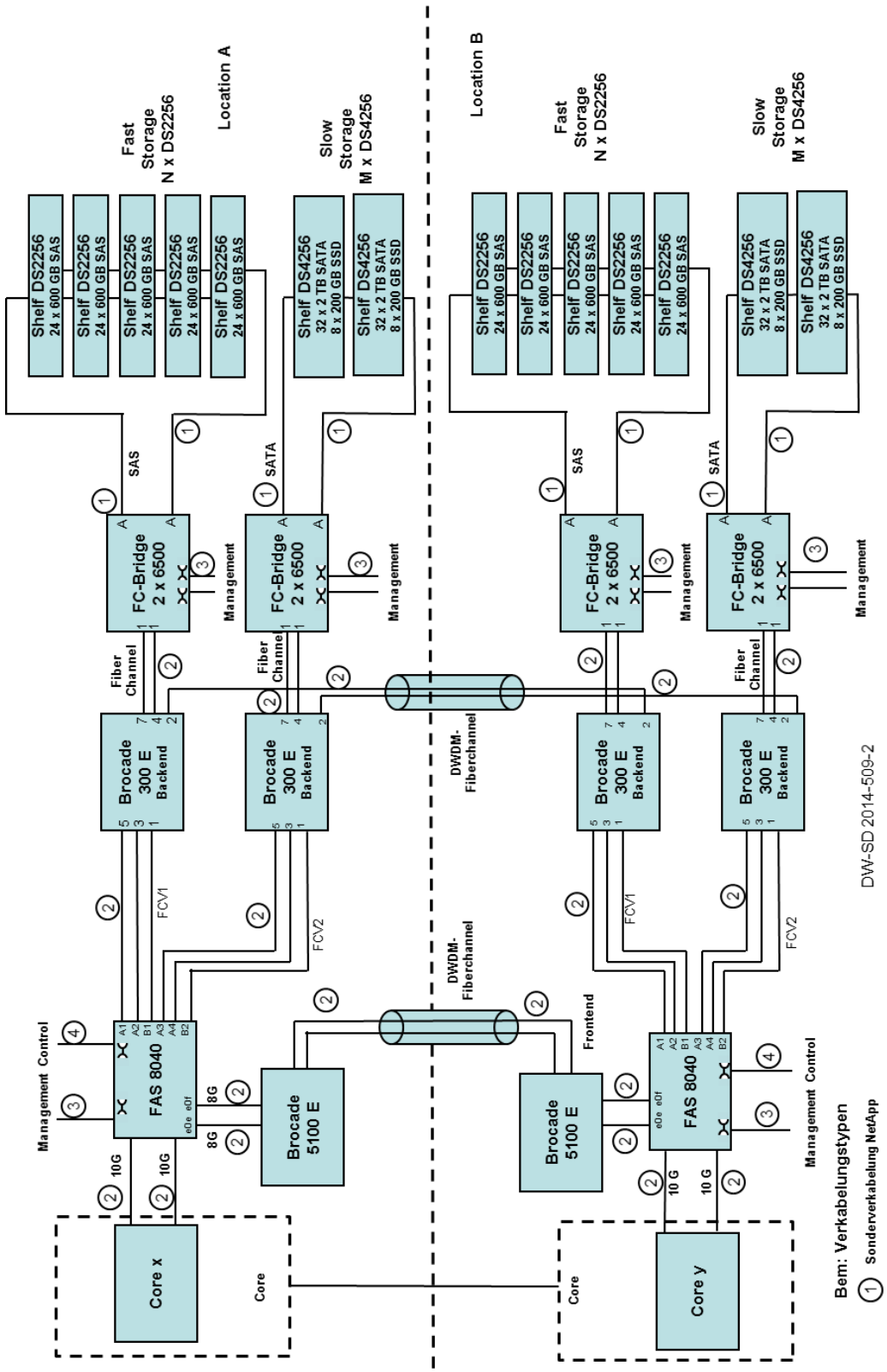


Figure 14: Redundancy in a MetroCluster

5.3 The Role of Hypervisors

A hypervisor is computer software, firmware or hardware that creates and runs virtual machines. A computer on which a hypervisor runs one or more virtual machines is called a host machine, and each virtual machine is called a guest machine. The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources. This means that, for example, Linux of different versions, Windows of different versions, and macOS instances can all run on a single physical machine. This contrasts with operating -system -level virtualization, where all instances (usually called containers) must share a single kernel, though the guest operating systems can differ in user space, such as different Linux distributions with the same kernel.

The term hypervisor is a variant of supervisor, a traditional term for the kernel of an operating system. The hypervisor is the supervisor of the supervisor.

Generally, two types of hypervisors are in use:

Type-1, native or bare -metal hypervisors
These hypervisors run directly on the host's hardware to control the hardware and to manage guest operating systems. For this reason, they are sometimes called bare metal hypervisors. Modern products of that kind include Xen, Oracle VM Server for SPARC, Oracle VM Server for x86, Microsoft Hyper-V and VMware ESX/ESXi.

Type-2 or hosted hypervisors

These hypervisors run on a conventional operating system (OS) just as other computer programs do. A guest operating system runs as a process on the host. Type-2 hypervisors abstract guest operating systems from the host operating system. VMware Workstation, VMware Player, VirtualBox, Parallels Desktop for Mac and QEMU are examples of type-2 hypervisors.

The distinction between these two types is not necessarily clear. Linux's Kernel-based Virtual Machine (KVM) and FreeBSD's bhyve are kernel modules that effectively convert the host operating system to a type-1 hypervisor. At the same time, since Linux distributions and FreeBSD are still general-purpose operating systems, with other applications competing for VM resources, KVM and bhyve can also be categorized as type-2 hypervisors.

5.4 The Role of the Applied System Design

There are three aspects which can be applied to aid the engineering software for critical systems.

- First is process engineering and management.
- Secondly, selecting the appropriate tools and environment for the system. This allows the system developer to effectively test the system by emulation and observe its effectiveness.
- Thirdly, address any legal and regulatory requirements, such as FAA requirements for aviation.

By setting a standard for which a system is required to be developed under, it forces the designers to stick to the requirements. The avionics industry has succeeded in producing standard methods for producing life-critical avionics software. Similar standards exist for automotive (ISO 26262), Medical (IEC 62304) and nuclear (IEC 61513) industries.

In the railway industry, the standards of EN apply, namely CENELEC EN 50126, EN50128, EN 50129 and EN50159. All standards have a high degree of similarity with respect to the methods to achieve functional safety.

Furthermore, it will be necessary for the certification of a production system, to use a certified compiler, and then generate the system's code from specifications. Another approach uses formal methods to generate proofs that the code meets requirements.

These approaches improve the software quality in safety-critical systems by testing or eliminating manual steps in the development process, because people make mistakes, and these mistakes are the most common cause of potential life-threatening errors
.

6. Operating Principles for Embedded Systems and Professional Data Centers

There are certain methods available to enhance safety, security and fault tolerance. These methods are independent of the technologies used. However certain methods are widespread only in embedded systems, others are current in professional data centers.

As it appears at the time being, the combination „outside of the usual“ may deliver excellent results in respect to safety and security. Therefore, these methods are listed and explained in detail and where they currently have their main application field.

6.1 Virtualization as a Method to separate Hardware from Software

To eliminate the interdependencies between HW and SW, virtualization is of essential use. This method is absolutely standard in all kinds of data centers.

For this purpose, the HW will have a virtual environment instead of the operating system. Several products are available, such as VMware or KMV. This combination of HW and virtual system provides and organizes the resources. To make these resources available, the virtual environment creates SW “connectors”, into which the necessary operating system plugs in. These connectors are available for all operating systems. As such, one processor may easily operate in several operating systems apparently at the same time for several applications.

The application software will now be installed on the basis of the suitable operating system on the virtual environment. As a result, an executable SW stack is created, which communicates with the resources via the virtual layer and gets resources under control of a hypervisor. It includes the SW from the operating system, the application and the connectors to the resources. The SW stack executes the application and is seen from the outside as one (virtual) machine, with an operating system, application system and resources.

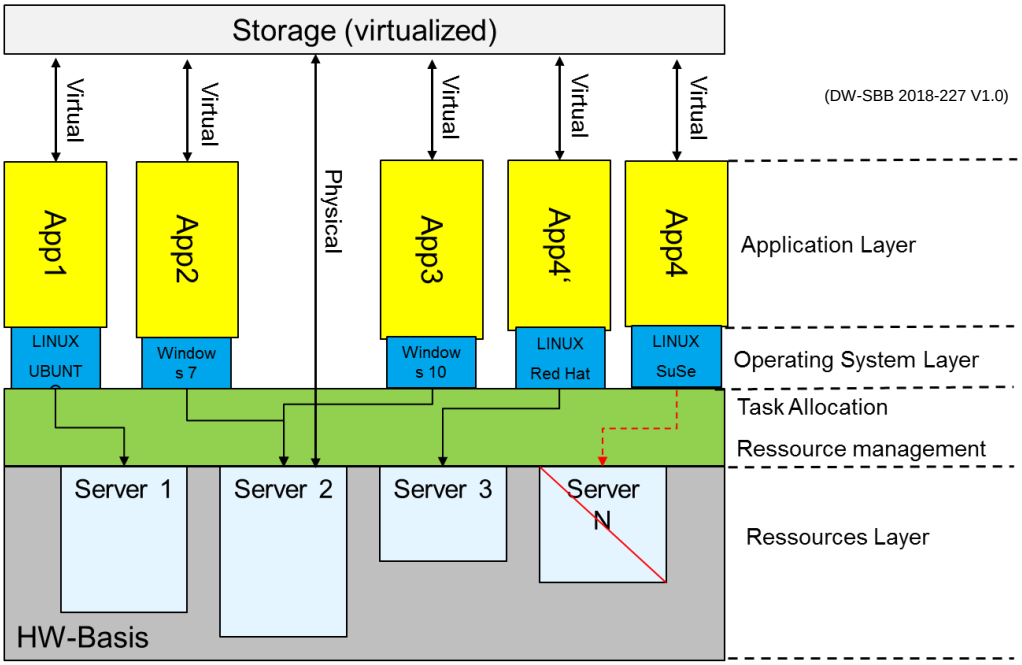


Figure 15: Virtualization Principles

The virtual environment is not limited to one physical server. Multiple physical servers with their resources are connected to a cluster with a pool of all resources of all (physical) servers. Typically, applications are allocated to this (virtual) cluster, but not to a dedicated server, if not specifically requested by the user.

Having now created the SW stack, it can be stored, transferred and copied as seen fit. If a copy of the stack is transferred to another (physical) server, the transfer immediately enables the operation of the server without any installation. If further processing power is needed, a copy of the stack is activated and a new (virtual) server is created which enters execution immediately.

This means that the classic assignment of hardware and software is dissolved and therefore a software is not necessarily permanently assigned to a specific hardware. This assignment is done by using resource control instead. This also means that the permanent fixed assignment of a function to a subsystem is not mandatory and also not static.

This allocation of applications or functions is based on the current hardware load and current order situation according to defined rules. Thus, the processing takes place depending on the order situation and the available computer capacities and the system can react load-dependent.

This procedure is particularly important when hardware defects occur. Resource control detects the failure of a resource and responds as follows:

- The computer stacks on the defective machine will be disabled.
- The available servers are checked for free resources.
- In the presence of such resources, the pending orders are transferred to the remaining computers.

- If there are insufficient resources, copies of the defective server's stack of servers will be transferred to the free server and used to process the orders.
- The defective server is reported and the troubleshooting is requested.

This also makes it very easy to build a disaster recovery system (DRS) because, in the event of a catastrophic malfunction (such as fire, airplane crash, flood), the corresponding stacks of computers only have to be copied to new machines with virtual environments and are immediately ready for use.

6.2 Multichannel Architecture with Voting as a Method to enhance Safety

The system architecture will be composed from multiple independent system channels, with voting of the intermediate and final results of the functions calculated. In general, multi-channel architectures are classified according to the “MooN” scheme, reading “M channels out of N independent system channels will control the system into a safe state upon failures of the other channels”. The requirements given above on hardware fault tolerance (HFT) relate to HFT=N-M, with the known simple topologies given in the following figure.

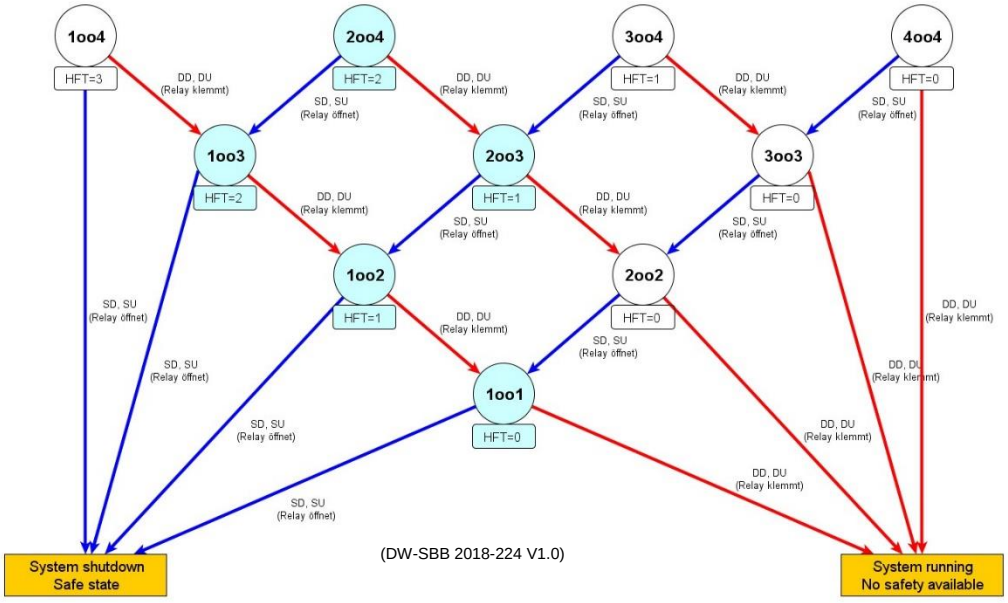


Figure 16: MooN scheme and degradation of simple topologies

. Considering the requirements given earlier in this document, with at least three independent channels (N>2) and a hardware fault tolerance of HFT>1, the possible applicable simple hardware architectures comprise the options with N>2 and M<5, therefore 1oo3, 1oo4, and 2oo4.

As shown in the figure, the topologies relying on a single channel to switch into the safe state immediately after a single fault result in a safe but unavailable state of “operation”. Considering the required high availability, the resulting reasonable “classical” architecture is of 2oo4 topology. Nevertheless, less common options also

include 2oo6, 3oo6, 4oo8, and others. Note that the standards don't give credit for HFT>2, and with more channels the proof of independency becomes increasingly difficult.

As shown with the requirements from the safety standards, more complex "hierarchical" architectures may be an option. IEC61508 explicitly allow a SIL4 system to be composed from multiple SIL3 channels. A well-known option is the 2*1oo2 configuration, closely resembling the conventional 2oo4 characteristics, but with advantages regarding independency of the channels. This architecture is applied to SIMIS PC in the railway domain.

7. Threats caused by External Sources

The system to be designed will be connected to other systems internal and external to SBB by means of IP-based networks. Several communications will have to be executed via wireless networks, such as GSM-R and LTE. Therefore, the introduction of malware poses a significant threat to the cyber security of the system, which may compromise the safety of the overall system.

It must be clearly understood, that even land-based lines, whether copper or LWL, also if operated exclusively by SBB, provide numerous attack vectors for criminal cyber activities. Therefore, severe efforts are necessary to counter these threats, protect the integrity of the system at any time, detect such threats and defend the system against the introduction of malware of any kind.

This cannot be achieved by using just one protective measure. It is necessary to create a complete bundle of measures, procedures and constructional features to shield from malware of any kind. These activities must be kept current at all times, requesting permanent care to counter the very volatile threat scenarios.

Additionally, it must be ensured that the data integrity in the field (at the object controllers) and in the RCDC is maintained at all times. This requires special measures such as ciphering of the transfer path and special processes to ensure data integrity.

7.1 Intelligent Design of System Structures

Since it is mandatory that parts of the SBB IT system are connected to public networks such as the Internet, the need for separated (isolated) systems inside the SBB IT system arises. Of special importance is the TMS system, which delivers the base data for the operation of the RCDC. This system also receives data back from the RCDC to correct the plan data with current data.

The commands from the RCDC are sent to the object controllers (actuators) in the field. Therefore, these data leave the protected data space and pass through public space to the object controllers. Therefore, this channel must be secured, and the data integrity checked at all times.

These sub-systems are linked via hardware and software bridges and gateways to counter illegal activity. To detect and counter such activities the following bundle of measures is seen to be necessary:

- To screen the RCDC from other subsystems a full two stage DMZ on APL-Level is required.
- To prevent falsification of data ciphered tunnels between DMZ and OC is recommended
- To achieve highest data integrity modern transfer technologies such as blockchains shall be used.

7.2 Prevention of the Introduction of Cybercrime Threats by Use of DMZ-Structures

In the military sense, a DMZ is not seen as belonging to either party (RCDC on one side and OC or TMS on the other side) bordering it. This concept applies to the computing use of the metaphor in that a DMZ which is, for example, acting as a gateway to the public Internet, is neither as secure as the internal network, nor as insecure as the public Internet.

In this case, the components that are most vulnerable to attack are those that provide services to users outside of the RCDC network such as components submitting information to OC or TMS. Because of the increased potential of these hosts suffering an attack, they are placed into this specific sub-network in order to protect the rest of the network should any of them become compromised.

