OCORA

Open CCS On-board Reference Architecture

CCS Communication Network

Addendum to SUBSET-147

Document ID: OCORA-TWS02-030

Version: 2.05

Date: 01.07.2024

Revision history

Version	Change Description	Initial	Date of change
1.00	Official version for OCORA Release R4	SSt	23.06.2023
2.00	Official version for OCORA Release R5	SSt	24.11.2023
2.05	Official version for OCORA Release R5.1	SSt	01.07.2024

Table of contents

Table of tables

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-TWS01-030 – System Architecture

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

[5] OCORA-TWS02-020 – CCS Communication Network – Proof of Concept (PoC)

[6] CTA-T3.5-D-BTD-002-12_-_Drive-by-Data_Architecture_Specification

[7] CTA2-T3.4-T-SIE-019-03 – Safety Analysis SDTv4

[8] EN 50129:2018 – Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

[9] EN 50159:2010 – Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

[10] IEC 61375-2-3: Railway Applications – Electronic railway equipment – Train communication network (TCN) – Part 2-3: TCN communication profile, 2015

[11] IEC 61375-3-4:2013 – Electronic railway equipment – Train Communication Network (TCN) – Part 3-4: Ethernet Consist Network (ECN)

[12] IEC 62443-3-3: Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels, 2013

[13] CENELEC TS 50701: Railway applications - Cybersecurity, Version D8E5

[14] ERTMS/ETCS SUBSET-026: System Requirements Specification, Version 4.0.0

[15] ERTMS/ETCS SUBSET-037-3: EuroRadio FIS - FRMCS Communication Functional Module, Version 4.0.0

[16] ERTMS/ETCS SUBSET-125: ERTMS/ATO System Requirement Specification, Version 1.0.0

[17] ERTMS/ETCS SUBSET-126: ATO-OB / ATO-TS FFFIS Application Layer, Version 1.0.0

[18] ERTMS/ETCS SUBSET-147: CCS Consist Network Communication Layers, Version 1.0.0

[19] ERTMS/ETCS SUBSET-148: ATO-OB/ATO-TS Interface Specification - Transport and Security Layers, Version 1.0.0

[20] ITxPT, S02P03-GNSSLocation, v2.2.1

[21] Europes Rail System Pillar – Shared Security Services Specification, BL0.85, 2024

[22] Internet Engineering Task Force (IETF), Network Time Protocol Version 4: Protocol and Algorithms Specification, 2010

[23] Internet Engineering Task Force (IETF), Internet Engineering Task Force (IETF), Request for Comments (RFC) 8915, Network Time Security for the Network Time Protocol, September 2020

[24] GPSd location service definition, https://gpsd.gitlab.io/gpsd/

1 Introduction

1.1 Purpose of the document

This document is based on the CCN evaluation report [4] elaborated in former phases. It contains specifications of what is left open in the SUBSET-147 [18] to get a standardised and unambiguous implementation of the onboard CCS process and message data communication and of the time synchronization service. The SUBSET-147 is a mandatory specification of the TSI-CCS 2023 release which aims to define the standard network technology to be used for the on-board CCS system. Although not belonging to communication functionality also the central train time synchronization service and location service are specified in this SUBSET-147.

This OCORA Addendum is intended to be used as input for further specification activities in ERJU e.g. Innovation Pillar focus project R2DATO work package WP23/24 or System Pillar Train CS domain as well as the standardisation activities in EuroSpec.

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

In the current version, the document adds some details to the specification of the SUBSET-147 [18]. This document defines an option for a standard process and message data communication (OSI-Layer 1 - 6 incl. Safety Layer) that can be used for the on-board CCS system to establish communication on the internal interfaces of the system and on the interfaces with the system TCMS. It does not define a standard communication technology within other systems (e.g. the TCMS, Passenger Information System). But especially for new vehicles it is highly recommended for railway undertakings to request the same communication technology in the CCS and TCMS domains.

