OCORA

Open CCS On-board Reference Architecture

Train Display System Onboard (TDS-OB)

Concept

Document ID: OCORA-TWS01-201

Version: 4.0

Date: 31.01.2025

Management Summary

In today's cab architecture, there are at least three main screens in a cab supporting three systems: European Train Protection (ETP), Train Control and Management System (TCMS) and Cabin Voice Radio (CVR). Each screen is usually dedicated to one system. The screen embeds only one business logic to enable data exchange with the appropriate system and elaborates the associated view. This paradigm leads to two main pitfalls:

- Firstly, a screen failure will result in a loss of the system. For instance, if the ETP's DMI fails, the ETP will go into system failure and apply an emergency brake. This will cause a delay to the train and can affect all the trains on a line. The availability of the screen is therefore a key factor in the overall availability of the train and the line.
- Secondly, space in the cab is limited especially since ergonomics for the driver needs to be ensured. By introducing new functionalities with the OCORA architecture, new building blocks and services (DAS, MDCM-OB, UID-Reader, etc.) may require space for their dedicated screen... However, the introduction of new display panels in both existing and new trains can be difficult for integrators due to the lack of space.

To solve these problems, OCORA is proposing the introduction of a new building block in line with the vision of ERA/European Commission for the future of the CCS-OB: the Train Display System (TDS). Other needs are also expressed with the introduction of TDS such as management of multiple systems on one display...

The third version of this document consolidates the operational and functional analysis and gives the TDS architecture chosen by OCORA's members.

Revision History

Version	Change Description	Initials	Date of change
1.0	Official version for OCORA Release R4	GH	23.06.2023
2.0	Official version for OCORA Release R5 affords • Operational analysis introduction • Requirements supplements • Functional analysis introduction • Architecture analysis supplements • Cross-industry analysis of displays • Train CS domain review	GH	23.11.2023
3.0	Official version for OCORA Maintenance Release R5.1 affords • Operational analysis supplements • Functional analysis supplements • TDS Architecture selection	GH	21.06.2024

4.0	Official version for OCORA Release R6. It affords
	• Operational analysis and Requirements modifications for remote driving
	  ◦ OCORA-10015 - Active configuration
	  ◦ 7 - Conclusion updated
	• New definitions: Configuration, Swap
	• Spelling corrections
		GH	31.01.2025

Author: Guilhem Herbelet (SNCF)

Contributors: Nicolas Bied-Charreton (SNCF), Mohand Hamiche (SNCF), Jérôme Lalouette (SNCF), Laurent Pinori (SNCF), Albert Ledermann (SBB), Thomas Martin (SBB), Martin Lindenmaier (SBB), Cirillo Ghielmetti (SBB), Robert Paleczek (OEBB)

Table of Contents

Table of Figures

References

Reader's note: please be aware that the document ids in square brackets, e.g. [OCORA-BWS01-010], as per the list of referenced documents below, are 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.

[OCORA-BWS01-010] – Release Notes
[OCORA-BWS01-020] – Glossary
[OCORA-BWS01-030] – Question and Answers
[OCORA-BWS01-040] – Feedback Form
[OCORA-BWS02-020] - Program Slide Deck
[OCORA-BWS02-030] - Technical Slide Deck
[OCORA-BWS02-040] - Program Posters
[OCORA-BWS02-050] - Technical Posters
[OCORA-BWS03-010] - Introduction to OCORA
[OCORA-BWS03-020] - Guiding Principles
[OCORA-BWS04-010] - Problem Statements
[OCORA-BWS05-010] - Road Map
[OCORA-TWS01-010] – Design Requirements
[OCORA-TWS01-011] – System Requirements
[OCORA-TWS01-020] – System Capabilities
[OCORA-TWS01-030] – System Architecture
[OCORA-TWS01-035] – CCS-On-Board Architecture
[OCORA-TWS05-020] – Stakeholder Requirements
[OCORA-TWS05-021] – Program Requirements
[OCORA-TWS05-022] – Design Requirements
[ERA ERTMS 015560] – ETCS Driver Machine Interface
[NF EN 1686] integration of displays, controls and indicators / design of display
[CLC/TR 50542] - Driver's cab train display controller
[CLC/TS 50459] - Railway applications - Communication, signalling and processing systems - European Rail Traffic Management System - Driver-Machine Interface

1 Introduction

1.1 Purpose of the document

This document is the OCORA Train Display System (TDS) concept. This document introduces the problem statement of the current HMI situation in the cabin. To solve this problem, the TDS concept (terminology and main characteristics of the architecture) and high level requirements are presented. All the concepts are still under discussion.

The requirements listed in this document are developed from a TDS onboard building block perspective. According to the OCORA definition, they are part of the OCORA D-Level requirements (refer to 1.4 - Requirements Engineering Process). The building block requirements (OCORA D-Level requirements) are detailing the OCORA system requirements [OCORA-TWS01-011].

The building block requirements captured in this document are developed to reach a common understanding and communicate a precise OCORA view of the functional and non-functional requirements towards future TDS.

The building block requirements listed in this document are prepared as an input for:

- EU-Rail and OCORA system architecture and design activities, shaping future TSI specifications, other legal frameworks, and other specifications
- Contracting entities, preparing tenders, and executing testing / certification activities for TDS

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA requirements for TDS. The reader is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping these requirements. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [OCORA-BWS01-040] .

If you are an organisation interested in developing TDS according to the OCORA requirements, information provided in this document can be used as input for your development.

1.2 Applicability of the document

The document is informative. Subsequent releases of this document will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

All requirements listed in status "Draft" are still under discussion within OCORA while the requirements in status "Approved" are agreed between the OCORA member organisations.

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 [OCORA-BWS01-010] . Before reading this document, it is recommended to read the Release Notes [OCORA-BWS01-010] . If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [OCORA-BWS03-010], and the Problem Statements [OCORA-BWS04-010]. The reader should also be aware of the Glossary [OCORA-BWS01-020] and the Question and Answers [OCORA-BWS01-030].

In addition to the requirements listed in this document, it is referencing the applicable ERA TSI CCS 2023 and TSI LOC & PAS 2023 documents. Requirements that are in conflict with the CCS TSI 2023 are highlighted in the remark section of the respective requirement.

1.4 Requirements Engineering Process

This OCORA requirement document is developed, using the Requirements Management Guideline [OCORA-TWS05-010]. The requirements are engineered in a top-down manner:

- As a starting point all **"Stakeholder Requirements"** towards the OCORA initiative **(A-Level requirements)** are captured and formalised.

- In a second step, the **"Program- and Design Requirements" (B-Level requirements)** are developed. These requirements define tools, processes, methodologies and design rules to be used within the program and to be considered during the system analysis and the system design/architecture work.

- As a next step, the A- and B-Level requirements are further developed in the MBSE analysis to become **"System Requirements" (C-Level requirements).**

- As part of the MBSE architecture work, building blocks are identified taking into account the MBSE analysis (C-Level requirements). All applicable requirements (A-Level, B-Level, and C-Level) are apportioned to the identified building blocks, resulting in **"Building Block Requirements" (D-Level requirements)**, forming the OCORA tender templates, together with the applicable program & design requirements.

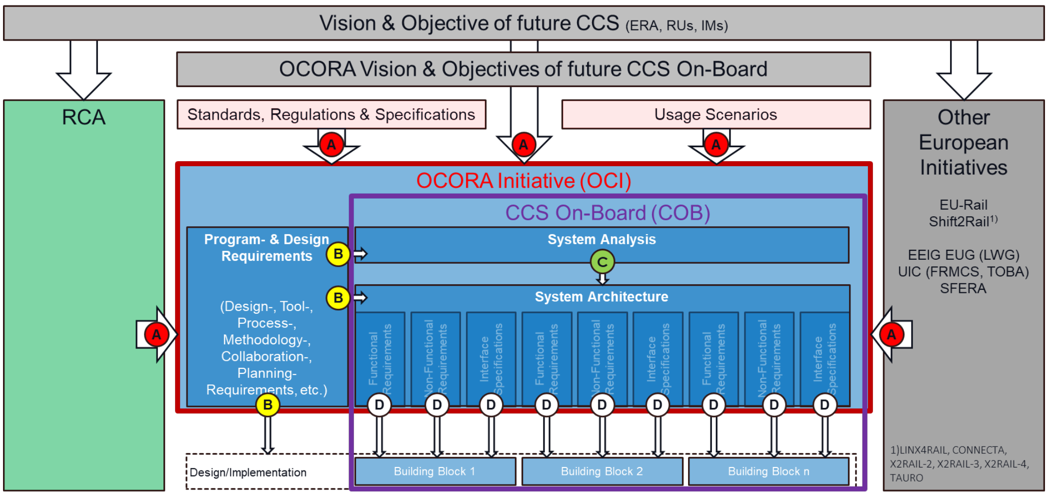


Figure 1 OCORA Requirements Engineering Process

Please note, that the A-Level requirements are applicable to the OCORA Initiative (OCI) while the B- and C-Level requirements are targeted towards the CCS On-Board System (COB) and its architecture. D-Level requirements are applicable to the respective building blocks.

2 Operational analysis

2.1 Problem statement

In today's cab architecture, there are at least three main screens in a cab supporting three systems: European Train Protection (ETP), Train Control and Management System (TCMS) and Cabin Voice Radio (CVR). Each screen is usually dedicated to one system. The screen embeds only one business logic to enable data exchange with the appropriate system and elaborates the associated view.

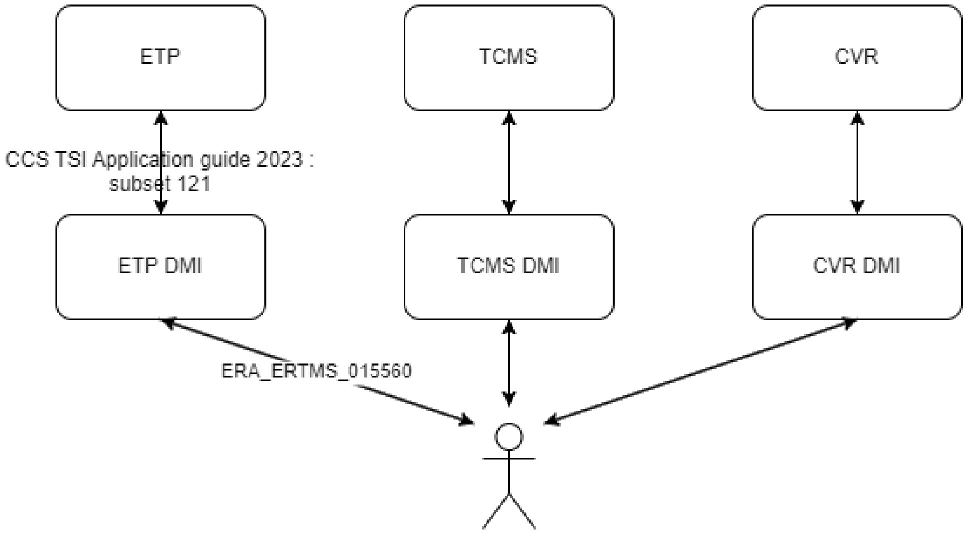


Figure 2 Problem statement

This paradigm leads to some pitfalls:

- Firstly, a screen failure will result in a loss of the system. For instance, if the ETP's DMI fails, the ETP will go into system failure and apply an emergency brake. This will cause a delay to the train and can affect all the train on a line. The availability of the screen is therefore a key factor in the overall availability of the train and the lines. To continue mission with a screen failure, supplier have created proprietary solutions. For instance, TCMS information can be displayed on ETP DMI when TCMS screen fails. This failure management meets an operational needs for Railway Undertaking. However, the lack of standardisation leads to non-portable solutions between trains.
- Secondly, space in the cab is limited especially since ergonomics for the driver needs to be ensured. By introducing new functionalities with the OCORA architecture, new building blocks and services (DAS, MDCM-OB, UID-Reader, etc.) may require space for their dedicated screen. However, the introduction of new display panels in both existing and new trains can be difficult for integrators due to the lack of space.
- Thirdly, an update of the ergonomic systems or the system itself might lead to an update of both parts. This interdependency increases costs, efforts and downtime involved in maintenance (update). This is more problematic for components with different SIL. For example, an ergonomic enhancement to the DMI of the ETP (SIL2 component) might lead to an update of the ETP (SIL4 component).
- Fourthly, data exchanged between the system and its ergonomical interfaces to the driver are supplier specific. As a consequence, screens are not exchangeable and modular. This issue creates a vendor lock-in situation. Despite the introduction of subset 121, which specifies the exchanges between the EVC and the DMI, the links between the other systems (CVR, DAS, MDCM-OB, TCMS, UID-Reader, etc.) and their displays need to be standardised. To date, two options are being considered: extending the use of subset 121 to all systems and their HMIs or dedicated standardisation between each system and its HMI.

To solve these problems, OCORA is proposing the introduction of a new building block: the Train Display System (TDS). This block provides independency between systems (ETP, TCMS, CVR, etc.) and DMIs. As the exact boundary of TDS is not yet clearly defined, the rectangle associated with this system is deliberately dotted. However, the main characteristics envisaged for the TDS are presented in 6 - TDS architecture and the high levels requirements are given in 4 - System Requirements.

Other needs are also expressed with the introduction of TDS such as management of multiple systems on one display.

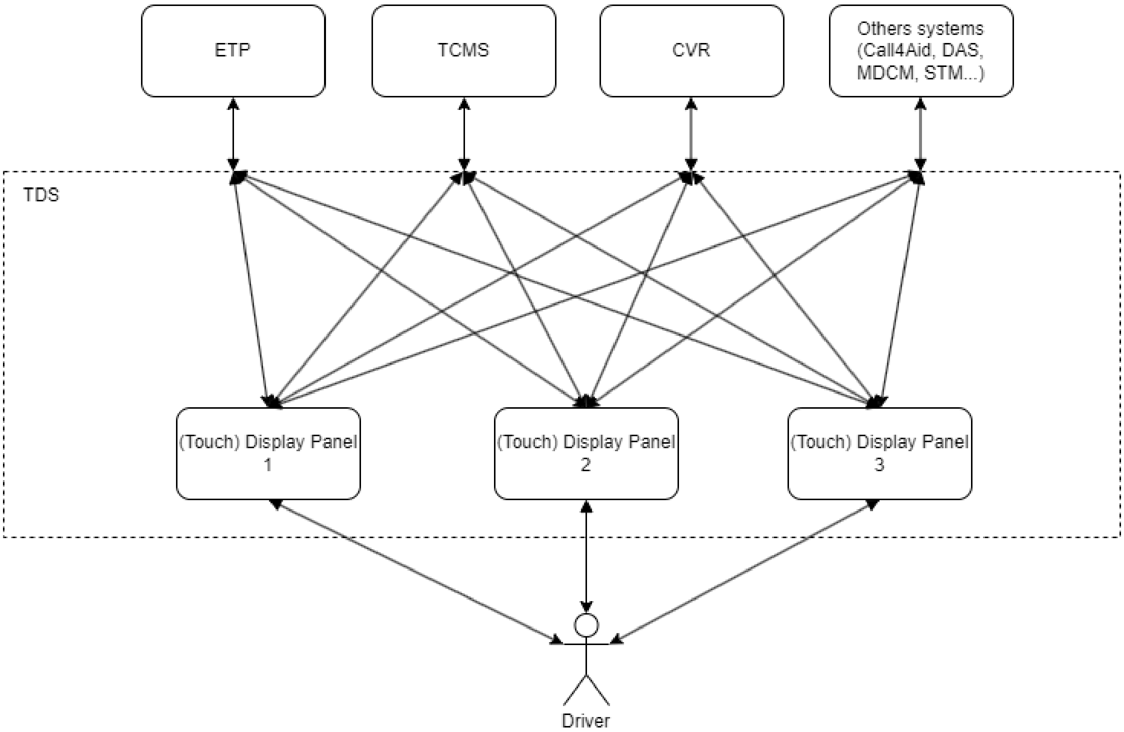


Figure 3 TDS principle

The figure above is limited to three (touch) display panels to depict the difference with the current situation. However, TDS shall not be limited to three (touch) display panels: one (extra-large) to n (touch) display panels might be managed by configuration. The amount of (touch) display panel is an operator choice.

