

# OCORA

Open CCS On-board Reference Architecture

## **System Requirements Specification**

Monitoring, Diagnostics, Configuration & Maintenance subsystem

This OCORA work is licensed under the dual licensing Terms EUPL 1.2 (Commission Implementing Decision (EU) 2017/863 of 18 May 2017) and the terms and condition of the Attributions- ShareAlike 3.0 Unported license or its national version (in particular CC-BY-SA 3.0 DE).



Document ID: OCORA-TWS08-030

Version: 1.01

Date: 19.06.2023

## Revision history

Version	Change Description	Initial	Date of change
0.01	Initial document template and structure created	KS	03.08.2021
0.02	Added first version of MDCM overview in chapter 2	KS	04.08.2021
0.03	Changed doc number to OCORA-TWS08-030	KS	14.11.2022
0.04	Doc title changed to MDCM-OB SRS Removed Management summary section Globally changed the subject "MDCM" to "MDCM-OB" Added informal contents for chapter 2 Updated References table	KS	17.11.2022
0.05	Draft version ready for initial OCORA-R3 review - Some of the contents need technical review and approval - Some formatting issues to be fixed for final R3 version - Some minor open points and pending changes to be concluded for final R3 version	KS	18.11.2022
0.06	Corrections after DB internal review - Various typo fixes in ch. 2, 3.1, 3.2, 3.13 - Wording of "Scope: All" changed to "Scope: MDCM global" in ch. 3.12 for SRS item OCORA-8045 - Slightly improved the wording used in ch. 5	KS	21.11.2022
0.07	Correction and improvements after OCORA technical review - Updated SRS-items 7629, 7630, 7631, 7426, 7425, 8216, 7628 - Removed SRS item 7424 - Added new SRS item 8220  Version was reviewed by OCORA Core Team for publication in R3	KS	23.11.2022
1.00	Fixed typos and adjusted wording figures from chapter 2 - Fixed "ERMTS" -> "ERTMS" in Figure 1 and Figure 4 - Partly replaced the term "OCORA" with "CCS-OB"  Fixed typos and improved wording in SRS-items 8220 and 7426 Improved Note-element "Accomplished through ..." in Figure 4 Improved Rationale of SRS-item 8214 Some final document formatting  Document version for publication in OCORA-R3	KS	01.12.2022
1.01	- SRS items 10220, 10221 added to chapter 3.11 - SRS items 10219, 10222 added to chapter 3.12 - Updated notes on acceptance criteria in chapter 4	KS	19.06.2023

# Table of contents

<b>1</b>	<b>Introduction .....</b>	<b>5</b>
1.1	Purpose of the document.....	5
1.2	Applicability of the document .....	5
1.3	Context of the document.....	5
<b>2</b>	<b>MDCM-OB overview .....</b>	<b>6</b>
2.1	System view .....	6
2.2	Use cases .....	7
2.3	Provided services.....	8
2.4	Functional components.....	9
<b>3</b>	<b>Requirements .....</b>	<b>10</b>
3.1	Operation modes .....	10
3.2	System capabilities .....	10
3.3	System external interfaces .....	15
3.4	System internal interfaces .....	18
3.5	System internal data .....	18
3.6	System configuration and upgrades .....	18
3.7	System safety .....	18
3.8	System security and privacy .....	18
3.9	System environments .....	18
3.10	Computing and communication resources .....	18
3.11	System quality and performance factors .....	18
3.12	Design constraints .....	19
3.13	Personnel and training .....	20
<b>4</b>	<b>Acceptance criteria .....</b>	<b>21</b>
<b>5</b>	<b>Traceability .....</b>	<b>21</b>

## Table of figures

<b>Figure 1</b> - MDCM-OB system view .....	6
<b>Figure 2</b> - MDCM-OB top-level use cases and associated actors.....	7
<b>Figure 3</b> - MDCM-OB provided services.....	8
<b>Figure 4</b> - MDCM-OB functional components.....	9

## References

- [1] OCORA-BWS01-010 – Release Notes
- [2] OCORA-BWS01-020 – Glossary
- [3] OCORA-BWS03-010 – Introduction to OCORA
- [4] OCORA-BWS04-010 – Problem Statements
- [5] OCORA-BWS01-030 – Question and Answers
- [6] OCORA-BWS02-030 – Technical Slide Deck
- [7] OCORA-TWS01-030 – System Architecture
- [8] OCORA-TWS01-035 – CCS-On-Board-(CCS-OB)-Architecture
- [9] OCORA-TWS05-010 – Requirements Management Guideline
- [10] OCORA-TWS08-010 – MDCM-OB Introduction
- [11] BAV, NS, ProRail, SBB; Proposal for a user requirement specification pertaining to a railway monitoring system (CR1362), version 0.7; 2021
- [12] ERTMS/ETCS SUBSET-149, Online Monitoring System, draft 0.0.5; 2022
- [13] ERTMS/ETCS SUBSET-147, CCS Consist Network Communication Layers, draft 0.1.10; 2022
- [14] ERTMS/ETCS SUBSET 140, ATO-OB / ORD FFFIS Application Layer, draft 0.0.8; 2021
- [15] ERTMS/ETCS SUBSET-027, FIS Juridical Recording, issue 3.3.0; 2016
- [16] UIC 612-1:2009, Rolling stock configurations and main activated functions for EMU/DMU, locomotives and driving coaches; 1st ed; leaflet in volume VI – Traction; 2009
- [17] CENELEC; IEC 61375-2-6:2018 E, Electronic railway equipment – Train communication network (TCN) - Part 2-6: On-board to ground communication; 2018

# 1 Introduction

## 1.1 Purpose of the document

This document defines the system-level requirements for the OCORA Monitoring, Diagnostics, Configuration, and Maintenance On-Board (MDCM-OB) building block.