On session layer it defines a standard protocol especially designed for the main CCS application process and message data communication within the CCS on-board system. It is not suited for other data classes like bulk data (e.g. for software update) or streaming data (e.g. for Cab Voice Radio).

For the central time synchronization service and the location service defined in SUBSET-147 it adds more detailed requirements to get an implementable solution that is fit for purpose. The added requirements on the train time service are in line with the shared security services to be specified by Eulynx and System Pillar Security domain [21].

The application layer data between CCS on-board building blocks is not part of this document. The application data between different CCS on-board building blocks is defined in different SUBSETs (e.g. SUBSET-119 for ETCS<>TCMS or Subset-121 for ETCS<>DMI data). Furthermore, it does not contain protocol specifications for other data classes like bulk data (e.g. for software update) or streaming data (e.g. for Cab Voice Radio).

1.3 Context of the document

This document is published as part of the OCORA Release R5.1, together with the documents listed in the release notes [1]. All abbreviations and terms used are defined in the Glossary [2].

1.4 Problem Description

Today the interfaces between CCS components on the vehicle are proprietary. The proprietary interfaces do not allow to exchange CCS components from different suppliers. The vendor lock-in created by proprietary interfaces leads to a complex lifecycle management. Furthermore, the existing proprietary interfaces do not allow to easily add new functions impeding innovation.

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

1.5 Concept

The OCORA architecture [3] aims for plug and play interchangeability within the CCS on-board domain through isolation of specific functions in combination with the specification of a generic, open and standardized communication backbone, the CCS Communication Network (CCN). The CCN connects different components of the future CCS on-board systems as for example:

- European Train Protection On-Board (ETP-OB)
- Localization On-Board (LOC-OB)
- Train Display System (TDS)
- National Train Protection (NTP) or Specific Transmission Module (STM)
- Cabin Voice Device On-Board (CVR-OB)
- Gateway to Train Control Management System Network, Operator Network, Communication Network or Security Network (ECN/ECN Gateway)

In the SUBSET-147 for the CCN the equivalent terms “Ethernet CCS Consist Network” or “One Common Bus” are used. Basically, all three terms cover the same CCS Communication backbone.

In the final vision of the system an open and standardized CCN (OSI-Layers 1 to 6 & Safety Layer) ensures safe data connections between CCS on-board components. The network allows simple upgrades / enhancements of the CCS on-board System by introducing new functions or components. It also enables procurement on a building-block-based granularity which leads to more flexibility in the lifecycle management and optimal components due to larger market size. For the CCN itself, modifications due to future technological evolutions are facilitated by the communication layering concept.

2 CCS Communication Network Requirements

2.1 Protocol Stack

The following protocol stack shall be used for local CCS communication of the data classes process and message data according to PCP values 3, 5 and 6 in Table 2. The definitions of physical and data link layers are in line with the Ethernet definition of SUBSET-147 v1.0.0 as part of the TSI 2023. This means, the interfaces for local CCS communication shall be compliant with the requirements of Subset-147 as defined for "newly developed vehicle designs". Hence, the interfaces shall be compliant with the Ethernet CCS Consist Network as defined in chapter 8 of Subset-147. MVB and CAN based solutions are no longer allowed for any connection of the local CCS communication.

Layer	Protocol	Standard
(Safety Layer[1])	(SDTv2/v4)	IEC 61375-2-3 and [7]
Session Layer	TRDP	IEC 61375-2-3
Transport Layer	UDP (for process and message data) TCP (for message data)	RFC 768 RFC 793
Network Layer	IPv4	RFC 791
Data Link Layer	Standard Ethernet with QoS	IEEE 802.3 IEEE 802.1Q
Physical Layer	1000BASE-T (optional 100BASE-TX for end devices)	IEEE 802.3 Clause 40 IEEE 802.3 Clause 25

Table 1: Protocol Stack for local CCS process and message data

2.2 Physical Layer

There are no further requirements on physical layer than the ones in SUBSET-147.

