D1.3

Initial Drive-by-Data Draft Concept Design

Project number:	730830
Project acronym:	Safe4RAIL
Project title:	Safe4RAIL: SAFE architecture for Robust distributed Application Integration in rolling stock
Start date of the project:	1st of October, 2016
Duration:	24 months
Programme:	H2020-S2RJU-OC-2016-01-2

Deliverable type:	Report
Deliverable reference number:	ICT-730830 / D1.3/ 1.1
Work package	WP 1
Due date:	March 2017 – M06
Actual submission date:	31st of March 2017

Responsible organisation:	TTT
Editor:	Mirko Jakovljevic
Dissemination level:	Public
Revision:	1.1

Abstract:	This document provides an initial set of concept considerations which will be used in the further work. It is a starting point for discussions on Drive-By-Data concepts and solutions.
Keywords:	Drive-By-Data, Integrated Architectures, Net-working, TCMS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 730830.

Editor

Mirko Jakovljevic (TTT)

Contributors (ordered according to beneficiary numbers)

Mirko Jakovljevic, Meta Saatci, Nataša Simanić-John, Georg Gaderer, Arjan Geven (TTTech)

Achim Agster, Bernd Löhr (NEW)

Bernhard Nölte (TÜV)

Mario Münzer (TEC)

Dobromil Nenutil (UNI)

Executive Summary

This document collects initial considerations on Drive-By-Data concepts and challenges, and investigates the capabilities required to create all the necessary preconditions for the development of system integration and topology to support a distributed integrated mixed-criticality embedded platform and architecture, which can host functions with the highest Safety Integrity Level (SIL) and integrate other less critical applications.

The document provides key objectives for integrated modular platform and system integration, and considers specific limitations on both railway industry standards and legacy systems, and networking technology constraints.

Finally an initial set of conceptual considerations and potential options on system topology and architecture are presented. The objective is to establish a foundation which will ensure the success of the later Shift2Rail program phases and lead to marketable integrated architectures for TCMS, in line with Shift2Rail objectives.

Contents

List of Figures

List of Tables

Chapter 1 Introduction

This document focuses on basic concepts for fundamentally simplified electronic architectures and a common distributed/shared embedded computing and communication infrastructure for modular integration of all safety-, time- and mission-critical, and non-critical train functions for railway vehicles. Iterative refinement of these concepts are planned to be released in September 2017 (Deliverable D1.4) and September 2018 (Deliverable D1.9).

SAFE4RAIL investigates the baseline technologies and the capabilities required to create all the necessary preconditions for the development of a distributed integrated mixed-criticality embedded platform and architecture for rolling stock, which can host functions with the highest Safety Integrity Level (SIL) and integrate other less critical applications.

1.1 Key Objectives for Integrated Modular Platform and Drive-By-Data Concept

Drive-By-Data concept aims to support the design of the integrated modular platform (IMP) which can host and integrate many distributed functions. As the network capabilities determine the system integration performance and architecture design space, Drive-By-Data concept is essential for further development of the platform. Drive-by-Data position in the platform is shown in Figure 1.

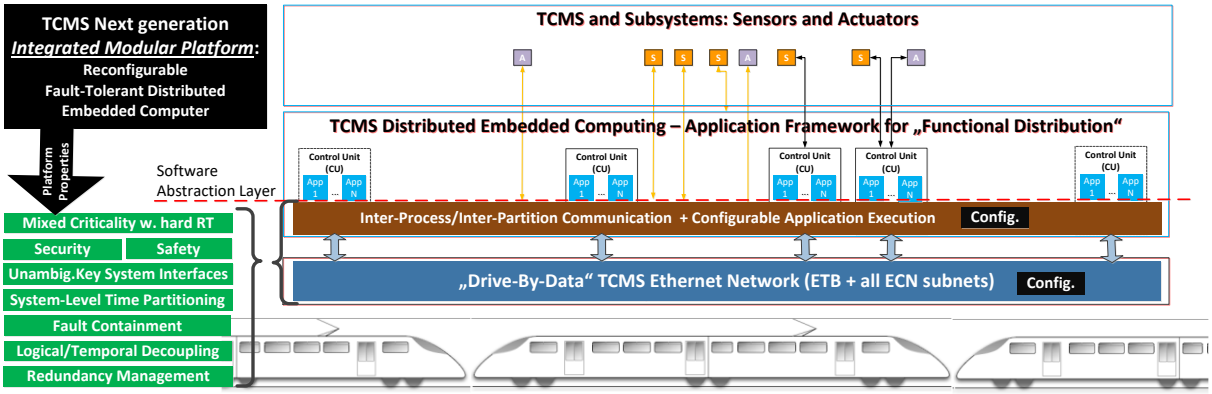


Figure 1. Drive-by-Data in Relation to IMP platforms

1.1.1 Simplified integration

Next generation TCMS will simplify integration of a large number of functions on common computing and hardware resources to reduce system lifecycle costs for design ,integration, V&V, testing, maintenance, upgrades, modifications, extension, incremental certification and modernization and reuse.

1.1.2 Reduced physical system complexity

Next generation TCMS will be highly available and highly reliable integrated platform, which will reduce physical system complexity, volume, number of connectors and decrease wiring length.

1.1.3 Distributed embedded computing

Next generation TCMS will operate as a fault-tolerant distributed computer hosting all TCMS and other brake-by-wire, signalling, safety line, and non-critical applications.

1.1.3.1 Mixed Criticality Integration and Converged Ethernet Integration

Next generation TCMS platform will be able to integrate all critical and non-critical functions relevant for train operation, including functional, performance, safety, security, availability and integrity requirements. Integrated platform for next generation TCMS will support safe (SIL4) and secure (SL 3 and SL4) operation.

1.1.3.2 Simplifed Certification

Integrated modular platform for next generation TCMS will support independent design, testing, V&V and certification/homologation of functions. Timing and performance of all critical functions will be guaranteed, based on system integration configuration. This will also support the reuse, upgrades, extensions, incremental modernization and obsolescence management, as it would not be needed to retest and verify already integrated functions.

1.1.3.3 Defined system behaviour at design time

Next generation TCMS platform will establish and guarantee timing and performance of all critical functions, based on system integration configuration.

1.1.4 Simplified Reconfiguration and Reuse

The IMP will support a (re)configuration management system that is robust and easy to maintain.

1.2 Key Objectives for System Integration

1.2.1 Simplified integration and certification

System integration for next generation TCMS will define all interactions, performance and timing among critical functions in the system by configuration, which will be closely monitored and prevent any network traffic congestion.

1.2.2 Reduced network complexity

High-bandwidth system integration for next generation TCMS will reduce wiring and the number of connectors, and reduce the weight, the number of connections and volume constraints of the embedded system. MVB and WTB will be not necessary at all.

1.2.3 Mixed-Criticality Integration and Converged Ethernet Integration

System integration for Next generation TCMS will provide system integration and communication means for all TCMS, brake-by-wire, signalling, safety line, and non-critical applications, without gateways.

1.2.4 Simplified Reconfiguration for Rolling Stock Use Cases

The system integration will support (re)configuration and interoperability of trains that is robust for different use cases.

Chapter 2 Design Space – Railway Industry

2.1 Introduction

During the search for solutions, an iterative process and trade-off analysis are required to propose viable solution concepts. There are two different sets of constraints – one coming from railway application considerations and specifics, the other from the constraints set by the networking technology constraints.

Railway use cases, standards and IMP objectives provide a set of constraints which shape the space of potential Drive-By-Data solutions. In addition railway use cases are redefined by the introduction of new Ethernet networking capabilities.

The design space of potential solutions and their direction is determined in an iterative process, which takes into account all different constraints and considers workaround, compromises and new solutions as depicted in Figure 2.

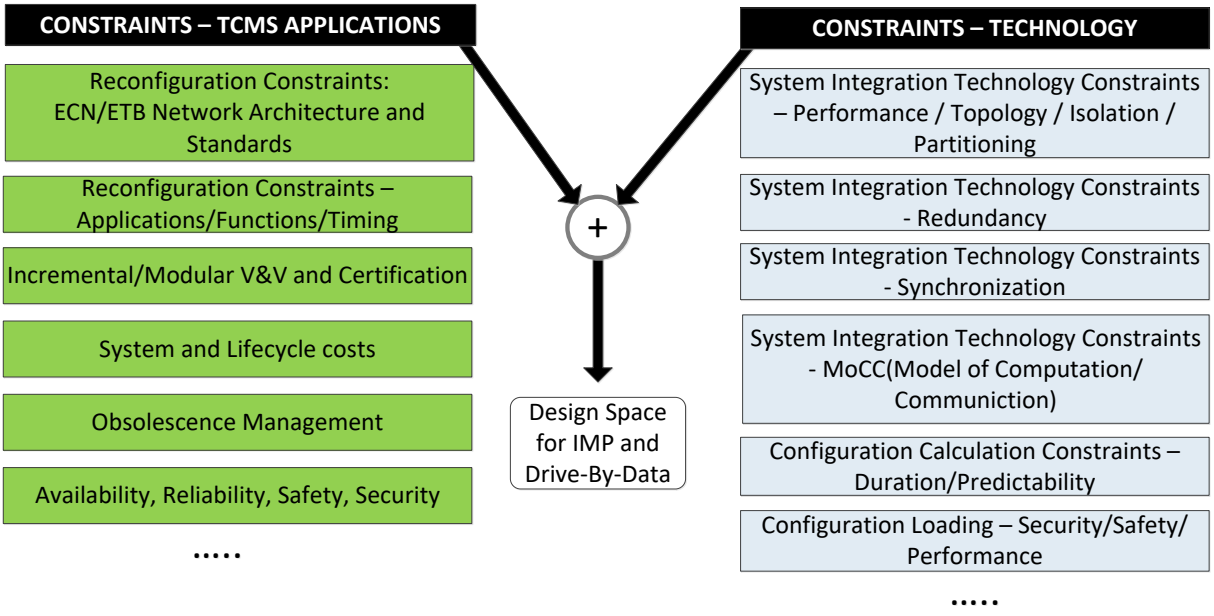


Figure 2. TCMS application and system integration technology constraints

2.2 Applicable Standards

2.2.1 Railway Networks

Communication systems in the railway industry exist mostly as proprietary solutions factorized to meet the requirements of national railway operators and vendors. Apart from the analogue Multiple-unit train control systems mainly used for traction control only the (legacy) WTB/MVB based TCN is described in IEC 61375-1 [1].