2.2 Operational Epics

In the following section, identified key operational epics related to Train Display System are listed. These epics tackle down the pitfalls expressed above. All epics descriptions follow the same pattern :

- initially it is stated, who benefits from the epics (e.g. infrastructure manager, railway undertaking and/or supplier);
- then the epics itself is formulated;
- and finally the rationale of the epic is provided.

Also, the derivation of the Operational Epics from the Common Business Objectives from ERJU are shown. This link will ensure a continuity with System Pillar activities.

OCORA-10277 - As a railway undertaking, I want to keep or increase the availability of all systems in my train that are using displays in order to increase the overall availability of my train: e.g. not to stop the train and ensure a continuity of service.

Linked Work Items	refines : OCORA-8805 - availability, robustness, reliability refines : OCORA-8820 - overall CAPEX/OPEX optimisation(1) has parent : OCORA-10263 - Operational Epics

OCORA-10268 - As a railway undertaking, I would like to add systems which require a display in the vehicle without integrating dedicated display panels in the cabs, in order to better manage the available space and limit the integration effort.

Linked Work Items	refines : OCORA-8813 - independent lifecycle, simple exchange refines : OCORA-8816 - Changeability and upgradeability(1) refines : OCORA-8818 - Changeability and upgradeability(3), simplified integration refines : OCORA-8829 - modularity refines : OCORA-8856 - reduce time to market has parent : OCORA-10263 - Operational Epics

OCORA-10276 - As a railway operator, I want to establish distinct segregation between systems and their Human-Machine Interface (HMI) functions to safeguard their individual functionalities. This strategy is vital to prevent any unintended side effects during future updates and to mitigate the risk of display loss resulting from failures in other interconnected systems.

Linked Work Items	refines : OCORA-8805 - availability, robustness, reliability refines : OCORA-8816 - Changeability and upgradeability(1) refines : OCORA-8817 - Changeability and upgradeability(2) refines : OCORA-8818 - Changeability and upgradeability(3), simplified integration refines : OCORA-8829 - modularity has parent : OCORA-10263 - Operational Epics

OCORA-10269 - As a railway undertaking, I would like to change display solution without vendor lock-in for spare parts in order to minimise OPerational EXpenditure (OPEX) and Mean Time To Repair (MTTR).

Linked Work Items	refines : OCORA-8813 - independent lifecycle, simple exchange refines : OCORA-8816 - Changeability and upgradeability(1) refines : OCORA-8818 - Changeability and upgradeability(3), simplified integration refines : OCORA-8819 - automate lifecycle processes, independent lifecycle refines : OCORA-8846 - standardized architecture(2) has parent : OCORA-10263 - Operational Epics

OCORA-10267 - As a railway undertaking, I would like to manage the least possible number of display solutions in order to reduce costs, efforts and downtime involved in maintenance (update).

Linked Work Items	refines : OCORA-8816 - Changeability and upgradeability(1) refines : OCORA-8819 - automate lifecycle processes, independent lifecycle has parent : OCORA-10263 - Operational Epics

OCORA-10275 - As a railway undertaking, I want to minimise the impact of any ergonomic enhancement in order to lower OPerational EXpenditure (OPEX):

- avoid/reduce certification process effort in case of "ergonomic" update,
- reduce time to market in case of this kind of update.

Linked Work Items	refines : OCORA-8813 - independent lifecycle, simple exchange refines : OCORA-8816 - Changeability and upgradeability(1) has parent : OCORA-10263 - Operational Epics

2.3 Involved Entities and Actors

The figure below gives an overview of the entities/actors involved in the context of TDS. The entities/actors are the driver, the maintainer, the systems, the TDS and the train itself. For each of them, their main characteristics and tasks are given below.

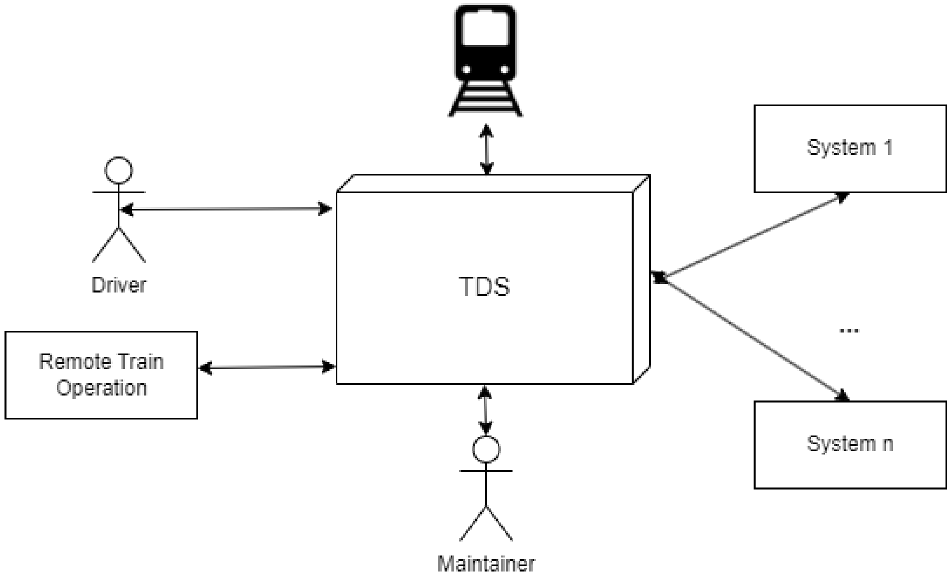


Figure 4 : Entities and actors involved with TDS

2.3.1 Driver

The driver is an operational actor. He is in charge of (un)preparing and driving trains. The main tasks of this actor are: activate/deactivate the cab, activate/deactivate systems, configure displays on the cab and operate systems.

2.3.2 Remote Train Operation

The Remote Train Operation (RTO) system is an operational entity. It provides the status of the train in terms of remote driving: stand-alone, monitored, observed and controlled. Depending on this status, the TDS can change the active configuration of the cab displays.

In addition to provide input to the TDS, the RTO may require a specific view on a display. If so, the interface between the RTO and the TDS will be the same as for the other systems described below.

2.3.3 Maintainer

The Maintainer is an operational actor. He is in charge of maintaining a system in a operational state. To do so, he can monitor, diagnose, repair, update and configure the system. The main tasks of this actor are: configure displays in the cab, diagnose issues of a system, repair a system and update a system.

2.3.4 Systems

In the context of TDS, systems are operational entities that require a human-machine interface. There are several systems in a cab. In this chapter, it is proposed to present the main systems considered in this paper in order to find the characteristic to be analysed from perspective of TDS. So descriptions of ETCS, TCMS, CVR and Rearview systems are given below and give an overview of their current situation. Other systems exist, such as Electronic Timetable Display, and should also be considered. However, it is assumed that the characteristics of the systems analysed would remain applicable to the other systems. An exhaustive analysis should be carried out to be sure of the relevance of this proposal. So far, the following characteristics have been considered: ergonomics, location in the cab, SIL requirements, when visibility is required, interface between the system and the driver's display.

ETCS (CCD display)

The display associated to this system is called CCD (Control Command Display) in UIC-612. The functionalities and the ergonomics of this system are standardised in the subset 026 and ERA DMI 15560.

The CCD display is located in front of the driver according to UIC-612-0, EN 16186-2 (chapter 7.21).

According to subset 091, some THR are related to the DMI and involve THR equivalent to SIL2.

Information of ETCS are mandatory when train is in motion. It could be debatable if this is also the case at standstill.

Communication between ETCS and TDS is standardised in subset 121.

TCMS (TDD display)

The display associated to this system is called TDD (Technical and Diagnostic Display) in UIC-612. The ergonomics of this system is also defined in UIC-612-3.

The TDD is located on the right side of the cab according to UIC-612-0, EN 16186-2 (chapter 7.21).

Depending of the configuration of the train, the SIL associated to TDD could be SIL2 (when safety related information are only displayed on TDD) or SIL0 / Basic Integrity (when safety related information is presented on TDD and also with safe lights in cab).

According EN 16186-3 (table B.2), if existing, some information is mandatory for high speed class 1 trains. Otherwise, other information is optional.

Current communication between TCMS and TDD is supplier-specific. To facilitate the deployment of the TDS solution, a migration to a generic communication used also by other systems should be considered.

CVR (TRD Display)

The display associated to this system is called TRD (Train Radio Display) in UIC-612. The ergonomics of this system is also defined in UIC-612-4.

The TRD is located on the left side of the cab according to UIC-612-0, EN 16186-2 (chapter 7.21).

The SIL is SIL0 (Basic Integrity).

Information is presented on demand when triggered by the driver or when external actors (passenger, traffic agent, etc.) call the driver.

Current communication between CVR and TRD is supplier-specific?To facilitate the deployment of the TDS solution, a migration to a generic communication used also by other systems should be considered.

Rearview system

The Rearview system permits to see the states of the doors at standstill. The ergonomics of this system is supplier specific; no norm or standard specify it.

Two displays are used for the rearview system. Two options exist for the position of the displays : one on the left side of the cab and the other on the right side of the cab (left doors vs. right doors). or the two displays side by side on the left or on the right side of the cab.

The SIL associated to this system is SIL0 (Basic Integrity).

Images from cameras are only displayed at standstill.

Current communication between Rearview system and its displays is supplier specific. To facilitate the deployment of the TDS solution, a migration to a generic communication used also by other systems should be considered.

Overview table

System	Ergonomics	Localisation of the display*	SIL	when view is required	System <-> display interface
ETCS	ERA DMI 15560	mandatory in the front of the driver	SIL2	Mandatory when in motion, but debatable at standstill.	subset 121
TCMS	UIC-612-3	usually on the right of the ETCS	SIL2 or SIL0/BI	Some information of High speed class 1 train are mandatory. Otherwise, information are optional.	supplier specific**
CVR	UIC-612-4	usually on the left side of the cab	SIL0/BI	On driver demand or when external actors call the driver.	supplier specific**
Rearview system	not standardised	position of the two displays is related of the train integration: - One on the left (left doors) and the other on the right (doors on the right) or - both 2 displays side by side on the left or on the right.	SIL0/BI	Supplier-specific, mainly useful only at standstill.	supplier specific **

*The localisation of displays is given according the recommendation of UIC-612. However, the chapter 3.3.2.4 of UIC-612 document considers also that ability to change the location of any display in case of major constraints.

**To facilitate the deployment of the TDS solution, a migration to a generic communication used also by other systems should be considered.

These systems are involved in the following tasks: activate/deactivate the cab, activate/deactivate system, configure displays on the cab, diagnose errors of a system, interact with systems, monitor the state of a system, repair a system and update a system.

2.3.5 Train Driver System (TDS)

The TDS is an operational entity that enables interactions between the driver and systems.

This system is involved in the following tasks: activate/deactivate the cab, configure displays on the cab, diagnose errors of a system, interact with systems, monitor the state of a system, repair a system and update a system.

2.3.6 Train

The train is an operational entity that provides informations to TDS such as cab is active, train in motion or at standstill.

The train is involved in the following tasks: activate/deactivate the cab and configure displays on the cab.

3 TDS terminology

In order to better understand the environment associated with managing the driver-machine interface in the driver's cab, the OCORA team needed to represent physical and logical views. Although these views do not offer an exhaustive list of possible integrations, nor the final architecture retained, they illustrate the key concepts used in this document.

3.1 Overview

The aim of the representation below is mainly to list all elements in the TDS context and to use it for the definition of the terms used in this document. This overview represents the link between systems such as Cabin Voice Radio, European Train Protection and TCMS to Controller unit dedicated to HMI. These control units use a set of HMI elements (buzzer, display panels, hard keys, etc.) to guarantee the interface with the driver.

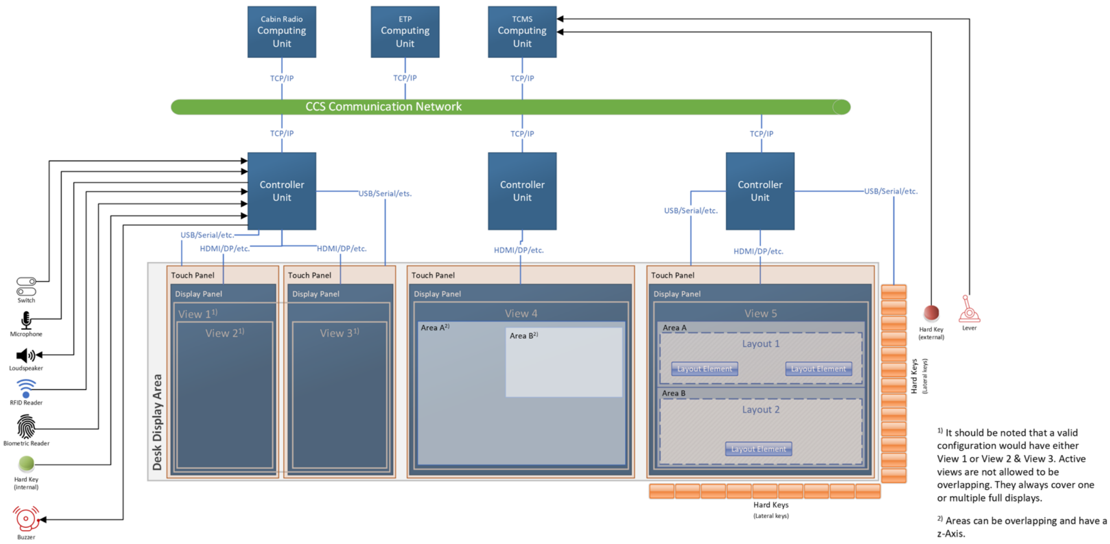


Figure 5 TDS context overview

Here, the communication between the computing units of systems are granted by the CCS Communication Network as OCORA consider mainly the integration of TDS for new train.

Switch, microphone, RFID Reader, Biometric Reader, Hard key and buzzer are connected to a central controller unit. A distributed configuration is also possible.

3.2 Physical terminology

This view represents the physical breakdown of the train down to the HMI elements integrated into a desktop.