2.3 Data Link Layer

2.3.1 Separation/segmentation

2.3.1.1 Separation/segmentation of traffic towards End Devices

If the end device supports tagged traffic, the end device has to tag every Ethernet frame with the PCP value according to the data class as in Table 2 in order to fulfil QoS requirements.

2.3.1.2 Authentication / Authorization of End Devices

Where the network component and end devices support it, the version IEEE 802.1X-2010 or newer shall be used for authentication / authorisation of end devices including MAC Security according to IEEE 802.1AE-2006 or newer.

2.3.2 Quality-of-Service

2.3.2.1 Quality-of-Service in general

Quality-of-service handling in the lower layers is envisaged on OSI Layer 2 by using Priority Code Points as defined in IEEE 802.1Q-2014 (sometimes referred as IEEE P802.1p, also known as VLAN priority).

To leverage the capabilities of prioritising traffic inside a VLAN, the CCS Communication Network specifies its

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

own rail-specific, vehicle-onboard interpretation of the Priority Code Points (PCP) as follows (identical to SS-147 [18]): [2][3]

Priority	PCP value	Service Class	Typical total bandwidth[4] [Mbit/s]	Typical max. delay[5] [ms]	Typical usage example
0 (low)	0	Best effort	-	-	Default Mass data transport (e.g., memory dumps, S/W update data)
1	1	Broadband stream data	500	200	CCTV Video stream
2	2	Preferred stream data	150	150	PIS display Non-critical outside display Passenger counting
3	3	Sporadic management data	50	100	IEC61375-3-4: “Message Data” CCS message data (e.g., diagnostics) SNMP HTTP switch management Netconf
4	4	Time-critical stream data	50	100	Cab radio audio stream
5	5	Ordinary process data	100	5	IEC61375-3-4: “Process Data” CCS process data
6	6	Time-critical process data	50	1	IEC61375-3-4: “Supervisory Data” time-critical CCS process data Appl. level time synchronization
7 (high)	7	Network control	1	1	Spanning tree Redundancy protocols NOT network management

Table 2: PCP value definition per data class / service class

2.3.2.2 Quality-of-Service inside the On-board Core Network

Every consist switch shall implement eight queues per port to use one dedicated queue per layer 2 priority (PCP value according to IEEE 802.1Q-2022).

Every consist switch shall support “strict priority” according to IEEE 802.1Q-2022 as transmission selection mechanism on all priority queues, i.e. all higher priority frames shall egress from port before the lower priority frames egress.

The use of other transmission selection mechanisms like “weighted round robin” or a combination of different mechanisms is up to the CCS system integrator.

[2] PCPs given here are a refinement of data classes of IEC61375-3-4 chapter 4.3

[3] The table does not contain a maximum jitter by intention. Tests with a 1 Gbit On-board Core Network (as required by this specification) based on Strict Priority Queuing have shown, that any jitter occurring is at least one magnitude lower than the maximum delay. Therefore, being sufficient for the respective applications.

[4] IEC61375-3-4 chapter 4.3 does not make a statement on bandwidth distribution.

[5] The delay values fulfil IEC61375-3-4 chapter 4.3. In fact, they are stricter here.

2.4 Transport and Session Layer

For CCS applications exchanging local CCS process or message data according to PCP values 3, 5 and 6 over Ethernet CCS Consist Network only the communication technology TRDP (according to IEC61375-2-3 [10]) is allowed. With the definition of the communication technology on session layer, the transport and network layers are implicitly defined.

Exception: In case of communication from on-board entities over FRMCS the corresponding specifications shall be applied (e.g. SUBSET-037-3 [15] and SUBSET-026-7/-8 [14] for ETCS, or SUBSET-148 [19], SUBSET-126 [17] and SUBSET-125 [16] for ATO).

For other applications (e.g. mass data transport for software update or streaming data) also for CCS devices no further requirements are defined in this document.