The intended audience are CCS domain experts, railway undertakings (RUs) and infrastructure managers (IMs), as well as CCS product vendors and vehicle manufacturers.

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 CCS-OB 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 CCS-OB 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 an OCORA Release, together with the documents listed in the release notes [\[1\]](#). Before reading this document, it is recommended to read the MDCM Introduction [\[10\]](#) and OCORA Requirements Management Guideline [\[9\]](#). The context and the motivation that drives OCORA is described in [\[3\]](#) and [\[4\]](#). Terms and abbreviations used throughout this document are listed in OCORA Glossary [\[2\]](#). Information on OCORA system architecture can be found in [\[7\],\[8\],\[6\]](#). Furthermore, there is the OCORA Questions and Answers document [\[5\]](#).

## 2 MDCM-OB overview

The Monitoring, Diagnostics, Configuration, Maintenance subsystem (MDCM-OB) is a building block of the OCORA CCS-OB architecture. Its main purpose is the provision of services for monitoring, diagnostics, and configuration of onboard functions.

The main stakeholders of the MDCM-OB are railway undertakings (RU) and infrastructure managers (IM). Envisioned users of the MDCM-OB are operators and technicians, as well as CCS equipment vendors and vehicle manufactures.

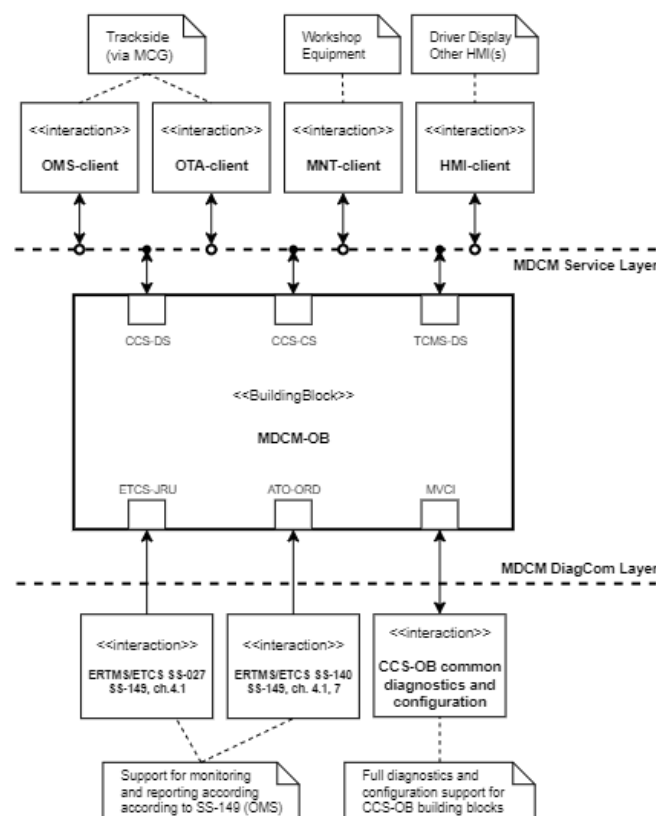
MDCM-OB objectives, envisioned development stages, and general design approaches are introduced and described in [10], ch. 3.

The remaining paragraphs of this chapter informally describe the MDCM-OB system view, main use cases and main functional components, based on which corresponding requirements will be defined in chapter 3.

### 2.1 System view

MDCM-OB pursues a service-oriented design approach, where MDCM-OB features for diagnostics and configuration will be provided as dedicated onboard services with a common, extensible service API.