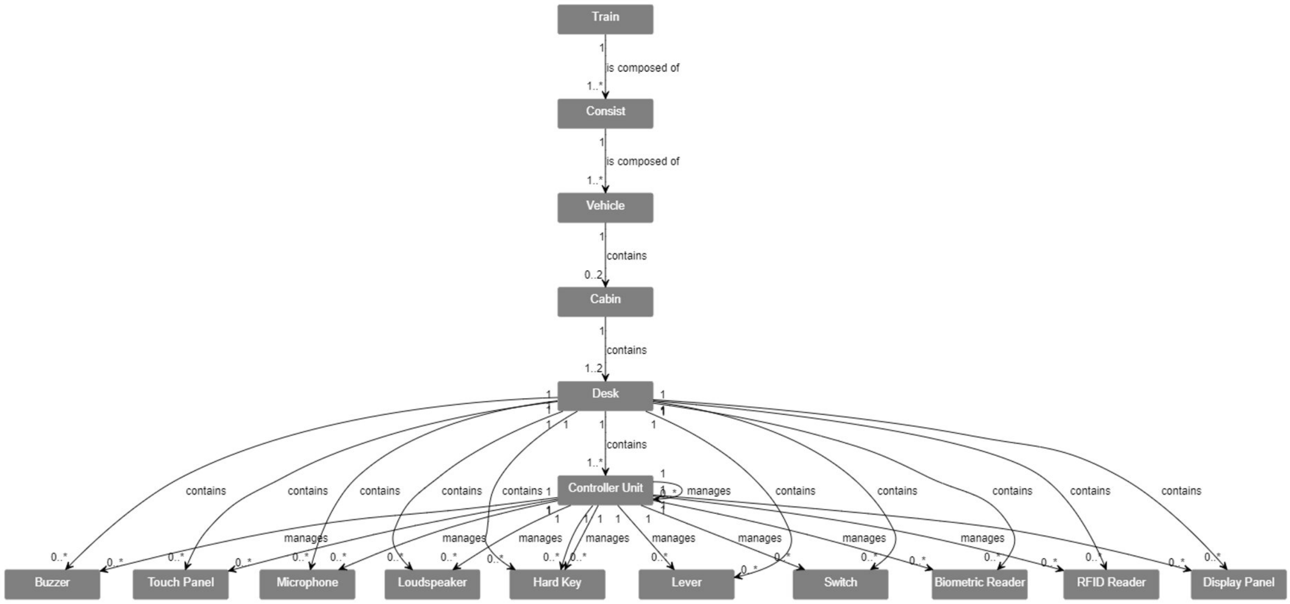


Figure 6 Physical terminology tree

The idea of OCORA is to limit the perimeter of TDS to the management of two desks:

- two desks in the same cabin, e.g. in a shunting engine.
- one desk per cabin limited to two cabins, e.g. centralised CCS integration in a consist.

3.3 Logical terminology

This logical view represents in detail all the logical and configuration elements involved in the elaboration of the view for a system (ETP, TCMS, etc.). Physical input and output devices are also represented in this view for contextual understanding.

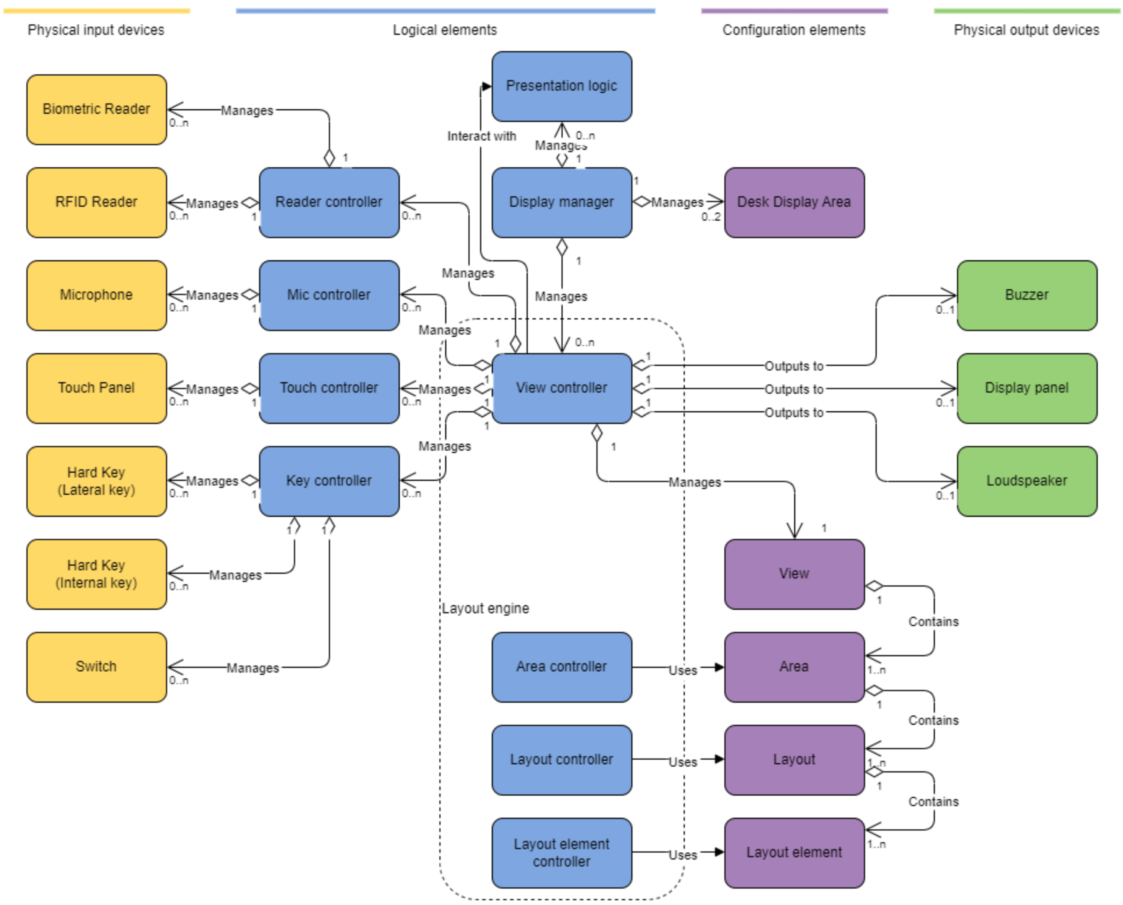


Figure 7 Logical terminology view

3.4 Definitions

The following definitions are used in the context of the TDS concept. Other definitions can be found in the Glossary documentation. [OCORA-BWS01-020]

Title (Abbrev.)	Description	Status
Area Controller ()	The *Area Controller* manages areas for the *View*.	**draft**
Biometric Reader ()	Device that reads the identity of a person by comparing some attribute of their physiological being or behavioral traits against a sample database. This reader permits the authentication of the actor.	**draft**
Button ()	A *Hard Key* allocated to a dedicated system on a cab. It's designed with a dedicated SIL. It allows a selection from two states and keeps one state as long as it is pressed.	**draft**
Buzzer ()	Electrical device that makes a buzzing noise and is used to provide an audible warning.	**draft**

Title (Abbrev.)	Description	Status
Configuration ()	Refers to an allocation of systems with TDS units. This allocation could be selected and applied by the TDS (Display Manager).	**draft**
Controller Unit ()	The *Controller Unit* is a hardware component which embeds logical controller(s). There may be only one Hardware or distributed to several HMI elements.	**draft**
Desk ()	Inside a cab, the set of operating controls*, which is dedicated to preferred movements in a given direction (i.e. forward movements, in which visibility from the cab is provided to the driver). Exception: some single cab locomotives are fitted with one single desk, allowing normal movements in both directions. *set of operating controls: screens, buttons, traction/brake lever, direction controller, radio control, switches, …Desk	**draft**
Desk Area ()	*Desk Area* is a location attribute (left, centre, etc.) associated to *HMI Element* for *Display Manager* to allocate elements to a *View*.	**draft**
Desk Display Area ()	The *Desk Display Area* identifies the desk controlled by TDS (in case of multiple cabins controlled only by one TDS such as locomotive or centralised integration).	**draft**
Display ()	Display is the combination of a display panel and a controller unit.	**draft**
Display Area - Area ()	A Zone displaying a piece of visual information of particular system and defined by a size (in cells) and an absolute position (x ,y, z axes). It is more commonly named *Area* in this specification.	**draft**
Display Manager ()	The *Display Manager* interacts with system (CCS, TCMS,CVR) and manages the *Desk Display Area*.	**draft**
Display Panel ()	Glass (LCD) showing pixels without controller.	**draft**
External Button ()	A button which is not directly managed by TDS.	**draft**
Hard Key ()	Physical key not part of view. This key can also have a text label or symbol.	**draft**
HMI Element ()	An *HMI Element* is a physical component that interacts with the driver: *Buzzer*, *Display Panel*, loudspeaker, *Hard Key, etc*.	**draft**

Title (Abbrev.)	Description	Status
Internal Button () The *Internal Button* is a button which is managed directly by TDS.		**draft**
Key Controller () Controller which manages states and failures of *Hard Keys* (internal and *Lateral Key*) and switches.		**draft**
Lateral Key () *Hard Key* located close to a *Display Area* allowing soft key technology.		**draft**
Layout () Layout is a list of layout elements which is displayed in an area.		**draft**
Layout Controller () The *Layout Controller* manages the *Layout* for an *Area*.		**draft**
Layout Element () Every element to be shown on the screen like button, speed gauge, video stream, symbol and text with their characteristics (size, position, type, colour, associated icon, etc.).		**draft**
Layout Element Controller () The *Layout Element Controller* manages *Layout Elements* of a *Layout*. It knows how to present itself and how to react on events.		**draft**
Layout Engine () The *Layout Engine* is a generic piece of software able to generate any *View* based on *Areas*, *Layouts* and *Layout Elements* as defined in a configuration.		**draft**
Loudspeaker () Device that converts an electrical audio signal into a corresponding sound.		**draft**
Microphone () Device that translates sound vibrations from the air into electronic signals and scribes them to a recording medium or over a loudspeaker.		**draft**
Microphone Controller () The *Microphone Controller* manages states and signals of *Microphone*.		**draft**
Presentation logic () The presentation logic controls the flow (dialogue sequence) and layout elements of the User interface using system specific layouts based on generic layout elements. The presentation logic may also include data validation.		**draft**
Reader Controller () The *Reader Controller* manages states and failures of the *Biometric Reader* and/or the *RFID Reader*.		**draft**

Title (Abbrev.)	Description	Status
RFID Reader ()	Radio Frequency Identification (RFID) refers to a wireless system comprised of two components: tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag. This reader permits the authentication of the actor.	**draft**
Soft Key ()	Context-dependent key which consists of a *Hard Key* with an associated label on the *Display Area*. When using a soft key technology, the driver action is done via the *Hard Key* adjacent to the label.	**draft**
Swap ()	Refers to the swapping of views displayed when multiple systems are using the same TDS unit. Swapping allows one of the stacked views to be displayed over the currently displayed view.	**draft**
Switch ()	Physical component which allows a selection of 2 to N states and keeps the state until its position is changed.	**draft**
Touch Controller ()	Controller which manages the states and failures of a *Touch Panel.*	**draft**
Touch panel ()	Hardware detecting where the finger touch the panel.	**draft**
Train Display System (TDS)	The Train Display System comprises and manages one or more TDS units on the driver desk. It offers a standardised communication interface to systems that need driver interaction.	**draft**
Train Display System Unit (TDS unit)	Train Display System unit consists of hardware elements associated with a display panel and software elements (display manager and layout engine). These units communicate through CCN to systems (ETCS, TCMS, etc.) and to each others.	**draft**
View ()	Aggregation of *Areas* required for systems (CCS, TCMS, CVR, etc.). A *View* can represent *Areas* of different systems at the same time.	**draft**
View Controller ()	The *View Controller* aggregates the *View*, the output devices and the controller of each input device.	**draft**

4 System Requirements

OCORA has expressed high-level requirements for the building block: Train Display System. These requirements come from the operational capabilities expressed above.

4.1 General requirements

OCORA-10011, D-Level - Managing input and output devices

The TDS shall manage a defined set of input and output devices that are used for user interaction on a desk.

Status	In Review
Classification	Requirement
Rationale	Reduce the number of HMI elements on the desk.
Category	Functional
Acceptance Method	Certification
Acceptance Criteria	
Remark	
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-10289 - General requirements is refined by : OCORA-10285 - Manage configuration defines : OCORA-10294 - Layout Engine defines : OCORA-10295 - Display Manager

OCORA-10012, D-Level - Managing desks

The TDS shall manage at most two desks.

Status	In Review
Classification	Requirement
Rationale	Limit the scope of TDS.
Category	Functional
Acceptance Method	Certification
Acceptance Criteria	
Remark	Allowing to manage shunting engine and centralised integration in a consist.
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-10289 - General requirements is refined by : OCORA-10284 - Manage the Desk Display Area defines : OCORA-10295 - Display Manager

OCORA-10308, D-Level - One desk activation

The TDS shall activate only one desk at a time.

Status	In Review
Classification	Requirement
Rationale	Avoid similtaneous activation of desks in the same consist.
Category	Functional
Acceptance Method	Certification
Acceptance Criteria	
Remark	• The activation of the desk command the wake up of all systems embedded in it. • The commands from the non active desks shall not command systems.
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-10289 - General requirements is refined by : OCORA-10284 - Manage the Desk Display Area defines : OCORA-10295 - Display Manager

OCORA-10013, D-Level - Allocating input/output devices to dedicated system

The TDS shall allocate input and output devices to a dedicated system.

Status	Draft
Classification	Requirement
Rationale	Provide necessary devices to a system.
Category	Functional
Acceptance Method	Certification
Acceptance Criteria	
Remark	Devices allocated to a system at a time shall not be used by another system. For instance on a shared display with ETCS view and TCMS view, buttons dedicated to ETCS shall not be used by TCMS. In a configuration with systems that share output devices (e.g. displays), each system must have a zone or events that guarantee dedicated use of the device. Open points: - sharing a loudspeaker among multiple systems has to be analysed with regards to current integration. - sharing a buzzer / loudspeaker with a stacked view should be investigated.
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-10289 - General requirements is refined by : OCORA-10285 - Manage configuration defines : OCORA-10294 - Layout Engine defines : OCORA-10295 - Display Manager

OCORA-10014, D-Level - Allocations registered as configuration

The TDS shall manage all device allocations as configuration.

Status	Draft
Classification	Requirement
Rationale	One configuration gives all input/output devices allocations for the systems.
Category	Functional
Acceptance Method	Certification
Acceptance Criteria	
Remark	Some configuration parameters are given as proposal. Nonetheless, a deeper analysis should be performed in a next release. • IP address of HMI elements allocated to a system. • the size and position of the area allocated to the system. • A priority parameter to avoid conflicts in case of multiple systems in one display. • To be more investigated (active/redundant channel, number of systems, type of system, etc.).
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) defines : OCORA-10294 - Layout Engine has parent : OCORA-10289 - General requirements defines : OCORA-10293 - System Presentation Logic is refined by : OCORA-10285 - Manage configuration defines : OCORA-10295 - Display Manager is refined by : OCORA-10280 - System Presentation Logic and Display Manager communication

OCORA-10015, D-Level - Active configuration

The TDS shall set the active configuration automatically (by events) or manually (by the driver) among a list of pre-approved configurations.