2.5 Safety Layer

For safety applications exchanging local CCS process or message data (according to PCP values 3, 5 and 6) over Ethernet CCS Consist Network the Safety Layer SDTv2 according to IEC/EN 61375-2-3 [10] shall be used for functions of SIL 1 and SIL 2.

For safety functions of SIL 3 and SIL 4 the Safety Layer SDTv4 according to the specification of Shift2Rail’s CONNECTA project [6], [7] shall be used. The specification of SDTv4 will become integral part of the IEC/EN 61375-2-3 [10] Annex B in unchanged manner in the subsequent version of the standard.

3 Train Time and Location Services

3.1 General

The Train Time and Location Services (TTLS) shall provide on one hand a common reference time and on the other hand the current location information for all applications on the vehicle. They are both defined as a non-safe service function. Both services are linked to each other over the common source of information which is the GNSS module. The device, which the services are running on, is out of scope of this specification.

3.2 Architecture

Primary using an external GNSS module as time and location source, the TTLS will provide an NTP server for time distribution and a location service delivering location and velocity information.

The time service implements an onboard NTP server. Over the NTP protocol every system (NTP client) can synchronize its system time to the system time of the NTP server. The system time of a client system (NTP client) is not continuous. Time jumps can be caused by leap seconds or transient effects for NTP synchronisation. For a continuous time (e.g. used for monitoring data), a detection and compensation (to make it monotonous and continuous) of time jumps can be foreseen in the client systems. The compensation is not part of the time service standardized in this document.

3.3 Requirements

3.3.1 General Requirements

The Train Time and Location Services (TTLS) shall be checked if they are running as expected. If they are detected as not running, the corresponding service shall be restarted automatically (watchdog function). (R)

3.3.2 Requirements on Time and Location Sources

The onboard NTP server shall work as Stratum 1 or 2. (R)

The onboard NTP server shall be able to use the following sources:

- Primary time source:
    - Battery-buffered local real-time clock (RTC). Note: to be used after startup as long as there is no time with higher precision available.
    - GNSS module
- Secondary time source:
    - NTP-Server (supporting NTS according to RFC 8915 [23]) Stratum 1 from trackside.

During time with GNSS reception or connected trackside NTP server the system time of the NTP server shall be written at least once per hour to the local real-time clock (RTC). (R)

The deviation of the system time of the NTP server to UTC shall be less than 30 µs with a steady 3-dimensional GNSS fix. (R)

Info: To meet the requirement, the GNSS receiver can output a pulse-per-second (PPS) signal. This PPS signal can be directly connected to NTP server and can be used as a time source signal. (I)

The clock drift of the NTP servers' system time shall not exceed ±2ppm within the operating temperature range class OT3 according to EN 50155:2021 in a cabinet. (R)

Justification: The deviation of the system time of the NTP server to UTC shall not exceed 10 ms within 1 hour GNSS reception loss. The accuracy of the system time shall be below the cycle time of client applications (e.g.

ATO 50 ms, JRU logs 50 ms). Additionally, the defined accuracy value of 10 ms corresponds to the resolution of the current onboard train time (T_TRAIN) defined in SS-026-7 7.5.1.154. (I)

Info: Using a high-quality temperature compensated crystal oscillator (TCXO) or using the NTP implementation “chrony” with its clock frequency calibration to PPS signal, the accuracy requirement can be met. (I)

3.3.3 Requirements on Interface to Applications

There shall be two services active building the two interfaces to the applications:

- Time Service providing Clock Synchronisation to UTC
- Location Service providing location (and velocity) information marked with a timestamp the location and velocity information was valid for. (R)

3.3.3.1 Time Service (Clock Synchronisation to UTC)

The local (onboard) distribution of the synchronisation to UTC time shall take place via NTP protocol RFC 5905 [22]. (R)

The derivation of the local time is in the responsibility of the client system (e.g. DMI). (I)