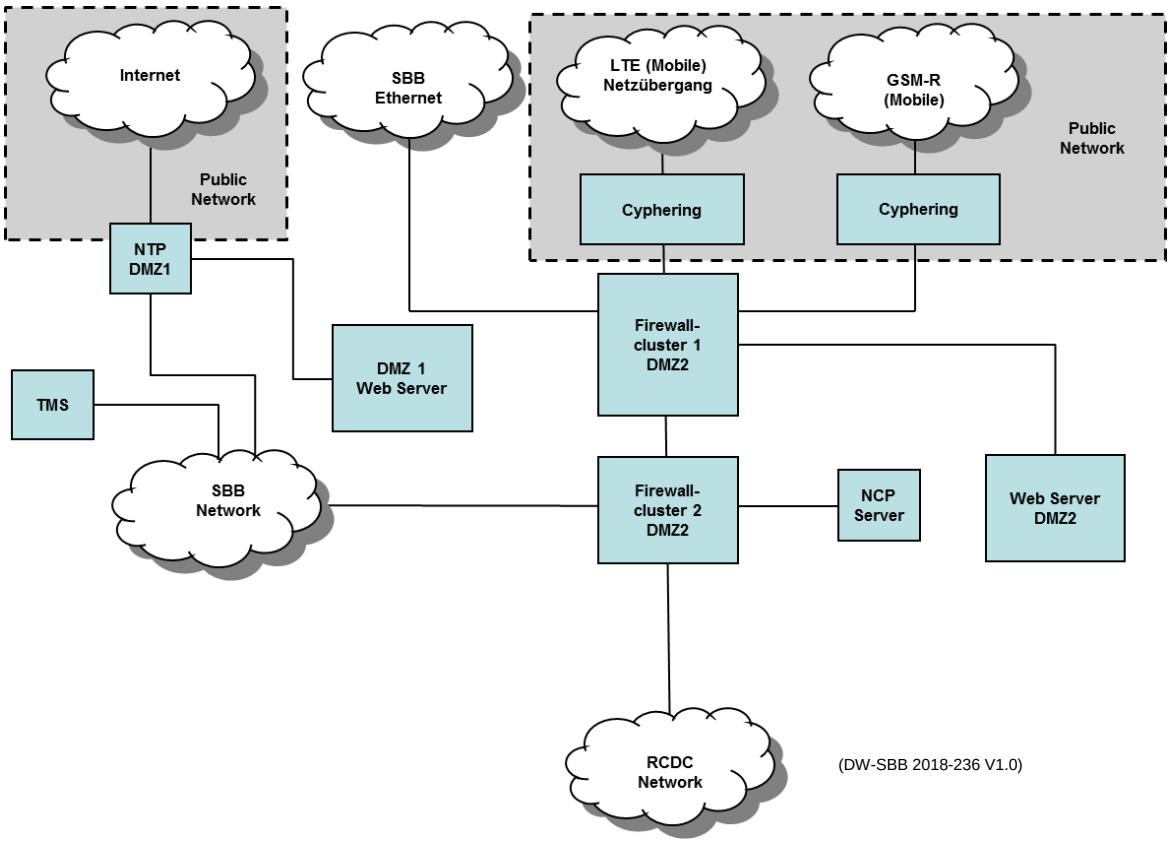


Figure 17: DMZ Structure of RCDC

Components in the DMZ are permitted to have only limited connectivity to specific hosts in the RCDC network, as the content of DMZ is not as secure as the internal network. Similarly, communication between components in the DMZ and to the external network is also restricted, to make the DMZ more secure than the public network, such as Internet or wireless systems, and suitable for housing these special purpose services.

This allows hosts in the DMZ to communicate with both the internal and external network, while an intervening firewall system controls the traffic between the DMZ servers and the internal network clients, and another firewall would perform some level of control to protect the DMZ from the external network.

A DMZ configuration provides additional security from external attacks. However, the means of communication to the outside world is of great importance. The firewalls are to be built at least of the application firewall type, allowing exclusively communication between known OCs and known application servicing these OCs or the TMS and the applications in the RCDC serviced by the TMS. Other communications will be excluded.

The mechanics of this communication have to be defined in a stringent and exclusive way. The service that is being provided to users on the external network can be placed in the DMZ, but may use Web services, FTP services, block chains and other principles.

The services which communicate with an internal database require access to an application or a database, which may not be publicly accessible and may contain sensitive information. The web servers can communicate with database servers either directly or through a second application firewall for security reasons.

Detection and blocking of virus threats is a further task of the firewall clusters. In conjunction with a suitable design of the DMZ it has to rely on continuous signature updates for updated attack vectors to prohibit viruses in a two-stage approach from entering the RCDC.

7.3 Ciphering as a Means to prevent Falsification of Data

The message from/to the RCDC to/from the OC may be transferred via public channels (like the internet) or via radio (like GSM-R or LTE), see Figure 17. To protect these connections from falsification and achieve data integrity as outlined in chapter 3.4. ciphering of this data is necessary. To protect the complete path, end-to-end ciphering is necessary.

Frequently “tunneling” is also used. Technically tunneling is also just an encryption between known entry and exit points. Tunnels are primarily used to build eavesdropping-proof connections across unsecured computer networks. The tunnel software ensures that the network packets are embedded in an encryption-capable protocol so that they can be decrypted and unpacked again on the other side. This means that encrypted data transmission is also realized for services that do not normally have their own encryption.

As the message initiates an immediate action in the OC and the data is valid only for a very limited time, the ciphering grade does not need to be very strong, i.e. military grade. As the deciphering of the message has to be done in the OC with limited resources, this selection guarantees minimum delays with a maximum of security (and subsequently safety). This applies also for the return path from OC to RCDC. As a general principle, the complete path from DMZ of the RCDC to the OC must be ciphered end-to-end.

Data from the RCDC is submitted to the DMZ. The DMZ contains a device to process ciphering. In Figure 17 NCP as ciphering algorithm is proposed. If tunneling (with a higher encryption grade) is required, GENUA products may be used. Vice versa the return message from the OC will also be deciphered in the DMZ and submitted to the RCDC.

7.4 Block-chaining as a Means to prevent Falsification of Data

A blockchain is a continuously expandable list of records, called "blocks", which are concatenated with each other using cryptographic methods. Each block typically contains a cryptographically secure hash of the preceding block, a timestamp and transaction data.

The term blockchain is used for a concept that allows a distributed system to be managed decentral and yet to receive consensus on the correct state of the data, even if many participants are involved in the process. This leads to maximum data integrity (as defined in chapter 3.4).

The basic principle is to build later transactions on earlier transactions and confirm them correctly by demonstrating the knowledge of previous transactions. This makes it impossible to manipulate or wipe out the existence or content of the earlier transactions without simultaneously destroying all subsequent transactions which are confirm by previous transactions. Other decentralized participants which have knowledge of the later transactions would easily recognize a manipulated copy of the blockchain, since it shows inconsistencies in the calculations.

8. Operational Aspects

The operation of a safety-critical data center is a complicated task, as it requires in-depth knowledge of the detailed business processes of the user. While standard business processes like accounting, billing or sales follow generally accepted business rules, the production process is unique for every company and reflects most of the know-how of the company.

This holds especially true for non-standard products like production of aircraft parts or operating the production system of a railroad system. While standard IT tasks are generally handled in data centers for a long time and are rather similar, production IT-systems achieve market penetration just now, usually connected somehow to the expression “Industry 4.0”. In the case of SBB this project is called SmartRail 4.0.

Much potential to save expenses and to improve the quality of service is frequently believed in operational models like housing, hosting or the usage of cloud services. The rational is to save expenses by buying the service from professionals, which are shared with other customers and to use their expertise in operating data centers. While this may be a usable model for standard data centers (although the anticipated cost savings could up to now not be proven, if a complete cost analysis is made) all external business models fall short for the case of production data center.

8.1 Some General Consideration

To assess the suitability of any business models like housing, hosting or the usage of cloud services, several facts are to be examined and duly considered.

Know how

The know-How to produce a product or a service is crucial for every organization. If an external organization is to provide IT-Services to control the production or the service, in-depths know how on the process to produce is necessary.

The process know how must be provided to the external organization. This is a painstaking and long-lasting process. Changes to the process cannot easily be introduced, since all changes may have a contractual/ financial impact. The definition of the tasks for the organization must be flawless and complete. Any gap in the requirements documents will cause an immediate request for compensation.

The know how must be kept current. Therefore, a retained organization must be kept to control and steer the external organization. As it is not possible to specify each and every incident, which need to be handled by the external organization, again every incident causes discussions and the request for compensation.

The know how must be protected for abuse, which requires significant legal and contractual issues.

Security

The external organization has to provide data security for their services. As the responsibility rests with SBB for a safe operation, SBB would have to specify how the security targets have to be reached. Due to the special requirements of SBB the necessary measures can only be deviated from the standard measures and need to be extended to suit the needs of a railway control system. As this would have to be done by SBB, significant efforts to accomplish that would rest with SBB. Furthermore, SBB would have to check compliance to the measures as requested at the external organization.

Safety

This document shows, that significant efforts have to be undertaken to cope with the requirements on safety. The impact on used components, HW, SW, the system design and operation is obvious. Therefore, the external organization must use exactly the same Hard- and Software system as specified in the certification, cannot use their purchasing advantages in equipment und has to separate the system completely from other systems – not only virtual!

Frequent safety checks may be mandatory, as the responsibility to execute the production in the specified manner rests generally with SBB.

Availability and reliability

The requirements for availability and reliability are extremely high. Standard data centers are unable to accommodate such requirements and would need further investment in personnel and material to fulfill the stated requirements. As these requirements are unique to SBB, any cost sharing is impossible.

Dependence

Experience at huge companies proved, that such contracts are normally issued for several years. In the clear majority of these cases the contracts are renewed many times, although there are severe doubts in service quality and price. Typically, such contracts last in excess of 15 years, 30 years are fairly common.

This apparent contradiction is based on the dependency from SBB to the external organization. A simple change to another organization is not possible due to the necessary huge amount of know how transfer. The know how rests more and more with the external organization. The effort to return the data center back in or to another external organization is literally enormous.

As a consequence of this dependency prices are constantly increased. From some samples in German prices of up to 5000 Euro to introduce a new user have been reported, not to mention requirement for funding of changes.

Expenses (Investment and Operation)

As stated above, the calculation of expenses is extremely difficult. Using an external organization looks interesting at the beginning, since no or only very limited expenses may apply. Due to the specialized nature of the tasks of SBB and the determined requirement to use special products in a special environment with special software, this may not even apply.

In any case the operating expenses will be significantly higher, as the expenses for the (special) equipment must be returned on top of the plain operating costs. These cannot be shared with other customers, leaving this apparent advantage not applicable.

Contracting the service to an external organization does not even reduce the personnel at SBB significantly. A retained organization must remain to control and monitor the external organization. Observations in other production data centers showed, that the operation personnel can be reduced by about 40-50%, but all other IT-personnel continued to be necessary. Additional personnel were to maintain the contractual basis, the scope-of work and numerous other documents and to supervise their duly execution.

If a complete assessment of all expenses for all business models for more than 5 years is made, ESG does not know any case, in which a total cost saving could be achieved. For that purpose, an assessment can be done by use of the tool WiBe 5.0. The description has been added as Annex 2 to this document.

8.2 Recommendation for RCDC

Based on the above, the use of an external organization to operate the RCDC is strongly discouraged.

It is recommended to integrate the RCDC in the IT-organization of SBB and install it in a suitable location at the SBB premises. Remote operation of the data center network can lower the costs significantly.

It is recommended to introduce already now an economic control component in the project to elaborate financial figures in a professional manner. Four main stages are recommended:

- Rough draft of the system design – possible already today.
- Fine design – after refinement of the rough draft
- Purchase and installation
- Project review

9. Three System Designs

In order to assess the pros and cons of a given system there are three sources of information necessary:

- A set of requirements with which a system to be designed shall comply
- A system design of the respective reference system
- An assessment of the system capabilities against the predefined requirements

As the systems to be defined are built on technologies of three different general designs, three different designs have been made to act as a basis for the assessment.

It must be clearly understood that numerous elements will have to be identical as described above to achieve the necessary performance in security and safety. However, the acting system cores can be built on three base technologies:

- A design based on embedded systems
- A design based on classical data center components, adapted to SIL4 requirements.
- A design based on automotive systems.

Please note that the expressions used to describe the respective system may differ from system to system as used in the respective technology sector.

10. A Solution based on Embedded Systems as used in Avionics

Wikipedia (contributors, Embedded system, 2018) gives a definition of an embedded system: “An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts.”

This definition means that embedded applications are not typically similar to what the SBB Rail Control Centre intends to be. Therefore, focus must be laid on a subclass of embedded systems, which integrate functions on a larger scale, such systems can be found in avionics, especially military mission avionics.

Another important property of embedded systems is expressed in the related definition of a “Cyber-Physical System” (contributors, Cyber-physical system, 2018): “A cyber-physical system (CPS) is a mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users. In cyber-physical systems, physical and software components are deeply intertwined, each operating on different spatial and temporal scales, exhibiting multiple and distinct behavioral modalities, and interacting with each other in a myriad of ways that change with context.”

This definition emphasizes the interactions of such system with the physical environment and with the Internet. As such it is similar to the characteristics of the SBB Rail Control Centre in terms of communication, in terms of its interaction with the physical world, this data center is expected to be decoupled from physical influences. Further, it delegates the interaction with the physical environment to the object controllers.
This means that this analysis should have the aim of examining individual concepts that are used in the context of embedded systems, analyze their applicability to the implementation of a Rail Control Centre and finally state the availability of commercially available components.
.

10.1 Generic Concept

The Standard AS SAE4893 establishes a Generic Open Architecture (GOA) Framework for application independent hardware/software systems. It classifies the available functions and interfaces defining a taxonomy for functions and interfaces of an embedded system. The following figure shows the structure of this architecture, identifying functions and interfaces. This framework is shown here as it is the basis for open systems concepts, especially IMA, which have been developed in the context of avionics.

The GOA Framework is also compliant with the scope of the SBB Rail Control Centre, therefore functions and interfaces that are identified by the GOA may serve as guidance for building an architecture.

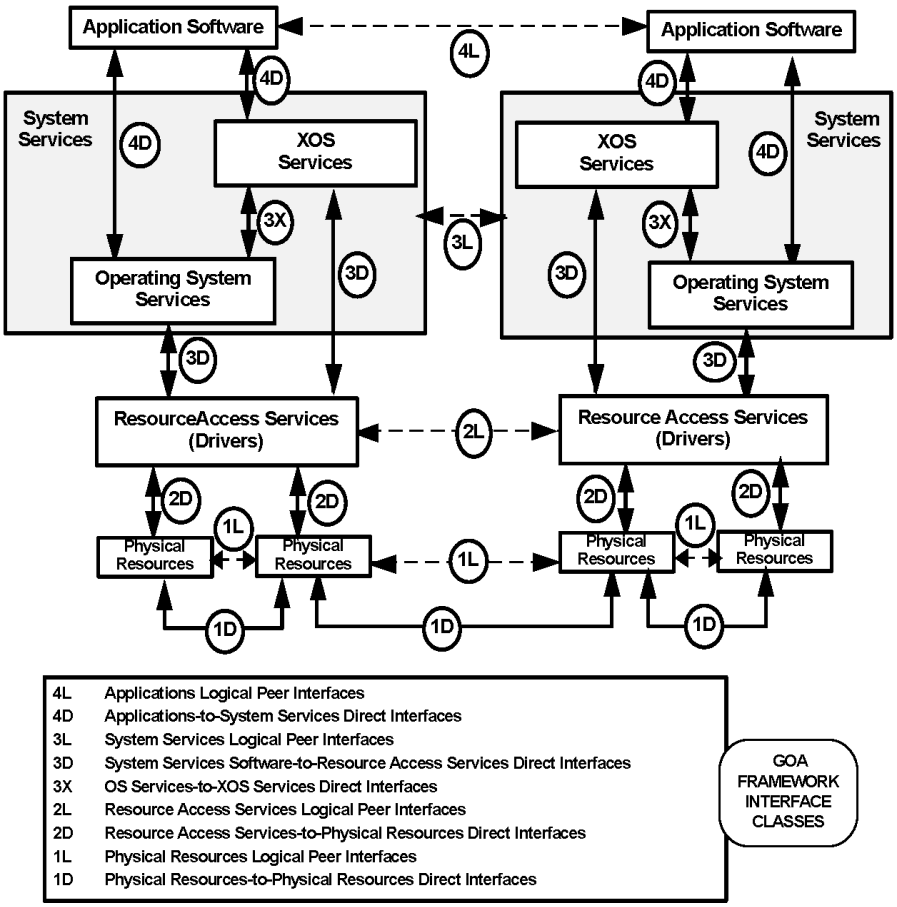


Figure 18: GOA Framework

10.2 IMA Concept

The aims of the IMA Concept as described by EN 4660 EN 4660 (ASD-STAN, 2011), (ASD-STAN, 2011), (ASD-STAN, 2011), (ASD-STAN, 2011), (ASD STAN, 2011) are similar to the aims for the SBB rail Control Centre as described in section 2. The main driver for this architecture is the reduction of life cycle cost for an avionics system, whose lifetime exceeds 20 years and may be up to 50 years for modern weapon systems. The main source of costs in a conventional avionics architecture is the dependence of hardware and software in a federated architecture, which consists of specialized computers. Each of these computers is built for a specific function, which is reflected by function specific hardware and function specific software. This means that hardware and software are heavily coupled and changes in hardware or changes in software (system upgrades, hardware obsolescence) always means knock-on effects leading to very expensive changes.

