OCORA

Open CCS On-board Reference Architecture

CCS Communication Network – Proof of Concept (PoC)

Document ID: OCORA-TWS02-020

Version: 1.00

Release: Delta

Date: 30.06.2021

Management Summary

Today the interfaces between CCS components on the vehicle are proprietary. The proprietary interfaces do not allow to exchange or update CCS components from different suppliers. The OCORA architecture [7] aims for plug and play interchangeability within the CCS domain through the specification of a generic and open communication backbone, the CCS Communication Network (CCN) formerly called Universal Vital Control and Command Bus (UVCCB). The CCN itself will be modifiable in accordance with future technological evolutions by means of strict separation of the different communication layers (OSI Layers).

This document is based on the CCN evaluation report of gamma release [10]. The CCN evaluation report of gamma release [10] proposes the CCN to be a TSN Ethernet based network with the use of SDTv2 / SDTv4 as safety layer. In order to be able to integrate the CCN on the next generation of train communication network (NG-TCN) every hard-real-time CCS device (e.g. CCU, BTM etc.) should have at least one TSN-capable Ethernet port whereas for soft- or non-real-time CCS devices a single standard non-TSN-capable Ethernet port is sufficient. Hard-real-time devices can use both planes of NG-TCN with two TSN-capable Ethernet ports in order to improve reliability and availability. On session layer TRDP 2.0, OPC-UA Pub/Sub (over TSN) or DDS/RTPS (over TSN) are suitable solutions.

The proposed protocol stack of CCN is listed in the following table. Highly recommended standards to be used as reference for procurement in OCORA are listed in **bold** font.

<table>
<tr><th>Layer</th><th colspan="2">Protocol for hard-real-time data</th><th>Protocol for soft- or non-real-time data</th></tr>
<tr><td>(Safety Layer[1])</td><td colspan="3">(SDTv2 / SDTv4)</td></tr>
<tr><td>Session Layer</td><td colspan="3">TRDP 2.0, OPC-UA Pub/Sub or DDS/RTPS</td></tr>
<tr><td>Transport Layer</td><td rowspan="2"></td><td>UDP
TCP</td><td>UDP
TCP</td></tr>
<tr><td>Network Layer</td><td>IPv4</td><td>IPv4</td></tr>
<tr><td>Data Link Layer</td><td colspan="2">Time-Sensitive Networking (TSN)
IEEE 802.1</td><td>Standard Ethernet IEEE 802.3</td></tr>
<tr><td>Physical Layer</td><td colspan="3">100BASE-TX or 1000BASE-T</td></tr>
</table>

Table 1: Protocol Stack CCN

The defined protocol stack allows safety-related and hard-real-time data traffic. For non-safety-related and soft- or non-real-time applications, standard TCP/IP or UDP/IP data traffic over standard Ethernet (IEEE 802.3) can be used on the same physical layer of the CCN.

A demonstrator shall show the feasibility of the CCN as a TSN-Ethernet network. During delta phase, two tasks were defined in this document to be performed during the subsequent phase.

[1] Safety Layer is only applicable for safety-related data traffic.

Revision history

Version	Change Description	Initial	Date of change
1.00	Official version for OCORA Delta Release	SSt	30.06.2021

Table of contents

1 Introduction 8

1.1 Purpose of the document 8
1.2 Applicability of the document 8
1.3 Context of the document 8
1.4 Renaming 8
1.5 Problem Description 8
1.6 Concept 9
1.7 Goal 10

2 Proof of Concept 12

2.1 Tasks 12
2.1.1 Task 1: Small TSN Network Test 12
2.1.2 Task 2: End-to-End TSN Connection Test 12

Table of figures

Figure 1: Technical architecture from [7] ... 9
Figure 2: Network topology task 1 ... 12
Figure 3: Network topology task 2 a) ... 13
Figure 4: Network topology task 2 b) ... 13
Figure 5: Network topology task 2 c) ... 14

Table of tables

Table 1: Protocol Stack CCN 2

Table 2: Protocol Stack CCN 10

References

Reader's note: please be aware that the numbers in square brackets, e.g. [1], as per the list of referenced documents below, is used throughout this document to indicate the references to external documents. Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g. SUBSET-026). OCORA always reference to the latest available official version of the SUBSET, unless indicated differently.