Recent additional parts of the evolving IEC 61375-family (Placeholder 8) define a faster TCN based on standard 100Mbit/s Ethernet conformant to IEEE 802.3 and IEC 61076-2-101. Ethernet communication is used as a backbone (ETB) and in car/consist networks (ECN) with higher layer protocols, e.g. TCP/IP, IPTCom or CIP, already. Aside from being

standardized in IEC 61375-2-5 (ETB) [2] , Train Switches/ETB nodes from several manufacturers already support Gigabit-Ethernet (1Gbit/s).

While current trains using these proprietary protocols implement their own coupling methods (inauguration), the evolving new parts IEC 61375-2-5 [2] and IEC 61375-2-3 [3] standardize the TCN in a way that shall allow the coupling of consists built by different manufacturers.

In the current state, this will resolve IP address conflicts and allows leading cab and direction determination.

TRDP [4] has been defined as the inter-consist communication protocol, providing Layer 3 + 4 services using UDP/IP and TCP/IP. For leading-direction related communication, a safety layer (SDTv2) has been standardized, which allows for safety functions up to SIL2. SDT fulfills IEC62280 (EN50159) and supports the transmission of safety related data between a safe data source and one or many safe data sinks.

IEC reference	CLC reference	Title	IEC situation	CLC situation
IEC 61375-1 Ed.3	EN 61375-1:2013	Part 1: General Architecture	Published (2012)	Published (2013) following // vote
IEC 61375-2-1 Ed.1	EN 61375-2-1:2013	Part 2-1: WTB – Wire Train Bus	Published (2012)	Published (2013) following // vote
IEC 61375-2-2 Ed.1	EN 61375-2-2:2013	Part 2-2: WTB - Wire Train Bus Conformance Testing	Published (2012)	Published (2013) following // vote
IEC 61375-2-3 Ed.1	EN 61375-2-3:2016	Part 2-3: Communication Profile	Published (2015) Corrigendum published in 2015	Published (2016) following // vote
TS 61375-2-4 Ed.1	-	Part 2-4: Application Profile	Work in progress	-
IEC 61375-2-5 Ed.1	EN 61375-2-5:2015	Part 2-5: Ethernet Train Backbone	Published (2014)	Published (2015) following // vote
IEC 61375-2-6 Ed.1	-	Part 2-6: On-board to Ground Communication	Work in progress	-
TR 61375-2-7 Ed.1	-	Part 2-7: Wireless Train Backbone	Published (2014)	-
IEC 61375-3-1 Ed.1	EN 61375-3-1:2013	Part 3-1: MVB - Multipurpose Vehicle Bus	Published (2012)	Published (2013) following // vote
IEC 61375-3-2 Ed.1	EN 61375-3-2:2013	Part 3-2: MVB - Multipurpose Vehicle Bus Conformance Testing	Published (2012)	Published (2013) following // vote
IEC 61375-3-3 Ed.1	EN 61375-3-3:2013	Part 3-3: CCN - CANopen Consist Network	Published (2012)	Published (2013) following // vote
IEC 61375-3-4 Ed.1	EN 61375-3-4:2015	Part 3-4: ECN - Ethernet consist network	Published (2014)	Published (2015) following // vote

Figure 3: TCN standards

2.2.1.1 Timebase dissemination

Relevant standards are IEEE1588 [5] and its profiles. For safety critical and fault-tolerant time dissemination SAE AS6802 [6].

Other ERTMS/ETCS standard discusses the dissemination of time over two independent fieldbuses [7] and could be theoretically considered for railway-specific design concepts in Ethernet networks.

2.2.2 Safety and Security

The set of standards containing the EN 50126 series [8] , EN 50129 [9] and EN 50128 [10], comprise the railway sector equivalent of the EN 61508 [11] series, a general standard for functional safety in electronic safety-related systems, as far as Railway Communication, Signalling and Processing Systems are concerned. To cover the safety-related communication in such kind of systems that set of standards was completed by EN 50159 [12].

Figure 4 shows the decomposition of total railway system and compares their scope.

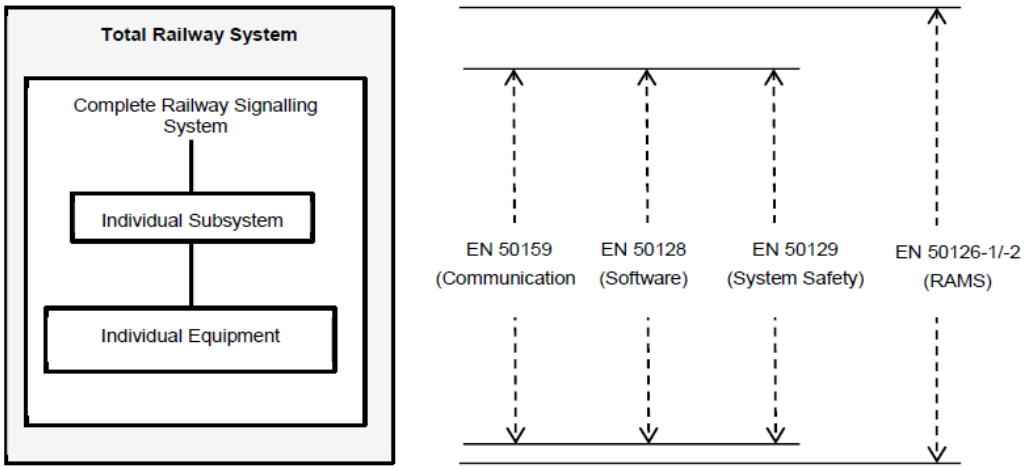


Figure 4: CENELEC railway safety standards and their scope

Even though the new versions of EN 50129 (prEN 50129:2016), EN 50126 (prEN 50126-1:2015, prEN 50126-2:2015) have been published, the original versions are active. The current pre-norms should be the working versions in Safe4Rail WP1 workpackage.

2.2.2.1 Safety

The set of standards containing the EN 50126 series, EN 50129 and EN 50128, comprise the railway sector equivalent of the EN 61508 series, a general standard for functional safety in electronic safety-related systems. Safety-related communication in railway applications is covered by EN 50159 . The following Figure 4 shows the scope of different safety standards.

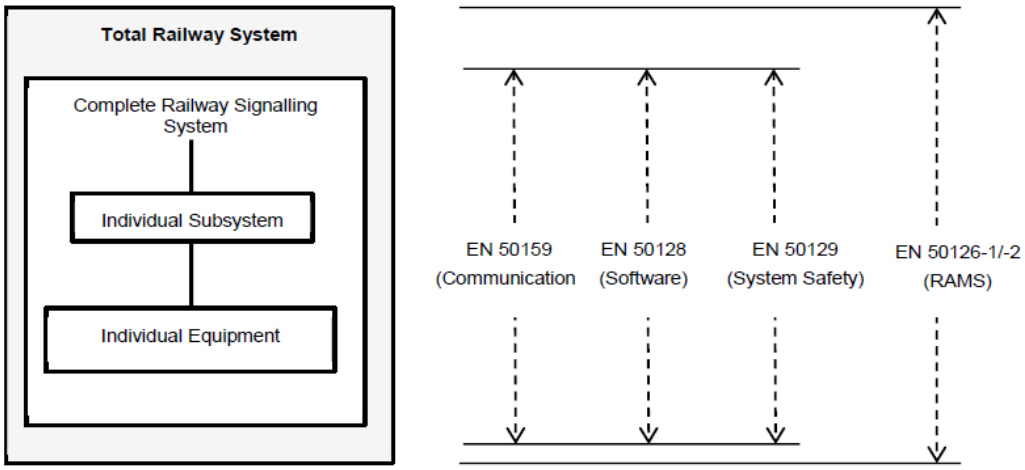


Figure 5: CENELEC railway safety standards and their scope (EN50129)

2.2.2.1.1 EN 50129

The standard EN 50129 “Safety related electronic systems for signalling” defines the lifecycle processes and certification evidence required for the acceptance of safety- related electronics systems, including the description of element required for defining safety cases.

This standard defines the requirements for the overall safety-related electronic system and for its hardware aspects. Other requirements (software, communication) are defined in associated CENELEC standards – EN50128 and EN50159.