The first step of building an appropriate architecture is done by separating peripheral functions from processing. This is illustrated in Figure 19. The peripheral functions, which in a federated architecture are integrated together with the processing functions in a set of different, specialized computers, are separated from the

processing functions, which are now integrated into a core system. The core system is based on modular hardware.

This step-in avionics architecture is similar to the transition made by SBB in inventing a RCDC, which is separated from the peripheral function represented by object controllers. Nevertheless, there are important differences and also shortcomings in the IMA architecture in relation to the requirements of the SBB RCDC. These will be discussed in the conclusions to this chapter.

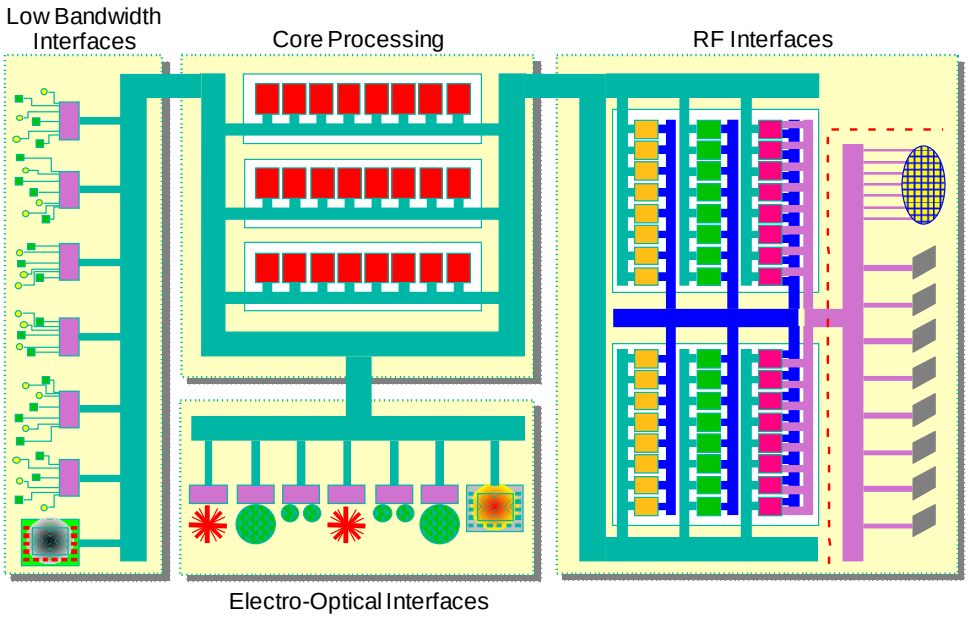


Figure 19: Separation of Core Processing from peripheral functions

One major goal of the IMA architecture is to achieve independence of hardware and software functions. Figure 14 shows the basic architecture concept:

Applications, denoted as “platform” functions, mean major investment in development and certification. Therefore, application functions need to be independent of any other changes, like changes of hardware or changes of operating system layer components, which are expected to happen much more frequently due to the short lifetime of these components due to technological evolution.

The hardware, if independent of software functionality (“platform” function), can easily be exchanged and as application software can be run on any of the hardware modules is scalable. Adding additional hardware modules adds additional resources to the system, which can immediately be used for running applications. Prerequisite for this is that the hardware is completely decoupled from the application software, ideally from system specific software functions at all.

The operating system layer is an abstraction layer providing abstraction of the IMA core system from hardware and core system dependencies.

The hardware layer representing the actual hardware components, which in Figure 20 is denoted as Module Support Layer, is fully decoupled from application or system dependencies. This has the effect that the hardware components / modules are independent of the software functions they are used for when the platform is in operation.

Orthogonal to the system layers, there is also a separation of payload function from system management functions. This separation is also important, as this additional step provides the separation of (payload) applications from system management. The architectural result is a virtualization of the processing functions. This architecture is quite close to a data center architecture as it provides virtualization for processing functions.

EN 4660 Part 2 (ASD-STAN, 2011) defines a (functional) module standard for an IMA core system. In total it discriminates six module types, it differentiates between three processing module types, data processing, signal processing and graphics processing, and three types of infrastructure modules, network support, power control and mass memory.

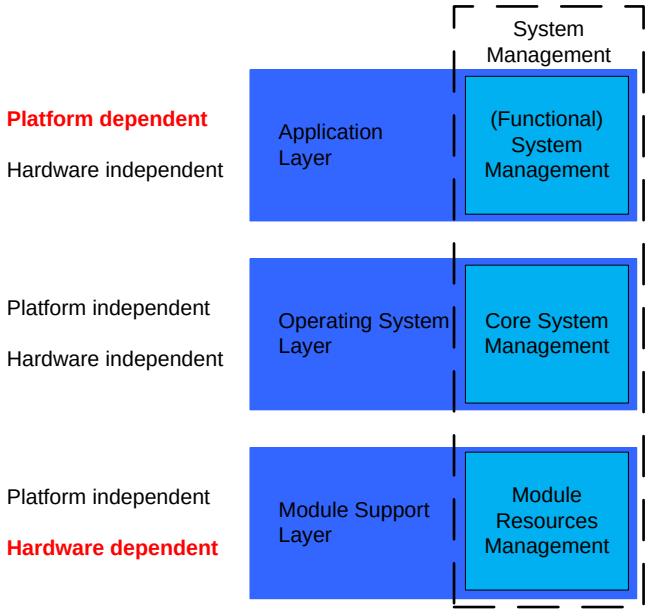


Figure 20: IMA Three layer stack

An important shortcoming of the EN 4660 architecture in the context of a data center is that it does not cover mass memory respectively storage virtualization.

Another problem is that today no modules are available for the hardware standards of EN 4660.

There are hardware modules available for other hardware standards, which are used in civilian aviation, e.g. as the modules used in Airbus A380 and A350, and also for military avionics mission systems. These modules do not provide a system management architecture as described in EN4660, but these modules have one big advantage that they can be certified (to avionics standards).

In order to use such modules in the context of a data center architecture as processing resources, the “core system management” functions must be provided by separate hardware. A sketch of such architecture is shown in Figure 21.

An unsolved question is the implementation of the storage system. This requires further analysis in order to understand the safety implications.

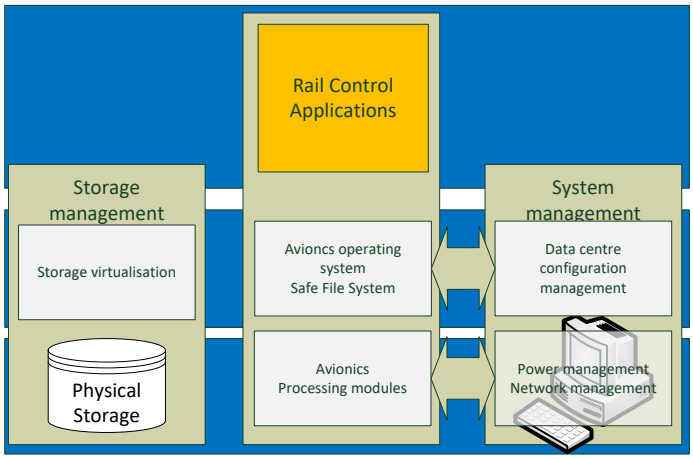


Figure 21: Sketch of an embedded data center architecture

10.3 TCMS Architecture Principles

A TCMS middleware architecture is driven by the vision of providing a platform for generic and reusable functional applications, which can be configured and instantiated for different platforms, federated sensors and actuators. The intention of this concept is to minimize the efforts for developing, testing and integrating applications on a particular platform / vehicle / train, which is described by the following top-level requirements:

- Applications are hardware-independent.
- Applications are independent of the operating system.
- The middleware provides access to all services, which are required by the applications.
- The middleware provides a robust execution environment for the applications.
- Middleware shall facilitate combination and instantiation (configuration / specialization) of generic application.

The main focus of this software architecture is to integrate legacy software and legacy hardware and to allow the migration towards reusable and generic functions. The main challenge in this concept is therefore the isolation of software functions from external influences. External influences could be the architecture and implementation of external units / peripheral functions as well as the hardware constituting the “core system”
.
The concept is also based mainly on the IMA architecture principles as described in section 10.2. In addition, a proxy pattern is used to

- decouple applications from details of the external infrastructure, like its structure and implementation

- decouple applications from the implications of message based communication

The application of the proxy pattern in this (software) architecture is illustrated by the two following figures 22 and 23.

Figure 22 shows the usage of a proxy function for decoupling generic application functions from the external architecture, which may exist in several versions or may evolve as time passes.

Figure 23 shows how a proxy would be used inside the “middleware” respectively the “operating system layer” in order to decouple applications from implications of legacy communication methods, which are usually based on message communication. Here the proxy function shall provide access to more abstract data items, which are based on a data pool.

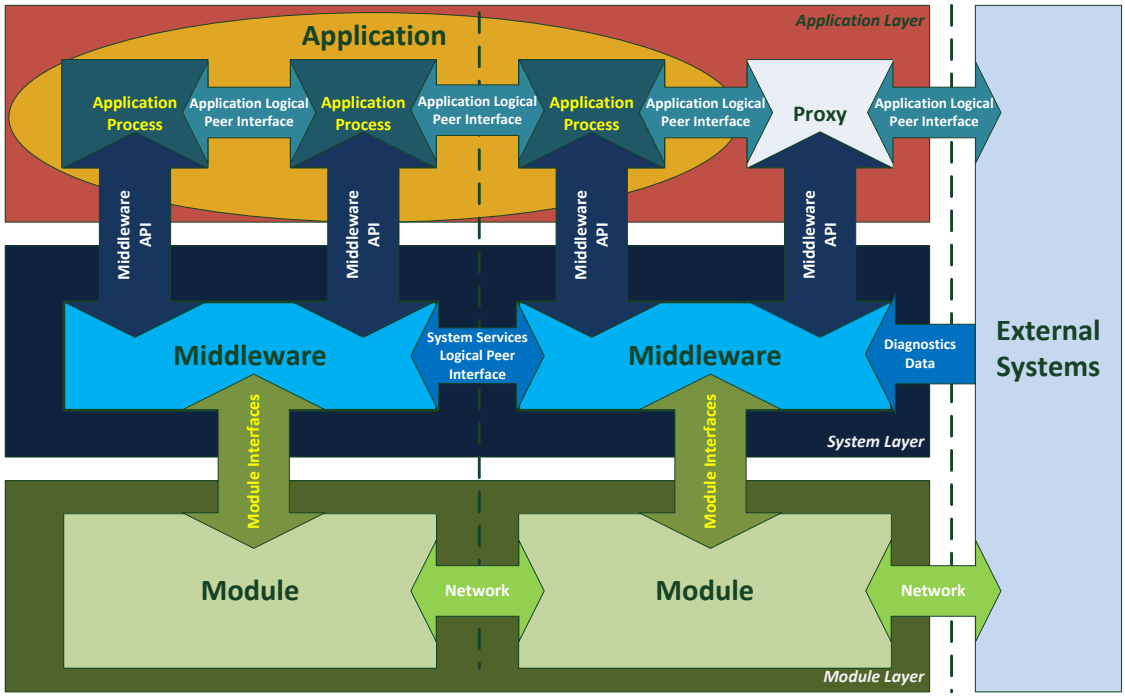


Figure 22: Architecture Context of TCMS Applications

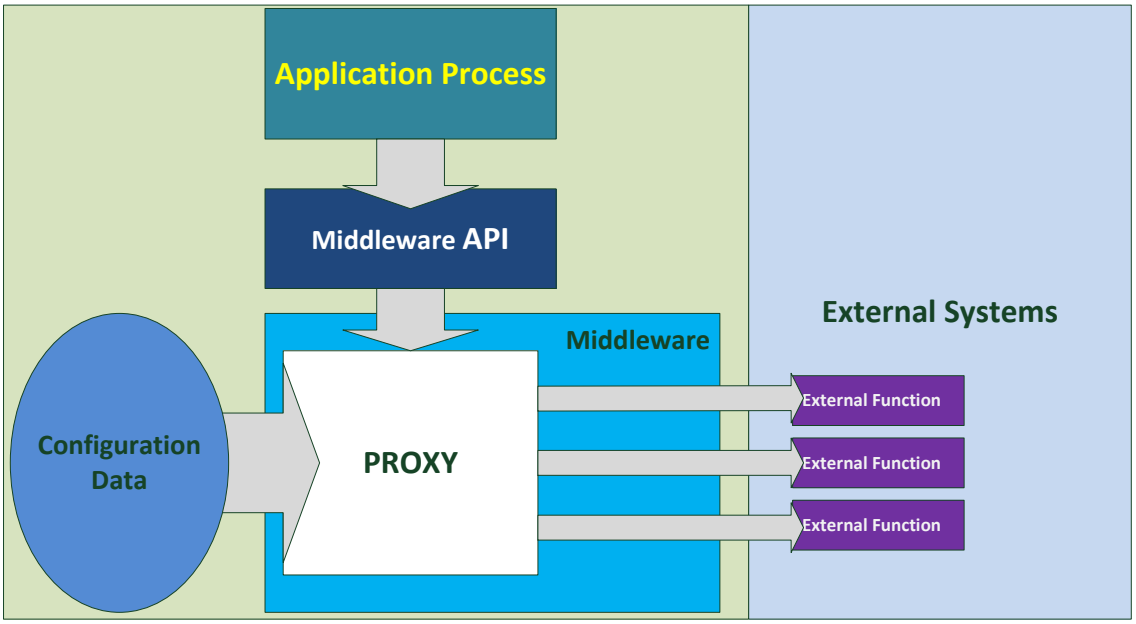


Figure 23: Proxy Model for Middleware Functions

10.4 Availability of COTS hardware

There are hardware modules available to other hardware standards than EN 4660. But there are avionics hardware vendors, who provide hardware, which may be used in a modified approach as proposed in section 10.2.

(when available data sheets of modules and ROM quotations will be provided)

10.4.1 Diehl Aerospace / THALES

Diehl Aerospace, respectively THALES has processing modules available, which are used in Airbus A380 and A350. These modules have been certified (partly up to DAL A – *this is not yet confirmed*). The modules provide integration of an avionics Realtime Operating System (RTOS), a proprietary product of THALES, which implements the ARINC 653 standard. Maybe also PikeOS could be available. This operating system is also certifiable, but offers more API options.

Shortcomings may be the limited performance and network bandwidth. Also, the modules usually provide ARINC 664 Network standard, which is limited to a static communication scheme and requires an excessive infrastructure. But probably, modifications to such modules concerning their network interfaces should be possible.

As Airbus planes are expected to fly 20+ years there is good hope that a long-term availability of such modules as well as technology updates will be available.

10.4.2 Hensoldt Sensor System

Another vendor is Hensoldt Sensor Systems, which can provide modules, which are certifiable up to DAL-C in the avionics world, as such certification also has to prove deterministic behaviour, the certification to railway standards may reach higher levels as well. The Hensoldt modules provide significantly higher performance and network bandwidth.
The Hensoldt modules are providing integration of Windriver VxWorks and is able to provide a certification package for each module respectively software function. A certifiable ethernet stack and a safe file system are also available.

Long-term availability of these modules and availability of technology updates are yet unclear. This might depend on whether such modules

10.4.3 Options

There may be other vendors as well. In military projects – this is supposed to be true for Airbus as well – usually only European vendors are used. With more foreign vendors there may occur problems with export or trade restrictions. This may not be true for Switzerland. If e.g. American vendors would be taken into account, there would be more options and more different designs. In the past, problems have occurred with American vendors with respect to certification.

At least two alternative vendors have been identified. This allows to provide dissimilar (hardware) implementations in order to exclude common mode failures.

10.4.4 Open Questions

The safety implications of a safe storage system have to be understood. Implementation of such storage system may be not based on COTS solution, but may need a software implementation. Therefore, it has to be understood, which functions of the storage system are safety critical, and which are not. There is hope that an architecture solution similar to the integration of avionics processing modules can be found.

Avionics safety standards and safety categories are different from railway safety standards. Therefore, investigations about the mapping of safety standards and – very important – safety requirements has to be investigated. This evaluation is required in order to judge, which safety level can be reached using available avionics hardware. This might evolve to be also an architecture question.

Separation of the certification of hardware and software has to be explored. Basis could be the approach that is described by RTCA DO-297.

10.5 Rail Control Centre Architecture (embedded)

The overall architecture of the Rail Control Centre, whether based on embedded technologies or others, is subdivided into three main hardware functions, the processing system, communication and the storage system.

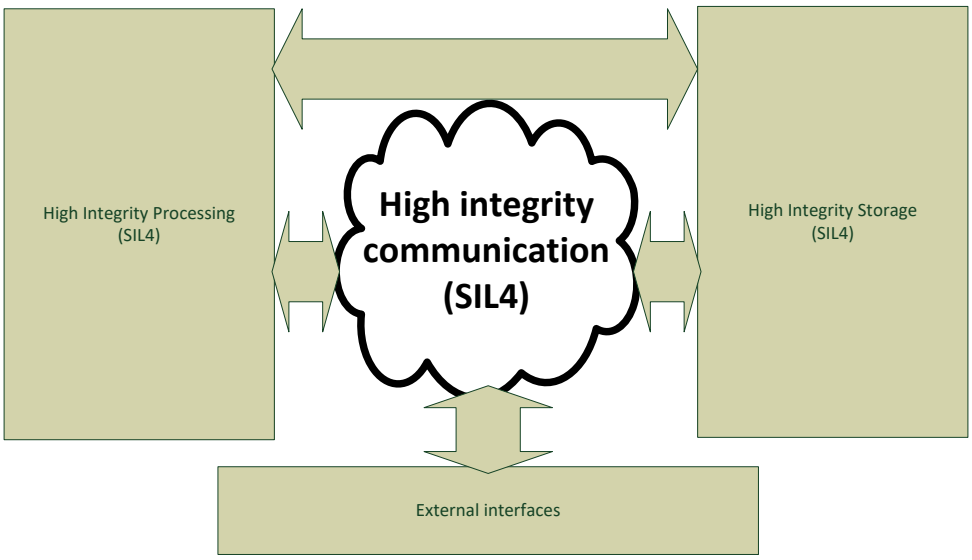


Figure 24: Main HW functions of Rail Control Data Center

10.5.1 Design patterns

10.5.1.1 Black channel communication – Main HW functions

A “black channel” is a design patterns that makes use of a communication channel, which is unsafe or whose SIL does not fit with the SIL requirements of the applications utilising it.