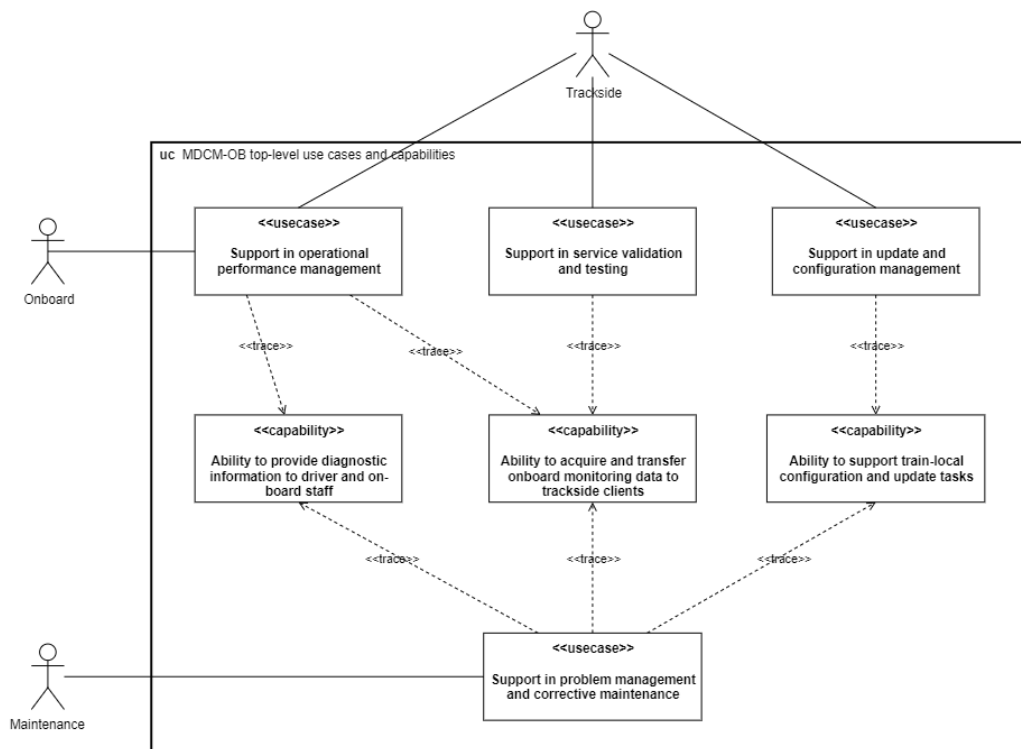
**Figure 1** depicts the MDCM-OB system view and envisioned MDCM-OB clients.



**Figure 1 - MDCM-OB system view**

## 2.2 Use cases

**Figure 2** depicts the MDCM-OB top-level use cases and associated actors. The MDCM-OB top-level use cases have been derived from user requirements defined in [11], ch. 5.

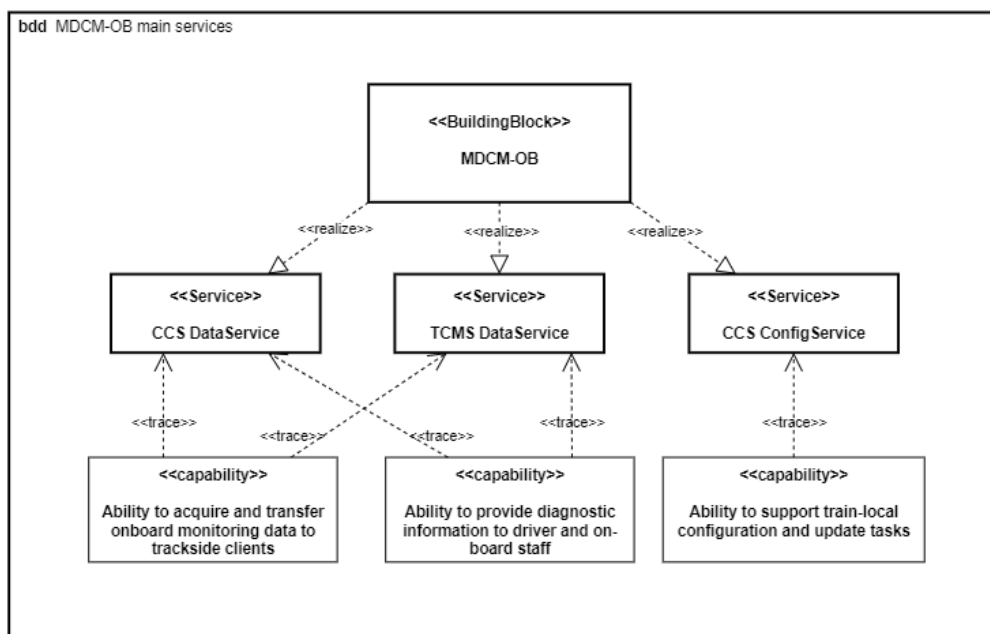


**Figure 2** - MDCM-OB top-level use cases and associated actors

Based on MDCM-OB top-level use cases the main MDCM-OB capabilities shown in **Figure 2** have been derived and will be subject to corresponding requirements in chapter 3.2.

## 2.3 Provided services

**Figure 3** depicts the MDCM-OB services derived from MDCM-OB capabilities and from MDCM-OB objectives for OCORA short-, mid-, and long-term perspectives stated in [10], ch. 3.1.