[1] OCORA-BWS01-010 – Release Notes

[2] OCORA-BWS01-020 – Glossary

[3] OCORA-BWS01-030 – Question and Answers

[4] OCORA-BWS01-040 – Feedback Form

[5] OCORA-BWS03-010 – Introduction to OCORA

[6] OCORA-BWS04-011 – Problem Statements

[7] OCORA-TWS01-030 – System Architecture

[8] OCORA-TWS02-010 – CCS Communication Network – Evaluation

[9] OCORA-40-003-Beta – UVCC-Bus Evaluation, Version 1.01

[10] OCORA-40-003-Gamma – UVCC-Bus Evaluation, Version 2.00

1 Introduction

1.1 Purpose of the document

This document summarizes the work done in the workstream CCS Communication Network (CCN) regarding Proof of Concept (PoC). It documents the foreseen tasks. In the upcoming versions the results will be reported in this document as well.

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for on-board CCS. The reader is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [4].

If you are a railway undertaking, you may find useful information to compile tenders for OCORA compliant CCS building blocks, for tendering complete on-board CCS system, or also for on-board CCS replacements for functional upgrades or for life-cycle reasons.

If you are an organization interested in developing on-board CCS building blocks according to the OCORA standard, information provided in this document can be used as input for your development.

1.2 Applicability of the document

The document is currently considered informative but may become a standard at a later stage for OCORA compliant on-board CCS solutions. Subsequent releases of this document will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

1.3 Context of the document

This document is published as part of the OCORA Delta release, together with the documents listed in the release notes [1]. Before reading this document, it is recommended to read the Release Notes [1]. If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [5], and the Problem Statements [6]. The reader should also be aware of the Glossary [2] and the Question and Answers [3].

1.4 Renaming

The CCS Communication Network was formerly called Universal Vital Control and Command Bus (UVCCB). The evaluations on different communication layers during beta [9] and gamma phases [10] concluded to use a time-sensitive Ethernet network as communication backbone. Therefore, the UVCC-Bus was renamed to CCS Communication Network.

1.5 Problem Description

Today the interfaces between CCS components on the vehicle are proprietary. The proprietary interfaces do not allow to exchange or update CCS components from different suppliers. The vendor locking created by proprietary interfaces leads to high costs. The existing proprietary interfaces do not allow to add new functions.

Moreover, these interfaces are implemented using heterogeneous bus technologies. This leads to increased complexity and extensive effort for the operator/maintainer to handle these heterogeneous systems.

1.6 Concept

The OCORA architecture [7] aims for plug and play interchangeability within the CCS domain through isolation of specific functions in combination with the specification of a generic and open communication backbone, the CCS Communication Network (CCN). In the following figure the technical view of the OCORA architecture [7] is shown. The CCN connects all components of the future CCS system. The most important CCS components are:

- CCS computing units (CCUs)
- Driver Machine Interfaces (DMIs)
- Vehicle Locator (VL)
- Balise Transmission Module (BTM)
- Loop Transmission Module (LTM)
- National Train Control System (NTC) or Specific Transmission Module (STM)
- Cab Voice Device (CVD)
- Train Recording Unit (TRU)
- Input / Output Ports (I/O Ports)
- Gateway to Train Control Management System Network, Operator Network or Communication Network (ECN/ECN Security Gateway)