2.2.2.1.2 EN 50126

The EN 50126 defines processes and analyses required for demonstrating the accomplishment of RAMS objectives in different railway applications. This documents applies to complete railway systems, separate major systems and sub-systems and components within these major systems which include software.

2.2.2.1.3 EN 50128

The EN 50128 – Software for railway control and protection systems - specifies the process and technical requirements for the development of software for programmable electronic systems for use in railway control and protection applications. The standard focuses on the design assurance processes and methodology required to meets the demands for safety integrity imposed on software items.

2.2.2.1.4 EN 50159

The EN 50159 - Safety-related communication in transmission systems - specifies the communication-related requirements for evidence of functional and technical safety. Safety requirements are generally implemented in the safety-related equipment, designed according to EN 50129. In certain cases these requirements may be implemented in other equipment of the transmission system, as long as there is control by safety measures to meet the allocated safety integrity requirements. The standard defines reference architecture for both closed and open transmission systems, classification of the transmissions systems, threats to the transmission systems and possible defences.

This standard does not discuss the confidentiality of safety-related information, and does not prevent overloading of the transmission system.

In Safe4RAIL, key mechanisms for congestion-free communication should be presented.

2.2.2.2 Security and the relevant standards

IT security in the Railway domain will be handled in new standardization project called *Railway Applications - Communication, signalling and processing systems – IT security requirements for electronic systems for signalling* is under preparation in SC9XA of CENELEC. This standard will focus on security risks in safety-related applications and intentional cyber-security attacks. The standard will profile IEC 62443 series, which deals with the cybersecurity in industrial systems. The approach adopted in IEC 62443 will be integrated into the established approaches of EN 50129. As such, the segmentation of the system into security zones and conduits connecting the zones, with separate security risk is required. Unfortunately Security Risk Assessment cannot be compared to systemic errors and therefore it is hard to assess in probabilistic terms. It is expected that potential security threats for safe communications EN 50159 will be incorporated in this standard.

In addition, other standards such as ISO/IEC 15408 has developed criteria for evaluation of IT security in SW/HW products. DIN VDE V 0831 standards relate to railway signalling IT security and common core criteria assessment..

2.2.2.2.1 ISA/IEC 62443

The ISA/IEC 62443 [13] is a series of standards addressing the cyber security for Industrial Automation and Control Systems (IACS). This standard was originally created as ANSI/ISA-99 by the International Society for Automation (ISA) and published as standard by American National Standard Institute (ANSI). Standard series was submitted to IEC for review and consequently approved as the IEC standards. The ISA is responsible for the further development of the standard.

The standard introduces the concept of the zone model reflecting the segmentation of the system into zones which are connected by conduits. The segmentation addresses the case where there are parts of the system with different security requirements, or with the same security requirements but communicating through an untrusted channel. Another key concept defined is *Security Level* (four levels are defined).

ISA/IEC 62443 can be applied to the system and the Common Criteria to some of its components. For instance network devices can be evaluated according to CC making use of existing Protection Profiles (PP). A PP can address a complete device of a given type or its part (e.g. Firewall, VPN Gateway, Web server, operating system).

2.2.2.2.2 DIN VDE V 0831-104

The draft standard DIN VDE V 0831-104 [14] named “IT Security Guideline based on IEC 62443” tailors IEC 62443 for railway signalling systems, and applies to electrical, electronic and programmable electronic safety-related systems. To enable the easy integration of IT security aspects to EN 50129 this DIN standard defines IT security tasks and assigns them to the phases of the safety life cycle. The EN 50159 as well as DIN VDE 0831-102, which deal with safety-related communication, are also the parts of this integration framework.

2.2.2.2.3 ISO/IEC 15408 – Common Criteria

The “Common Criteria for Information Technology Security Evaluation”, standardized as ISO/IEC 15408 [15], is a framework in which computer system users can specify their security functional and assurance requirements through the use of Protection Profiles (PPs), developers can then implement and/or make claims about the security attributes of their products, and evaluators can evaluate the products to determine if they actually meet the claims. In other words, the CC provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a

rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

The CC define 7 assurance levels (EAL – Evaluation Assurance Level), whereas for the levels above EAL 4 secure-by-design techniques with enhanced formality are required (semi-formally or formally designed/verified/tested).

2.2.2.2.4 DIN VDE V 0831-102

The draft standard DIN VDE V 0831-102 [16] “Protection profile for technical functions in railway signalling” (Placeholder11) tailors ISO/IEC 15408 (Common Criteria - CC) for the domain of railway signalling. As it addresses the transmission of safety-related data, this standard complements the EN 50159 as well as EN 50129 with the aspects of integrity, authenticity and confidentiality.

2.3 Train Topology

2.3.1 General Train Topology

IEC 61375-1 defines a train as a composition of closed trains and consists, each consist having one or several vehicles, and each closed train having one or several consists.

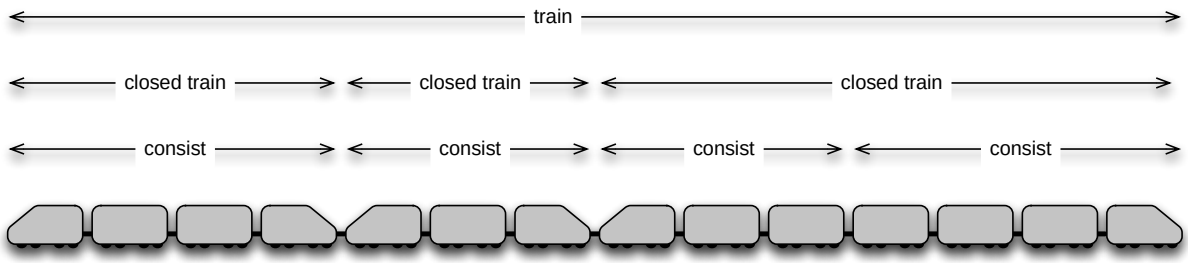


Figure 6: Train composition and hierarchy (IEC61375-1)

Each Ethernet train backbone consists of two redundant 100Mbit/s lines using link aggregation (IEEE 802.1AX).

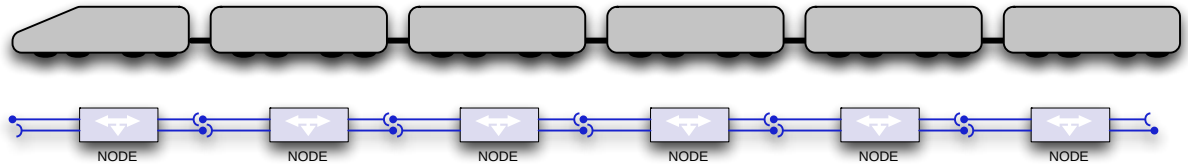


Figure 7: Redundant train backbone archtiecture

Link aggregation as described in IEEE 802.1AX is managed at OSI layer 2 and allows one or more lines to be aggregated together to form a logical group, able to manage the link redundancy.

Link aggregation combines several individual lines, each having a physical and MAC layer. From the MAC client, a single MAC interface is provided.

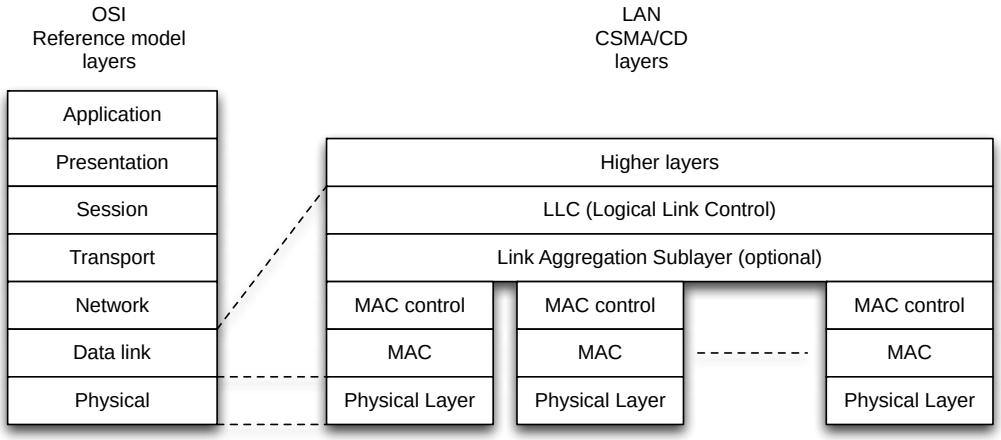


Figure 8: Link Aggregation

Between two ETBNs, there is only one link aggregation group, which contains the redundant Ethernet segments. The link aggregation process is only defined as a relation between 2 ETB nodes. IEC 61375-2-3 and 2-5 define up to 4 parallel backbones (1, 2 or 4).

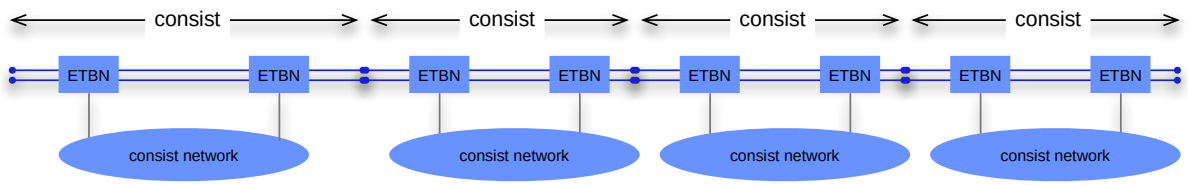


Figure 9: Consists on ETB

The ECN is connected to the ETB via train switches. The label ‘switch’ is misleading – beside switching Ethernet packets on the backbone, it must also route packets between ETB and ECN and also be able to manage a train inauguration.