Status	In Review
Classification	Requirement
Rationale	Only one configuration is active at a time.
Category	Functional
Acceptance Method	Certification
Acceptance Criteria	

Remark	TDS should consider a nominal configuration by default and other configurations when required: • Nominal configuration (with all systems and HMI elements operational) • Event based configurations (e.g. driver selection, train in motion/at standstill, etc.) • Degraded configurations (in case of system or HMI element failure) • Remote driving configuration (depending the states of RTO system: stand-alone, observed, monitored, controlled) The configuration shall take under consideration the mandatory systems for operation (e.g ETCS in a front location) and the optional systems. For each system, an evaluation of the possible location on the desk shall be performed with the associated events. The driver can only select a pre-approved configuration. In case of failure, the TDS shall switch the active configuration in a fully transparent way for systems. This reconfiguration shall not require a reboot of TDS, systems or HMI elements.
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-10289 - General requirements defines : OCORA-10293 - System Presentation Logic is refined by : OCORA-10285 - Manage configuration defines : OCORA-10294 - Layout Engine defines : OCORA-10295 - Display Manager is refined by : OCORA-10281 - System Presentation logic send health information to Display Manager

OCORA-10016, D-Level - Extended view concept

The TDS shall allow by configuration a view that extends on multiple display panels which are adjacent to each other.

Status	Deleted
Classification	Operator Choice
Rationale	- Save space in comparison to two full grid screens, i.e. two half grid screens are smaller (1.5 vs. 2). - Keep the screen in a central area for drivers. - Being resilient to a failure in order to continue a mission (by displaying only "speed" half-grid part in case of screen failure).
Category	Functional
Acceptance Method	Test
Acceptance Criteria	
Remark	Example: ETCS information is extended on 2 half-grid screens (one screen display the “speed” half-grid part and a second screen display the “planning area” half-grid part). OCORA review : As displaying speed and planning area are mandatory in ETCS level 1 and 2 in mode FS, SM and AD and has to remain adjacent for operational and safety reason, extended view concept is no longer acceptable. In deed, in degraded configuration, only speed is displayed. The planning area remain accessible but with a lower priority given to speed half-gird. As the ERA analysis is ongoing and the removal of this concept facilitates the architectural analysis, this requirement is deleted in this version. It could be re-opened if needed.
Linked Work Items	has parent : OCORA-10289 - General requirements

OCORA-10017, D-Level - Modularity

The TDS shall enable systems to link all their input/output to any touch/display panel based on a pre-approved configuration.

Status	In Review
Classification	Requirement
Rationale	• Enhance flexibility for configuration • Rationalise the number of display panels in the cab for space and costs saving
Category	Functional
Acceptance Method	Design Review
Acceptance Criteria	

Remark	Limitation to physical characteristics The modularity concept should be weighted depending on the pre-approved configuration ([OCORA-10015]) which take under consideration the location of the display panel in the cab. Indeed, some systems could be only displayed in some location (e.g. ETCS in front of the driver).
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-10289 - General requirements defines : OCORA-10295 - Display Manager

OCORA-10018, D-Level - Systems management

The TDS shall manage the HMIs of multiple systems (e.g., ETP, TCMS, CVR, etc) in parallel.

Status	In Review
Classification	Requirement
Rationale	Enhance availibility, concurrency management, prioritisation
Category	Functional
Acceptance Method	Design Review
Acceptance Criteria	
Remark	Legacy train: multiple means limited to specific systems supporting TDS. New train: multiple means all systems
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-10289 - General requirements defines : OCORA-10294 - Layout Engine defines : OCORA-10295 - Display Manager is refined by : OCORA-10280 - System Presentation Logic and Display Manager communication

OCORA-10019, D-Level - Multiple systems on one display

The Train Display System may display areas from different systems on the same display panel.

Status	In Review
Classification	Optional Requirement
Rationale	Depending the size of the display panel (e.g. wide screen), several areas might be displayed on the same panel. It may decrease the number of panels embedded in cab.
Category	Functional
Acceptance Method	Test
Acceptance Criteria	
Remark	In case of Multiple systems on one display area, SIL supervision should be done accordingly to system needs. A priority parameter should be used to avoid conflicts in case of simultaneous display for multiple applications.
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-10289 - General requirements defines : OCORA-10295 - Display Manager

OCORA-10114, D-Level - Supporting Testing tools

The TDS shall be able to support testing tools that emulate driver interactions with systems e.g., ETP, TCMS, etc.

Status	Deleted
Classification	Operator Choice

Rationale	For testing purposes, it is interesting to automatically interact with systems, e.g. ETP, TCMS, etc. For instance, start of mission of the ETP can be performed automatically before a test run.
Category	Functional
Acceptance Method	Test
Acceptance Criteria	
Remark	Testing tools are external components that can be connected to TDS and could host some scripts. Scripts may be time or event based e.g., one shot timer. Such tool and scripts shall not be used on operation. Requirement deleted : A connected device to ETP could emulate TDS, a display and driver interaction. In case of shadow testing, ETP would not be connected to the official TDS. Thus, TDS should not support such functionalities.
Linked Work Items	has parent : OCORA-10289 - General requirements

OCORA-10475, D-Level - Common brightness and volume management

The TDS shall adapt automatically or manually the brightness and volume level of all or subset of the displays in the cab.

Status	Draft
Classification	Operator Choice
Rationale	• Ensure uniform behaviour of TDS units with few actions by the driver • Adapt brightness to light level in the cab. (e.g at night) • Adapt volume to the noise emission in the cab (e.g. related to speed)
Category	Functional
Acceptance Method	Test
Acceptance Criteria	Conformity to TSI LOC & PAS for noise emission (6dB over cab noise).
Remark	Need to calibrate volume and brightness on each system. Even if TDS could apply the same level of brightness and volume on each TDS units. The driver or TDS should have the possibility to modify these characteristics only to one TDS unit (sunlight only on one display, etc.).
Linked Work Items	has parent : OCORA-10289 - General requirements

To illustrate the concepts of configuration, modularity and multiple display, the following pictures show the displays of four systems on four displays: CVR, CCD, TDD and an unidentified system (XYZ). The first figure shows the nominal configuration.

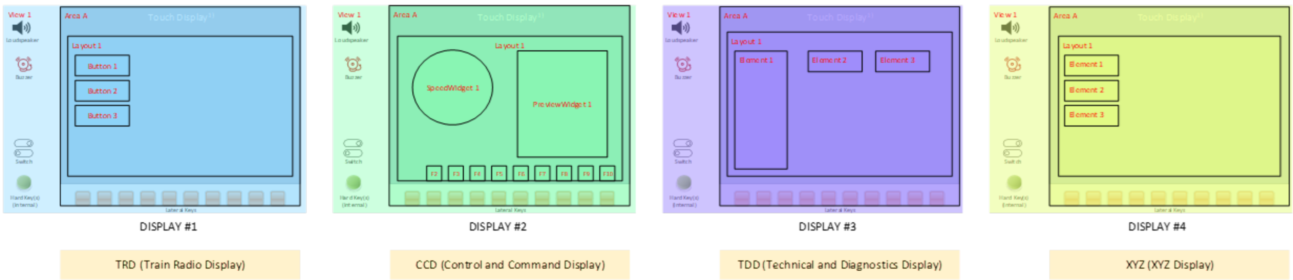


Figure 8 : Nominal configuration

If display 2 fails, a degraded configuration is automatically used. As the CCD display is mandatory for operation, this system is moved to display 3 in order to remain in a central position. As a result, the TDD display is moved to display 4. The XYZ display is now stacked in display 4 behind the TDD display.

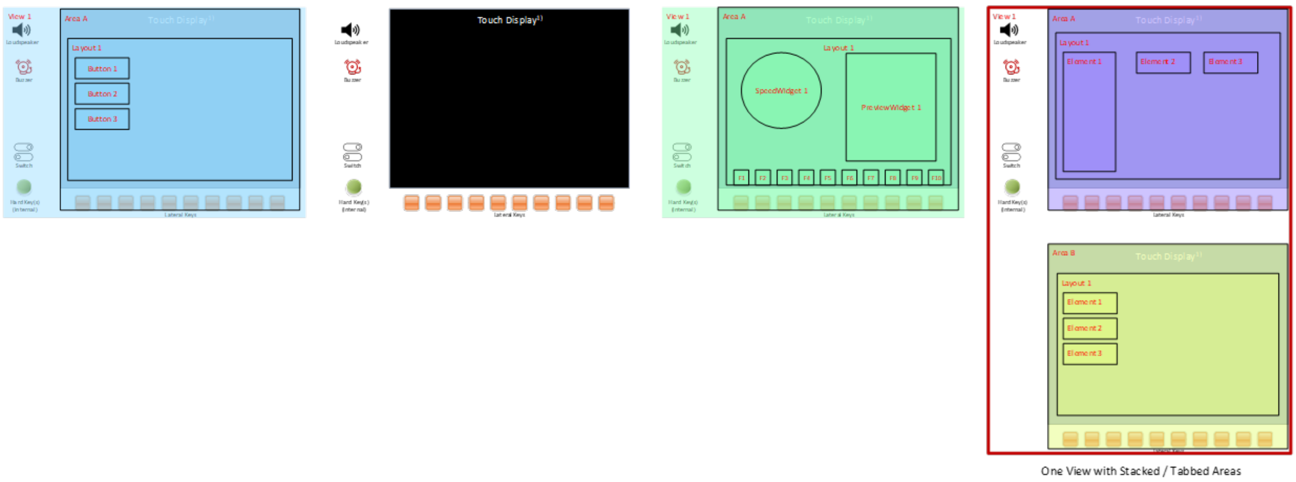


Figure 9 : Degraded configuration - display 2 failure

If display 4 fails, another degraded configuration is automatically used. The XYZ display is stacked in display 3 behind the TDD display without affecting the other displays.

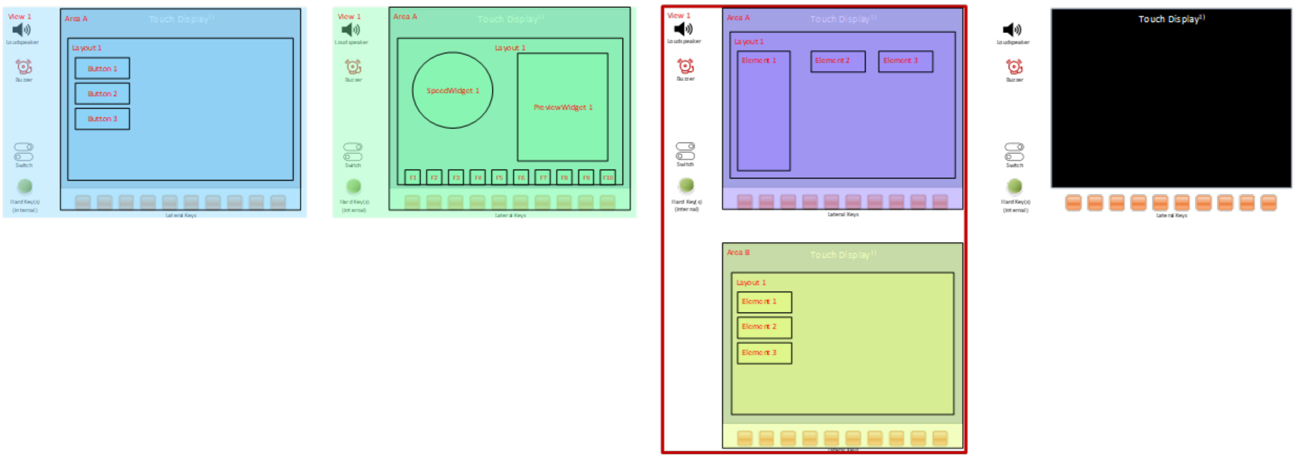


Figure 10 : Degraded configuration - display 4 failure

In the case of multiple display, the driver or hidden systems could request to have their areas displayed on the view. The figure below shows a view with TDD and XYZ display areas combined on display 3.

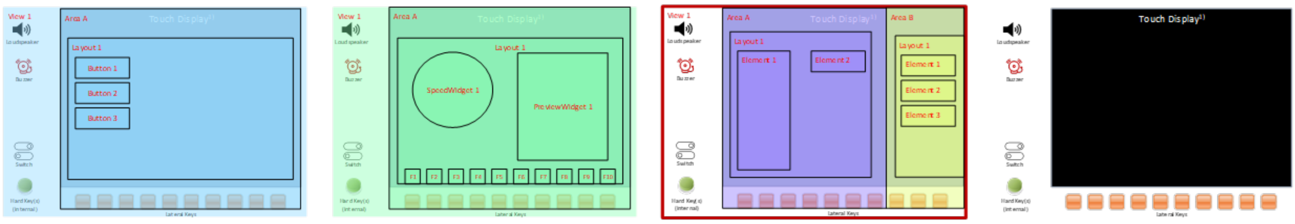


Figure 11 : Multiple display on display 3

4.2 External interfaces

4.2.1 Data exchange interfaces

OCORA-7675, D-Level - Compliance with a single data exchange standard (OSI layer 7)

The TDS shall exchange data on application level (OSI layer 7) with any other CCS-OB building block, and any CCS-OB external system, compliant with a single standard (to be defined).

Status	In Review
Classification	Requirement
Rationale	Rational for the interfaces: • To allow exchange of information between the TDS and any CCS-OB building block, and any CCS-OB external system. Rational for standardisation of the interfaces: • To support the possibility to manage the life-cycles and the sourcing of the TDS independently of the original supplier(s) of the TDS, of any other interfacing CCS-OB building block, and of any interfacing CCS-OB external system. • To allow the manufacturers of the TDS, of any other interfacing CCS-OB building block, and of any interfacing CCS-OB external system, developing their products according to a standard and therefore to reduce product variety and costs. • To facilitate the integration, installation, testing, and maintenance of a TDS. • To support the compatibility between different implementations of the TDS, of any other interfacing CCS-OB building block, and of any interfacing CCS-OB external system.
Category	Maintainability
Acceptance Method	Certification
Acceptance Criteria	
Remark	• Subset 121 introduced by TSI-CCS 2023 for the interface between ETP and DMI could be a promising solution. However, this subset should be consolidated for TDS needs. • Legacy application such as TCMS and CVR can continue using their proprietary solution. However, design products with direct compliance to this single standard or use an adaptor supporting it would ease the integration of TDS. • New applications such as DAS, MDCM shall integrate this protocol.
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-8002 - Data exchange interfaces defines : OCORA-10293 - System Presentation Logic defines : OCORA-10294 - Layout Engine defines : OCORA-10295 - Display Manager

4.2.2 Communication interfaces

OCORA-7981, D-Level - Compliance with SUBSET-147

The TDS shall communicate (OSI layer 1 - 6) with any other CCS-OB building block and with any CCS-OB external system, compliant with SUBSET-147.