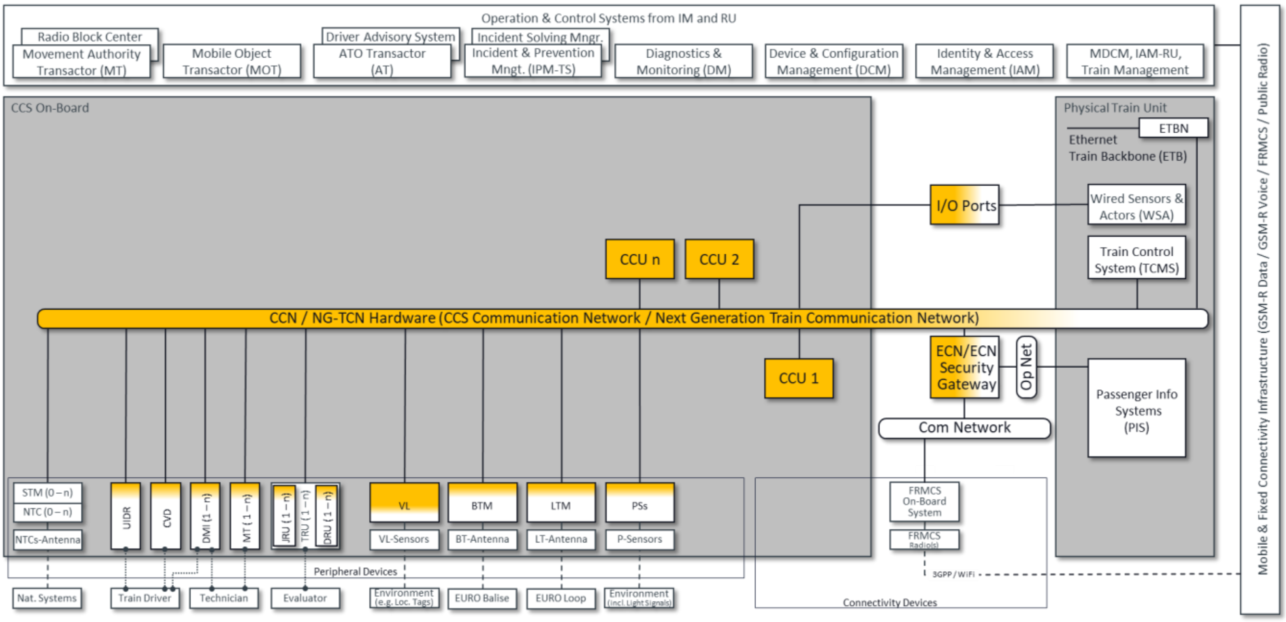

Figure 1: Technical architecture from [7]

In the final vision of the system an open standardized CCN (OSI-Layers 1 to 7 & Safety Layer) ensures the safe data connection between all CCS components. The bus topology allows simple upgrades of the CCS System by new functions or components. It also enables procurement on a component-based way which leads to more flexibility in the life cycle management and optimal components due to larger market size. The CCN itself will be modifiable in accordance with future technological evolutions by means of strict separation of the different communication layers (OSI Layers).

The CCN evaluation report of gamma release [10] proposes the CCN to be a TSN Ethernet based network with the use of SDTv2 / SDTv4 as safety layer. In order to be able to integrate the CCN on the next generation of train communication network (NG-TCN) every hard-real-time CCS device (e.g. CCU, BTM etc.) should have at least one TSN-capable Ethernet port whereas for soft- or non-real-time CCS devices a single standard non-TSN-capable Ethernet port is sufficient. Hard-real-time devices can use both planes of NG-TCN with two TSN-capable Ethernet ports in order to improve reliability and availability.

On session layer TRDP 2.0, OPC-UA Pub/Sub (over TSN) or DDS/RTPS (over TSN) are suitable solutions. These three options will be further investigated considering the system architecture with platform/CCU and the subcomponents.

The proposed protocol stack of CCN is listed in the following table. Highly recommended standards to be used as reference for procurement in OCORA are listed in **bold** font.