In future TCM architectures only one common (or redundant) Ethernet network is envisioned, so that the reconciliation among several train-wide Ethernet networks will not be required.

2.3.2 Changing ETB Topology

The basic network topology originates from the classic train car/consist notion, where, in opposite to the automotive or avionic use cases, the overall network topology is not constant. Cars or consists can be coupled, train composition may change. A train fleet usually exists of a series of consists or cars, equipped with the same network (and device addresses).

Although a car is the smallest item from the physical view, it will not necessarily show up as a separate network item. The smallest network part is usually the consist, a group of coupled cars not separated or changed during normal operation.

In this project we are interested only in changing topology configurations and they exist at the interface of consist. Depending on the use case, one consist can have several cars, or only one car.

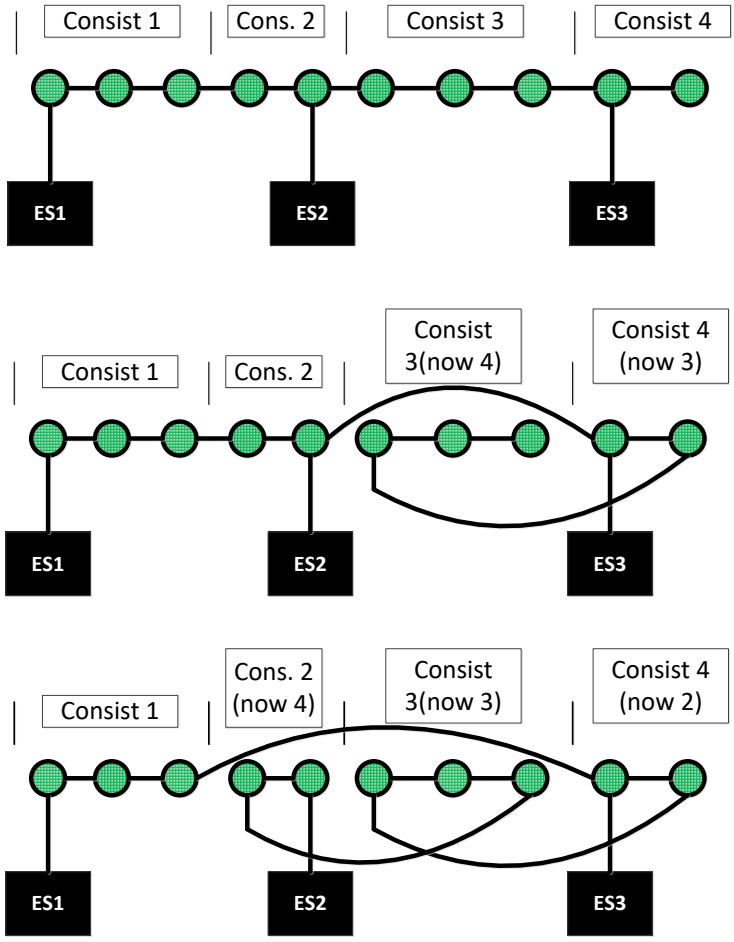


Figure 10: Modifications of ETB topology

2.3.3 ETB Bypass

The nodes on the train backbone are actual switches (on the ETB-side) and routers between the backbone network and the consist network. To ensure high reliability, there should always be a redundant switch in each consist – also to overcome the maximum Ethernet cable length of 100m. In case of a malfunction (e.g. power supply failure), each ETB Node (ETBN) must provide failsafe relays to allow the passive bypassing of ETB traffic.

In passive bypass setting, the ETB lines will bypass the ETB switch, which then is decoupled from the ETB lines (see Figure 11). The Passive Bypass Setting is the default setting in the powerless state and the ETB switch is out of order. This means that in cases when a consist is not powered, the ETB Ethernet network will operate and connect two consist which are separated by non-operational switching devices. This solution was matured and is proven in the railway industry over the last 10 years.

Any ETB solution should ensure that unpowered trains do not interrupt the topology, but also that unpowered train cars, consist or switches may change the topology.

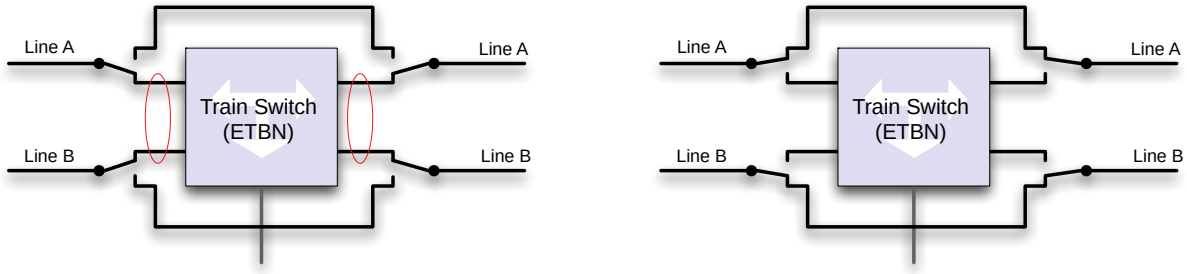


Figure 11: Fallback on ETBN – left: active, right: passive mode

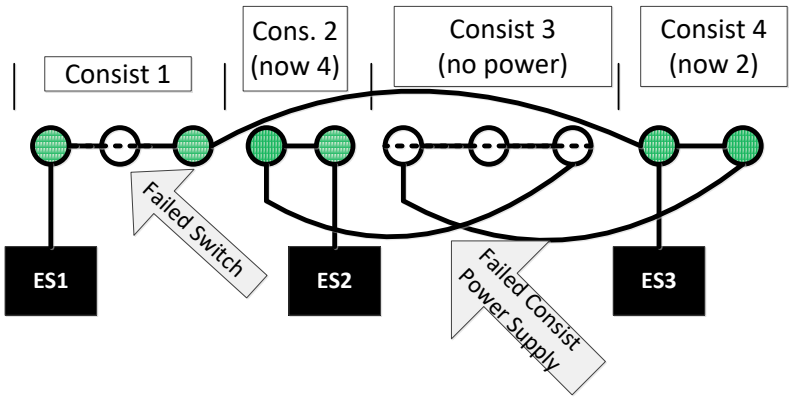
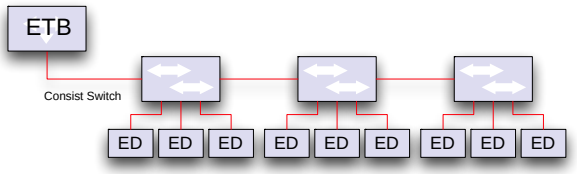
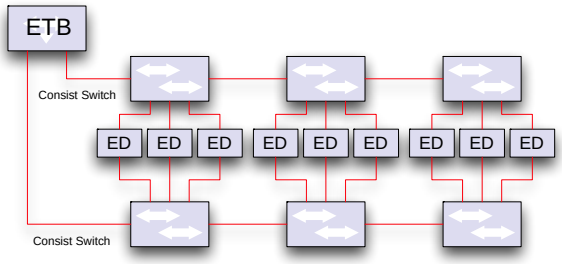


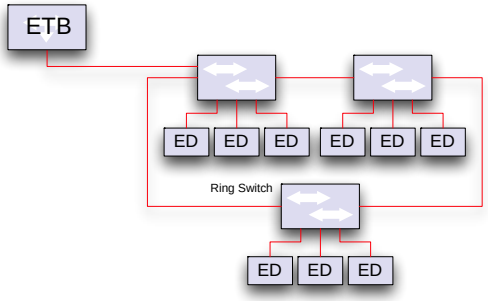
Figure 12: By-pass for topology modification



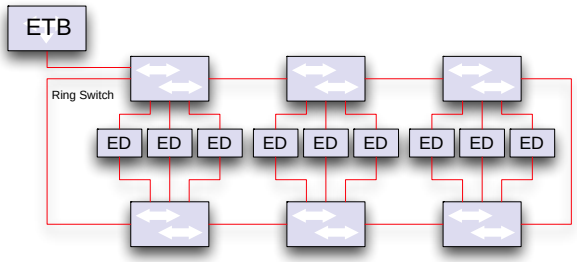
Linear Topology



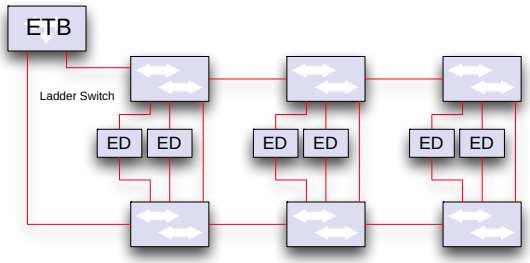
Linear Topology with dual homing



Ring Topology



Ring Topology with dual homing



Ladder Topology with dual homing

Figure 13: Topology Variants for the ECN

2.3.4 Initiating Inauguration

Inauguration is a process which utilizes asynchronous broadcasting messages (TLVs) and a modified LLDP protocols [17] to assess the topology of the network. Afterwards the topology can be complemented (and compared or complemented) with known ETB configuration of the consist. This is used to minimize any errors due to late ETBN switches or startup faults.