Status	In Review
Classification	Requirement
Rationale	• To be compliant with the TSI-CCS Rational for the interfaces: • To allow exchange of information between the TDS and any CCS-OB building block, and any CCS-OB external system. Rational for standardisation of the interfaces: • To support the possibility to manage the life-cycles and the sourcing of the TDS independently of the original supplier(s) of the TDS, of any other interfacing CCS-OB building block, and of any interfacing CCS-OB external system. • To support the compatibility between different implementations of the TDS, of any other interfacing CCS-OB building block, and of any interfacing CCS-OB external system. • To allow the manufacturers of the TDS, of any other interfacing CCS-OB building block, and of any interfacing CCS-OB external system, developing their products according to a standard and therefore to reduce product variety and costs. • To facilitate the integration, installation, testing, and maintenance of a TDS.
Category	
Acceptance Method	Certification
Acceptance Criteria	
Remark	Currently, the subset 147 version 1 covers only OSI layer 1 and 2.
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-7998 - Communication interfaces defines : OCORA-10293 - System Presentation Logic defines : OCORA-10294 - Layout Engine defines : OCORA-10295 - Display Manager

OCORA-7982, D-Level - Compliance with the OCORA addendum to SUBSET-147

The TDS shall communicate (OSI layer 1 - 6) with any other CCS-OB building block, and with any CCS-OB external system, compliant with addendum to SUBSET-147.

Status	In Review
Classification	Requirement

Rationale	• To ensure unambiguous implementation of the communication. • To consider currently not specified functionalities. Rational for the interfaces: • To allow exchange of information between the TDS and any CCS-OB building block and any CCS-OB external system. Rational for standardisation of the interfaces: • To support the possibility to manage the life-cycles and the sourcing of the TDS independently of the original supplier(s) of the TDS, of any other interfacing CCS-OB building block, and of any interfacing CCS-OB external system. • To support the compatibility between different implementations of the TDS, of any other interfacing CCS-OB building block, and of any interfacing CCS-OB external system. • To allow the manufacturers of the TDS, of any other interfacing CCS-OB building block, and of any interfacing CCS-OB external system, developing their products according to a standard and therefore to reduce product variety and costs. • To facilitate the integration, installation, testing, and maintenance of a TDS.
Category	
Acceptance Method	Test
Acceptance Criteria	
Remark	• The addendum to subset-147 covers OSI layers 1-6. • The Contracting Entity must decide what requirements of the OCORA addendum shall be applicable to a specific tender. Current topics are: selection of the protocols, etc. • EU-Rail and OCORA system architecture and design activities shall ensure that the points addressed in this requirement are considered for standardisation. Eventually, this requirement can disappear.
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-7998 - Communication interfaces defines : OCORA-10293 - System Presentation Logic defines : OCORA-10294 - Layout Engine defines : OCORA-10295 - Display Manager

4.3 PRAMSS requirements

4.3.1 Performance requirements

OCORA-10020, D-Level - Compatible performance according existing systems

The TDS shall be compatible with the performance requirements of each system it is interfaced with e.g., ETP, TCMS, CVR, etc.

Status	In Review
Classification	Requirement
Rationale	Keep compliance with subset 041 (chapters 5.2.1.X), TSI LOC & PASS (noise emission, etc.).

Category	
Acceptance Method	Certification
Acceptance Criteria	
Remark	
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-8015 - Performance requirements defines : OCORA-10293 - System Presentation Logic defines : OCORA-10294 - Layout Engine defines : OCORA-10295 - Display Manager

4.3.2 Reliability requirements

OCORA-10297, D-Level - Preservation of system's reliability

When a configuration is set, the TDS shall not decrease the reliability of existing systems (ETP, TCSM, CVR, etc.).

Status	Draft
Classification	Requirement
Rationale	The use of a generic display solution should not lead to a different behaviour depending on the display solution used (latency, data exchanged, type of the key, etc.).
Category	
Acceptance Method	Certification
Acceptance Criteria	
Remark	
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-8016 - Reliability requirements defines : OCORA-10293 - System Presentation Logic is refined by : OCORA-10282 - System Presentation Logic and Layout Engine communication defines : OCORA-10294 - Layout Engine

OCORA-10460, D-Level - Reconfiguration only upon context change

The TDS shall only apply a reconfiguration if a change in the context (inputs) justifies it.

Status	Draft
Classification	
Rationale	Reconfiguration should not be a source of disruption or misleading behaviour for systems and drivers.
Category	
Acceptance Method	Certification
Acceptance Criteria	
Remark	

Linked Work Items	has parent : OCORA-8016 - Reliability requirements defines : OCORA-10295 - Display Manager

4.3.3 Availability requirements

OCORA-10022, D-Level - Active configuration monitoring

The TDS shall monitor the health of every system and HMI element involved in the active configuration, and apply a configuration accordingly.

Status	Draft
Classification	Requirement
Rationale	- To improve display availability for systems. - To choose the appropriate configuration.
Category	Availability
Acceptance Method	Test
Acceptance Criteria	
Remark	• For example, in the event of a display failure, TDS could change the configuration to provide a new display to the system using the failed display.
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-8017 - Availability requirements defines : OCORA-10293 - System Presentation Logic defines : OCORA-10294 - Layout Engine defines : OCORA-10295 - Display Manager is refined by : OCORA-10281 - System Presentation logic send health information to Display Manager

OCORA-10329, D-Level - Preservation of system's availability

The TDS shall not decrease the availability of existing systems (ETP, TCMS, CVR, etc.).

Status	In Review
Classification	Requirement
Rationale	• The introduction of TDS as a configuration component should not affect the availability of systems. • A failure in a TDS component should not lead to a failure of the displays.
Category	Availability
Acceptance Method	Certification
Acceptance Criteria	
Remark	
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-8017 - Availability requirements defines : OCORA-10293 - System Presentation Logic is refined by : OCORA-10283 - System Presentation Logic and active or redundant Layout Engine is refined by : OCORA-10282 - System Presentation Logic and Layout Engine communication defines : OCORA-10294 - Layout Engine defines : OCORA-10295 - Display Manager

4.3.4 Maintainability requirements

OCORA-10113, D-Level - Recording TDS data

The TDS shall send diagnostic and monitoring data to MDCM: root cause of reconfiguration (e.g. failure, driver selection, etc.), configuration applied, etc.

Status	Draft
Classification	Requirement
Rationale	Provide information to the maintainer.
Category	Maintainability
Acceptance Method	Test
Acceptance Criteria	
Remark	All the messages should have a timestamp. MDCM collects the data and adds all the context information relative to these messages.
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-8012 - Maintainability requirements defines : OCORA-10295 - Display Manager

Note: To date, the need for TDS to send to a system what is displayed, is under discussion (acknowledgement of a proper display or all information displayed). OCORA is only aware of a potential need for ETCS. So this functionality is specific to a system and not generic. If other systems have the same need, it could be considered to create a generic requirement in this paper.

4.3.5 Safety requirements

OCORA-10021, D-Level - Compatible safety requirements according to existing systems

The TDS shall be compatible with the safety requirements of each system it interfaces with (ETP, TCMS, CVR, etc.).

Status	In Review
Classification	Requirement
Rationale	Keep compliance with subset 091 (DMI-XXX reported on ETCS_OB10).
Category	Safety
Acceptance Method	Certification
Acceptance Criteria	
Remark	The maximum current SIL for train display depends on ETP's DMI. Nowadays, no system requires higher SIL Level.
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-8013 - Safety requirements

OCORA-10288, D-Level - Ensure configuration compatibility of SIL between systems and display panels

The TDS shall ensure a compatible configuration between the SIL requirements of the systems and the SIL functionality of display panels.

Status	In Review
Classification	Requirement
Rationale	Ensure safety level needs of systems. E.g.: Keep compliance with subset 091 for ETP (DMI-XXx reported on ETCS_OB10)
Category	
Acceptance Method	Certification
Acceptance Criteria	
Remark	Display panels could be only compatible SIL0, SIL2. Some systems requires SIL2 functionality for display solution, for other systems SIL0 display solution is enough. For all systems, safety analysis should be performed to determine the suitable safety level supported by the display solution (e.g fault tree with regard to DMI-XXx reported in subset 091).
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-8013 - Safety requirements defines : OCORA-10295 - Display Manager

4.3.6 Security requirements

OCORA-10298, D-Level - HMI elements allocation limited by configuration

The TDS shall allocate HMI elements only to systems that are registered in configuration.

Status	In Review
Classification	Requirement
Rationale	Prevent access to system by a HMI elements that are not allowed by configuration.
Category	Security
Acceptance Method	Certification
Acceptance Criteria	
Remark	
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-8014 - Security requirements defines : OCORA-10295 - Display Manager

OCORA-10299, D-Level - TDS and Configuration update

The TDS shall only allow updates (software and configuration) by a trusted person (e.g. maintainer).

Status	In Review
Classification	Requirement

Rationale	Prevent access to TDS by a third party.
Category	Security
Acceptance Method	Certification
Acceptance Criteria	
Remark	
Linked Work Items	defines : OCORA-7587 - Train Display System (TDS) has parent : OCORA-8014 - Security requirements defines : OCORA-10294 - Layout Engine defines : OCORA-10295 - Display Manager

5 Functional analysis

5.1 Logical component identification

With regard to TDS terminology, this section lists all the logical components that should be involved in the TDS context. These components are linked to dedicated functions, defined in chapter 5.2, which refine the TDS requirements.

More concretely, the TDS building block consists of the following main components:

The *Presentation Logic* is a logical component embedded within a system. It selects the view to be displayed (e.g. : data entry view / main view, etc.) and sends it to the Layout Engine with the dynamic data from the system. It also considers the driver interaction sent by the Layout Engine to update the view selection and data to be sent (to the System or Layout Engine).

The *Display Manager* interacts with system (CCS, TCMS, CVR) and manages the *Desk Display Area*.

The *Layout Engine* is a generic piece of software able to generate any *View* based on *Areas*, *Layouts* and *Layout Elements* as defined in a configuration.

5.2 Functional allocation

TDS requirements defined in chapter 4 are refined in this chapter as component requirements and allocated to the logical components described above.

Concerning systems (ETP, TCMS, CVR, etc.), requirements have been written assuming that core system functions are considered not in scope of TDS (e.g. braking curves for ETP, setting calls for CVR, command doors for TCMS, etc.).

The structure of this chapter will follow the structure of the subset 121. First, requirements will be given for the components Presentation Logic, Display Manager and Layout Engine. Then a dialogue sequence will depict the basic requirements. Afterwards, the data exchange on the CCN is defined. Finally, performance requirements will be written for each component.

To date, this chapter is considered as a draft. It will be consolidated in the next release especially with the results from the Proof of concept of OCORA.

The main functions considered are:

- Cab management
- Master Display Manager determination
- Health Monitoring
- Configuration selection and application
- Communication between Systems Presentation Logic and Layout Engine
- Building views
- Views swap

6 TDS architecture

The consolidation of logical and physical views has led to a review of the architectural definitions and proposals listed in the OCORA release R3 of the System Architecture document. Some concepts have been added in OCORA release R4 and R5 and are evaluated too.

First, rather than presenting numerous allocations that after evaluation would be abandoned in favour of a single variant, it has been decided to document and evaluate their key characteristics. This analysis permits to refine the number of variants to consider in the second analysis.

Secondly, the previous evaluation leads to the creation of six functional allocations that have been analysed in more detail and documented in OCORA Releases 5 and 6. The evaluation has been performed with a list of criteria that has been defined based on the OCORA's objectives, TDS stakeholder requirements and other criteria that are regarded as relevant in the TDS context. After listing all possible criteria, OCORA only considered the criteria that remained relevant for the functional allocation comparison. This evaluation leads to the final functional allocation that is taken under consideration by OCORA.

6.1 TDS integration

Regarding the integration of TDS within CCS-OB, three options have been identified. Without considering a computing platform as solution, the two first options are only software based. The third option is hardware and software based.

1. The first option is hosting TDS software on an existing HMI element such as a display.
2. The second option is hosting TDS software on an existing system (ETP, TCMS, etc.) - considered in the scope of the system or just hosted on the same HW.
3. Third considered option is a stand-alone building block using dedicated hardware and software.

Depending on the exact boundary of TDS and the allocation of logic elements to system, the final integration of TDS could be a mix of these three options.

Analysis :

Architectural views considered are presented in chapter 6.6.

- The first option, hosting TDS software on an existing HMI element, is depicted by functional allocation 5.
- The second option, hosting TDS software on an existing system, is depicted by functional allocation 6.
- The third option, stand-alone building block using dedicated hardware and software, is depicted by functional allocation 3.
- Others functional allocations (1, 2 and 4) are a mix of previous options.

6.2 HMI elements managed by TDS

With regards to HMI elements, such as the emergency brake button, two solutions can be considered. As these are considered to be used by the driver, these buttons should be directly interfaced with the TDS. This building block would manage this information and transmit it to the train. Otherwise, it is debatable whether such buttons are part of the Physical Train Unit Operation System (PTU-OS), as proposed in the technical slide deck OCORA-BWS02-030_Technical-Slide-Deck.

Analysis:

As external buttons, biometrics reader, levers, RFID reader and switches are dedicated to systems and therefore not reconfigurable, OCORA proposes to leave these devices directly linked to the dedicated system or to the Physical Train Unit Operation System. This is an operator choice.

Note : the external HMI elements required for TDS functionality could be linked to any display for TDS purpose if Display Manager is hosted by a display computing unit. If not the case, they could be managed by Physical Train Unit Operation System. This is also an operator choice.

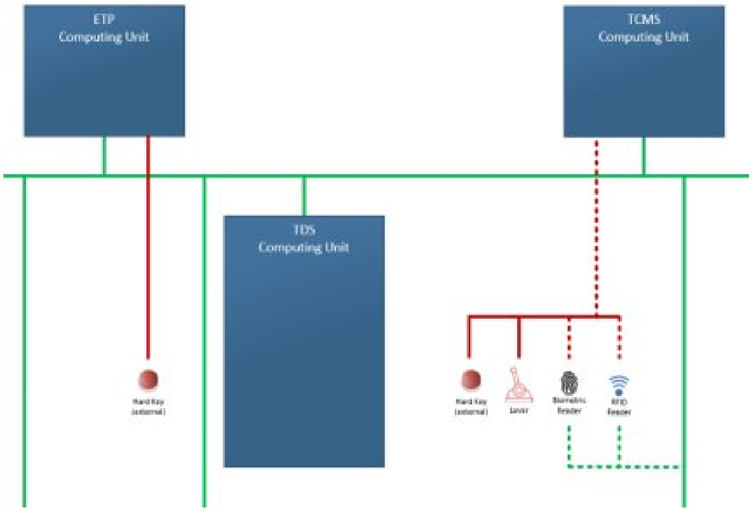


Figure 12 HMI elements in the scope of systems

The HMI elements that remain within the scope of the TDS are therefore: buzzer, internal hard-keys, lateral keys and loudspeaker.

These elements could be connected to a display computing unit or a display controller. Connecting these elements to the CCN does not provide any advantage and may even complicate the overall architecture. Only the displays would be connected via CCN to TDS or systems. More information is given in chapter "HMI elements connectivity".

With regards to loudspeakers OCORA considers that they support the ergonomic aspects of the HMI for a system but do not support intercom and voice communication functionalities. The possibility of sharing one loudspeaker for all system usage has been analysed. However, due to the noise level requirements (TSI LOC and PAS) and the risk of noise distortion, this idea is not acceptable. Like the loudspeaker, the shared buzzer is no longer considered.