In accordance with SUBSET-147 [18] chapter 8.4.4.1.2 the NTP packets for time synchronization shall be sent with PCP value 6 in order to get high priority in the network and therefore high synchronisation accuracy. This requirement is not only valid for the NTP server (train time service) but also for the NTP clients (clients of the train time service). (R)

Network Time Security (NTS) according to RFC 8915 shall be supported by the onboard NTP server. (Rational: IEEE 802.1X:2004 as defined in SUBSET-147 [18] on layer 2 is not sufficient to secure the time synchronisation.) (R)Info: The usage of a correctly configured service “chrony” on a Linux based system would normally fulfil the requirements above. (I)

3.3.3.2 Location Service

The location and velocity shall be derived from GNSS. The time information contains the time, when the location and the speed information was valid. (R)

After having once a steady GNSS reception after startup, the location and velocity information shall be available even in areas without GNSS reception (e.g. tunnels, stations etc.). For this function of “dead reckoning”, additional sensors (e.g. accelerometer, gyroscope, counting of external wheel tick pulses) to the GNSS receiver are needed. (R)

Info: The “dead reckoning” function is already in scope of ITxPT localisation standard. [20]

The information shall be distributed locally (onboard) over the traffic mechanisms “process data” and “request/reply”. (R)

For process data the following packet shall be distributed (R):

LOC Packet 1:

Properties:

ComId:	configurable
Data class:	Time-critical process data (VLAN Prio 6)
Cycle Time:	≤1000 ms

Byte Offset	Type	Name	Description	classification in case of 2D/3D fix
0	UINT8	STATUS	Status: 0: unknown 1: no fix 2: 2D GNSS fix 3: 3D GNSS fix 4: Dead Reckoning (DR) 5: Dead Reckoning (DR) + 3D GNSS fix	
1	INT64	TIME_UTC	Date and Time in milliseconds (UTC) associated to the data collection. Integer value is the number of (non-leap) milliseconds since the January 1st 1970 at 00:00:00.000 UTC. (in alignment to UNIX time leap seconds are not counted)	mandatory
9	UINT32	TIME_ERROR_EST	Estimated time error in milliseconds associated to the data collection.	optional
13	FLOAT32	POSITION_LAT	Latitude in degrees in the WGS84 reference system Range: -90.000000° to +90.000000° +/- signifies North/South	mandatory
17	FLOAT32	POSITION_LONG	Longitude in degrees in the WGS84 reference system Range: -90.000000° to +90.000000° +/- signifies North/South	mandatory
21	FLOAT32	POSITION_ ERROR_EST	Estimated horizontal position error in meters	optional
25	FLOAT32	ALT_MSL	Altitude above mean sea level in meters	mandatory (only 3D fix)
29	FLOAT32	ALT_ERROR_EST	Estimated vertical position (altitude) error in meters	optional
33	FLOAT32	TRACK	Course over ground in degrees from true north	mandatory
37	FLOAT32	TRACK_ERROR_EST	Estimated track direction error in degrees	optional
41	FLOAT32	SPEED	Speed over ground in meters per second	mandatory
45	FLOAT32	SPEED_ERROR_EST	Estimated speed error in meters per second	optional
49	FLOAT32	CLIMB	Climb (positive) or sink (negative) rate in meters per second	mandatory
53	FLOAT32	CLIMB_ERROR_EST	Estimated climb error in meters per second	optional

For “request/reply” traffic mechanism, a service should be implemented that acts identically like the open-source service “GPSD” [24] commonly used on unix-like systems. (R)

The service shall listen on TCP/IP port 2947 for incoming requests from clients. (R)

The commands shall use the JSON-based syntax and shall provide JSON-based responses. (R)

Multiple clients shall be able to access the service concurrently. (R)

Example of basic service: After a “?WATCH” command by the client, the service will activate the GNSS sensor. The sensor will start pushing reports periodically (usually every second) and the location service will then put the sensor report into a JSON-based “TPV” (time, position, velocity) message that will be sent to the client. (I)