The black channel allows transparent communication in a layered communication model as illustrated in Figure 25: Transparent Communication through black channel

- The layer “standard protocol” is responsible to perform the communication between the communication end-points.
- the layer “safety protocol” is responsible for monitoring the integrity of the communication of the unsafe standard protocol.
- the layer “safety-critical application” uses the transparent communication means. It gets provided with communication data with integrity guarantees, in addition it can be informed, if communication has failed, because data integrity had been compromised.

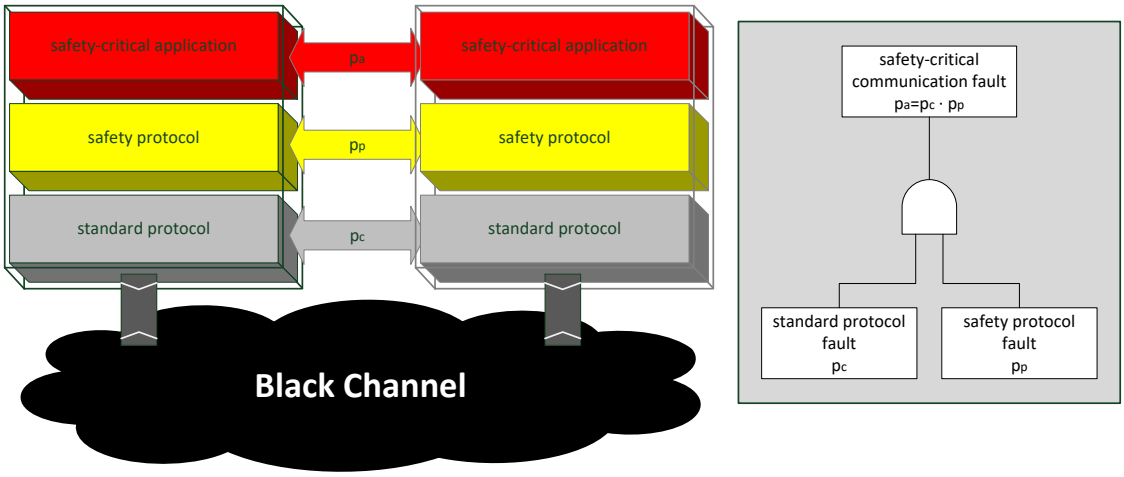


Figure 25: Transparent Communication through black channel

The safety protocol adds another level of safety, which applies within a fail-safe environment. It would not work the same way under safe-operational requirements.

Figure 25 shows a sketch of a fault tree for a black channel communication stack on the right side. It shows that the safety protocol reduces the fault probability of the standard protocol. There are different types of faults, which should be handled by the safety protocol, these are:

- loss of data / packets
- repetition of data / packets
- insertion of data / packets
- wrong sequence of data / packets
- corruption of data / packets
- delay of data / packets
- others (dependent on network technology).

This is an important pattern for network communication within a rail control data centre. It means that network communication can be based on standard protocols, which is available, robust, and affordable technology.

10.5.1.2 Black Channel Storage

The concept of black channel communication can be extended to the storage system. In principle, storage is equivalent to communication, but with an undefined data latency. In the communication case, a sender provides a message to a receiver. The data delivery is done immediately, respectively as fast as possible. In the storage case, the writer/provider of some data (record) takes the place of the sender, while the place of the receiver is taken by the reader/consumer of these data. In the communication case, the period between data emission and data reception is determined by the communication mechanism, in the storage case it is an event triggered by the receiving application.

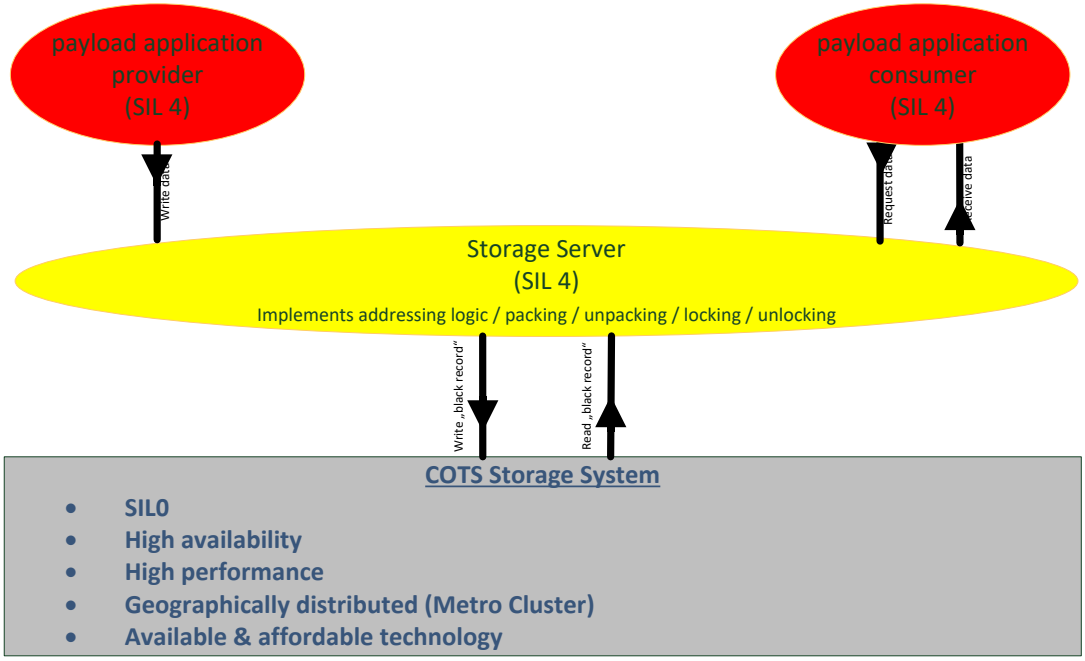


Figure 26: Sketch of a black storage system

As already explained above, the principle of a black storage system is analogous to the pattern of black channel communication. Figure 26: Sketch of a black storage system
stresses this analogy with Figure 25: Transparent Communication through black channel
5. The black storage system adds another level. The items in Figure 26: Sketch of a black storage system
contribute to a safe storage as follows:

- The **COTS Storage System** at the bottom is a conventional storage system as it is being used for conventional data centers. It is unsafe (SIL0), but it has a lot of other, very interesting properties, which are important for data centers: it is highly available, it may be geographically redundant or distributed and it provides high performance, i.e. short delays for writing and reading data.

- The **Storage Server** is an application function. It interacts with the COTS Storage System and with the rail control center's payload applications. Like the safety protocol in the communication case, its goal is to reduce the fault probability of the storage function to the required extent. It provides records to the storage system, which are provided with additional information, which shall ensure the integrity of the data read from the storage system relative to the data that had been written to the storage system before. In addition to this function the storage server may provide additional functions like locking / unlock9ing data for the serialization of data access, if required (e.g. for manipulations of rail system state).

- The **payload applications** have at their command methods for storing and retrieving high integrity data (SIL4) transparently for the applications to and from the COTS Storage System.

- The **storage server function** could be implemented as a centralized or a distributed function. It can be provided either as a standalone application or as a library function. Final decision of the implementation should be taken after an analysis of the efficiency the implementation alternatives make use of its resources.

10.5.1.3 Safe Processing Unit

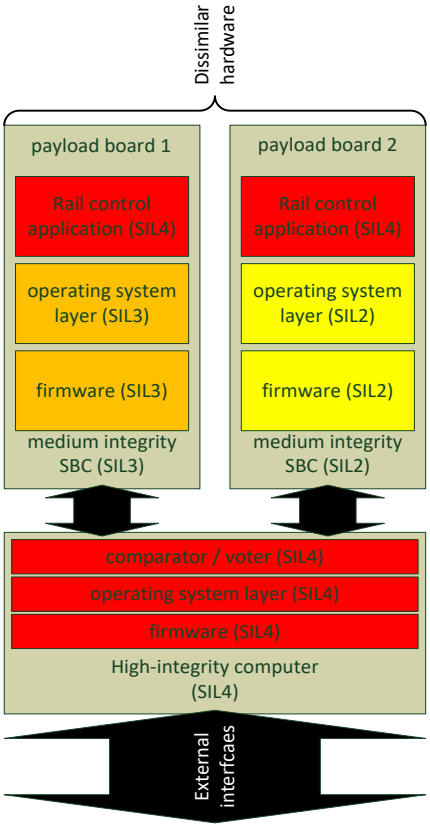


Figure 27: Example for SPA architecture

The availability of a high-integrity processing function is fundamental for the implementation of a rail control centre. The main pattern, which is relevant for the implementation and for the architecture of the rail control centre is the “Safe Processing Unit”. This term denotes a hardware function that provides a high-integrity (SIL4) processing function associated with the following resources:

- processing performance
- (volatile) memory resources
- bandwidth of network interface

The implementation of a Safe Processing Unit depends on the availability of processing hardware of appropriate SIL and availability figures.
Available figures suggest that MTBF / loss rate of COTS hardware components lay between 10,000 h (Gansler & Lucyshyn, 2008) and 1,000,000 h respectively 1.0 E-4/h and 1.0 E-6/h and therefore greater than the loss rate target of 1.0 E-7. This means that at least two redundant modules are required to reach the availability, respectively loss rate target. Usually loss is attributed to hardware degradation, therefore a common cause for simultaneous hardware loss appears to be unlikely. Therefore, loss rate does not introduce a requirement for dissimilarity.

As stated before, there is DAL A hardware available, with respect to aviation safety standards. This does not necessarily mean that this hardware can be used as equivalent for SIL4 hardware. An analysis of this would require deeper knowledge of the hardware and to which safety requirements it has been developed. This knowledge is not available now, it may be only available to the manufacturer of this hardware. Therefore, we take the assumption that the avionics hardware safety requirements are at least very similar to railway safety standards and therefore we assume that such hardware reaches at least SIL3.

Figure 25 shows an example for an SPU architecture, which may be realistic or not. In this case it consists of two dissimilar processor boards and an additional SIL4 computer, which may be internally redundant and

performs a comparator or voter function. The configuration of such SPU may be a virtual one by using data centre resources to build 'virtual SPUs' by configuring the communication links accordingly. The fault probability of such architecture could be calculated like that:

$$p_{spu} = p_{payload1}p_{payload2} + p_{high-Intgr}$$

10.5.1.4 Virtualisation

Virtualisation primarily means that Application Software is decoupled from specific hardware dependencies and therefore can run on any processing resource in the system. Therefore, Virtualisation is a mean of balancing processing and network loads in the system.

For implementation of virtualisation two main management tasks have to be implemented by a system management application:

- the management of processor resources and the distribution of applications onto these resources, and
- the management of network resources and the configuration of communication links in between applications, between applications and the storage system, and between applications and external interfaces.
- additionally, if SPU are put together from a pool of resources for the individual module types, a kind of resource management is required.

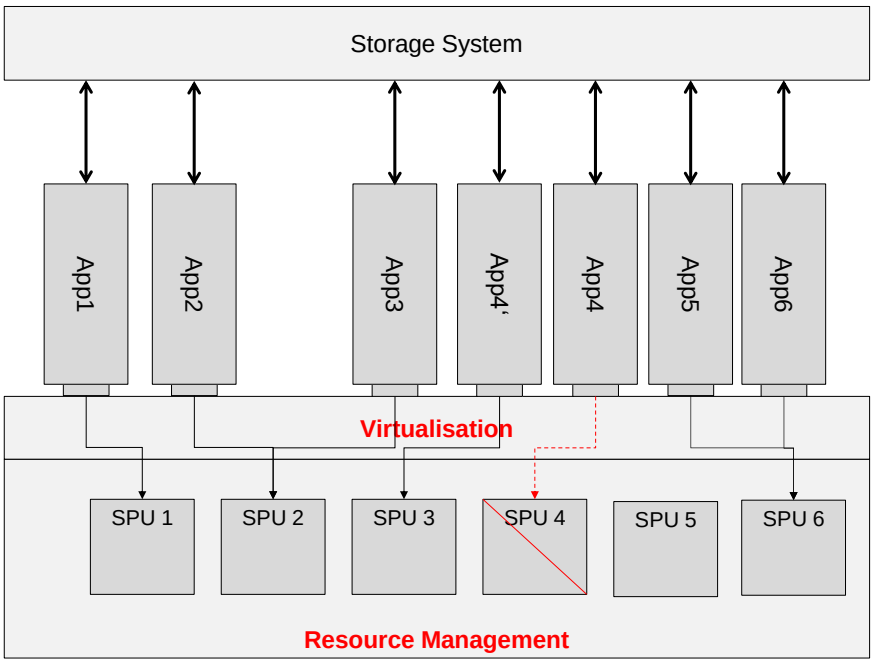


Figure 28: Sketch of a virtualized data center

Figure 28: Sketch of a virtualized data center shows the principle of such virtualisation. In this picture, also a hardware failure of SPU 4 has occurred and application4, which was running on SPU 4 is relocated to SPU3.

The resource management function ensures the availability of SPU resources. As such, it contributes to the availability of SPU resources and does not contribute to erroneous behaviour. This means that the resource management function has a low SIL, maybe SIL0.

Virtualisation function ensures the availability of Rail Control functions as well as the correctness of their configuration. For the Virtualisation function erroneous behaviour may occur, when an incorrect configuration would be the result of the configuration process. If a low SIL would be preferable for the virtualisation function, the integrity of the software configuration could be verified by means of a test scan.

10.5.1.5 Scan Testing

A test scan can be provided as a continuous test, which verifies the availability and the correct configuration of distributed functions.

It may be implemented in analogy to a boundary scan test of hardware. This means there are some test instrumentations and some test interfaces, which are used to execute specific tests, e.g. a connection test and to assess the results of such tests.

Scan testing should be incorporated into the Rail Control functions. It therefore should be qualified as SIL4. It is monitoring and verifying the correctness and completeness of the SW configuration of a virtualised network of application processes. It therefore disburdens the data centre's system management functions from its safety requirements. This could allow the utilisation of COTS function for data centre organisation.

10.5.2 External Interfaces

A next step towards the generation of an architecture (HW and SW) of a rail control data centre would be an analysis of the external interfaces of such data centre, but there is not sufficient information available about these interfaces.

The known interfaces are:

- Interface between "EI Interlocking Logic" and "TMS ARS" (Automatic Route Setting) – This interface generates the operation plan
- "Topo4" provides topographic information, which require regular updates
- OC controllers are monitoring and controlling trackside devices
- GLAT monitoring and control provides localization information of personnel.
- ETCS (European Train Control System) / ATO (Automatic Train Operation) interfaces
- interfaces to external regions (e.g. other nations)
- interfaces with legacy functions

10.5.3 Internal Interfaces

This section analyses the impact of internal interfaces, which are implied by architectural choices. This is mainly the choice of an operating system. It does not analyse the influence of rail control functions and the internal interfaces that are generated by the implementation of these functions.

The following kinds of interfaces have to be taken into account:

- operating system interfaces
- interfaces with legacy functions
- interfaces with partial COTS implementation of Rail Control functions.

10.5.3.1 Operating System Interfaces

There are different types of operating systems with associated APIs.

State-of-the-art for avionics systems are operating systems, which are implementing robust partitioning in a two-level scheduling scheme that implements pre-emptive priority-based scheduling at the lower level and a cyclic executive scheduling at the higher level. The associated standard is the ARINC 653 specification. The higher-level scheduling is determined by a static scheduling table, which is taking into account the timing requirements of applications.

Such an approach is appropriate in an avionics environment with limited processing resources and requiring deterministic behaviour. For a data centre, this approach is very inflexible and it is associated with a lot of effort in generating an application configuration.

The choice of an operating system is facing the following requirements:

- Virtualization demands the availability of concurrent processes on a single resource.
- Safety may require diversity in the implementation of the operating systems.
- Virtualization would be easier if diverse operating systems with identical APIs would be available.

As LINUX operating system provide a POSIX API and there are several other (embedded) operating systems, which are providing POSIX API or POSIX SE, which is a standardised embedded subset of POSIX, this appears to be the right choice and ensures full portability – at least at source code level - of applications within the data centre.

Possible choices for POSIX compliant RTOS are:

- VxWorks
- QNX
- LynxOS
- PikeOS
- LINUX

10.5.3.2 Interfaces with Legacy functions

In order to be able to provide some architectural recommendations, more information on interfaces of Legacy systems are required.

The integration of legacy functions may be important for a stepwise transition of the current rail control systems to SmartRail 4.0 implementation.

10.5.3.3 Partial COTS Implementations

A partial COTS implementation may be an option for facilitating a stepwise development of a rail control system, therefore it may be interesting to analyse the economic impact of integrating existing solutions. Considering Life Cycle Costs this may be only a mid-term solution, and it may depend about the amount of investment and risk to be accepted for the implementation of a rail control centre.