After inauguration, this service is executed permanently and establishes train topology status every 400-500ms. This can be used for ETB health monitoring.

Initial inauguration consists of two steps, which are executed as a distributed algorithm. First "Hello TLV" messages are spread to the left and right neighbour, and their response is obtained. Afterwards in the second step every node sends its own perception of topology to all other ETBNs in the systems. After every ETBN switch has all information from all other switches it can send out its own complete TOPOLOGY TLV frame. If all received frame CRCs are equal, all ETBN switches have a common agreement on the network topology. If this is not so an application (or driver) shall decide on topology approval after the train consist reconnection process, which from the networking perspective, represents topology reconfiguration.

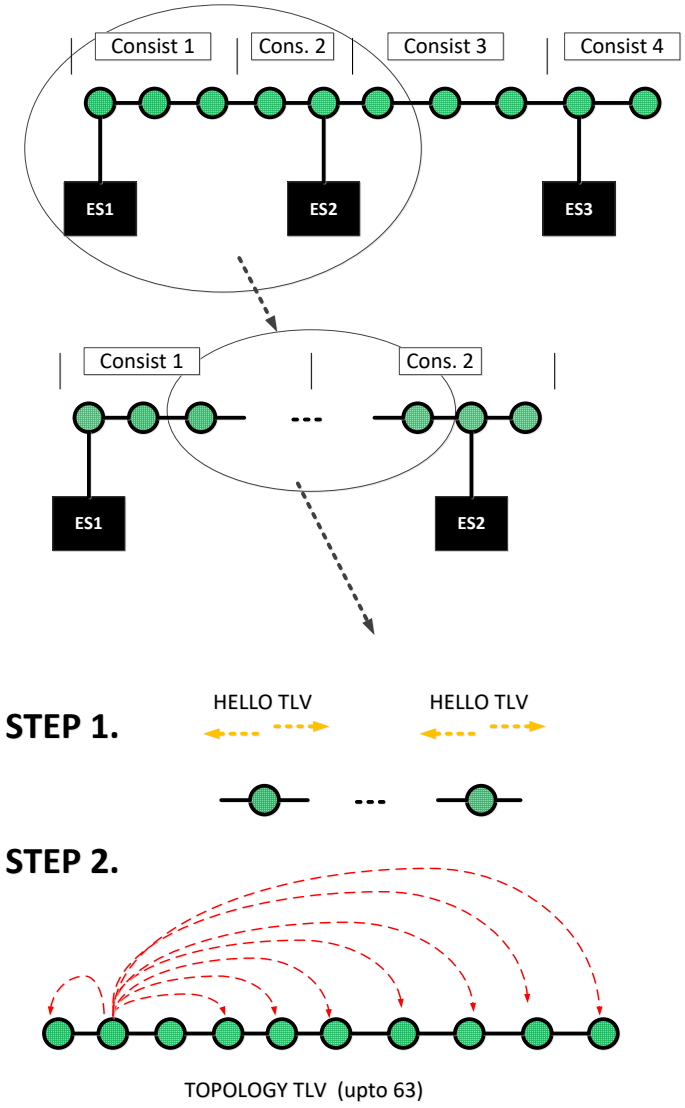


Figure 14: Topology Variants for the ECN

2.3.5 Railcar and Consist Length

As the consist length and internal ETB network topology is not standardized, system architects shall take care of the maximum lengths and margins required for the robust operation of Ethernet physical layers.

If the cable length between two ETBNs exceeds 50m, a repeater needs to be provided (if one ETBN fails and is bypassed, the resulting effective distance would exceed the 100m limit).

2.3.6 Fixed Consist Network

The physical layer of the ECN is defined in IEC 61375-3-4, while addressing and ETB-related control services (ECSP, ECSC) are laid down in IEC 61375-2-3.

The topology of the ECN can be quite different and depends on the vendor's preferences. While some vendors prefer the ladder topology, where each end device is connected to two lines, others use a ring topology or favour a hierarchical approach. Figure 13 presents several topology variants, which can have different availability and redundancy properties.

This consideration is insofar interesting as the ECN network may be just seen as a lower hierarchy network to the ETB network in some design scenarios, but in an unified train network, this may lead to different solutions.

2.3.7 Network redundancy

Network redundancy is not standardized, and every train manufacturer uses redundancy mechanisms which are selected for their own ECN (or ETB) topology. The objective is to create a common set of network and path redundancy mechanisms which can be deployed by all train manufacturers.

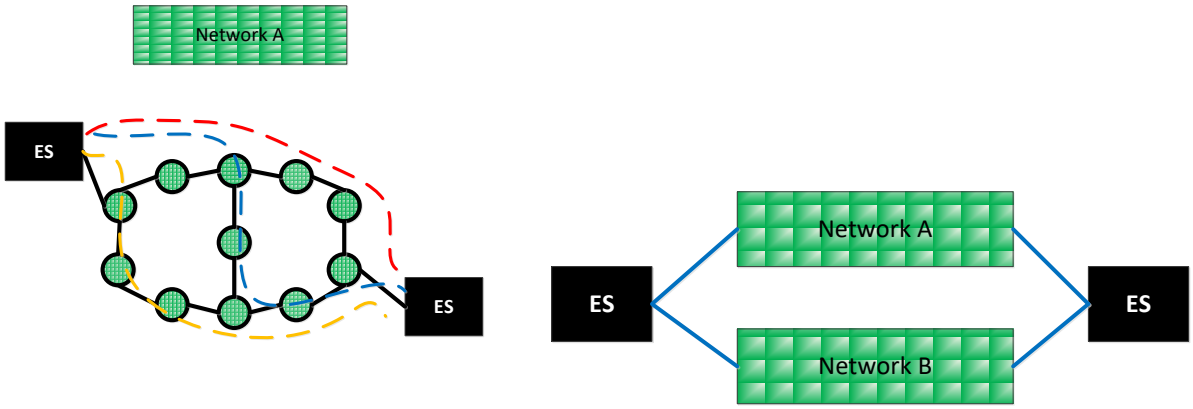


Figure 15: a) Left - Network Path Redundancy b) right – network redundancy

2.3.8 Use Cases

While the mechanisms for network topology finding can be similar, the performance of system configurations, their network size and modification frequency can vary. Several classes of use cases can be recognized, as example:

- High-speed train

- Regional Train
- Metro
- City-Tram

2.4 Obsolescence Management

There is a clear tendency to ensure simplified obsolescence management for different critical and non-critical functions, without any additional retesting and homologation of the whole train. This can be accomplished with zonal approach and robust isolation of zones – physically or logically.

Network certification requires:

- synchronization testing, verification and validation
- network timing constraint verification
- dataflow configuration verification
- workload and fault-injection testing
- network operation V&V
- reconfiguration/topology-related testing

Therefore, on every modification, the system architecture and topology shall be designed to minimize above verification steps on already integrated functions.

2.5 System and Lifecycle Costs

Railway industry provides highly reliable and available means of communication, but the business viability is determined by the system lifecycle costs and CAPEX (initial capital expenses).

The objective of this program is not to reduce the cost of networking components, but to provide further capabilities to support system optimization and integrate all functions on a common infrastructure.

The system architecture optimization can lead to overall cost reduction for the train structure, systems, embedded infrastructure and to enhance rolling stock capabilities.

2.6 Availability, Reliability, Safety and Security

Railway industry provides key infrastructure and transportation needs which guarantee high safety, reliability and availability of transport. In addition it should be robust against security breaches and threats which should not influence safety, reliability or availability of railway infrastructure.

Chapter 3 Drive-By-Data Design Space and System Integration Constraints

Frequent change in topology due to operational requirements (coupling and decoupling of trains, car rotations) can cause many permutations in ETB topology. Additional transient modifications can be induced by power outages on separate railcars or consists via by-pass functions. This is one of essential challenges in design of distributed systems for railway applications.

3.1 Device and Protocol Implementation: White Channel vs. Black Channel

In systems with fail-safe state which can be turned off on any fault of hazard, it is possible to design critical application by using a black channel approach. In addition, the applications are designed not to rely on network for its operation, and may also include some backup or graceful degradation strategies. With integrated complex Ethernet-based systems which host many functions on different computers, “white channel” designs can provide predictable performance, high integrity, availability and reliability required for safe system operation. To become certified, network components are designed using safety assurance processes which support the system safety objectives and high dependability, or the devices should have sufficient operating history in similar critical applications. “White channel” (Figure 16) will require also protocols services and network components to be designed in line with IEC 61508-2.

Figure 7 (a) White channel

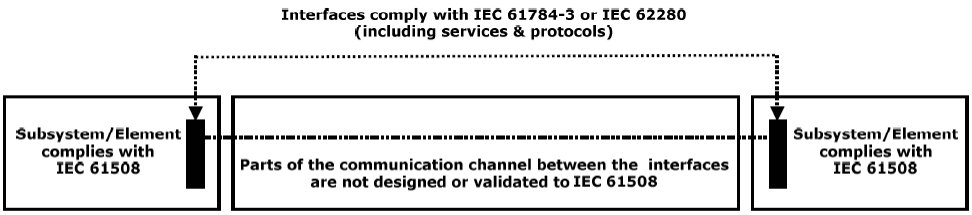


Figure 7 (b) Black channel

Figure 16. IEC61508 Black channel vs White Channel (ref. IEC61508-2:2010)

In aerospace industry, the continuous operation is the only safe state, so the systems are fail-operational. DAL A applications with Ethernet require “white channel” with mandatory deployment of DO-254/DO-178C DAL A design practices (similar to SIL4 safety design assurance practices for software and electronics) on network devices, switches and end-stations. This is done because the availability of the system and seamless recognition of

network device failures shall be ensured. In order to accomplish that more detailed analyses of the internal device functions are required.