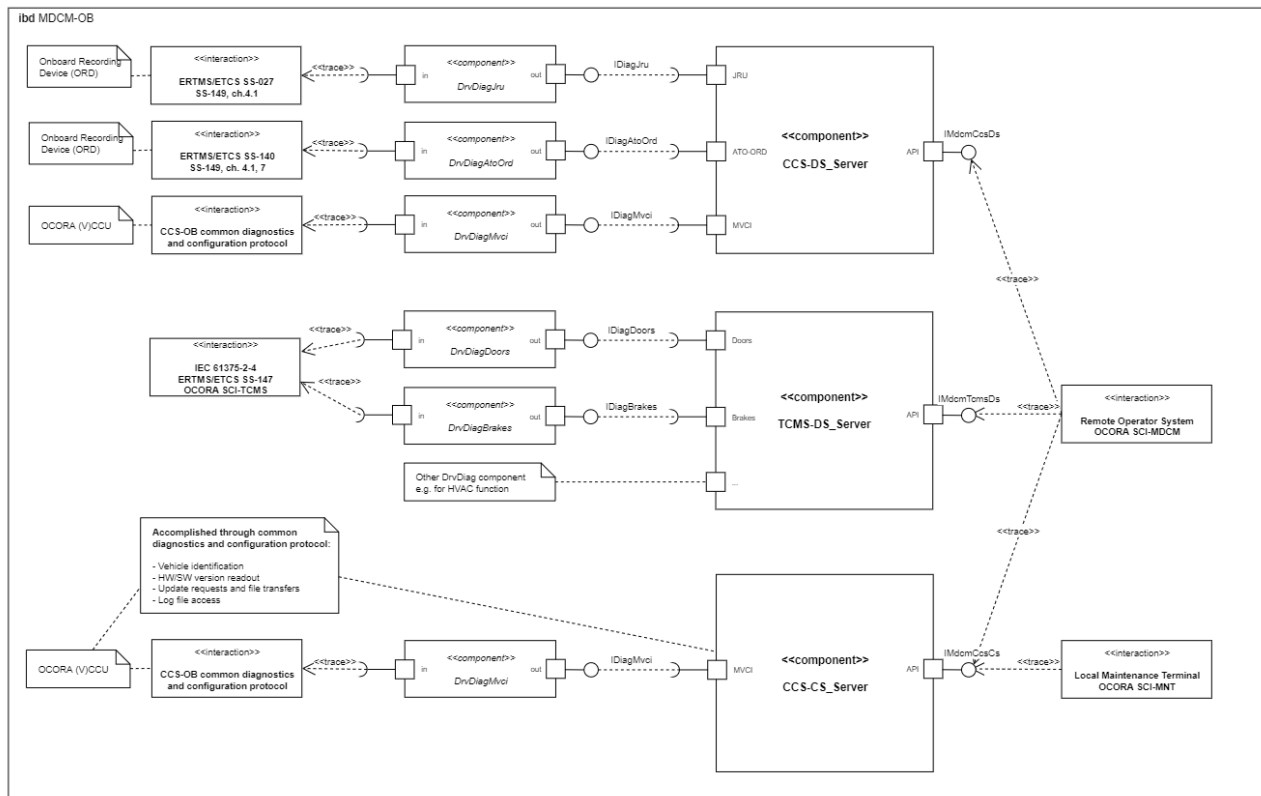


**Figure 3** - MDCM-OB provided services



## 2.4 Functional components

**Figure 4** depicts the white-box view of the MDCM-OB building block containing the envisioned functional components and associated interfaces necessary to realize the MDCM-OB services from chapter 0.



**Figure 4 - MDCM-OB functional components**

The white-box-view of the MDCM-OB building block is a design recommendation, which is provided here to outline the desired product design.

Using this design recommendation facilitates a modular MDCM-OB structure that can be incrementally developed with respect to MDCM-OB objectives for OCORA short-, mid-, and long-term perspectives.

## 3 Requirements

### 3.1 Operation modes

This chapter defines the required operation modes (OpModes) of the MDCM-OB. Each OpMode constitutes a particular system context, for example Normal-operation, Commissioning or Maintenance.

#### **OCORA-8196, D-Level - Supported operation modes**

The MDCM shall operate in all train configurations defined by UIC 612-1:2009, except the ShutDown and SelfProtection configuration.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Onboard diagnostics and configuration services provided by the MDCM shall be available after the train has been switched on</li> <li>Attempts to perform diagnostics or configuration tasks in certain train configurations, where one or more targeted functions are not available, will be acknowledged by the MDCM with a negative response</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM global</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>It shall be the responsibility of the targeted function to allow or deny diagnostics and/or configuration requests sent by the MDCM</li> <li>See, UIC 612-1:2009, A.1, Table 1, for the list of all train configurations and constituting operating condition</li> <li>The full set of train configurations where the MDCM shall be operational comprises the following modes <ul style="list-style-type: none"> <li>SwitchedOn</li> <li>StandBy</li> <li>InService</li> <li>Driving</li> <li>EnergySaving</li> <li>Degraded</li> </ul> </li> </ul>

### 3.2 System capabilities

This chapter defines the required capabilities of the MDCM-OB. Capabilities constitute groups of related requirements concerning services, features and functionalities of the MDCM-OB.