10.5.4 Safe Storage System

10.5.4.1 Storage Functions

The storage system shall provide access to common data such as the global schedule data or rail topology data:

- Common data are updated regularly, the update frequency varies between seconds and years.
- Common data are read only to the Rail Control Applications (applications in the Rail Control Centre).

The storage system shall hold a common, consistent status of the rail system (Object Controllers, Trains, etc.).
The Rail Control Applications modify this state in a safe (SIL4) way.
Response of the Rail System may confirm or deny state changes.
Separate applications may concurrently request access to the same object's state.
Therefore, there may be multiple modification requests to one data item.

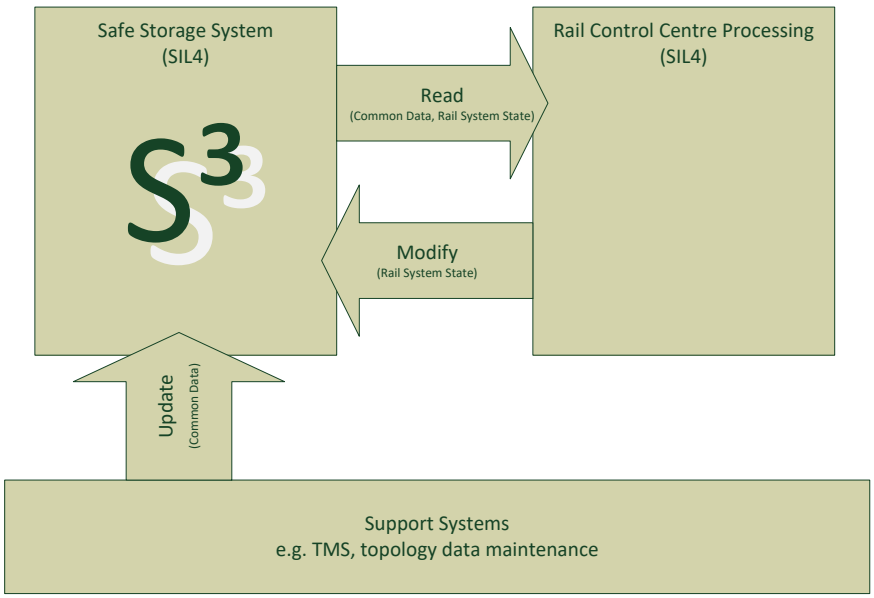


Figure 29: Access variants to the Safe Storage System

Because of this, access to objects must be protected. For the protection different cases must be considered (illustrated in Figure 29: Access variants to the Safe Storage System

- **Read access to Rail System object's state**.
  Assumption: Read access to an object's state may happen before or after the state changes due to the processing of a concurrent application. As the processing is performed in a periodic manner, with a period that is at least one order of magnitude smaller than the safety margins, the state will be read correctly in the next period, leading to an updated solution, that considers the updated status.

- **Modify access to Rail System object's state**.
  Any modification must be an atomic operation to maintain a consistent state of the object.

- **Read access to Rail System Common Data**.
  There are many readers and only one writer to this kind of data. Here no access protection is required, but an effective read mechanism. Effectiveness may be gained by implementing an effective addressing mechanism.
  The most important requirement to Common Data are their availability.
  In addition there may be moderate freshness requirements.

- **Update of Rail System Common Data**.
  Update of Rail System Common Data may be performed in the background, when the update has been completed, Rail Control Applications refer to the new data, while the old data become obsolete.

10.5.4.2 Synchronous vs. Asynchronous operation

Operation of the Rail Control Centre is asynchronous. This appears to be the most effective way of operation, as it allows for parallel processing, while the fraction of objects, which are accessed concurrently is assumed to be small in relation with the total number of objects being processed.

Synchronous operation operating on a common status of the Rail System, may work as well. It could be accomplished by prioritisation of modifications to an object's state as well. It has the advantage, that race conditions are excluded. Processing within one cycle's period may be asynchronous as well, i.e. it needs not to be serialised. E.g. the following scenario:

- At the beginning of a cycle the Rail System Status is acquired.

- Processing begins, while processing is done, the Rail System Status is not modified, but modification requests are collected.

- When the cycle's processing has completed, the modifications requests are executed. If there are concurrent modification requests on the same object, only the request with the higher priority is executed. Lower priority requests are discarded.

- the next cycle is started.

Problem: This may lead to oscillatory behaviour of the state, if two applications require contradicting state changes.

This problem may be solved by a prioritisation logic (prioritisation of interest) within the applications and an associated time within which only same or higher priority can do other modifications. Oscillatory behaviour may occur for synchronous processing as well as for asynchronous processing schemes.

Asynchronous processing appears to be better scalable and easier to manage that a synchronous solution. Both alternatives can solve the problem of oscillatory behaviour. Therefore, asynchronous processing appears to be the better solution.

10.5.4.3 Storage System Operations

The Safe Storage System shall implement the following operations:

Read common data:
Reading common data gets data from the storage pool. As these data may be updated always the newest data have to be referenced. The specification of the data to be read is dependent on the kind of data and the application's requirements. It may be complex, as in case of topology data. This could e.g. specify a sub-graph out of the complete topology graph by a geographic range condition.

Parameters:
- in condition - Selection of data to be read
- out data data that have been read are returned.

Read status data:
The specification of status data is more specific, if we assume that single objects are accessed. Status data may therefore be addressed by means of a unique key.

Parameters:
- in key identification of a specific object.
- out data data that have been read are returned.

Write status data:

This service is actually a write service, assuming that the data value has been read before and that the value read is up to date.

Parameters:
- in key identification of a specific object,
- in priority priority of the write operation (may be associated with the priority of the managed entity)
- in data data value
- out success indication, whether the write operation was successful (only required for asynchronous processing)

Update data:

Update data refreshes the content of some common data item. this operation may be performed in the background and when completed, the Rail Control Application shall refer to the refreshed data, rather than to the old data values.

Safety / implementation considerations

The integrity of data is safety critical (SIL4), but to our knowledge there is no storage system hardware or software, which is compatible with safety requirements. Therefore, it must be assumed, that an affordable Storage System consists of COTS HW and SW and consequently the storage system is assigned a SIL0! This means there is a conflict between affordability and safety.

This conflict can be resolved by storing "black data", i.e. data, which are protected against unwanted modifications. This has the advantage, that these data are integer by definition, it has the disadvantage, that the way of accessing data must be pre-defined, random access to such data is not possible. Therefore, such data are addressed by means of a key. Such key may be translated by the storage system into a location in a file system.

In case of common data, a key may also represent a database query or some complex specification if the function of retrieving data is also qualified as SIL4, if data are classified as safety relevant (Schedule data may be not safety relevant, while topology data are). There may be different update strategies for safety relevant data and non-safety relevant data. The update process of safety relevant data must ensure the integrity of the data, which arrive at a Rail Control application.

To ensure data integrity two properties, have to be ensured:

- The integrity of the data themselves, and
- the validity of the data (is this the right data item?).

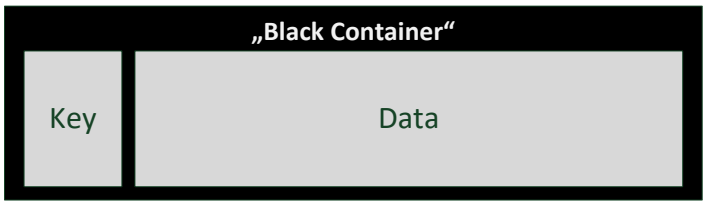


Figure 30: Storage Unit "Black Container"

Such data integrity requirements can be accomplished by storing a "black container" containing a tuple of key and data (refer to Figure 30: Storage Unit "Black Container"
). Data integrity is ensured by encoding/decoding the tuple into a black channel. Validity of the data can be verified by checking whether the returned data has the same key. as data are stored as a black channel, integrity is ensured also if the storage system is not safe (i.e. SIL 0).

Note: the request of the data will require also a black channel.

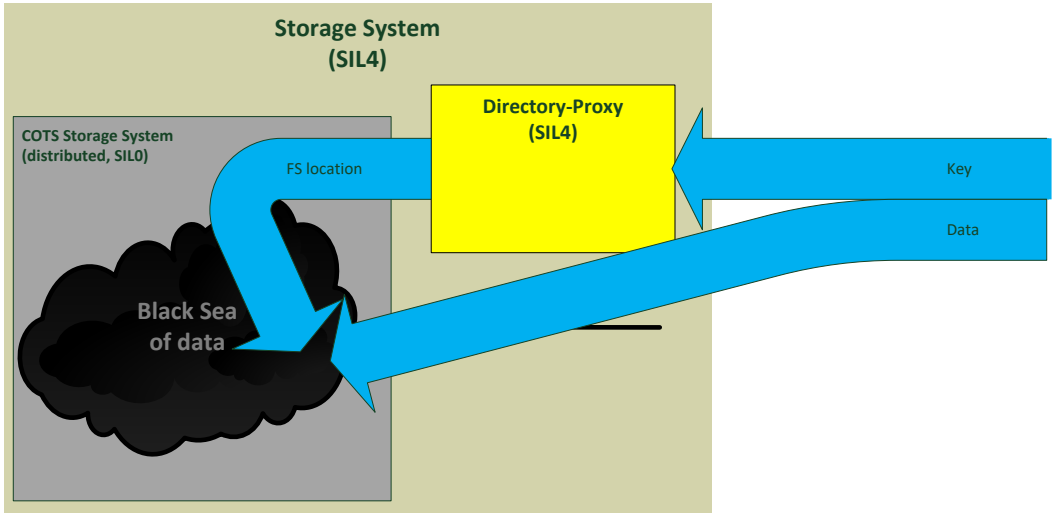


Figure 31: Writing data (Rail System State)

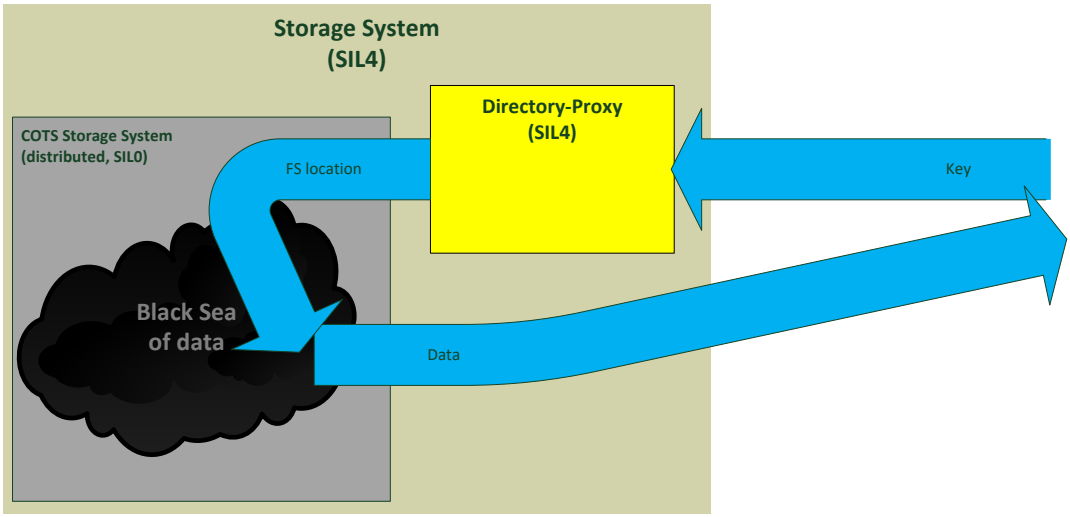


Figure 32: Reading Data (Rail system State)

11. A Solution Based on COTS Equipment as Used in Classical Data Centers

11.1 Design Guidelines

The demands for maximum data security, operational safety and high performance are based on the concept of a georedundant high-availability design of the RDZ according to the state of the art and the needs of the users, taking into account the budgetary concerns of the Required and Thrifty; The exact level of availability is determined in the context of the detailed planning.

The following principles are applied:

- The RDZ-hard-and software is divided equally between a fully functional plant at the location A and location B
- both sub-systems are always active. No splitting in live and backup RDZ (Active/Active clusters)
- load distribution between A and B is carried out by a resource manager system.
- The subsystems are connected to each other on several levels: DMZ, Server and SAN including Disaster Recovery
- Each sub-system has identical DMZ groups
- As far as technically possible, all server systems are virtualized and mirrored between A and B.
- Training is carried out on a (virtually) deposed system part.
- A separate (virtual) test system is provided for training and testing system changes.
- A separate cluster of SIL4 certified HW controls all Output data as voter between the channels

Designing the data center structure, it should be considered, that the standard IEC61508 and EN5012X have different requirements concerning Diagnostic Coverage (DC). In IEC61508 Diagnostic Coverage is required and in EN5012X it is not explicitly required.

It has to be clarified, which standard has to be referred and which solutions could be certified.

Diagnostic Coverage could be achieved mainly with two different solutions:

One solution will have DC realized “remotely” by the SIL4 Cluster via the existing or a special monitoring network over which the SIL 4 Cluster can monitor the COTS Clusters. For this solution it might be possible to have the COTS Clusters as SIL 0 Components, but probably with minor modifications to provide sufficient “insight” for the monitoring functions run by the SIL4 Cluster. This is the typical structure in modern data centers. (see Figure 33).

The other possibility is to have special DC Hardware components like plug-in cards or special onboard Chipsets which are monitoring the COTS Hardware “directly” (see Figure 34). Both approaches may be merged to cover the requirements existing for use of COTS components in a safety-related system either “remotely” or “directly”.

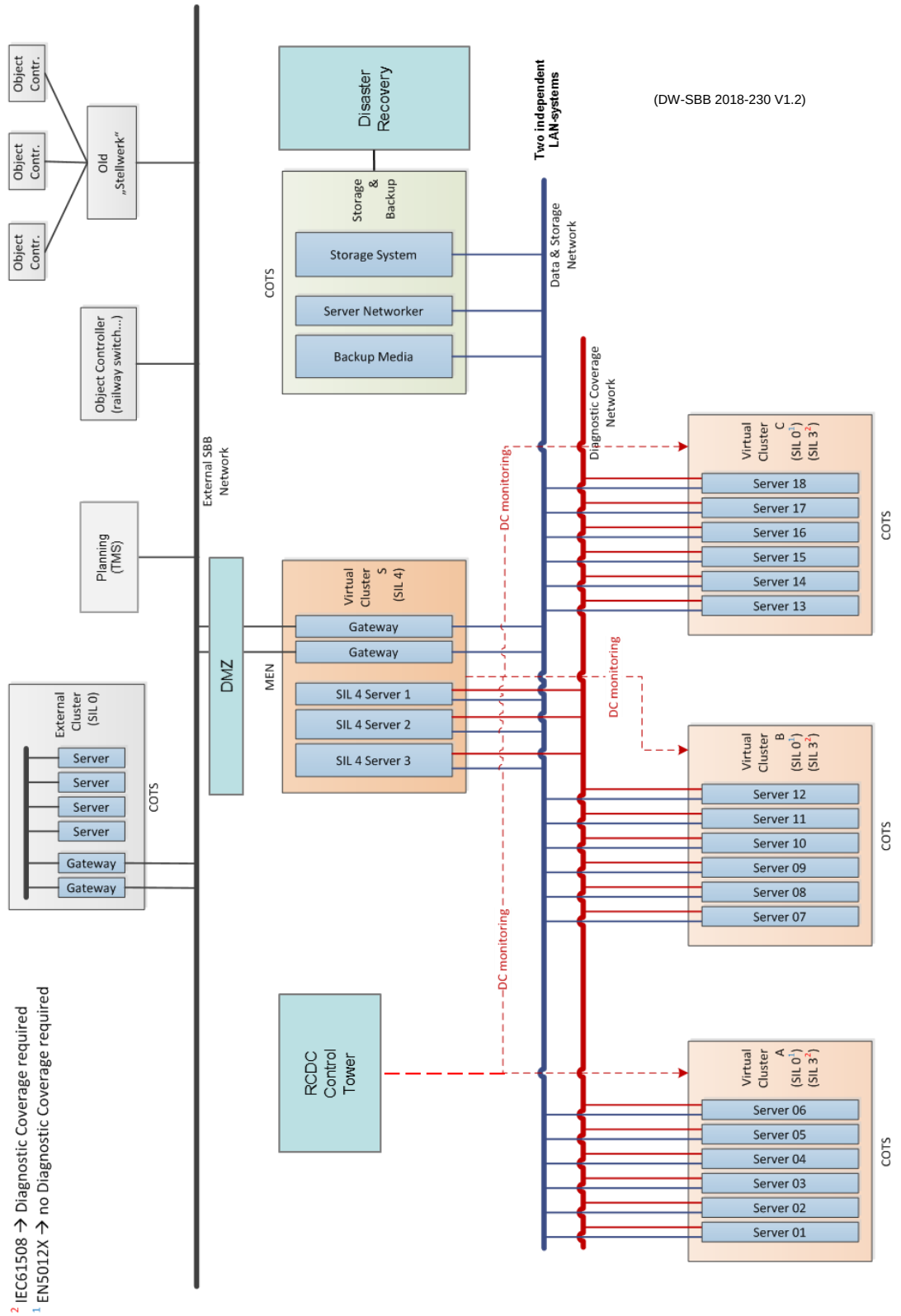


Figure 33: A data center structure built on classical COTS-Components with own management network