As for the internal hard-keys, the change of configuration may result in the loss of these internal hard-keys. To avoid such a loss, OCORA recommends to avoid or limit the number of these HMI elements. If only limited, the functions associated with these internal hard-keys shall be a shortcut to a dedicated functionality which can also be accessible by other means (laterals keys or touch keys). So a reconfiguration will not result in a loss of this functionality.

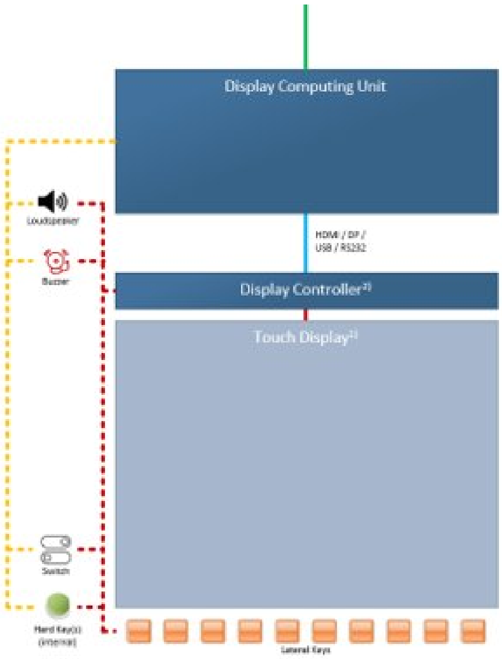


Figure 13 HMI elements in the scope of TDS

6.3 HMI elements management

HMI elements shall be managed by a controller unit and there are two possible implementations. The first option is to connect all the HMI elements to a central controller unit. The second option is a distributed management of HMI elements supported by multiple controllers.

Analysis :

OCORA considers too complex having a single control unit for all display panels. Moreover, this might lead to a vendor lock-in situation which is in contradiction with the Operational Epics. So, any display panels should be connected to a dedicated computing unit.

As a consequence, OCORA considers the necessity to have a distributed management of HMI elements.

6.4 HMI elements connectivity

Another issue is related to the HMI elements that interface with the TDS. Two options are considered.

The first option is to use direct proprietary interfaces or standard from different industries such as DIN connector or Jack plug for buzzers or loudspeakers. Considering that TDS is compatible with many connectors, this option allows the use of HMI elements as they are designed today, thus allowing more suppliers to be involved, and minimises latencies to TDS. However, this may involve a lot of physical connectors.

The second option is to use the CCS consist network. This option requires HMI elements to be adapted to fit with subsets 146 and 147, may increase latencies to TDS but will limit the number of connector for TDS. With this option, the data exchanged shall be standardised to ensure modularity.

Analysis:

With regards to §6.2, HMI elements remaining in the scope of TDS are loudspeakers, buzzers, switch, internal keys and displays (controller unit and display panels). A list of connectors types allowed for this HMI elements is given below.

HMI elements	Connector types	Comments
Buzzer	-	Buzzers are essentially electrical dipoles that can be connected or soldered directly to an electronic circuit board. As a consequence, they should be considered as an integral part of the display.
Display (controller unit)	CCN connector	CCN connector should be used to ensure direct connection to TDS or systems.
Display panels	Display Port, DVI, HDMI, RS-232, USB type C, VGA	Currently, video and audio standards exist in industries and ensure the absence of vendor lock-in situation. The creation of a dedicated CCN connector for display panels doesn't seem relevant. As Display Ports, HDMI and USB type C are newer and widely used, these ports must be adopted in preference to DVI, RS-232 or VGA.
Internal keys	-	Internal keys are essentially electrical dipoles that can be connected or soldered directly to an electronic circuit board. As a consequence, they should be considered as an integral part of the display.
Loudspeakers	Din connector, Jack plug, RF connectors, SUB D9. etc.	Standard connectors are already used in other industry should be supported. Indeed, the usage of CCN connector would not lead to a significant benefit.

6.5 Number of Display Manager

The first logical view presents Display Manager as a unique logical component. However, it is conceivable to design a solution based on multiple Display Managers. A master would be required to control Desk Display area and invoke slaves Display Manager. The communication between all these controllers should lead to a better availability. However, this would imply a higher complexity, too.

Analysis :

Architectural views considered are presented in chapter 6.6.

Functional allocations 1, 3, 4 and 6 represent a single component called the "Display manager", which integrates the Display Manager.

Functional allocations 2 and 5 represent multiple "Display managers", thus multiple Display Managers.

6.6 Physical and logical architectures

OCORA has evaluated six TDS architectures called "Functional Allocation". These functional allocations address the main characteristics presented above.

For larger scale representations of the figures below refer to the appendix in [OCORA-TWS01-035].

The evaluation of these functional allocations has been performed with the list of criteria and sub-criteria below:

- **Availability** (weight = 8),
  - Impact of a system failure
  - Impact of TDS computing unit failure (if it exists)
  - Impact of display computing unit failure
- **Integration effort for new system and update of existing systems** (weight = 5),
  - Integration of a new system or change in an existing system impacting their presentation logic
- **Avoid vendor lock-in situation** (weight = 1),
  - Dependency among logical elements/systems
- **Hardware costs** (weight = 3),
  - Need for a TDS computing unit hardware
  - Need for resources in display computing unit
  - Need for resources in systems for TDS functionalities
- **Implementation effort of TDS** (weight = 7),
  - Integration of TDS computing unit (space, cables, etc.)
  - Complexity for the development
  - Installation effort (time to install the same SW package)
  - Testing effort (independence of tests regarding installation)
- **Certification effort** (weight = 6),
  - Impact of a System change
  - Impact of a Presentation Logic change
  - Impact of a Display Manager change
  - Impact of a Layout Engine change
- **Maintenance costs** (weight = 3),
  - Installation of a Presentation Logic update
  - Installation of a Display Manager update
  - Installation of a Layout Engine update
  - Management of TDS computing unit spare parts
- **User experience** (weight = 4).
  - Latency between a driver interaction and the reaction of the system
  - Latency between a driver interaction and the application of a new configuration
  - Latency between an external event (system failure, standstill, etc.) and the application of a new configuration

First, a comparison and ranking between the functional allocations has been performed by giving the highest score (6) to the best functional allocation, and the lowest score (1) to the worst for each of these sub-criteria. In the case of equal scores, the functional allocations have the same score.

Then, by adding the score of each sub-criteria, a score is given for the criteria, which have been weighted with a priority given by OCORA. This priority is given in relation to the need for TDS. As 8 criteria have been considered, the most important criteria is given a weight of 8 and the least important criteria is given a weight of 1. In case of equality, the

same weight is given. However, the next score is relatively lower. This weight is given in brackets after the list of criteria above. By multiplying the weight of the criteria and the previously obtained score, the score of the functional allocation for this criteria was calculated.
Finally, the final functional grouping score is obtained by adding all the scores for each criterion. The highest score of each functional allocation should be considered as the most promising architecture from an OCORA perspective.

For the ease of reading, only the final scores of all criteria are given for each functional allocation. A detailed analysis is available upon request.

Functional allocation 1: This allocation leaves the Presentation Logic in the scope of the single systems. A central Display Manager manages the displays and the views.

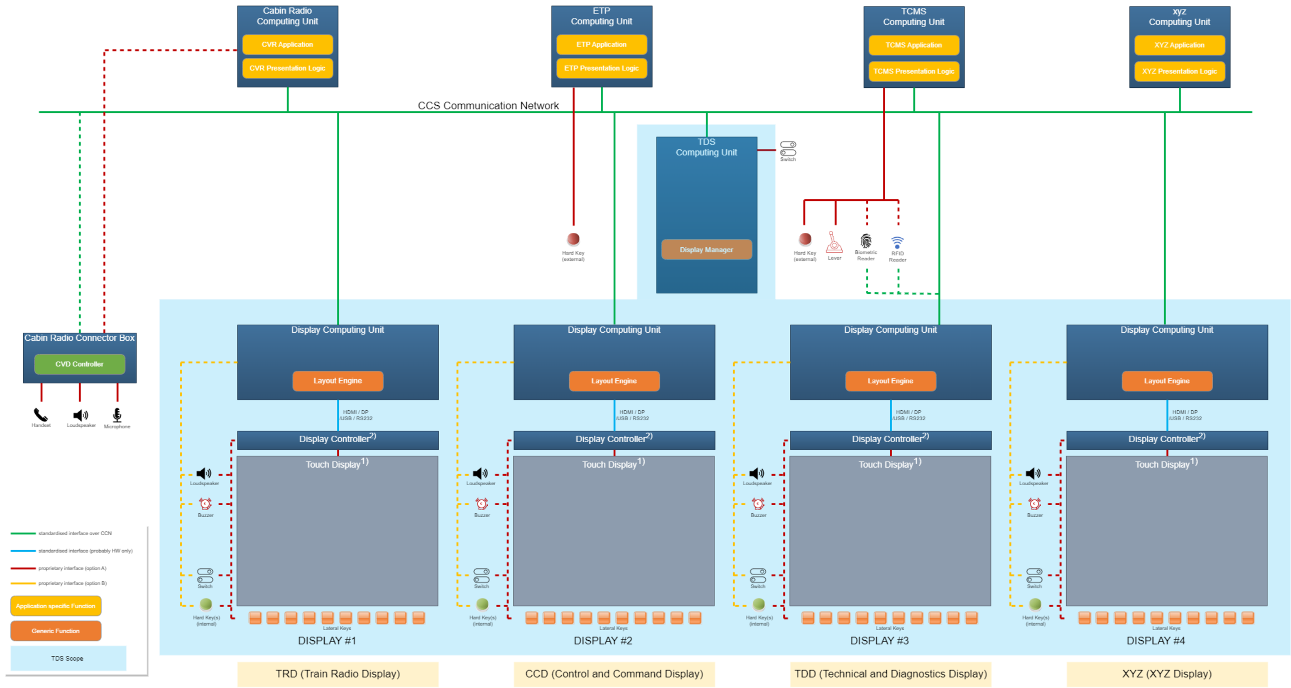


Figure 14: Functional allocation 1

Criteria / sub-criteria	Analysis	Score
Availability (weight = 8)		**120**
Impact of a system failure.	The failure of a system computing unit doesn't lead to a loss of TDS functionality.	6
Impact of TDS computing unit failure (if it exists).	In case of a Display failure, switching configurations is not available - could be mitigated with redundant TDS computing units.	3
Impact of display computing unit failure.	The failure of a Display computing unit doesn't lead to a loss of TDS functionality.	6
Integration effort for new system and update of existing systems (weight = 5)		**30**
Integration of a new system or change in an existing system impacting their presentation logic.	An evolution on system does not affect the Display Manager and Layout Engine.	6
Avoid vendor lock-in situation (weight = 1)		**6**
Dependency among logical elements/systems	No dependencies is created between systems.	6

Criteria / sub-criteria	Analysis	Score
Hardware costs (weight = 3)		**36**
Need for a TDS computing unit hardware.	A TDS computing unit is required.	3
Need for resources in display computing unit.	Display computing units only host Layout Engine. So the resources required for display computing unit are low.	6
Need for resources in systems for TDS functionalities.	System units embed core functionalities and Presentation logic. The resources needed for TDS functionalities are medium.	3
Implementation effort of TDS (weight = 7)		**147**
Integration of TDS computing unit (space, cables, etc.).	Introduction of a TDS computing unit.	3
Complexity for the development.	Development do not need to take under consideration the integration of elements from different vendors on computing unit(s).	6
Installation effort (time to install the same SW package).	Display Manager and presentation logic are installed once.	6
Testing effort (independence of tests regarding installation).	System test could be performed as soon as Display Manager and one display is available.	6
Certification effort (weight = 6)		**126**
Impact of a System change.	A system change may impact only the presentation logic linked to the system.	3
Impact of a Presentation Logic change.	A presentation logic change (modification of existing system or integration of a new system) does not affect computing units where Display Manager and Layout engine are embedded.	6
Impact of a Display Manager change.	A display manager change only impacts this software.	6
Impact of a Layout Engine change.	A layout Engine change only impacts this software.	6
Maintenance costs (weight = 3)		**45**
Installation of a Presentation Logic update.	Limited to the system itself.	6
Installation of a Display Manager update.	Limited to TDS computing unit only.	6
Installation of a Layout Engine update.	No differences between Functional Allocations	-
Management of TDS computing unit spare parts.	Stock for TDS computing units required	3
User experience (weight = 4)		**32**
Latency between a driver interaction and the reaction of the system.	Layout engine and presentation logic should transmit data through CCN.	4
Latency between a driver interaction and the application of a new configuration.	Layout engine and Display Manager should transmit data through CCN and Display Manager should send the new configuration to Layout Engine and Presentation logic/systems through CCN.	4
Latency between an external events (system failure, standstill, etc.) and the application of a new configuration.	Latency is dependent to the number and the repartition of logical elements.	5

Criteria / sub-criteria	Analysis	Score
Final Score		**542**

Functional allocation 2: This allocation leaves Presentation Logic in the scope of the single systems. Multiple "Display Managers" manage a single display and a single view.