#### **OCORA-7427, D-Level - Ability to acquire and transfer onboard monitoring data to trackside clients**

The MDCM shall provide means to receive, store and forward diagnostics and monitoring data from onboard building blocks.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>The diagnostic and monitoring data is needed to inform on-board staff about issues, allowing the staff to handle appropriately.</li> <li>The diagnostic and monitoring data is needed to inform trackside, allowing to follow adequate operational procedures.</li> </ul>

	<ul style="list-style-type: none"> <li>The diagnostic and monitoring data is needed to inform trackside, allowing to plan accordingly.</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM short-term and mid-term, CCS DataService</li> <li>MDCM long-term, TCMS DataService</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>See also requirements from OMS spec. and SS-149 draft related to details on storing monitoring data for a limited time.</li> <li>The MDCM shall handle the monitoring and diagnostics data payload, as much as possible, as opaque, application- and/or component-specific data.</li> <li>The meaning and interpretation of monitoring- and diagnostics payload data format shall be transparent to the MDCM.</li> <li>Changes to the monitoring- and diagnostics payload data format shall have minimal side effects on the MDCM.</li> </ul>

#### OCORA-8048, D-Level - Ability to provide diagnostic information to driver and on-board staff

The MDCM shall support displaying diagnostic information from CCS-OB and TCMS functions to the driver and/or other on-board staff.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Provide a central source for diagnostic information about CCS-OB and TCMS functions</li> <li>Provide means to access this information from the driver display</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>CCS DataService, MDCM mid-term</li> <li>TCMS DataService, MDCM long-term</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>Displaying the information is not in scope of the MDCM. This shall be done, for example by the driver display function. However, the MDCM shall be capable to provide diagnostic information to driver display when needed.</li> </ul>

#### OCORA-8046, D-Level - Support of train-local configuration and update tasks

The MDCM shall support performing configuration and update tasks on-board the vehicle.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Need is for maintenance tasks performed in workshops and depots</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>CCS Configuration Service</li> <li>MDCM mid-term</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>Support technicians and other authorized staff in performing change-, release-, and configuration management tasks for CCS-OB component on-board the vehicle</li> <li>Target use cases such as SW updates, and HW/SW versions readout</li> </ul>

### OCORA-7425, D-Level - Ability to issue commands to CCS-OB building blocks

The MDCM shall provide means to issue commands to CCS-OB building blocks.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>• Needed for CCS-OB update and configuration tasks</li> <li>• Needed for some CCS-OB diagnostic tasks (e.g. retrieval of logging data)</li> </ul>
Remark	Scope: <ul style="list-style-type: none"> <li>• MDCM mid-term</li> <li>• CCS ConfigService</li> </ul>

### OCORA-7426, D-Level - Ability to manage configuration data transfers

The MDCM shall provide means to receive, store and forward configuration data from trackside systems to CCS-OB building blocks.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>• Needed for CCS-OB update and configuration tasks</li> </ul>
Remark	Scope: <ul style="list-style-type: none"> <li>• MDCM mid-term</li> <li>• CCS ConfigService</li> </ul> Remarks: <ul style="list-style-type: none"> <li>• Configuration and update of CCS-OB building blocks is envisioned to be performed either remotely (from trackside clients) or locally (from onboard clients)</li> <li>• Storing of configuration data in MDCM means here, that the MDCM shall maintain a temporary data buffer per transfer-session containing the data successfully received from associated trackside client.</li> <li>• The data buffer shall be maintained by MDCM until the transfer to the targeted onboard unit has been either successfully completed or dropped by the trackside client.</li> <li>• The MDCM shall handle the configuration data payload as opaque, application-specific data.</li> <li>• The exact configuration payload data format shall be transparent to the MDCM.</li> <li>• Changes to the configuration data payload format shall not have any side effects on the MDCM.</li> </ul>

### OCORA-7629, D-Level - Ability to provide logging data from CCS-OB building blocks

The MDCM shall provide means to download logging data from CCS-OB building blocks. Access to this logging data shall be possible from both onboard (local access) and trackside (remote access).

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>• This feature is needed, for example, for detailed issue analysis.</li> </ul>
Remark	Scope: <ul style="list-style-type: none"> <li>• MDCM mid-term</li> <li>• CCS ConfigService</li> </ul>

	<p>Remarks:</p> <ul style="list-style-type: none"> <li>Local logging data access shall be available to authorized staff via Maintenance Terminal.</li> <li>Remote logging data access shall be available to authorized staff via T2G link and MCG.</li> <li>Logging data shall be provided by the MDCM as file(s) transferred to the requesting site.</li> <li>The logging data to be transferred will be acquired by the MDCM from the corresponding onboard components on demand.</li> <li>Depending on the train configuration (train is driving, at the station, in the workshop, etc.) the access to logging data might be allowed or rejected by an onboard component. In the latter case the MDCM shall indicate a negative response.</li> <li>Furthermore, when it comes to remote access, the MCG might decide, depending on the available T2G communication bandwidth and/or quality, whether or not logging data transfers will be allowed.</li> </ul>
--	---

#### **OCORA-7630, D-Level - Ability to provide onboard identification and configuration data from CCS-OB building blocks**

The MDCM shall provide means to retrieve identification and configuration data from CCS-OB building blocks.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Need to observe and identify available CCS-OB components of a particular vehicle (architecture identification request).</li> <li>Need to readout CCS-OB component configuration data such as hardware version, software version, other configuration parameters.</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM mid-term</li> <li>CCS ConfigService</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>This information shall be provided to (will be used by) both onboard and trackside clients.</li> </ul>