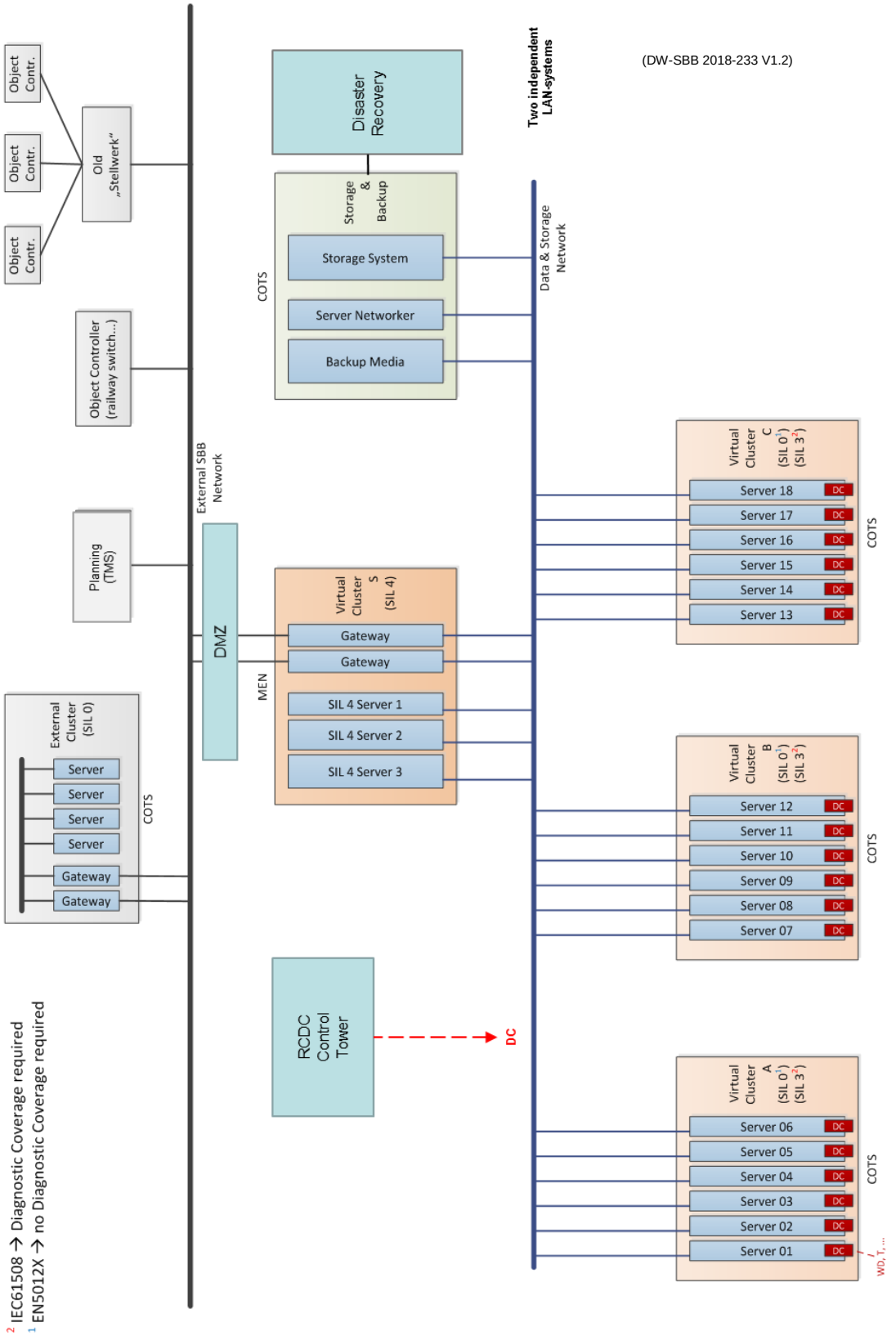


Figure 34: A data center structure built on classical COTS-Components without separate management network

It shall be noted, that there are deviating requirements on the SIL-levels of COTS-equipment stemming from different standards on the same subject. If IEC61508 is considered binding, all COTS equipment under supervision and control of a SIL4 component required to be certified to SIL3. If EN5012X is quoted instead, such equipment can be standard COTS with SIL0.

COTS equipment certified with SIL3 is not available, and the environment of railways considers EN5012X as the preceding standard. Therefore, this standard is considered to be applicable, resulting in a significant cost saving of the Non-SIL elements of the concept.

The functionality of the system is completely independent from the used hardware. The hardware operates under control of a virtualization layer (for SIL4-equipment see chapter 11.3). The operation of these clustered systems is described in chapter 6.1.

On top of this virtualization layer operating systems are used, forming a general API to present the basis for the applications.

As shown in the diagrams above, the storage is also a SIL0 -component. Despite the fact, that this SAN is a high-performance system (see figure 14) with high internal and geo redundancy, it remains therefore a non SIL4 component. Therefore, special techniques in use also in the embedded world will have to be used to store and retrieve data in a safe way. This can be achieved by the use of a black channel (see figure 31 and 32) to read and write data.

The SAN contains also subsystems to store data for backup and disaster recovery with auditing acceptability. The processes and storage duration requirements have not yet been specified. Taken of comparable data centers, a storage time of at least 10 years seems appropriate. The requirements are subject to SBB regulations and Swiss jurisdiction and need to be defined in cooperation with legal bodies of Switzerland.

The only hardware components which have to have a true SIL4-certification are the servers of the safe cluster. This applies also for the operating system, the virtualization layer and also any firmware, which may be necessary. There are operating systems such as Pike OS or Integrity available which fulfill the SIL4 certification already now. Although there are possible configurations – depending on the usage of the system – this may not be required in any case, it is a hard requirement for the intended use depicted in figure 33 and 34.

The appropriate license model for such operating systems need to be further examined under financial considerations, as these costs are significant (one time and LCC).

From the system structure it may be derived, that the SIL4-cluster constitutes a bottleneck in the design.

As this is the safety critical path, this component must at least be doubled to achieve fail functional status. This would lead to a degraded performance in case of failure, but keep the functionality intact.

It is necessary to size the system in a next design step to assess the processor load in this function. Components could be identified, which use standard XEON processors and provide therefore significant performance. Given the fact, that a first assessment assumes some thousand messages per second to be processed, and the design goal to shift all computation tasks as far as possible into the COTS-clusters, the load is not high compared to the capabilities of the applied hardware.

It is proposed to build a demonstrator and to size the total system to assess the stress on all involved parts. This holds true not only for servers, but also for switches, firewalls, storage systems etc.

At this point in time it is still too early to define detailed processing strategies. As a typical example for such strategies the processing based on asynchronous or synchronous modes shall be mentioned.

The SIL4 HW to be used is available from the shelf and therefore in some way specialized COTS-equipment. Like regular COTS equipment for data centers it will be available for 15 to 20 years for operation and service. After that timespan, a replacement is recommended, as the manufacturers service will be terminated due to lack of spare parts. However, the use of extremely reliable components is mandatory for COTS servers and storage, resulting in the application of proven components, processors etc. being in the market already in high quantity and for some time. This holds also true for the SIL4 components as mentioned above and is reflected in the use of XEON processors.

As standard processors can be used in this design, the command set is well known. Design flaws are well documented as the processors are in the market for some time in huge quantities. This eases the design of the applications, which need to be transferred from the embedded world to the data center world. For that purpose, the generation of a generalized API is highly recommended.

The question of the sizing of the data center can yet not be answered, as there are several factors influencing the quantity and performances of components, such as the overall number of data centers and the distribution of computing power between SIL4-components and COTS-components. Also, security considerations will have impact on the sizing, such as the number of channels to be used per process and the quantity of voting steps inside the process itself.

Depending on the workload of the SIL4 components some minor deviations from the design depicted in Fig 33 and 34 may prove useful. Especially traffic separation from/to the DMZ will reduce workload on the (expensive) SIL4 components. This will result in some specialized channels with independent SIL4 HW for each direction.

As all data resides in the storage system, it is easily possible to create situation descriptions of the full railroad network or parts thereof, such as regions at a given time by the use of snapshots on the database contents. Synchronization problems are eased, if not completely solved using those technologies. TMS will have at any time the complete situation at hand.

11.2 Data Security and Data Protection, Safe Operation

Only a systemic data protection design covering all components of the RDZ can guarantee sustainable data protection and the highest data security. In essence, the following design parameters must be fulfilled:

- Control of all output Data via a SIL4 certified Gateway cluster as voting function in a separate Network directly from/to the DMZ
- Interfaces only via a DMZ with double firewall protection to RDZ and external network. The firewalls must conform to the EAL4 classification and must be certified for the appropriate level of secrecy.
- In- and Outbound traffic touching public networks must be encrypted
- Appropriate and approved anti-virus measures with constant updating of virus profiles.
- access from/to other SBB-IT systems only via secure channels and the use of gateways.
- Application of a separate storage area network (SAN). The use of RAID systems is not sufficient.
- Distribution of the SAN between two identical georedundant sites A and B
- All data is mirrored synchronously between A and B.
- Backup of the SAN content via SNAPVAULT. The use of tape drives and corresponding software (such as Networker) is discouraged due to the high amount of data and the high manual effort. Use of modern long-term storage medias is recommended.
- Creation of a virtual disaster Recovery Center (DRC) within the SAN.

11.3 The Design of the SIL4 certified Gateway Cluster

The Data Center Gateway is the SIL4 manager for controlling the data in- and output to the main server clusters. The gateway server provides the services and functions to provide a SIL4 data center to the outer world. It utilizes subordinate, standard data center server-clusters for performing the actual data storage, data handling and computational tasks.

In general, the data center gateway is set up from standard COTS components, accompanied by specific hardware and software for providing a safety system. This leads to the usage of standard components like processors enriched with special additional Hardware and Software to fulfil the certification requirements.

The target is, to provide a long term available system with minimized obsolescence management risks. With this combination of standard COTS equipment and SIL4 certified COTS equipment the safety targets are reached with an optimized usage of the high cost SIL4 components, while all simple computational tasks are performed by cost efficient and easy exchangeable standard equipment. Therefore, the following design targets are achieved.

- Use of COTS for all obsolescence sensitive components
- Minimized design effort for SIL components
- Security due to Trusted platform module support
- Long term available

11.3.1 Technical Description of a COTS CPU Board with SIL4 Certification

The complete data center will consist of several data center clusters of standard COTS server hardware and storage. These clusters will be connected via high speed ethernet links (40GBit//100GBit/...) as depicted in Figure 33 or 34. The data center gateway will be the central point of communication to and from the data center. It will hand the data as well as the computational tasks to the subordinate data center, retrieve the computational results, check the data integrity of the obtained results and provide the data to the external communication partners.

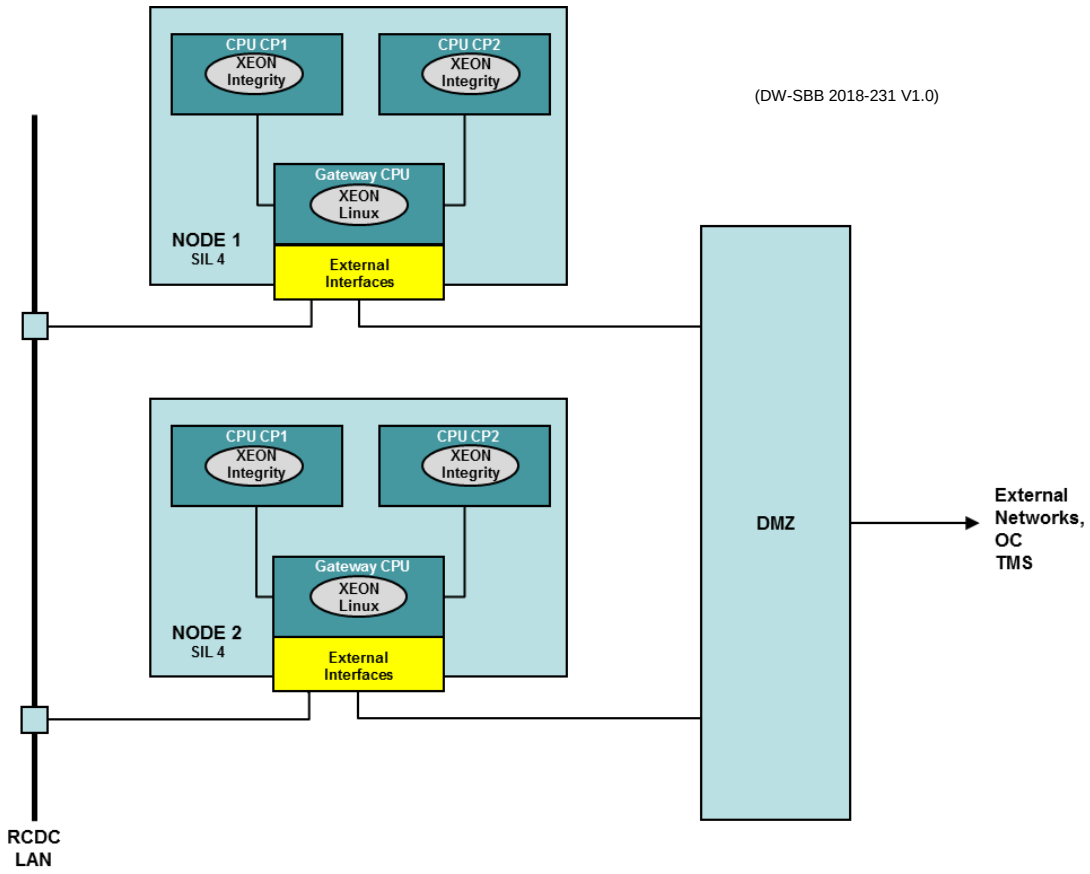


Figure 35: Structure of the SIL4 cluster of the data center (MEN)

Figure 35 shows a generic architecture of this part of the data center, as the environment of the SIL4 data center gateway to the public WAN. It operates in close context with the DMZ although not being part thereof.

The actual context of this concept are the redundant two gateway nodes. Each of these nodes is referenced as a data center gateway cluster. Based on traffic requirements, every cluster consists of hardware and software designed to be certifiable to Safety Integrity Level SIL4 according the CENELEC standards EN50129 and EN50128. Every cluster by itself is capable to handle the full traffic of the RCDC with a max calculated load of 50% of the available computation power.

The design and development requires close interaction with the manufacturer of the equipment. Usually there is a software development kit added to this hardware which is to be used to develop application software. The SDK has to be used by the customer together with the development tools and SDKs sourced from the operating system provider(s).

As shown in Figure 35 the two independent nodes are working in hot-standby mode, for high availability. One is configured as the master, the other one as the slave. The master/slave management and synchronization is completely handled by the DC control tower.

11.3.2 External Interfaces

The SIL4 cluster gateway has interfaces to external components only through the DMZ. Therefore, all traffic is screened on malware and also on data integrity. This applies also for SBB-internal traffic, as the damage of introduced malware may have a direct impact on safety and may cause catastrophic damages. Therefore, all communication between the SIL4 cluster gateway and external systems are using safety protocols to protect the transmission via untrusted communication channels

The SIL4 cluster gateway has also dedicated interfaces to the data center control tower for operational purposes, monitoring and control.

Internally in the RCDC the SIL4 cluster gateway has interfaces to the RCDC LAN system to operate with the server and storage clusters as described above.

11.3.3 Functional Architecture

Figure 36 shows the technical concept for a single node. The node is combined from two safe sections (CP1 and CP2) and the gateway / I/O node (GW). All sections are directly linked via 10GBaseT Ethernet links for cross comparison and synchronization between the safe nodes as well as for communication to external partners via the gateway node.

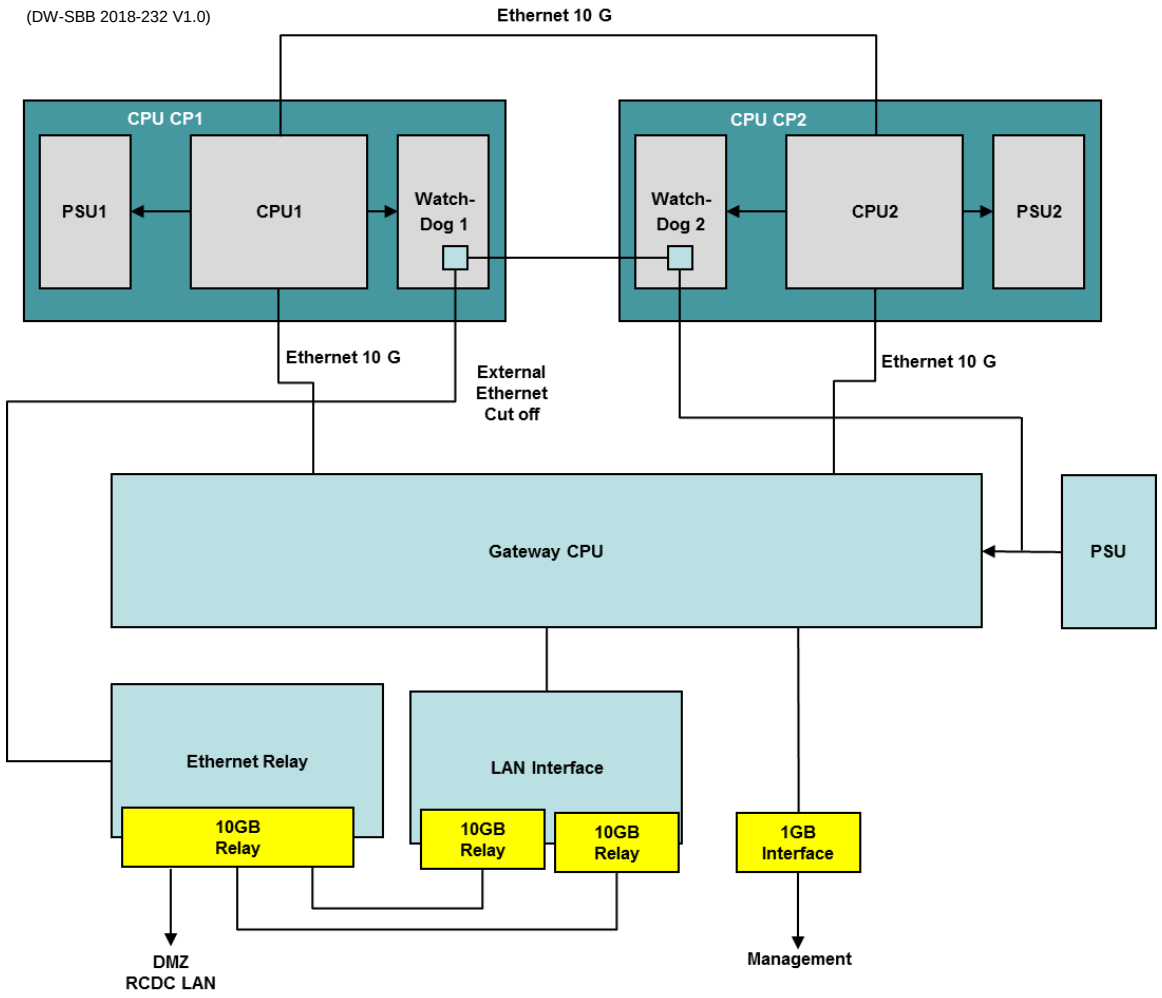


Figure 36: technical concept for a certified SIL4 cluster element (MEN)

The gateway node is equipped with two additional 10GBaseT network interfaces for communication to the server cluster network and to the field network and WAN. This data transfer value has been taken from existing equipment and may not be sufficient. A fine design is required to define the necessary needs. However, for the time being in the document 10 GB interfaces to be sufficient are assumed.