<table>
<tr><th>Layer</th><th colspan="2">Protocol for hard-real-time data</th><th>Protocol for soft- or non-real-time data</th></tr>
<tr><td>(Safety Layer[2])</td><td colspan="3">(SDTv2 / SDTv4)</td></tr>
<tr><td>Session Layer</td><td colspan="3">TRDP 2.0, OPC-UA Pub/Sub or DDS/RTPS</td></tr>
<tr><td>Transport Layer</td><td rowspan="2"></td><td>UDP
TCP</td><td>UDP
TCP</td></tr>
<tr><td>Network Layer</td><td>IPv4</td><td>IPv4</td></tr>
<tr><td>Data Link Layer</td><td colspan="2">Time-Sensitive Networking (TSN)
IEEE 802.1</td><td>Standard Ethernet IEEE 802.3</td></tr>
<tr><td>Physical Layer</td><td colspan="3">100BASE-TX or 1000BASE-T</td></tr>
</table>

Table 2: Protocol Stack CCN

The defined protocol stack allows safety-related and hard-real-time data traffic. For non-safety-related and soft- or non-real-time applications, standard TCP/IP or UDP/IP data traffic over standard Ethernet (IEEE 802.3) can be used on the same physical layer of the CCN.

1.7 Goal

The first aim of the delta phase of the workstream TWS02 CCS Communication Network is to investigate network architecture with detailed technical implementation of CCN in NG-TCN (network configuration), cybersecurity, new standards and regulations as well as an evaluation of data serialization formats.

Further, a demonstrator shall show the feasibility of the CCN as a logically separated network on a common physical train communication network (NG-TCN). The composition of the demonstrator helps to investigate the technical implementation details of the CCN in NG-TCN.

The following tasks have been performed during delta phase:

- **Evaluation CCN**
    - **Network Architecture**: Network architecture regarding connections from train to trackside (mobile communication gateway) must be further investigated together with TCMS domain / CONNECTA. Also, DMI concept with different displays from different domains on the driver desk must be clarified in order to define network architecture with its zones and conduits
    - **Detailed technical Implementation of CCN in NG-TCN**: The detailed technical implementation of CCN in NG-TCN shall be elaborated together with CONNECTA. The composition of the demonstrator (WP2) helps to investigate the technical implementation details.
    - **Cybersecurity**: The impact of the security concept of CONNECTA (NG-TCN) on the CCN shall be investigated. As a result of the investigation, the security requirements on the CCN (layers 1 to 6) shall be defined.
    - **New Standards and Regulations (e.g. TSI 2022)**: The work done in different working groups (e.g. IEC TC9 WG43 or ERA TWG Archi) shall be aligned in order to get consistent new standards and regulations (e.g. IEC 61375, TSI 2022, ERA Subsets, OCORA specifications)
    - **Evaluation of Data Serialization Formats**: Data serialization formats of application data shall be evaluated. Possible solutions are: bitstream like in today's subset specifications, XML, JSON, CBOR, Apache Thrift, Protobuf.

[2] Safety Layer is only applicable for safety-related data traffic.

- **Proof of Concept / Demonstrator CCN**: A demonstrator shall show the feasibility of the CCN as a logically separated network on a common physical train communication network (NG-TCN). Also, the impact of TSN-Ethernet versus non-TSN-Ethernet in congested network situation shall be demonstrated. The composition of the demonstrator helps to investigate the technical implementation details of the CCN in NG-TCN.

This document contains the current tasks for the Proof of Concept / Demonstrator. The evaluation part is documented in [8].