In railway industry, typically all functions can be covered by “black channel” approach, which assumes that the recognition of all relevant failures can be done in the safety software layer, and that any type of communication network or protocol can be used, as the system can get into a safe state relatively quickly. For other special cases, additional mechanisms can be developed which would minimize the severity of safety hazards.

The platform for complex IMA architectures is seen as a subsystem which provides the “hosting” service to all other functions. Any system integration faults and errors can create potential dependencies between functions hosted by different hardware modules, and reliability, integrity or availability issues. Therefore an uncontrolled failure of one Ethernet switch could potentially induce a partial failure of the channel, platform and other hosted functions. It is necessary to assess the effects of cumulative functional failures and effects due to single and multiple resource failures at system level.

For IMA architectures, the aerospace industry avoids the use of components which do not have well-understood internal architecture and functionality, can fail unpredictably, and do not provide unambiguous fault diagnostics. The great value is laid on the evidence showing that safety analyses and design assurance for network components has been completed according to best practices and can be accepted by regulatory bodies.

Another important issue for design of systems with a failure rates at 10e-9/hr are so called byzantine faults, which can defeat the fault hypothesis, and no network redundancy could prevent it. “White channel” approach may add value in this case, especially if the network host SIL4 functions, synchronization or mixed criticality dataflows.

3.2 Time-driven Ethernet Communication

Synchronous Ethernet communication has its own set of configuration rules. While asynchronous packet switching was designed for best effort networks, using a limited number of parameters, the synchronous communication requires precise management of dataflow paths in every switch. Typically a switch knows about all incoming dataflows and packets on every port, and the configuration should change with changing topology, on every switch.

This is especially important for functions which are distributed across consists. For functions which are located in one consist it does not make a big difference. The synchronization creates tight coupling among network devices and functions, and topology changes require new configuration for all devices and functions.

The following figure shows how the network path changes on train reconfiguration. The signal or message path will have different latency and jitter in different configurations. Therefore every switch on the dataflow path shall be rescheduled and reconfigured.

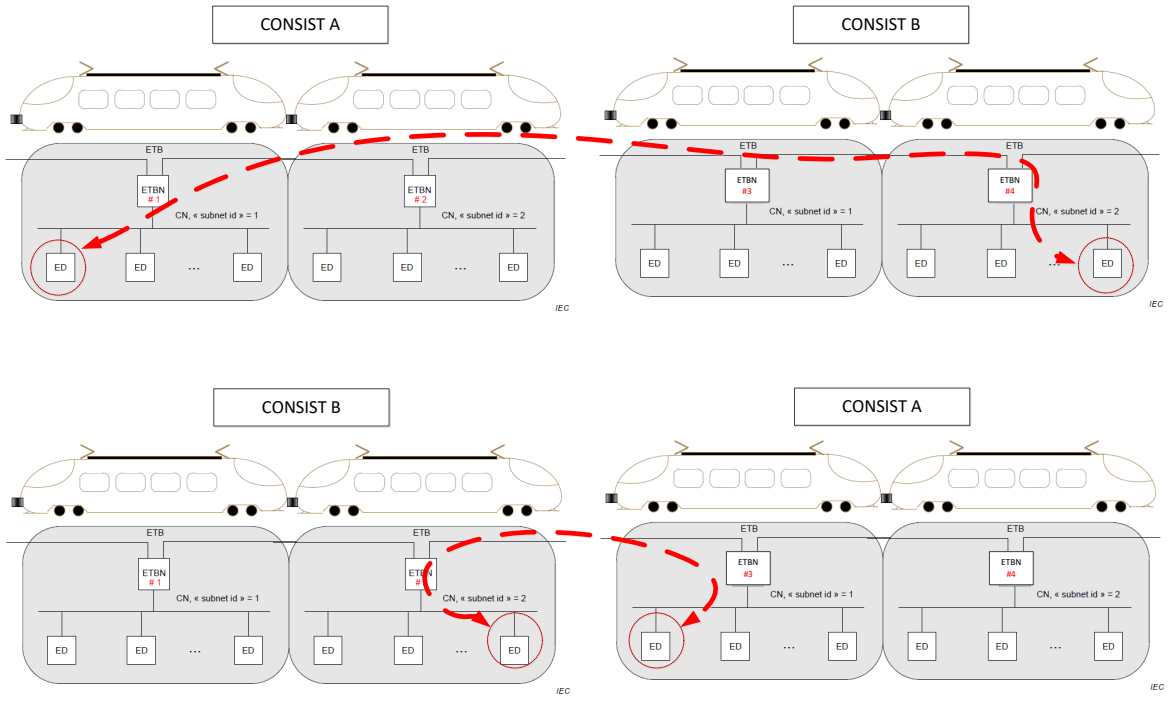


Figure 17: Modifications of ETB topology change the number of hops and path length among two end devices

3.3 Synchronization

In critical integrated systems, the meaning of clock synchronization is significantly different in comparison to data acquisition, measurement or monitoring system applications. The synchronization is essential, as all mixed criticality mechanisms, partitioning and isolation of hard RT control functions rely on robust and predictable synchronization, with synchronization fault detection and isolation. System synchronization is common to all functions and computers in the systems. System synchronization faults can occur in different parts of the system which can lead to functional failure, partitioning/isolation failure or disagreements between different functions about the current system state.

There are two key types of synchronization:

- Distributed system clock with accurate alignment of local clocks
- World time or system clock dissemination

The first variant requires static network with known wiring length and topology and does not require any external time source. System timebase is created by periodic exchange of asynchronous messages between network devices (Placeholder1)[SAE AS6802].

The second variant simply disseminates time information from one source to many or all end stations in the system (Placeholder2)[IEEE1588, (Placeholder3)802.1AS, …]. It does not require static network configuration and can on its own measure wiring length or oscillations.

In design of highly dependable integrated systems, it is essential to cover byzantine synchronization faults which can emerge from the combination of relatively simple errors which can work around fault hypotheses used in system design and propagate to system failure. If not handled correctly, they can lead to hard to predict platform and application behaviour.

3.4 Different Traffic Types and Bandwidth Use

Network configuration and bandwidth use depend on different types of traffic. The numbers can vary depending on the topology and application data exchange constraints. The selected types of traffic will influence the maximum potential information exchange among distributed functions, and integration with audio/video sources.

Traffic Type / Combinations	**Scenario**	**Maximum Bandwidth Use**
Scheduled (Time-Triggered)	Arbitrary Traffic	30-70+% depending on traffic schedulability
	Sensor Fusion from several ports, with equal periodicity/latency/jitter req., and forwarding over one physical link	<95%
	Sensor Fusion from several ports, with different periodicity/latency/jitter req., forwarding over one physical link	40-70%
Reserved (Rate-constrained, bounded latency)	Arbitrary traffic	<30% (typ. <10-15%)
	Sensor Fusion from several ports, with equal periodicity/latency/jitter req and forwarding over one physical link	<50%
	Sensor Fusion from several ports, with different periodicity/latency/jitter req, forwarding over one physical link	<5-30%

. Figure 18. Bandwidth Use for Reserved (asynchronous) and Scheduled (synchronous) Traffic

Traffic Type / Combinations	Scenario	Maximum Bandwidth Use
Reserved + Scheduled	-	See **Reserved**
Reserved + Scheduled + Best effort	-	See **Reserved** + some additional traffic % viable
Reserved + Best effort	-	NA
Scheduled + Best effort	-	See **Scheduled** + additional traffic % viable

. Figure 19. Bandwidth Use and Mixed-Criticality Network Traffic

Traffic Type / Combinations	Scenario	Maximum Bandwidth Use
Reserved + Scheduled + Best effort	**ED send synchronously)**	See **Scheduled** (but a bit lower bandwidth use, due to statistics in multi-hop networks)
Reserved	**ED send synchronously)**	Viable only if best effort is prevent. This mode can be used if network switches recognize the synch loss and turn off all synchronous and best effort communication.

. Figure 20. Bandwidth Use for Reserved (Asynchronous) traffic, and EDs sending synchronously

3.5 Network Configuration

3.5.1 Configuration Calculation Interval

Network configuration is a process which requires the analysis of different traffic and its temporal constraints within the scope of provided ETB/ECN topology. Constrains can be different temporal interdependencies in the network, buffering size, traffic profile requirements (latency, jitter, message order), but they can be also driven by application-level interdependencies, I/O access and delivery, and software partition setup. Topology is also a constraint as it defines the number of hops and paths for every single dataflow.

The calculation interval is not deterministic, and can vary depending on the number and variety of constraints. The network calculation can take between seconds to minutes or hours, depending on the network size and the number of constraints and interdependencies.

This is essential as the complexity of calculation will define the time required after ETBN reconfiguration to recalculate all constrains in the system and generate new configuration.

3.5.2 Configuration Loading

New configuration will be loaded on every switch in the system, which may require some time, assuming there is a calculation application within the train TCMS.