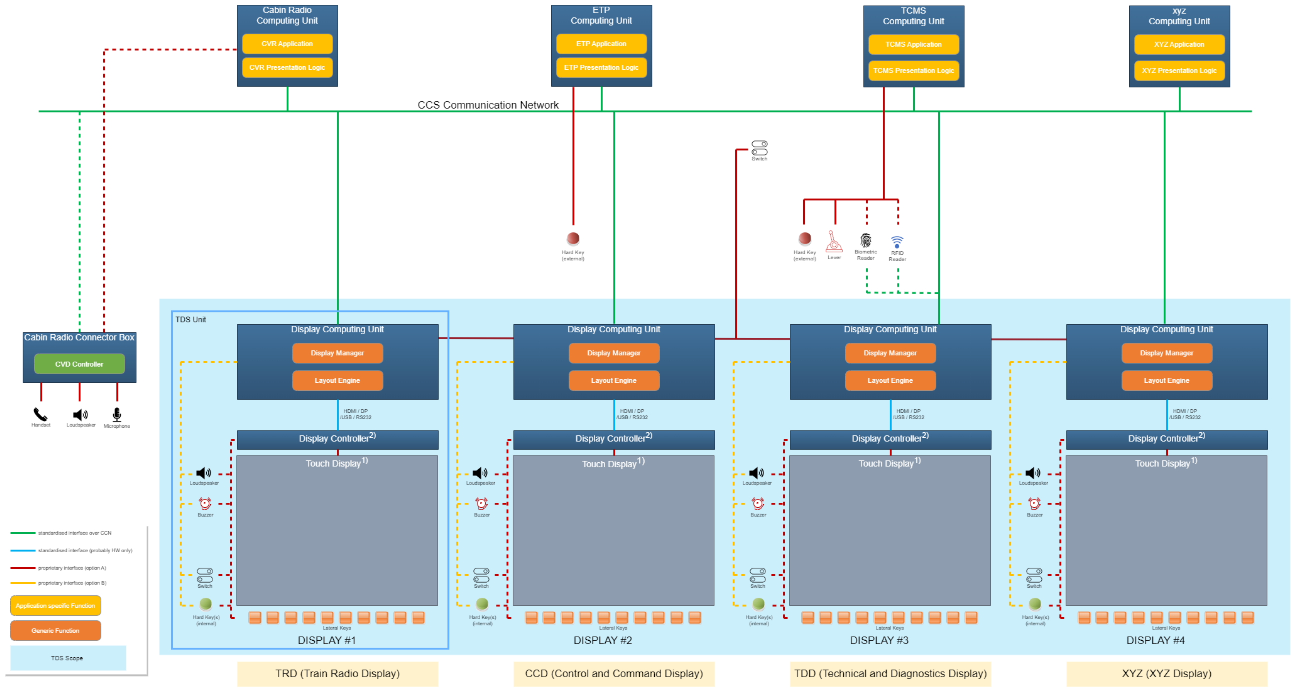


Figure 15: Functional allocation 2

Criteria / sub-criteria	Analysis	Score
Availability (weight = 8)		**144**
Impact of a system failure.	The failure of a system computing unit doesn't lead to a loss of TDS functionality.	6
Impact of TDS computing unit failure (if it exists).	No TDS computing unit in this functional allocation.	6
Impact of display computing unit failure.	The failure of a Display computing unit doesn't lead to a loss of TDS functionality.	6
Integration effort for new system and update of existing systems (weight = 5)		**30**
Integration of a new system or change in an existing system impacting their presentation logic.	An evolution on system does not affect the Display Manager and Layout Engine.	6
Avoid vendor lock-in situation (weight = 1)		**6**
Dependency among logical elements/systems.	No dependencies is created between systems.	6

Criteria / sub-criteria	Analysis	Score
Hardware costs (weight = 3)		**36**
Need for a TDS computing unit hardware.	No need of TDS computing unit.	6
Need for resources in display computing unit.	Display computing units host Layout Engines and Display Managers. So the resources required for display computing unit are medium.	3
Need for resources in systems for TDS functionalities.	System units embed core functionalities and Presentation logic. The resources needed for TDS functionalities are medium.	3
Implementation effort of TDS (weight = 7)		**168**
Integration of TDS computing unit (space, cables, etc.).	No need for TDS computing unit.	6
Complexity for the development.	Development does not need to take under consideration the integration of elements from different vendors on computing unit(s).	6
Installation effort (time to install the same SW package).	Presentation logic are installed once. Display Manager are installed multiple times (once by display computing unit). However, this installation may not represent a higher workload for installation team if Display Manager is provided by the same company as the layout engine or/and these two logical elements are merged in a single software.	6
Testing effort (independence of tests regarding installation).	System test could be performed as soon as Display Manager and one display is available.	6
Certification effort (weight = 6)		**102**
Impact of a system change.	A system change may impact only the presentation logic linked to the system.	3
Impact of a Presentation Logic change.	A presentation logic change (modification of existing system or integration of a new system) does not affect computing units where Display Manager and Layout engine are embedded.	6
Impact of a Display Manager change.	A display manager change can affect display computing units where Display Manager and Layout Engine are embedded. However, it is assumed that Display Manager and Layout Engine are provided by the same supplier. This can affect different types of displays.	4
Impact of a Layout Engine change.	A Layout Engine change can affect display computing units where Display Manager and Layout engine are embedded. However, it is assumed that Display Manager and Layout Engine are provided by the same supplier. This can affect different types of displays.	4
Maintenance costs (weight = 3)		**42**
Installation of a Presentation Logic update.	Limited to the system itself.	6
Installation of a Display Manager update.	To be applied on each display computing units.	2
Installation of a Layout Engine update.	No differences between Functional Allocations.	-

Criteria / sub-criteria	Analysis	Score
Management of TDS computing unit spare parts.	No spare parts dedicated to TDS.	6
User experience (weight = 4)		**36**
Latency between a driver interaction and the reaction of the system.	Layout engine and presentation logic should transmit data through CCN.	4
Latency between a driver interaction and the application of a new configuration.	Layout engine and Display Manager should transmit data through CCN and Display Manager should send the new configuration to Layout Engine and Presentation logic/systems through CCN. If a new configuration is required on the master Display Manager, data for/from Layout Engine could be provided directly in the display computing unit. Nevertheless, the information should be transmitted to the Presentation Logic.	5
Latency between an external event (system failure, standstill, etc.) and the application of a new configuration.	Latency is dependent to the number and the repartition of logical elements.	5
Final Score		**564**

Functional allocation 3: This allocation concentrates all Presentation Logics and a single "Display Manager" in a TDS computing unit. Display Manager manages displays and views.

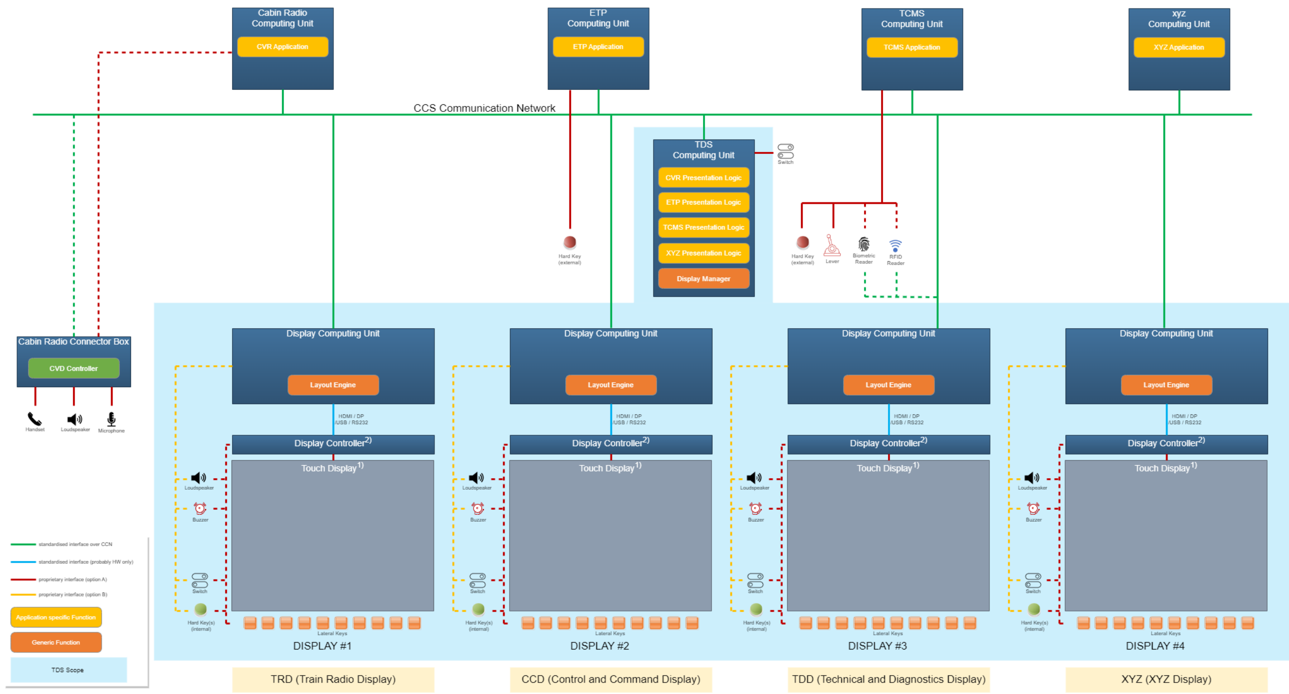


Figure 16 : Functional allocation 3

Criteria / sub-criteria	Analysis	Score
Availability (weight = 8)		**104**
Impact of a system failure.	The failure of a system computing unit doesn't lead to a loss of TDS functionality.	6

Criteria / sub-criteria	Analysis	Score
Impact of TDS computing unit failure (if it exists).	In case of a display failure, all displays are lost as presentation logic are embedded in TDS computing unit.	1
Impact of display computing unit failure.	The failure of a Display computing unit doesn't lead to a loss of TDS functionality.	6
Integration effort for new system and update of existing systems (weight = 5)		**15**
Integration of a new system or change in an existing system impacting their presentation logic.	An evolution on any system requires an update of the computing unit where the Display Manager is running.	3
Avoid vendor lock-in situation (weight = 1)		**6**
Dependency among logical elements/systems.	No dependencies is created between systems.	6
Hardware costs (weight = 3)		**39**
Need for a TDS computing unit hardware.	A TDS computing unit is required High resources are required due to the integration of all presentation logic.	1
Need for resources in display computing unit.	Display computing units only host Layout Engine. So the resources required for display computing unit is low.	6
Need for resources in systems for TDS functionalities.	System units embed core functionalities. The resources needed for TDS functionalities are low.	6
Implementation effort of TDS (weight = 7)		**105**
Integration of TDS computing unit (space, cables, etc.).	Introduction of a TDS computing unit.	3
Complexity for the development.	Development needs to consider the integration of elements from different vendors on computing unit(s).	3
Installation effort (time to install the same SW package).	Display Manager and Presentation Logic are installed once.	6
Testing effort (independence of tests regarding installation).	System test could be finished only when all Presentation Logic are installed.	3
Certification effort (weight = 6)		**102**
Impact of a system change.	A system change doesn't impact Presentation Logic, Display Manager and Layout Engine.	6
Impact of a Presentation Logic change.	A Presentation Logic change (modification of existing system or integration of a new system) can affect TDS computing unit where Display Manager and other Presentation Logic are embedded.	3
Impact of a Display Manager change.	A Display Manager change can affect TDS computing unit where Display Manager and other Presentation Logic are embedded.	2
Impact of a Layout Engine change.	A Layout Engine change only impacts this software.	6
Maintenance costs (weight = 3)		**39**
Installation of a Presentation Logic update.	Impact TDS computing unit and may be the system itself.	4

Criteria / sub-criteria	Analysis	Score
Installation of a Display Manager update.	Limited to TDS computing unit only.	6
Installation of a Layout Engine update.	No differences between Functional Allocations.	-
Management of TDS computing unit spare parts.	Stock for TDS computing units required.	3
User experience (weight = 4)		**32**
Latency between a driver interaction and the reaction of the system.	Layout engine and presentation logic should transmit data through CCN.	4
Latency between a driver interaction and the application of a new configuration.	Layout engine and Display Manager should transmit data through CCN and Display Manager should send the new configuration to Layout Engine and Presentation Logic/systems through CCN.	4
Latency between an external events (system failure, standstill, etc.) and the application of a new configuration.	As Presentation Logics are hosted with a central Display Manager latency is decreased in comparison to other configurations where all logical elements are spread among the computing units.	5
Final Score		**442**

Functional allocation 4: This allocation concentrates all Presentation Logics in displays. A single "Display Manager" is hosted in a TDS computing unit, it manages displays and views.

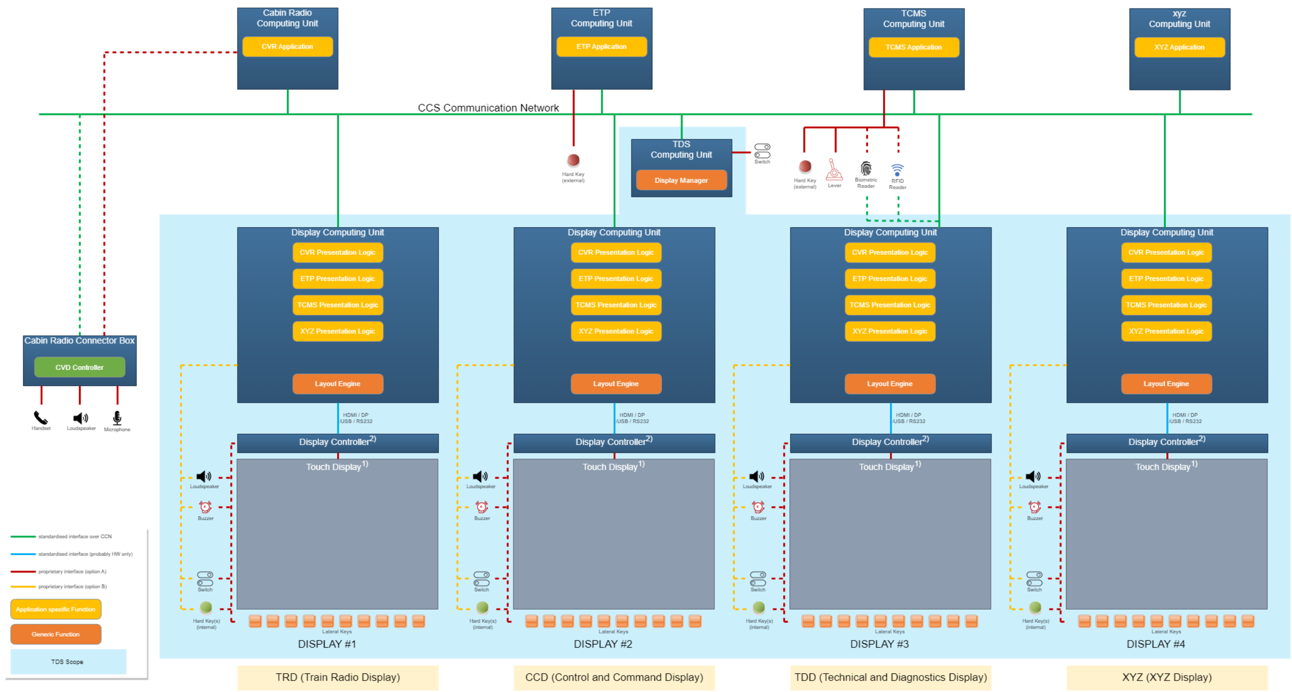


Figure 17 : Functional allocation 4

Criteria / sub-criteria	Analysis	Score
Availability (weight = 8)		**120**
Impact of a system failure.	The failure of a system computing unit doesn't lead to a loss of TDS functionality.	6

Criteria / sub-criteria	Analysis	Score
Impact of TDS computing unit failure (if it exists).	In case of a Display failure, switching configurations is not available - could be mitigated with redundant computing units.	3
Impact of display computing unit failure.	The failure of a Display computing unit doesn't lead to a loss of TDS functionality.	6
Integration effort for new system and update of existing systems (weight = 5)		**10**
Integration of a new system or change in an existing system impacting their presentation logic.	An evolution on any system requires an update of all Display computing units.	2
Avoid vendor lockin situation (weight = 1)		**6**
Dependency among logical elements/systems.	No dependencies is created between systems.	6
Hardware costs (weight = 3)		**33**
Need for a TDS computing unit hardware.	A TDS computing unit is required.	3
Need for resources in display computing unit.	Display computing units host Layout Engines and all presentation logic. So the resources required for display computing unit is high.	2
Need for resources in systems for TDS functionalities.	System units embed core functionalities. The resources needed for TDS functionalities are low.	6
Implementation effort of TDS (weight = 7)		**77**
Integration of TDS computing unit (space, cables, etc.).	Introduction of a TDS computing unit.	3
Complexity for the development.	Development needs to consider the integration of elements from different vendors on computing unit(s).	3
Installation effort (time to install the same SW package).	Display Manager is installed once. Presentation Logics are installed multiple times (once by display computing unit). It is assumed that Presentation Logics and Layout Engine are provided by different suppliers. So, it may not be possible to merge these elements in a single software. Therefore, installation team would have to install these elements one by one and multiple times.	2
Testing effort (independence of tests regarding installation).	System test could be finished only when all Presentation Logic are installed.	3
Certification effort (weight = 6)		**96**
Impact of a System change.	A system change doesn't impact Presentation Logic, Display Manager and Layout Engine.	6

Criteria / sub-criteria	Analysis	Score
Impact of a Presentation Logic change.	A Presentation Logic change (modification of existing system or integration of a new system) can affect display computing units where Layout Engine and others Presentation Logic are embedded. This can affect different displays.	2
Impact of a Display Manager change.	A Display Manager change only impacts this software.	6
Impact of a Layout Engine change.	A Layout Engine change (modification of existing system or integration of a new system) can affect display computing units where Layout Engine and others Presentation Logic are embedded. This can affect different types of display.	2
Maintenance costs (weight = 3)		**36**
Installation of a Presentation Logic update.	Impact all display computing units and may be the system itself.	3
Installation of a Display Manager update.	Limited to TDS computing unit only.	6
Installation of a Layout Engine update.	No differences between Functional Allocations.	-
Management of TDS computing unit spare parts.	Stock for TDS computing units required.	3
User experience (weight = 4)		**40**
Latency between a driver interaction and the reaction of the system.	Layout Engine and Presentation Logic could communicate directly on display computing unit.	6
Latency between a driver interaction and the application of a new configuration.	Layout Engine and Display Manager should transmit data through CCN and Display Manager should send the new configuration to Layout Engine and Presentation Logic/systems through CCN.	4
Latency between an external events (system failure, standstill, etc.) and the application of a new configuration	Latency is dependent on the number and the repartition of logical elements.	5
Final Score		**418**

Functional allocation 5: This allocation concentrates all Presentation Logics and "Display Manager" on all display computing units. Display Manager manages a single display and a view.