2 Proof of Concept

2.1 Tasks

2.1.1 Task 1: Small TSN Network Test

A demonstrator shall show the feasibility of the CCN as a TSN-Ethernet network. In a first step a small TSN network shall be set up. The network topology is shown in the following figure. It contains two TSN capable switches, four standard PCs with standard network interface cards (NIC) and a configuration PC. Between two TSN switches a TSN connection will be established by configuring the switches accordingly through the configuration PC. The connections of the PCs will be best effort standard Ethernet connections, since no TSN MAC layer on PCs with standard network interface cards (NIC) is available. Nevertheless, with this simple network topology with only one TSN connection the TSN features can be shown. The aim of this first task is to show, that the guaranteed traffic (shown in green) cannot be influenced even by a large amount of best effort traffic (shown in red). The bandwidth of the guaranteed traffic will be reserved with the scheduling scheme IEEE 802.1Qbv. To achieve a higher degree of bandwidth reservation the frame preemption scheme IEEE 802.1Qbu shall also be applied. Therefore, different priorities for the two different traffic classes must be established. This can be done easily by separating the traffic in two virtual LANs (VLANs) and setting their priority fields suitably.

The traffic on the network shall be analysed with a suitable network protocol analyser (e.g. wireshark) using a passive tap on the switch-to-switch connection.

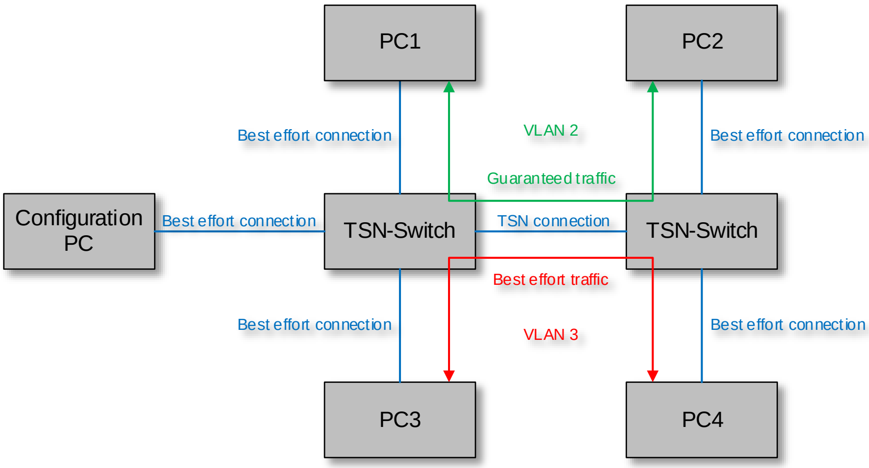

Figure 2: Network topology task 1

In this first task, the transmitted data is standard TCP/IP or UDP/IP data. Only the switch-to-switch connection is covered by TSN technology. The sender and the receiver do not notice anything of the TSN at all.

2.1.2 Task 2: End-to-End TSN Connection Test

2.1.2.1 Part a): Deterministic and Best-effort Traffic on different End Devices

In a second step an end-to-end TSN connection should be established. The end devices PC1 and PC2 should implement a TSN MAC layer in order to send the data packets synchronously to the network. Therefore, a session layer protocol, which can send TSN-Ethernet-Frames, should be implemented on the end devices for the guaranteed traffic. The session layer protocol shall be TRDP 2.0 or OPC UA PubSub over TSN. DDS/RTPS is not yet an option since the DDS/RTPS over TSN standard is not yet released. The protocol stack therefore corresponds to Table 2.