Per switch it could take seconds to minutes to load full configuration. At this time the train will not be operational.

Chapter 4 Design Concept and Solution Space

4.1 Introduction

Previous sections provided some of key boundaries for the definition of design concepts for “drive-by-data” system integration layer which integrates all computer and remote IO units, and can integrate and synchronize the executon of all different application partitions in the system with upto 70 hops (theoretically upto 128 hops if all switches in ETB/ECN network are counted).

4.2 Safety

From the safety perspective, it is assumed that all applications can be hosted by using a black channel approach and turn into fail-safe state. Safety layer will be in addition supported by the network and system integration layer to support congestion-free communication, and guarantee timing and isolation of different functions.

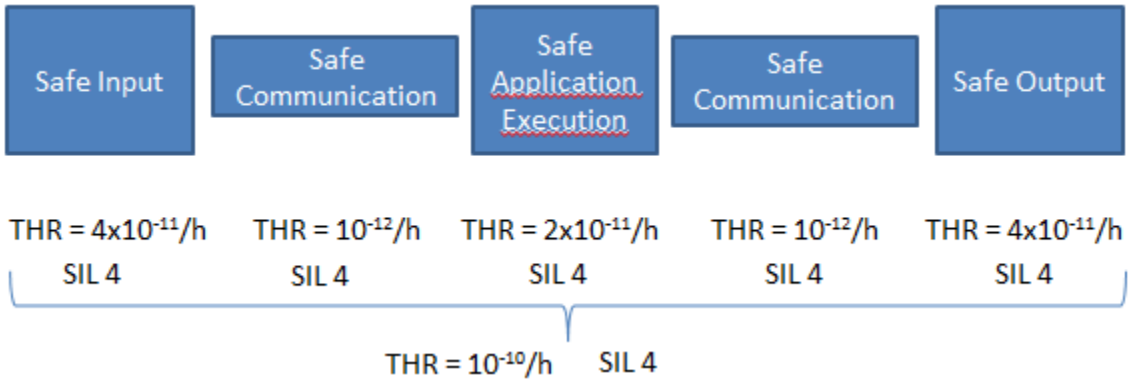


Figure 21. Assumption on Tolerable Hazard Rates For Integrated Systems

SIL4 will require redundant paths for all functions, and the probability of undetected dangerous failure (or Tolerable Hazard Rate in EN50129) per hour should be in the order of 1e-12/hr.

It is assumed that dual electronic structure based on composite/ diverse fail safety with fail-safe comparison, as described in EN 50129 (SIL 4) will be necessary.

4.3 Availability and Reliability

Availability is important to keep the system in operation. The availability of a system depends on the system’s design reliability and maintainability.

System integration availability and reliability can be supported with improved diagnostics and redundancy.

Based on initial assessments the failure rate of the overall train network should be at 1e-12 per hour, and this will probably require ETB redundancy and the redundancy of all data exchange paths to safety IO, assuming the integration of distributed SIL4 functions.

4.4 Asynchronous vs. Synchronous Operation

Tight integration may create challenges in systems which can change their topology due to reconfiguration. Therefore the combination of asynchronous and synchronous communication approaches can be considered. As example, the ETB network can be operated asynchronously and synchronously, while ECN consist networks can be fully synchronous.

Other mechanisms can be considered to decouple ETB network from reconfiguration details, such as virtual bus emulation, with defined maximum latency.

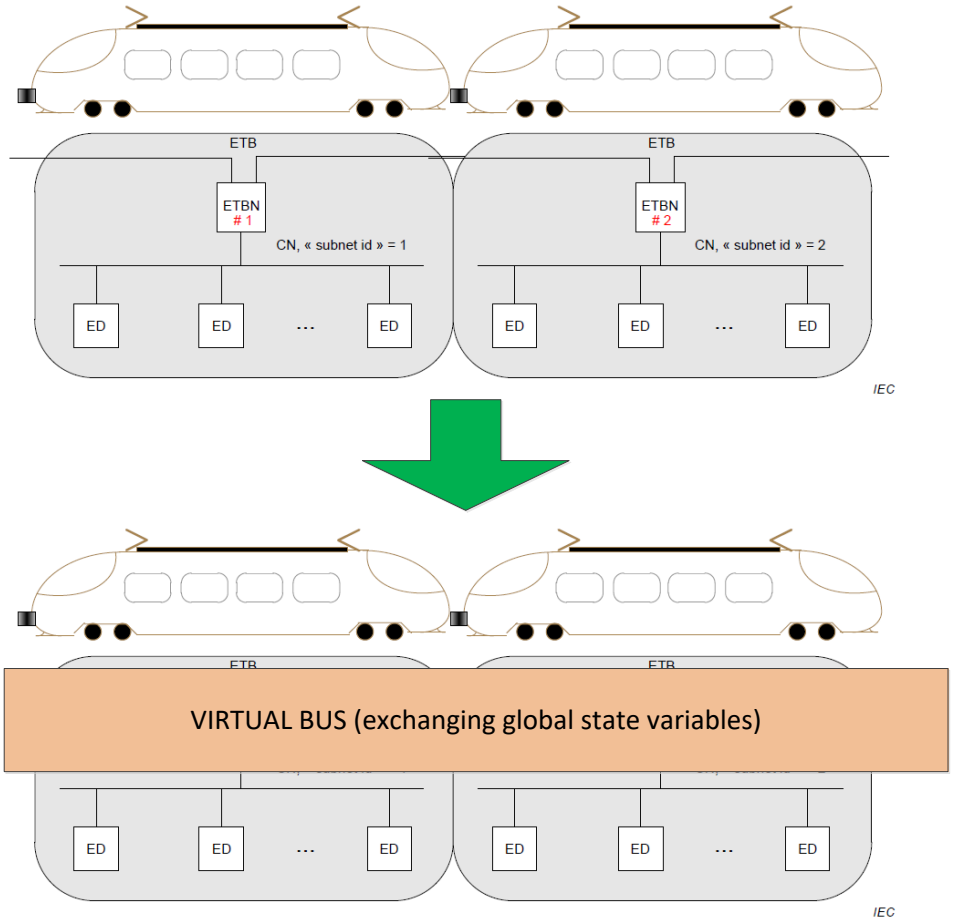


Figure 22. Decoupling of consist via virtual bus emulation

4.5 Separation / Isolation of Functions and Zones

The separation and isolation of different zones can be accomplished by ETB switches which can isolate all different data coming from dedicated ECN subnets, and transfer this data among consists.

In case that the ECN subnets mix all types of traffic, it is possible to exchange less critical or passenger system subnetworks, but the modifications of electronics systems will not be viable without taking a look at all other critical functions and possibly doing complete V&V for the whole train.

4.6 Maintainability, Obsolescence Management and Reuse

Maintainability is a design property of system and determines the simplicity and effort of system repaired or maintenance. The maintainability of a system depends on the standardization, and the modularization of the system.

While it is possible to mix all different traffic classes in one ECN subnet and ETB, this approach would not be aligned with industrial approaches to security, and will increase the cost of obsolescence management, incremental certification and reuse. Therefore some form of physical separation along with logical separation, isolation and resource partitioning will make sense.

4.7 Synchronization

The synchronization of the network will be fault-tolerant and can be controlled at the leading car or consist, and disseminate this system or global time to all other end devices (ED) via redundant channels. It is necessary to prevent simple and complex fault synchronization scenarios. It may be possible to have the synchronization in every consist or define two consist which are allowed to synchronize the system, while the ultimate decision can be approved by a driver based on driving direction.

Furthermore a variant of dual redundant synchronization with additional hot stand-by can be defined to strengthen the robustness of the system.

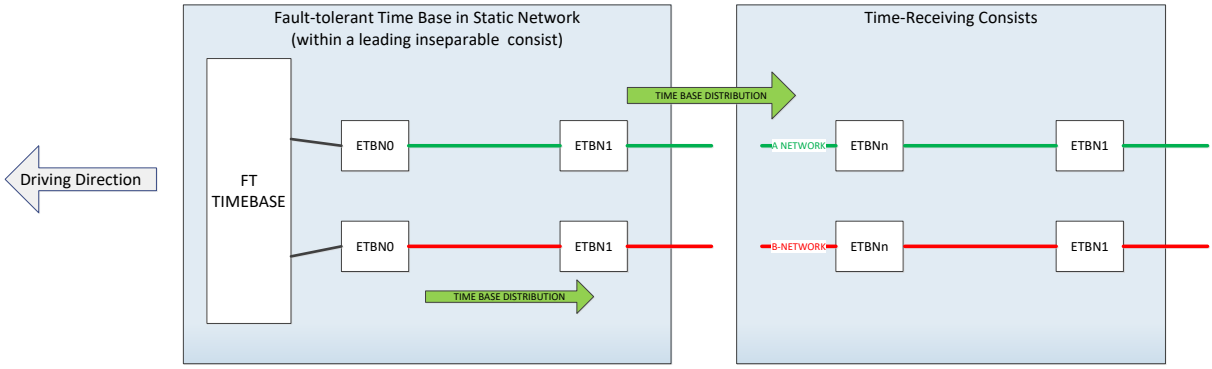


Figure 23. Potential synchronization approach

4.8 System Architecture and Topology

4.8.1 Network Topology

The topology should always be considered in relationship to different industry-specific standards, OEM, regulatory and technology constraints, and should pass the evaluation of different criteria listed in Chapter 2 and Chapter 3.