As the main safety function of the complete system is to fail silent, these two interfaces can be cut off safely by two watchdogs of both sections CP1 and CP2.

From an electrical point of view, each section is galvanically isolated from the other sections, therefore providing independence between the sections. Each section has its own power supply.

The only interfaces between sections are

- Ethernet Connection between Section CP1 and Section CP2 for synchronization and data
- exchange
- Ethernet Connection between Section CP1 and GW: For sending/receiving field/WAN

- data and to access GW services from Section CP1.
- Ethernet Connection between Section CP2 and GW: For sending/receiving field/WAN
- data and to access GW services from Section CP2.
- CutOFF Signal for the GWs external Ethernet interfaces (orange line in diagram in Figure 35)

11.3.4 Hardware Concept

CPU-Board

All three sections use the same CPU board: From an existing solution a design has been taken to summarize the properties and special features for SIL4 reasons.

A standard XEON/PENTIUM processor is used. This processor is designed for server applications. By using such a product, standard SW-tools can easily be used, as the command set of the processor is well known and widely used.

The section CP1/CP2 CPU boards use a PENTIUM dual core processor, while the gateway CPU uses a quad core processor.

The BIOS of the section CP1/CP2 CPU boards is configured for best deterministic behavior. CPU cores are configured to run at fixed clock speed and BIOS interrupts are disabled when necessary.

The gateway board has a removeable SSD attached which is used as the boot medium and stores application specific data, such as logging data. The boot images of section CP1/CP2 are also stored on the SSD. The section CP1/CP2 CPUs fetch those boot images via network from the gateway CPU. As such the Board is independent. In regular data centers, such information is always stored in the storage cluster, but due to safety reasons this deviation is useful.

Safety Watchdog

Both sections CP1/CP2 have an independent safety watchdog, supervising the CPU activity. In case, the CPU is no longer triggering the watchdog, the watchdog opens an onboard switch, therefore cutting off the power of the systems Ethernet switch to prevent any Ethernet communication from the system, which is now considered faulty.

The watchdog is a specific hardware designed for this project, as an CPCI S.0 peripheral board.

From a software point of view, the watchdog appears as a serial interface (UART). For communication with the watchdog, a simple but safe protocol is used that detects errors introduced by PCIe or other buses/components involved in the communication to the watchdog and the gateway / I/O node (GW).

All sections are directly linked via 10GBaseT Ethernet links for cross comparison and synchronization between the safe nodes as well as for communication to external partners via the gateway node and the control tower to oversee the system status.

11.3.5 Software Concept

Software on section s CP1/CP2

On sections CP1/CP2, Green Hills operating system INTEGRITY is used. INTEGRITY is a EN50128 SIL4 certified operating system. It has a microkernel architecture, which means that the code size of the kernel is minimized. All drivers and applications can run in separated protected virtual address spaces to provide freedom of interference.

In addition, the Green Hills Safety Layer “GSL” is to be used by the application layer, to supervise timing constraints, to run hardware diagnostic tests, handles errors and reports anomalies to the application.

The components to be developed for the intended use are:

- A board support package, providing support for the necessary chipset features and interfaces.
- A Voter – for synchronization and data exchange between sections CP1 and CP2
- Safety Layer – for safe communications/tunneling the communication to external networks/components through a black channel via the DMZ
- BEXCH – for non-safe (black channel) data exchange between section CP1/CP2 and gateway CPU
- watchdog services
- Diagnostics – diagnostic services

For application development, the Green Hills MULTI IDE (edit, compile, link, debug) may be used, which is a EN50128 SIL4 certified tool chain.

Software on Gateway

On the gateway section, a Linux operating system is used. Linux can be used here because the gateway section has no safety function. In addition, Linux provides all necessary support for file systems and network servers needed for this application.

In an existing product Yocto Project is being used. Yocto is a cross development environment. The Yocto sources are installed on a development host, the result of the build process is a SSD image or tar-ball that is installed on the gateway SSD.

With Yocto, it is possible to build applications, configure the kernel, tailor the content of the file system and the behavior of Linux for the gateway application needs.

To provide deterministic behavior of the gateway application, the Yocto recipes include support for real-time (RT_PREEMPT patch).

Further recipes provide support for network boot of sections CP1/CP2, G25A board management controller and fan monitoring.

For communication with sections CP1/CP2 BEXCH component, a BEXCH component for Linux is provided.

11.3.6 Safety Concept

Random Fault Control

The data center gateway systems safety is based on an 1oo2 architecture, i.e. two channels (section CP1 and CP2) are used, where each channel has its local diagnostic and the possibility to force the overall system into safe state. The safe state of the system is the “silent state”, i.e. no communication to the WAN interfaces.

Sections CP1 and CP2 are both running the safety application. During an application cycle, applications are synchronizing each other and exchanging/comparing their states and data. This communication is done via 10GBit Ethernet links between sections CP1 and CP2. Only if the two applications agree on the computed results, they produce data packets that are sent to the gateway. This cross compare provides high diagnostic coverage for any random fault.

In addition, each section has local diagnostic, such as built-in tests and monitoring of error indications provided by hardware. These diagnostics shall avoid that both sections fail in the same way, so that the cross-compare would fail to detect the error.

Not all the diagnostic information will have SIL4 quality (for example those coming from non-safe hardware), but the combination of different diagnostic measures will provide the required coverage. The frequency of periodic diagnostic tests can be low (several hours), as defined in EN50129, chapter D.4 (Formula for Tsf).

An additional safety watchdog on each section is monitoring the CPU activity. The application must trigger the watchdog with the correct sequence number within a time window.

Information from several temperature monitors is evaluated to encounter over-temperature situations.
Both safety sections can bring the system to safe state, independently from each other, using the local watchdog. If either, the application or the watchdog, detects a fatal error, it cuts-off the Ethernet links to external networks, therefore disabling external Ethernet communication.

Any external communication is done through Ethernet. Ethernet communication is regarded as black channel as defined in EN50159, all packets travelling through this black channel are protected by a safety layer. The gateway CPU and Ethernet switch is part of the black channel. The Communication is protected between the safety application and the external systems (represented and presented by the DMZ).

Systematic Fault Avoidance

Correct execution of the safety application logic is provided by:

- Using the EN50128 SIL4 operating system INTEGRITY (together with the BSP and GSL)
- Using a processor (Intel X86 on G25A) which is used in many different applications and has published errata. Therefore, it is unlikely that the processor has unknown systematic faults.
- Using a safety watchdog designed for EN50128/50129-SIL4
- Using SIL4 processes for system design, test, qualification and validation

System Security

In the current envisioned applications, the data center components are always operated in closed networks and a secure environment. Additionally, only authorized personal has physical access to the system. Therefore, security threats do not need to be considered in the SIL4 cluster gateway.

11.4 General API and Software Aspects

Software in use today in embedded systems can only be migrated to the new data center with significant efforts. Most likely it will hardly be usable, since the processes differ significantly, if the capabilities of a data center structure shall be used to the best possible extend. Therefore, the majority of software will have to be designed from scratch.

In order to bring the usability time to a maximum, it is recommended to create a general Application Programming Interface (API) and to use this mandatory for all new developments. This creates a further abstract layer to insulate the application from the operating system, the virtualization layer and the hardware. The API provides a unified access to the operating system and to standardized services, executed from the operating system on behalf of the application. It is very likely, that an independent API will be required for every operation system.

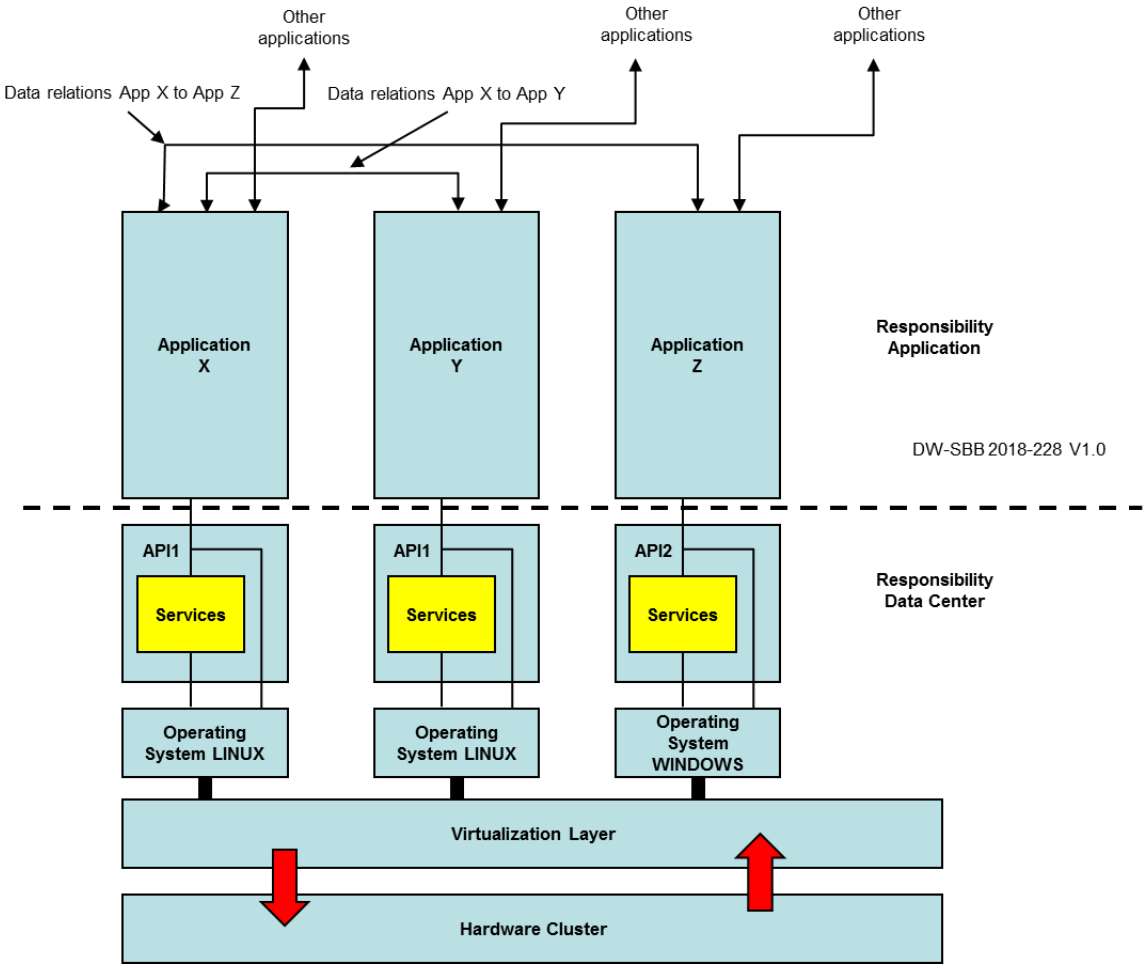


Figure 37: Software interaction and API

To distribute the functions and the input/output relations between the different applications in the best possible way, it is recommended to create an Interface Control Document (ICD), which specifies the data interrelations between the applications. Based on these data-sources and -sinks a unified software architecture can be created and maintained for the lifespan of the system.

The software architecture, the development process and its certification is an extensive task outside of the scope of this document and must be discussed in a separate document.

11.5 System Fault tolerance and Graceful Degradation

By means of the structure shown above, a complete system failure is practically impossible. A complete failure of a subsystem reduces only the reaction speed of the system, so there is a "graceful degradation".

The failure of a large component, such as the complete SAN at a site, does not cause any noticeable loss of performance. Via the cross connections, the respective parallel component at the other site takes over the function without transition time, since both systems are active at all times at the same time anyway. This is another major reason for the need for synchronous data mirroring.

Essential for the effectiveness of the measures is a close cross coupling between the sites is mandatory.

11.6 The use of virtual systems to decouple HW and SW and create multichannels

For this purpose, the HW will have a virtual environment instead of the operating system. Several products are available, such as VMware or KMV. This combination of HW and virtual system provides and organizes the resources. To make these resources available, the virtual environment creates SW- “Connectors”, into which the necessary operating system plugs in. These connectors are available for all operating systems. As such, one processor may easily operate in several operating system apparently at the same time. for an application.

In the design above, there are several clusters planned. Each cluster consists of various computers, which may be of the same kind to easy resource management. However, this is not mandatory. Clusters with different HW components are very common and avoid safety issues based on SPOF due to the variety of systems.
Each cluster is operated by a virtual system. As there are two to three independent clusters planned, different virtualization platforms can be applied, avoiding again SPOFs in the said SW.

The application software will now be installed on basis of the suitable operating system on the virtual environment. As a result, an executable SW - stack is created, which communicates with the resources via the virtual layer and gets resources under control of a hypervisor. It includes the SW from the operating system, the application and the connectors to the resources’ SW-stack executes the application and is seen from the outside as one (virtual) machine, with operating system, application system and resources.

Based on these virtual platforms copies of the application SW can operate on varies platforms in various virtual machines. Each machine represents therefore a channel, several machines create a multi-channel environment as basis for the voting process.

As the process is distributed between

- Different HW
- Different virtual platforms
- High possible number of machines

The basis for voting is very simple to be implemented and creates an extreme high level of safety. w

12. A Solution Based on AUTOSAR

12.1 Automotive Trends and IT-Backend

In automotive industry automated driving is a major technology trend. The standard SAE J 3016 /Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, SAE International/ provides definitions of automation levels for vehicles, which separate different levels of driver interactions and driver responsibilities.

The higher the level of automation, the more responsibilities migrate from the driver to electronic systems, which replace partly or completely driver abilities. For example, during automated driving vehicle electronics takes over the longitudinal and lateral control instead of a human driver. Compliance of vehicle electronics with functional safety becomes significant as in the case of an error a controlled oversteering by a human driver being not feasible.

This especially applies for high levels of automated driving, where the human driver is even released from monitoring of the traffic.

12.2 Safety Compliance for Automotive IT-Backend

An IT-backend provides high computational power and information from the infrastructure, which is not available in local electronic systems. Hence, the IT-backend plays an important role for core tasks of automated driving which depend on high computational power and information from the infrastructure. Examples for such core tasks are complex traffic interpretation, cognitive decision processes for maneuvers or driving strategies.
Finally, the responsibility for the driving task and functional safety compliance extends from local vehicle electronics to the IT-Backend. This results in challenging requirements regarding functional safety for the IT-Backend, which processes the maneuver information and data flows of all included vehicles.

The basis for the realization of driver assistance supported by an IT-Backend is most notably a secured connection of the vehicles, which shows a high level of data security and functional safety. The same accounts for transportation, where connection of vehicles and infrastructure is key.

12.3 Standardization Efforts for Automotive System Software: AUTOSAR

The automotive software standardization AUTOSAR aims at applicability for future automotive market trends like automated driving and IT back-end. For a functional safe IT back-end, which is an overall system consisting of HW, SW and communication, the AUTOSAR SW architecture represents its system software.

AUTOSAR is a worldwide development partnership, which pursues from the beginning the objective of establishing an open and standardized software architecture for automotive embedded computing devices, the AUTOSAR SW architecture.

The key properties of the AUTOSAR SW architecture are the support of scalability to different platform variants, portability of software and availability of different SW architecture implementations by different AUTOSAR solution providers. AUTOSAR SW architecture consist of interface description of basic software modules (BSW), specified black-box behavior of BSW, defined application interfaces between BSW modules and builds a common development methodology based on standardized exchange format. The implementation of software modules themselves is proprietary to AUTOSAR solution providers. Established AUTOSAR solution providers by 2018 are for example Vector-Informatics, dSpace / Elektrobit (now subsidiary of Continental), ETAS, KPIT and Mentor Graphics. Since a couple of years several open source communities are established which push open implementations of software modules like COMASSO or TOPPER. But as of now there is no series implementation existent for such an open source community approach.

BSW modules made available by the AUTOSAR SW architecture can be used in vehicles of different car manufacturers and embedded computing devices of different suppliers. AUTOSAR SW architecture and BSW provides system transparency. SW applications are contained in software components (SWC). Standardized RTE (Runtime Environment) on top of BSW triggers execution of SWCs.