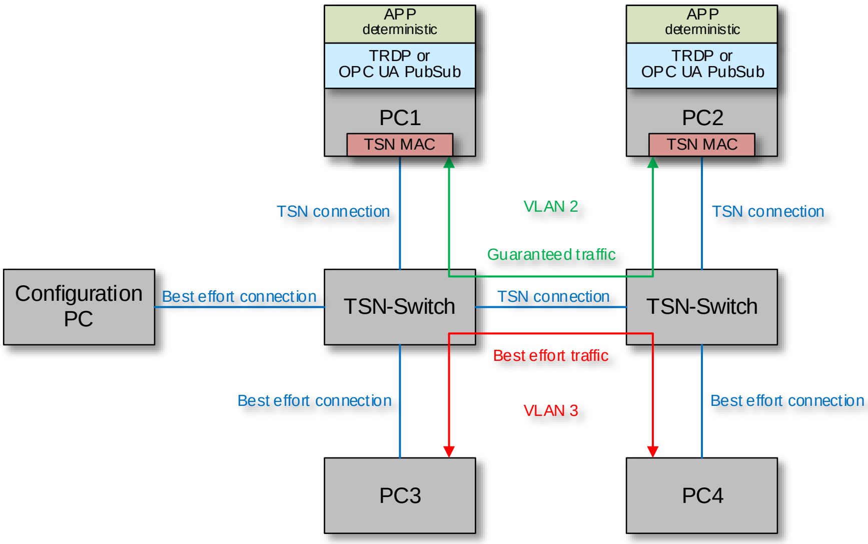

Figure 3: Network topology task 2 a)

The traffic on the network shall be analysed with a suitable network protocol analyser (e.g. wireshark) using a passive tap on the switch-to-switch connection.

2.1.2.2 Part b): Deterministic and Best-effort Traffic on same End Devices with different applications

To show the consolidation of best effort traffic and guaranteed traffic in a single PC, the network is reduced to comprise only PC1 and PC2. Two separate applications will run on each PC where one generates and listens to best effort traffic and the other sends and receives data over the guaranteed traffic channel. This will demonstrate the possibility to differentiate communication priorities within one end-device.

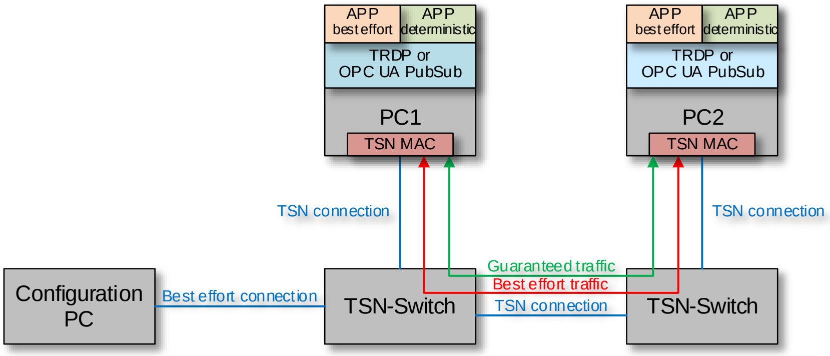

Figure 4: Network topology task 2 b)

2.1.2.3 Part c): Deterministic and Best-effort Traffic on same End Devices with same applications

This part is similar to part b). It differs in the fact that one application is used to send 'sensitive' data using a guaranteed channel and to send 'non-sensitive' data over a best-effort channel. The aim is to investigate how one can segregate the traffic into different priorities on an application level.

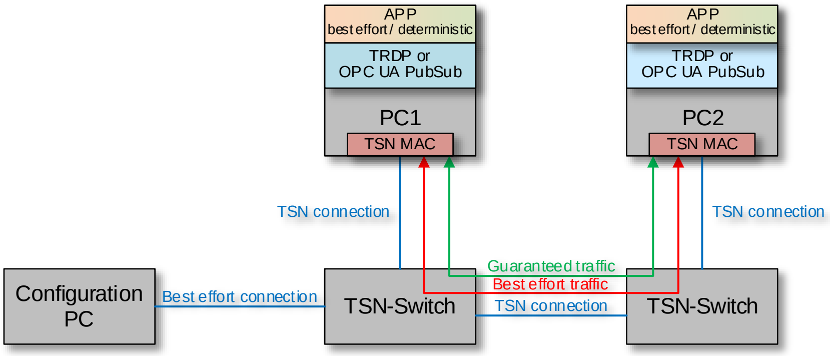

Figure 5: Network topology task 2 c)