#### **OCORA-7631, D-Level - Ability to provide batch data transfers to trackside**

The MDCM shall provide means to realize batch data transfers from onboard to trackside. Individual batch data transfers shall be configurable in terms of contents, trigger points, connectivity/bandwidth constraints.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Batch data transfers will be used to download large chunks of aggregated data from the vehicle.</li> <li>A batch of data will be transferred within a single and potentially long-running transfer operation.</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM mid- and long-term</li> <li>CCS DataService and TCMS DataService</li> </ul> <p>Remarks:</p>

	<ul style="list-style-type: none"> <li>Batch data comprises non-realtime information, which is not immediately needed for train operation, but will be accessed, for example, at particular points in space or time.</li> <li>Examples for batch data transfers to trackside are:</li> <li>Readouts performed at the end of a service period</li> <li>Transfers performed at the train station</li> <li>Transfers scheduled and performed at fixed time intervals when the train is in operation</li> </ul>
--	---

#### OCORA-7632, D-Level - **Ability to provide instantaneous data transfers to trackside**

The MDCM shall provide means to realize instantaneous data transfers to trackside in "near real-time".

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Transmit process data and diagnostics data to the trackside that is required in "near real-time", for example by the Planning System to influence train operations.</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>short-term, CCS DataService</li> <li>long-term, TCMS DataService</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>Instantaneous data transfers shall be data driven. That is, instantaneous transmissions shall be performed onUpdate (for process data) respectively onEvent (for diagnostic data).</li> <li>Instantaneous data transfers to trackside shall be realized as telegram/message-based transfers.</li> <li>The queue length and priority for instantaneous data transfers shall be individually configurable.</li> <li>The term "near real-time" shall here refer to the "best-effort" principle, accepting time delays introduced by automated data processing and network transmission between the occurrence of an event and the reception/use of the processed data by recipients.</li> <li>The delay in "near real-time" shall be typically within a range of 1-10 seconds; see also <a href="#">Wikipedia:Real-time computing</a>. This given that a radio connection providing sufficient bandwidth is available, while not having a good radio connection is the rare exception and not the normal operation.</li> </ul>

#### OCORA-8044, D-Level - **Ability to provide ETCS/JRU data**

The MDCM shall provide means to retrieve information related to Juridical Recording Unit (JRU) according to ERTMS/ETCS subset 027, chapter 4.2.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Support of subset 149 (OMS)</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM short-term</li> <li>CCS Data Service</li> </ul>

### OCORA-8053, D-Level - Ability to provide ATO/ORD data

The MDCM shall provide means to retrieve information related to ATO/ORD data defined in ERTMS/ETCS subset 149, appendix 1.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Support of SUBSET-149 (OMS)</li> <li>Provide ATO/ORD data to trackside</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM short-term</li> <li>CCS DataService</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>The ATO/ORD data in scope of the MDCM is defined in ERTMS/ETCS SUBSET-149, appendix 1, which is currently only in draft status</li> <li>The mapping of ATO/ORD binary message data to MDCM message data, which is sent to trackside, is not yet included in SUBSET-149</li> </ul>

### OCORA-8047, D-Level - Ability to map event codes to text modules

The MDCM shall provide means to map diagnostic event codes from on-board functions to text-modules containing human-readable descriptions for these events.

- The mapping shall be such that there is one dedicated text module defined per event code
- Each text module shall contain texts displayed to the driver, as well as texts displayed to maintenance staff
- The mapping shall be configurable and updateable
- The mapping shall support different languages
- The mapping shall support the adaption to different vehicle configurations, e.g. adaption to different SW/HW versions where event codes might differ

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Having human-readable descriptions of event codes in different levels of details</li> <li>Having the MDCM as central database for providing and maintaining this mapping on-board the vehicle</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>CCS DataService, MDCM mid-term</li> <li>TCMS DataService, MDCM long-term</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>Event codes comprise both operational events and error codes</li> <li>Today, event codes are usually application- and/ or project specific and maintained by vehicle vendors</li> </ul>

## 3.3 System external interfaces

This chapter defines the required interfaces of the MDCM towards other actors. External interfaces are derived from MDCM capabilities.

### OCORA-7628, D-Level - Provide diagnostic data service for CCS-OB building blocks

The MDCM shall provide a dedicated service for retrieving monitoring- and diagnostic-data from CCS-OB building blocks.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Having a dedicated service for CCS-OB monitoring- and diagnostic-data access in OCORA system architecture.</li> <li>The MDCM deals with diagnostic communication with other CCS-OB building blocks and the provision of diagnostic data to requesting sites.</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM short- and mid-term</li> <li>CCS DataService</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>Monitoring- and diagnostic-data access for CCS-OB components will be realized by CCS DataService.</li> </ul>