Hardware transparency is achieved by software layer MCAL (Microcontroller Abstraction Layer), which is contained in AUTOSAR BSW and simplifies microcontroller obsolescence management for manufacturers of embedded computing devices. Hence, utilizing AUTOSAR BSW avoids complete redesign of embedded computing devices if an automotive chip manufacturer introduces a new CPU generation.
.

12.4 AUTOSAR for IT-Backend. AUTOSAR Adaptive

In the past years AUTOSAR was extended by several features. E.g. since AUTOSAR 4.0 compliance with functional safety and security mechanisms is integrated in AUTOSAR SW architecture. In 2017, a new branch of AUTOSAR was introduced by AUTOSAR consortium, the AUTOSAR “adaptive” platform. AUTOSAR adaptive addresses the support of huge computational power devices and the transfer of software functions into an IT back-end. Since the introduction of AUTOSAR adaptive, the original branch of AUTOSAR is denoted as “classic” platform.

AUTOSAR adaptive provides Service-Oriented-Communication on IP, POSIX API and Object-Oriented-Programming, which extends applicability of AUTOSAR SW architecture to the IT back-end and derived applications outside automotive electronic devices. Ultra-hazardous activities like aerospace and aviation, nuclear power, chemical and/ or biological reactors, petrochemical, or military stay outside the scope of AUTOSAR adaptive, transportation now is included.

12.5 AUTOSAR for Safety and Security Application

The BSW of the AUTOSAR SW architecture represents the system software in a layered middleware stack. The GOA Framework as established by standard AS SAE4893 is depicted in Figure 18, AUTOSAR BSW satisfies system services of GOA framework and MCAL of AUTOSAR BSW satisfies resource access services of GOA

framework. As stated above, since AUTOSAR 4.0 functional safety mechanisms in the BSW are supported, which enable implementation of functional safe applications.

This is achieved by the separation of functional safe and functional unsafe shares of the BSW and the certification of freedom from interference between the shares. Freedom of interference in AUTOSAR is compliant with ISO 26262, which enforces spatial freedom from interference, temporal freedom from interference and freedom from interference by exchange of information. Spatial freedom of interference refers to the storage. Safety critical data must be protected from access by functional unsafe applications.

This can be achieved either by HW like MPUs (memory protection units), or by SW like redundant bit-inverted data storage. Temporal freedom of interference refers to execution of functions. This is achieved by intelligent watchdogs, which ensure availability of computational power and order of execution for different SW functions, priority-based scheduling with priority ceiling, deadline monitoring and control flow monitoring.

Freedom of interference by exchange of information is achieved by end-2-end-protected communication with checksums and message counters, which enable the detection of inconsistent, corrupted or mislead messages. The AUTOSAR solution from Elektrobit for example, Tresos Safety, provides functional safety compliant AUTOSAR-OS (see Figure 38).

Security extension of AUTOSAR adds data integrity and encryption mechanism to AUTOSAR SW architecture, which enables the inclusion of wireless communication as communication path and finally simplifies implementation of embedded function shares into the IT back-end. The use of high computational power in IT back-end finally is achieved by AUTOSAR adaptive approach, which even is intended to spread AUTOSAR from automotive embedded electronic to other technology sector as transportation, for example.

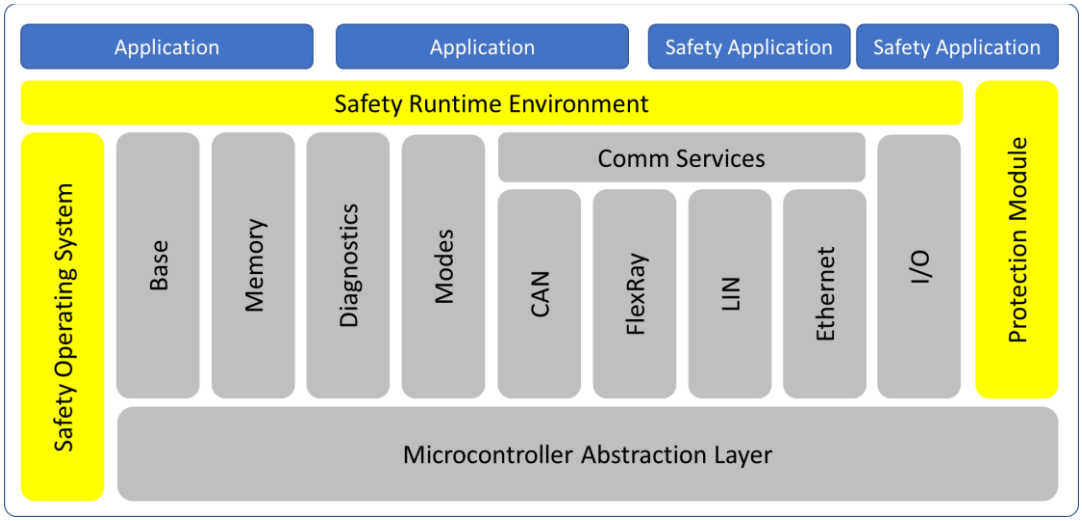


Figure 38: AUTOSAR SW Architecture with safety BSW

12.6 Hardware for AUTOSAR SW Architecture

Predominantly AUTOSAR SW architecture is an approach for middleware or system software standardization. It provides taxonomy and processes in order to easily port and maintain application software and thus reducing overall design costs for electronic devices. AUTOSAR does not specify composition nor architecture of computation hardware, it only takes microcontrollers or CPUs as a given. Actually, AUTOSAR SW architecture is completely HW independent.

In order to adapt to a variety of computation hardware, MCAL as a layer of AUTOSAR stack (see Figure 381) abstracts microcontroller resources like memory, communication, I/O and CPU services (watchdog, general purpose trigger etc.). MCAL layer strongly depends on individual internal design of the microcontroller and is mainly provided by the automotive chip manufacturer. In turn providing an MCAL layer means additional effort and costs for the automotive chip manufacturer, so development of AUTOSAR MCALs lead to a narrowed product spectrum of automotive microcontrollers. This was intended by AUTOSAR consortium achieving nearly standardized HW with low piece costs without defining real standard HW. On the other hand, not having a real fix standard for HW leaves room for innovation in microcontroller design.

Finally, having a standardized middleware but no real standardized microcontroller HW leads to the market situation, that no standardized COTs for AUTOSAR currently exists. There are some IMA-like (Integrated Modular Avionics, see above) electronic devices with high computational power already developed for on-board integration (e.g. Samsung and TTTech) and some companies advertise own hypervisors for AUTOSAR and non-AUTOSAR mixed virtualizations for such devices (e.g. Lynx Software Technologies). But there's still a way to go for the manufacturers of these devices until off-board solutions based on AUTOSAR, especially AUTOSAR adaptive platform, will be available.

12.7 Functional Safe Software Development based on Standardized Software Architecture

Software is different than hardware. Software consists of algorithms, that have no deterioration nor spontaneous failures. Thus, redundancy for software is not necessary, as long as hardware platforms carrying the software have redundancy for the case of a hardware failure. Diverse redundancy for software development in the way of having separated organizations mainly addresses ensuring unambiguity and completeness of software safety requirements.

Thus, any software architecture used for computation units in the RCDC must provide the same interface to the functional safe software module to be integrated unchanged. POSIX is a standard for application interface, which supports same interface for a software module on different hardware and middleware platforms. Hence AUTOSAR consortium promoted POSIX as application interface to achieve support of functional safety for AUTOSAR adaptive platform.

13. Comparison of the Three Solution Approaches

In this section, the conclusions for the usability of the different approaches will be summarizes. Main driving factor is the compliance to the requirements for a SBB Rail Control Centre as outlined in chapter 2.

For that purpose, a complete validation of the requirements against the properties of the three approaches has been made. As the validation brought many results, it is attached as Annex A.

13.1 Conclusion for a Solution based on Embedded Systems as used in Avionics

The architecture concepts of Integrated Modular Avionics (IMA) are not directly applicable to the design of a data center implementing rail control functions. The main reason for this separation is a difference in the environmental conditions and requirements. In an avionics environment environmental conditions are a main driver for hardware design. This is certainly a reason together with safety attributes that avionics hardware is much more expensive than usual COTS computers.

A second reason may be that the IMA architecture concept is more than 10 years old and it is built on technological assumptions, which might no longer prove true today or in additional 10 years. The main reason is that the IMA architecture is based on an assumption on how avionics applications must be built in order to optimize SWaP (Space Weight and Power) attributes of an avionics system. This approach integrates the management of storage resources into the applications. This has the effect that IMA architecture does not provide concepts for storage virtualization. SWaP attributes are of much lesser importance for the design of a data center.

Therefore, a key-turn solution is not available.

Nevertheless, an approach has been described, which is based on IMA architecture principles and available hardware. For this approach there are still open questions, which have to be investigated in order to find an architecture that fulfils the requirements.

This is a feasibility study. The result is that there are no show stoppers, yet. A more detailed architecture has to be defined and assessed.

13.2 Conclusion for an Overall Design based on AUTOSAR

An overall system design of the computation units of the RCDC based on AUTOSAR is also not available yet. AUTOSAR classic platform and AUTOSAR adaptive platform provide inherent properties for future computation units like the support of a defined level of functional safety (compliant to ISO 26262), provided that electronic device manufacturers will address off-board solutions for high computational power units. This scenario is very likely for the future, because off-board applicability is one of the key-feature, that is addressed by AUTOSAR adaptive platform. Additionally, on-board integrated high computational power units are currently on their way to series production and will be COTs in a few years (we estimate quicker than 5 year).

The remaining issue to be resolved is the design of an SIL4 compliant RCDC based on ISO 26262 compliant computation units.

A possible solution would be the separation into system functions with lower safety requirements of SIL 3 and below, provided that SIL 3 compliance is achievable with ASIL D compliant computing units, and system functions with SIL 4 in own SIL 4 compliant computing units.

A further solution is finding an appropriate composition of ASIL D compliant computing units to achieve SIL 4 compliance (see chapter “System architecture” above).

Finally, motivating ASIL D compliant electronic device manufacturers to design SIL 4 compliant electronic devices, that may be utilized in a ASIL D product strategy, is an additional possible solution.

By now, a single possible solution of the three proposed cannot be favorized. Because of the significant economic potential of utilizing large scale production electronic devices with a high share of standardized components, SW and partially HW, it is recommended to further follow up on AUTOSAR classic and adaptive platforms.

It must be noted, that today’s AUTOSAR is only used for single cars with only 1 to 7 persons on board, reflecting a certain maximum of causable damage.

The current main application of AUTOSAR classic platform today is not in data centers, but as stand-alone device on board with numerous interfaces to other devices. AUTOSAR adaptive platform aims at high performance computing for on-board-devices and data center. It is available since 2017 and hence not implemented in current solutions yet. ESG expects, that within 5 year market penetration of AUTOSAR adaptive will be achieved.

13.3 Conclusion for a Solution based on a Classical Data Center Design

The intended use of a classical data center structure with inexpensive IT mass products for a safety critical use is breaking new ground. The requirements to be fulfilled tend very much to embedded solutions and cannot be transferred totally to a data center architecture. However, the above-mentioned mass products have reached a very high grade of maturity with a significant rise in performance and an even higher drop of price.

The draft concept for a RCDC has shown, that a pure professional data center will not be able to fulfil the requirements. Certification to SIL4 will be – if not at all impossible – very difficult and expensive. Therefore, a special design has been developed for the RCDC.

The base thought is to mix elements from classical data centers, automotive and avionic components and safety critical SW design in a way to use the best performances from the different components in a suitable system design to compensate for shortfalls some components may have in price or performance.

Finally, a design was applied, which, based on a classical data center, uses SIL4 certified equipment only in limited way, and mass products for the majority of computation tasks. If operated with certified SW this design is not only able to replace the current solutions with partly by far outdated HW, but provide an even better service at a significant lower price. Certification is especially possible, if for the few locations being in need for SIL4 certified equipment already certified equipment is used, despite the high cost for these products.

As far as SW is concerned, the design of new SW needs to follow several special principles in design, production and auditing typical for railway use and other safety critical applications in order to be able to be certified. This holds water also for today's SW, which has been developed for specific HW and may now be up for replacement. Therefore, it is recommended to use SW-Design processes as being common in automotive and air traffic use. Some statements on applicable principles have been shown in that document.

All solutions – even existing Hard- and Software - would have to cope with new requirements, stemming from the system design of SBB. Mainly data transfer and remote operation is an increased requirement, which is to be fulfilled in a new way, and risks from that new remote structuring have to be countered. A cyber-attack on operational systems is todays reality, anybody acting in any way in the public, is subject for such an attack. Padlocks at doors provide no security anymore, as the telecommunication paths outside the building will be attacked. Using highly spread technology opens the way to highly spread counter measures at very low costs. Using specialized equipment from yesterday makes hardening for such components necessary – and this may very well be in vain, as these components have not continued to develop in a more complex threat environment and lack the necessary properties for countermeasures.

Although the proof of feasibility for this approach seems to be successful, it must be understood, that this document is just a feasibility study. A real design has to be undertaken, and the proof of SIL4 capability has to be presented. Sizing to the requirements of SBB has not yet been touched. Interfaces have not yet been defined and the IT-reality outside the data center is still rather unclear.

But due to the high number of datacenters around, a vast amount of solutions for all kinds of applications of similar kind and a fast-growing community in the field of industry 4.0 knowhow is growing fast and works towards solutions based on data centers.

It is therefore recommended to follow on with a detailed design of the overall system, sized to the requirements of SBB and start preparation of the certification process as soon as possible.

14. Summary and Way Ahead

14.1 Summary

Based on the findings and considerations above, the design basis for the system design of the RCDC is defined.

The use of IMA (avionics) as embedded approach needs adaptation and further investigation on suitability. Economic factors speak against the currently available solutions as well as the limited market for such products. The properties of such existing systems deliver high performance in areas, which are not required in a data center, but lack features to use the advantages of modern data center in design, operation, maintenance and life cycle costs.

The automotive AUTOSAR approach proves not yet to be mature. Due to the fast development in this area and a growing market further observation is recommended. In the future, the currently available components with SIL4 certification may well be replaced by that approach.

The best todays methodology to develop such a system will be a concept, which combines the advantages of the presented technologies with the requirements on system safety to a classical data center with special features and structures. Therefore, the RCDC shall have the following properties:

Layered safety approach

As the gateway to the external systems SIL4 system and safety management computers with moderate level of SIL shall be used. The approach separates resources running applications from resources managing the system and its overall safety. The main computational tasks will be provided by standard servers and other mass items of general use in data centers such as storage devices, networks etc. These COTS-products would require reduced SIL capability (depending on the certification approach, see below). Management resources would be specific SIL4 devices with limited COTS percentage.

Cross-certified COTS servers

The achievable percentage of COTS depends on the certification basis (IEC61508 or EN5012X) and possible cross-standard-certification, as well as the level of diagnostic coverage of the COTS parts possible from remote or by attached watchdog-like diagnostic devices. Close cooperation with selected equipment manufacturers would ease qualification of the COTS parts.

14.2 Way Ahead

Actually, there are two rather independent paths which need to be followed in parallel:

- Certification and hardware
- Preparation of application software interface.

Related activities can be prioritized as detailed hereafter. While priority 1 and 2 activities can be executed in parallel and rather independent of each other, priority 3 activities are to commence at a later date, when all actions 1 and 2 are – if not completely finished – far advanced.

Priority 1a: Certification and Pre-Certification

Early involvement of certification authorities is highly recommended as this design is a ground-breaking concept. The early inclusion of authorities will identify safety concerns which may have immediate impact on the system design.

Various types of Standard COTS servers with SIL0 should be selected and the gaps identified to be used in the proposed system structure early.

The use of already qualified COTS components with SIL4 capabilities, but general server structure for the use in data centers is recommended, as it could be proven, that such equipment exists. Further manufacturers are to be identified to trigger the intended market and competition, and to provide the necessary diversity.

It is recommended to build a downscaled demonstrator as subject for the certification, which is to be refined during the certification process if the need arises.

Priority 2b: Fine System Design of RCDC

Subsequently the design of the RCDC has to be completed to a - by far higher! - detailed grade than today, considering also the surrounding elements, interfaces and the total environment of the RCDC. Such a design requires close interaction between designer and SBB to define the necessary input data to produce a reasonable system. Some necessary items to commence with the design are listed in Annex C to this document.

The availability of equipment with SIL0 and SIL4, their maintainability and their safety and security features need to be combined in an optimized structure, using state-of-the-art data center topologies and techniques. A mix of standard COTS equipment for SIL0 and of nonstandard (embedded?) systems may be considered.

Very important are also descriptions of the interfaces, bringing the design in the top-down process one step further.

The applications to be used need to be taken into consideration at that point in time, as there are interactions to the virtual layers, the used operating system(s), and the programming tools.

A LCC estimation is to be done in line with the definitions of SBB on the planned design and a design completely made from SIL4 components to compare the cost impacts.

Priority 2c: Definition of a standardized API

The use of standardized operating systems allows the definition of a standardized API as basis for software development and engineering. This API should be defining inn due course and contain also standardized services beside of the direct access of the applications to the operating systems. There will be at least two APIs necessary for SIL4-equipment and for COTS as the operating systems differ.

Priority 3: Launching of tendering

Based on the findings of this document a general separation and structuring of the tender objects according to their properties is possible.

As a result, detailed technical descriptions can be produced for the tender process as requirement documents.

These technical descriptions serve as frame requirements for software development/engineering.

It is worthwhile to start a dialog with potential providers of services and material to introduce their know how into the design.

Intentionally left blank