4.8.1.1 ETB Networks

There are several options which can be considered for rolling stock topologies. One variant (Figure 24) may allow the integration of less critical legacy ECN networks, while all SIL4 functions are integrated only at ETB level.

The second variant (see Figure 25) handles all SIL4 functions in a separate ECN subnetwork.

And finally the third variant (see Figure 26) is to have all mixed criticality functions in one ECN network. With such considerations, this variant can be extended and open for full integration of hierarchical Ethernet network into one flat networked architecture.

ETB topology can be designed as two independent networks or one meshed network with multiple path redundancies. Bypass mechanism at this point seems to be irreplaceable, and there is a need to find solutions which can work around this constraint.

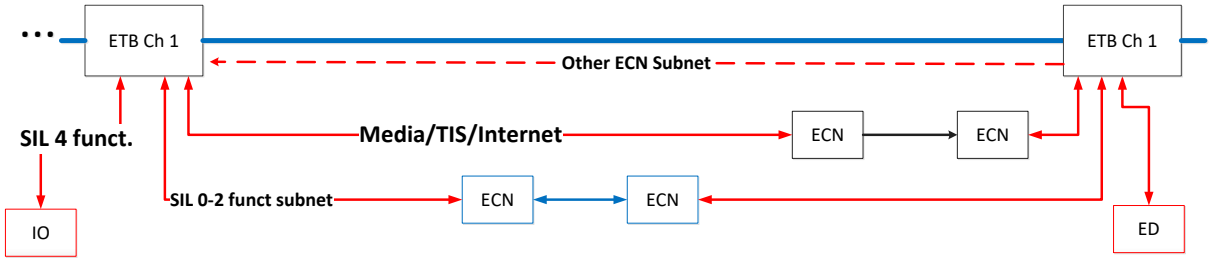


Figure 24. SIL4 functions connected only to ETB

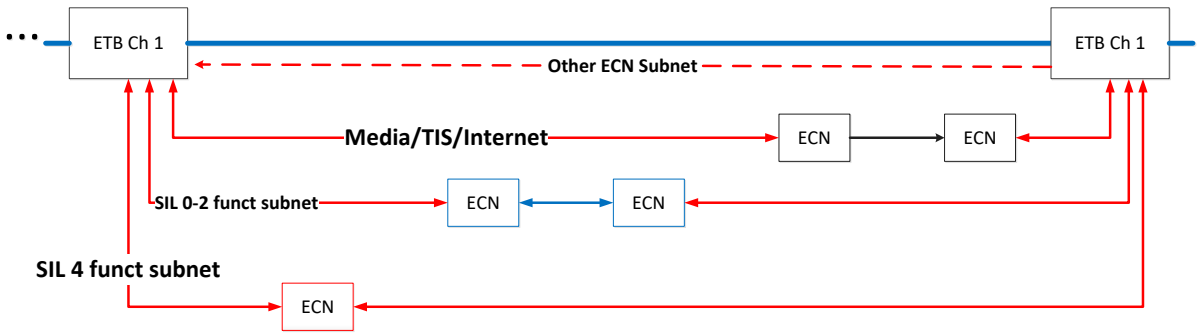


Figure 25. SIL4 functions connected only to ETB and dedicated ECN

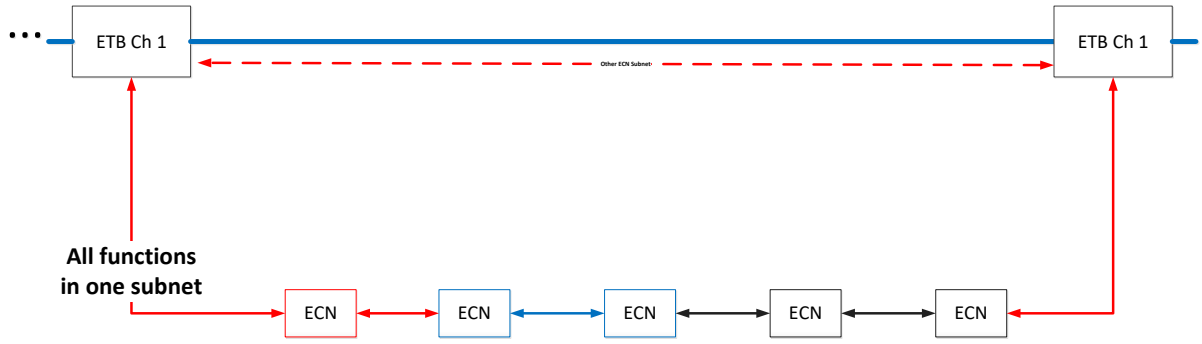


Figure 26. All functions mixed in one Ethernet network – ETB and ECN hierarchy disappears

4.8.1.2 ECN Networks

ECN topology is at the moment free for OEM-specific optimization and considerations. However if the ECN and ETB lose their hierarchical structure and the system architect consider them as one flat networks, then ECN and ETB design space cannot be analysed separately.

Chapter 5 Summary and conclusion

Railway industry is a transportation industry with a specific set of requirements which are different in comparison to automotive and aerospace transportation.
Especially, the differentiating factor is the need for frequent reconfiguration of network topology, and special considerations on failures and safe network switch states in linear topology. In general the number of Ethernet switches can be up to 10x higher in comparison to complex aerospace systems. The system complexity is at least one to two orders of magnitude higher in comparison to automotive systems.

Safe4RAIL focuses on the baseline concepts and technologies and viable proofs of concepts for advanced integrated TCMS, which are emerging from other safety-critical industries (aerospace, automotive, industrial) and from the latest cross-industry electronics and networking developments and standards. Safe4RAIL will undertake all steps to identify and mitigate technology, certification and market risks, and enable the development cycle for advanced integrated Ethernet-based systems and architectures with SIL4 functions.

This documents summarizes a set of considerations which will frame the design space and detailed Drive-By-Data concept in WP1. Core considerations relate to the train topology and the changes therein during operation (inauguration), compared to specific network aspects related to the distribution of a global time base, the establishment of safe communication and the availability of the network required for safe high-integrity operation.

Chapter 6 List of Abbreviations

CAPEX	CAPital EXpenses (initial investment)
CRC	Cyclic Redudancy Check
EAL	Evaluation Assurance Level
ECN	Ethernet Consist Network
ED	End Device
ERTMS	European Railway Traffic Management System
ETB	Ethernet Train Backbone
ETBN	ETB Node (also referred to as Train Switch)
ETCS	European Train Control System
IMP	Integrated Modular Platform
LLDP	Link Layer Discovery Protocol
MVB	Multifunction Vehicle Bus
OEM	Original Equipment Manufacturer
SIL	Safety Integrity Level
SL	Security Level
TCMS	Train Control and Management System
THR	Tolerable Hazard Rate (probility of undetected dagnerous failure per hour)
TLV	Type, Length Value
TRDP	Train Real Time Data Protocol
V&V	Verification & Validation
WTB	Wire Train Bus

Table 1: List of Abbreviations

Chapter 7 Bibliography

[1] IEC, “IEC 61375-1:2012. Train communication network (TCN) - part 1: TCN general architecture.”.

[2] IEC, “EC 61375-2-5:2014. Electronic railway equipment - train communication network (TCN) - part 2-5: Ethernet train backbone.,” 2014.

[3] IEC, “IEC 61375-2-3:2015. Electronic railway equipment - train communication network (TCN) - part 2-3: TCN communication profile.,” 2015.

[4] TCNOpen Project, “TCNOpen,” 2015.

[5] IEEE 1588 WG, “1588-2008 - IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems,” IEEE Instrumentation and Measurement Society.

[6] SAE International, “http://standards.sae.org/as6802/,” SAE Standards, Warrendale, PA, 2011.

[7] UNISIG, “STM FFFIS Safe Time Layer - SUBSET-056,” UNISIG, 2016.

[8] CENELEC, “EN 50126-1:2015. Railway applications - the specification and demonstration of reliability, availability, maintainability and safety (rams),” 2015.

[9] CENELEC, “EN 50129:2016. Railway applications - communication, signaling and processing systems - safety related electronic systems for signaling,” 2016.

[10] CENELEC, “EN 50128:2011. Railway applications - communications signaling and processing systems - software for railway control and protection systems.,” 2011.

[11] IEC, “IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems - part1: General requirements.,” IEC, 2010.

[12] CENELEC, “EN 50159:2011. Railway applications - communication, signaling and processing systems - safety-related communication in transmission systems.,” 2011.

[13] IEC, “IEC TS 62443-1-1:2009. Industrial communication networks - network and system security - part 1-1: Terminology, concepts and models.,” 2009.

[14] DIN, “DIN VDE V 0831-104. Electric signaling systems for railways - part 104: It security guideline based on IEC 62443, draft. October, 2015.,” 2015.

[15] ISO, “ISO/IEC 15408-1. Information technology - security techniques - evaluation criteria for it security - part 1: Introduction and general model.”.

[16] DIN, “DIN VDE V 0831-102. Electric signaling systems for railways - part 102: Protection profile for technical functions in railway signaling, draft. December, 2013.,” 2013.

[17] IEEE802, “802.1AB-2009 - IEEE Standard for Local and Metropolitan Area Networks--Station and Media Access Control Connectivity Discovery”.