#### OCORA-8220, D-Level - Provide diagnostic data service for TCMS functions

The MDCM shall provide a dedicated data service for retrieving monitoring and diagnostic data from TCMS functions.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Technicians can use the MDCM to commonly access onboard diagnostic data from both CCS-OB and TCMS functions</li> <li>Also needed for future ATO GoA 3/4 use cases, where MDCM is supporting automated fault management and recovery</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM long-term</li> <li>TCMS DataService</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>For future ATO GoA 3/4 use cases, fault management and recovery onboard the vehicle has to be automated</li> <li>The corresponding fault management function is assumed to be part of CCS-OB domain</li> <li>For troubleshooting and recovery of faults, the corresponding fault management function requires diagnostic data from TCMS functions as well</li> </ul>

#### OCORA-8214, D-Level - ETCS/JRU data acquisition interface

The MDCM interface for acquisition of ETCS/JRU data shall be compliant to ERTMS/ETCS SS-147 communication layer requirements.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Derived from OCORA-8044 - Ability to provide ETCS/JRU data</li> <li>Compliance to SS-149 (OMS), ch. 4.1, dropping support for legacy OBUs</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>CCS DataService</li> <li>MDCM short-term</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>SS-147 is currently only in draft status</li> <li>Support for migration scenarios as mentioned in SS-149 (OMS) is not supported</li> </ul>



### OCORA-8215, D-Level - ATO/ORD data acquisition interface

The MDCM interface for acquisition of ATO/ORD data shall be compliant to ERTMS/ETCS SS-147 communication layer requirements.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Derived from OCORA-8053 - Ability to provide ATO/ORD data</li> <li>Compliance to SS-149 (OMS), ch. 4.1, dropping support for legacy OBUs</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>CCS DataService</li> <li>MDCM short-term</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>SS-147 is currently only in draft status</li> <li>Support for migration scenarios as mentioned in SS-149 (OMS) is dropped</li> <li>The ATO/ORD dataset is according to SS-149 (OMS), appendix 1</li> </ul>

### OCORA-8216, D-Level - Common diagnostic communication interface to CCS-OB building blocks

The diagnostic communication between MDCM and CCS-OB building blocks shall use a common, standardized and service-oriented application-level protocol. Lower-level communication layers shall be compliant to ERTMS/ETCS SS-147.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Having a common solution for diagnostics and configuration of all CCS-OB building blocks</li> <li>Derived from <ul style="list-style-type: none"> <li>OCORA-7427 - Ability to acquire and transfer onboard monitoring data to trackside clients</li> <li>OCORA-7425 - Ability to issue commands to CCS-OB building blocks</li> <li>OCORA-7426 - Ability to manage configuration data transfers</li> <li>OCORA-8046 - Support of train-local configuration and update tasks</li> <li>OCORA-7630 - Ability to provide identification and configuration data from CCS-OB building blocks</li> </ul> </li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM mid-term</li> <li>CCS DataService and CCS ConfigService</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>CCS-OB building blocks have to implement standardized diagnostic service primitives that can be consumed by the MDCM</li> <li>Diagnostic service primitives provided by CCS-OB building blocks will be used by the MDCM to perform, amongst other tasks, <ul style="list-style-type: none"> <li>Identification of installed equipment</li> <li>HW and SW version readout</li> <li>Diagnostic data access</li> <li>Update and configuration tasks</li> </ul> </li> </ul> <p>Design recommendations:</p> <ul style="list-style-type: none"> <li>Use of ISO 14229-1 (UDS) and ISO 14229-5 (UDSonIP) for realizing diagnostics and configuration for CCS-OB building blocks</li> <li>Adaption to different communication protocols can be accomplished by the MDCM using the MVCI stack (ISO 22900-2/3)</li> </ul>

- |  |   |
|--|---|
|  | <ul style="list-style-type: none"> <li>• Vendor- and system-specific diagnostic data mapping and variant management can be accomplished by the MDCM using ISO 22901-1 standard (ODX)</li> </ul> |
|--|---|

### 3.4 System internal interfaces

Requirements imposed on internal MDCM-OB interfaces are left to be defined either in future versions of this document, or in corresponding design specification documents.

### 3.5 System internal data

Requirements imposed on internal MDCM-OB data are left to be defined either in future versions of this document, or in corresponding design specification documents.

### 3.6 System configuration and upgrades

Requirements for MDCM-OB configuration and upgradability will be defined in future versions of this document.

### 3.7 System safety

Safety related requirements for the MDCM-OB will be defined in future versions of this document. Currently, the MDCM-OB is only rated as basic integrity according to EN 50126.

### 3.8 System security and privacy

Requirements on MDCM-OB security and data privacy will be defined in future versions of this document.

### 3.9 System environments

Requirements concerning environmental characteristics and conditions in which the MDCM-OB must either operate or withstand will be defined in future versions of this document.

### 3.10 Computing and communication resources

Requirements concerning computing and communication demands of the MDCM-OB will be defined in future versions of this document.

### 3.11 System quality and performance factors

This chapter defines requirements concerning the expected quality and performance of MDCM-OB operation.

**OCORA-10220**, D-Level - Maximum service latency

During normal operation, the MDCM service latency shall be less than 1 second.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Requests sent to the MDCM shall be acknowledged instantaneously</li> <li>Under normal operating conditions (i.e. proper hardware, connectivity, usage, etc.) the MDCM shall process a client request and respond with the processing status (e.g. ok, inprogress, error) within 1 second</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM global</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>Normal MDCM operation does not include update or reboot. For these cases, MDCM latencies might be higher.</li> <li>In case of multiple parallel client sessions this requirement implies a multithreaded MDCM operation</li> <li>If the client request relates to a long-running routine, e.g. a logfile download or a SW update, then this requirement implies the ability of the MDCM to send periodic progress updates to the client, every second.</li> </ul>

#### **OCORA-10221, D-Level - Required service uptime**

During normal operation, the onboard platform shall be capable to accomplish an MDCM uptime of 99.999%.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>For OCORA CCS-OB platform, a MTBF of at least 10.000 hours can be expected</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM global</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>A MDCM failure is here meant to be a "loss of MDCM service due to an unforced internal error", which is caused, for example, due to platform hardware defects, or insufficient processing resources</li> </ul>

## 3.12 Design constraints

This chapter defines requirements concerning the general design of the MDCM-OB, such as platform support, deployment aspects and HMLs. Furthermore, this chapter defines requirements concerning processes for system development, documentation, qualification, and homologation of the MDCM, as imposed by sector standards and/or national regulations.

#### **OCORA-8045, D-Level - Use of MCG for train-to-ground communication**

The MDCM shall use the MCG of the vehicle for communicating with trackside systems.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>The MCG provides the Mobile Communication Gateway for train-to-ground communication with trackside systems from RU zone.</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM global</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>MCG shall here refer to the corresponding component defined in OCORA CCS-OB architecture</li> <li>The MCG is supposed to be compliant to latest applicable IEC 61375-2-6 standard</li> </ul>

### OCORA-10219, D-Level - Development process according to EN 50657

The MDCM supplier shall realize an EN 50657 compliant development process for the MDCM product. Applicable process elements shall be all "HR" and "R" items from EN 50657, A.2, Table A.1, for "Basic Integrity" software.

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Accomplish CENELEC compliance for OCORA CCS-OB building blocks</li> <li>The MDCM building block is a software product</li> <li>The MDCM product fulfils SIL-0 (basic integrity)</li> <li>Ensure a traceable product development process</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM global</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>For particular projects, some or all "R" process items might be dropped for MDCM product development, as acceptable process deviation; for example, to reduce development costs, or accept the use of COTS products where some of the otherwise required documents are not available.</li> </ul>

### OCORA-10222, D-Level - Provision of log and trace information

The MDMC shall provide means to trace its internal operation and resource consumption, as well as to detect internal processing errors. For that purpose, the MDCM shall realize proper logging and error handling functions that can be accessed remotely and locally, and can be controlled by authorised users through a dedicated API.

The following design constrain shall be met:

- Supported MDCM log levels shall be WARN, INFO, DEBUG, or equivalent
- The default log level shall be WARN
- The MDCM log and trace information shall be provided in a common human readable text format
- The log format shall be configurable, in particular the timestamp format and the language format

Classification	Requirement
Rationale	<ul style="list-style-type: none"> <li>Support optional EN 50567 architecture element D.26 (error handling and diagnostics)</li> <li>Facilitate assessment of MDCM performance during integration testing and during operation</li> </ul>
Remark	<p>Scope:</p> <ul style="list-style-type: none"> <li>MDCM global</li> </ul> <p>Remarks:</p> <ul style="list-style-type: none"> <li>For the meaning of log levels WARN, INFO, DEBUG, see: <a href="https://en.wikipedia.org/wiki/Syslog#Severity_level">https://en.wikipedia.org/wiki/Syslog#Severity_level</a></li> </ul>

## 3.13 Personnel and training

This chapter defines requirements for the MDCM-OB concerning the accommodation to different skill levels, training needs, or other information about the personnel who will use or support the system.

Currently, there are no specific requirements for the MDCM-OB concerning personnel and training. In future document versions such items may be added, though.

## 4 Acceptance criteria

The set of qualification methods and acceptance criteria that shall apply for MDCM-OB verification and validation are defined in [9], ch.6.

In future versions of this document the individual qualification method(s) to be applied per requirement will be defined as corresponding Verification Method attribute.

In the current document version, most of the requirements from chapter 3 shall be verified by Design Reviews. Performance related requirements from chapter 3.11 shall be verified by Inspections. Process related requirements from chapter 3.12 shall be verified by Process Reviews.

## 5 Traceability

The OCORA project uses a hierarchical requirements structure which is described in [9], ch. 3.1.

Within this requirements hierarchy all of the MDCM-OB requirements from chapter 3 are classified as D-Level (Building Block) requirements, that shall be either directly backward-traceable to higher-level OCORA requirements, such as C-Level (System) and B-Level (Program & Design) requirements, or backward-traceable to A-Level requirements constituting external stakeholder needs and applicable norms and standards.

If no direct backward-traceability of a MDCM-OB requirement to an existing higher-level requirement can be established, then there must be at least a Rationale statement provided as part of the requirement.