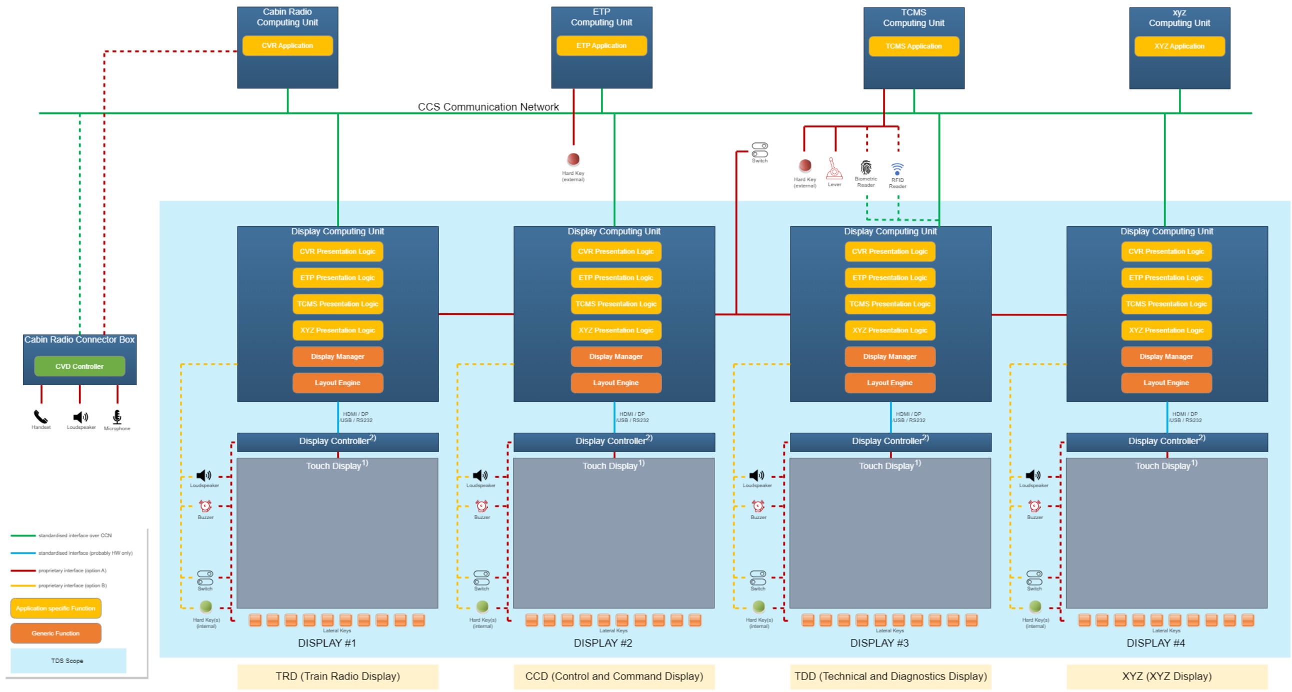


Figure 18 : Functional allocation 5

Criteria / sub-criteria	Analysis	Score
Availability (weight = 8)		**144**
Impact of a system failure.	The failure of a system computing unit doesn't lead to a loss of TDS functionality.	6
Impact of TDS computing unit failure (if it exists).	No TDS computing unit in this functional allocation.	6
Impact of display computing unit failure.	The failure of a Display computing unit doesn't lead to a loss of TDS functionality.	6
Integration effort for new system and update of existing systems (weight = 5)		**10**
Integration of a new system or change in an existing system impacting their Presentation Logic.	An evolution on any system requires an update of all display computing units.	2
Avoid vendor lock-in situation (weight = 1)		**6**
Dependency among logical elements/systems.	No dependencies arecreated between systems.	6
Hardware costs (weight = 3)		**39**
Need for a TDS computing unit hardware.	No need of TDS computing unit.	6
Need for resources in display computing unit.	Display computing units host Layout Engine, Display Manager and all Presentation Logic. So the resources required for display computing unit is very high.	1

Criteria / sub-criteria	Analysis	Score
Need for resources in systems for TDS functionalities.	System units embed core functionalities. The resources needed for TDS functionalities are low.	6
Implementation effort of TDS (weight = 7)		**98**
Integration of TDS computing unit (space, cables, etc.).	No need for TDS computing unit.	6
Complexity for the development.	Development needs to consider the integration of elements from different vendors on computing unit(s).	3
Installation effort (time to install the same SW package).	Display Manager are installed multiple times (once by Display computing unit). However this installation may not represent a higher workload for installation team if Display Manager is provided by the same company as the Layout Engine or/and these two logical elements are merged in a single software. Presentation Logics are installed multiple times (once by Display computing unit). It is assumed that Presentation Logics and Layout Engine are provided by different suppliers. So, it may not be possible to merge these elements in a single software. Therefore, installation team would have to install these elements one by one and multiple times.	2
Testing effort (independence of tests regarding installation).	System test could be finished only when all Presentation Logic are installed.	3
Certification effort (weight = 6)		**60**
Impact of a System change.	A system change doesn't impact Presentation Logic, Display Manager and Layout Engine.	6
Impact of a Presentation Logic change.	A Presentation Logic change (modification of existing system or integration of a new system) can affect Display computing units where Display Manager, Layout Engine and others Presentation Logic are embedded. This can affect different displays.	2
Impact of a Display Manager change.	A Display Manager change (modification of existing system or integration of a new system) can affect Display computing units where Display Manager, Layout Engine and others Presentation Logic are embedded. This can affect different types of displays.	1
Impact of a Layout Engine change.	A Layout Engine change (modification of existing system or integration of a new system) can affect Display computing units where Display Manager, Layout Engine and others Presentation Logic are embedded. This can affect different types of displays.	1
Maintenance costs (weight = 3)		**33**
Installation of a Presentation Logic update.	Impact all Display computing units and maybe the system itself.	3
Installation of a Display Manager update.	To be applied on each Display computing unit.	2
Installation of a Layout Engine update.	No differences between Functional Allocations.	-
Management of TDS computing unit spare parts.	No spare parts dedicated to TDS.	6

Criteria / sub-criteria	Analysis	Score
User experience (weight = 4)		**48**
Latency between a driver interaction and the reaction of the system.	Layout Engine and Presentation Logic could communicate directly on display computing unit.	6
Latency between a driver interaction and the application of a new configuration.	Layout Engine and Display Manager should transmit data through CCN and Display Manager should send the new configuration to Layout Engine and Presentation Logic/systems through CCN. If new configuration is required on the master Display Manager, data for/from Layout Engine and Presentation Logic could be provided directly in the display computing unit.	6
Latency between an external events (system failure, standstill, etc.) and the application of a new configuration.	New configuration could be applied quicker if it only impacts the display computing unit where the master Display Manager is hosted. Indeed, all logical elements (Display Manager, Layout Engine and Presentation Logics) are hosted in Display computing unit. Otherwise, as all elements are hosted in every display computing unit, a new configuration is applied with low latency.	6
Final Score		**438**

Functional allocation 6: This allocation leaves Presentation Logic in the scope of systems. A central "Display Manager" is hosted in an existing system and manages displays and views.

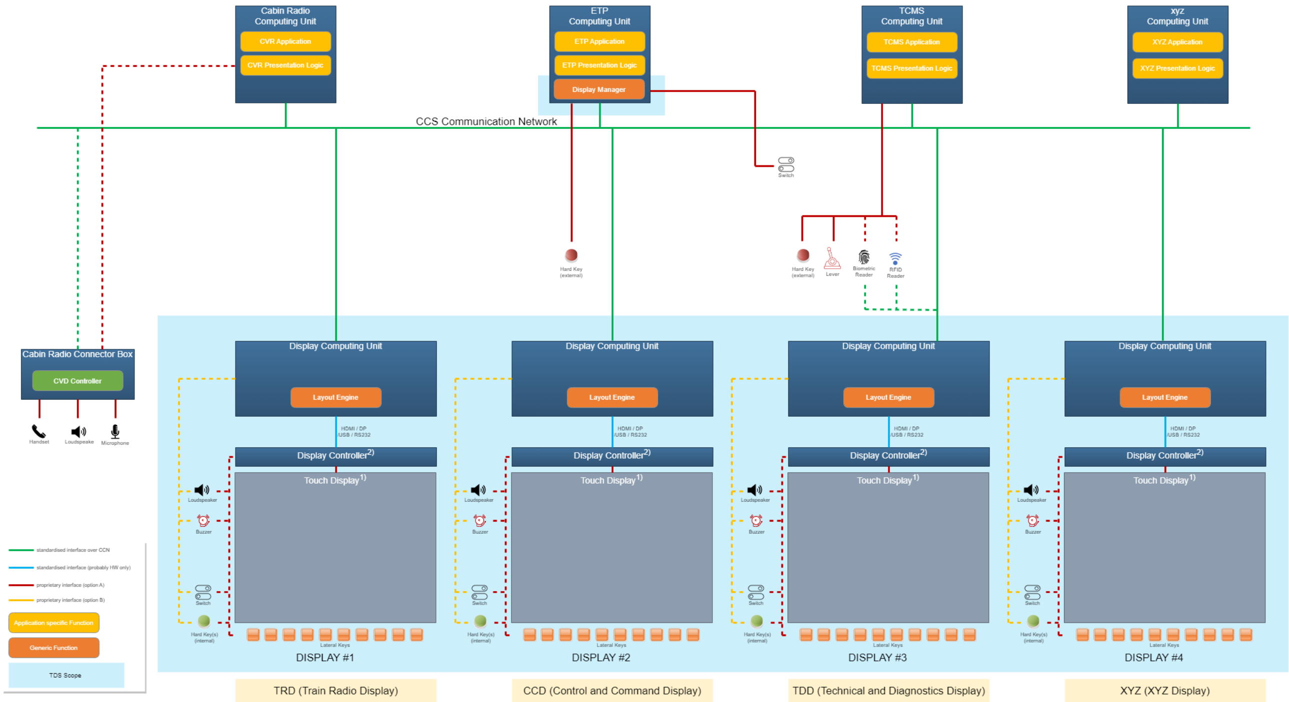


Figure 19 : Functional allocation 6

Criteria / sub-criteria	Analysis	Score
Availability (weight = 8)		**104**
Impact of a system failure.	The failure of a system computing unit which hosts Display Manager could lead to a loss of TDS functionality.	1

Criteria / sub-criteria	Analysis	Score
Impact of TDS computing unit failure (if it exists).	No TDS computing unit in this functional allocation.	6
Impact of display computing unit failure.	The failure of a Display computing unit doesn't lead to a loss of TDS functionality.	6
Integration effort for new system and update of existing systems (weight = 5)		**30**
Integration of a new system or change in an existing system impacting their Presentation Logic.	An evolution of the system does not affect the Display Manager and Layout Engine.	6
Avoid vendor lock-in situation (weight = 1)		**1**
Dependency among logical elements/systems.	As Display Manager is hosted in a system computing unit, the capacity to change Display Manager is linked to the capacity of the system itself. A strong dependency is created which can lead to a vendor lock-in situation.	1
Hardware costs (weight = 3)		**39**
Need for a TDS computing unit hardware.	No need of TDS computing unit.	6
Need for resources in display computing unit.	Display computing units only host Layout Engine. So the ressources required for display computing unit is low.	6
Need for resources in systems for TDS functionalities.	A system unit should embed core functionalities, Presentation Logic and Display Manager. The resources needed for TDS functionalities are high.	1
Implementation effort of TDS (weight = 7)		**140**
Integration of TDS computing unit (space, cables, etc.).	No need for TDS computing unit.	6
Complexity for the development.	Development needs to consider the integration of elements where Display Manager is hosted.	4
Installation effort (time to install the same SW package).	Display Manager and Presentation Logic are installed once.	6
Testing effort (independance of tests regarding installation).	System test start only when the system which hosts Display Manager is installed.	4
Certification effort (weight = 6)		**84**
Impact of a System change.	A system change may impact only the Presentation Logic linked to the system. Moreover, a system change where Display Manager is hosted may also impact the Display Manager. A system change where Display Manager is hosted.	1
Impact of a Presentation Logic change.	Only a change in the Presentation Logic where Display Manager is hosted (modification of existing system or integration of a new system) can affect Display Manager.	4
Impact of a Display Manager change.	A Display Manager change can affect the system and the presentation embedded in the same building block.	3

Criteria / sub-criteria	Analysis	Score
Impact of a Layout Engine change.	A Layout Engine change only impacts this software.	6
Maintenance costs (weight = 3)		**54**
Installation of a Presentation Logic update.	Limited to the system itself.	6
Installation of a Display Manager update.	Limited to the system which hosts the Display Manager.	6
Installation of a Layout Engine update.	No differences between Functional Allocations.	-
Management of TDS computing unit spare parts.	No spare parts dedicated to TDS.	6
User experience (weight = 4)		**36**
Latency between a driver interaction and the reaction of the system.	Layout Engine and Presentation Logic should transmit data through CCN.	4
Latency between a driver interaction and the application of a new configuration.	Layout Engine and Display Manager should transmit data through CCN and Display Manager should send the new configuration to Layout Engine and Presentation Logic/systems through CCN. If the new configuration impacts only the system which hosts the Display Manager, communication between Display Manager and system is shortened but information should still be sent to all the Layout Engines.	5
Latency between an exernal events (system failure, standstill, etc.) and the application of a new configuration	Latency is dependent to the number and the repartition of logical elements.	5
Final Score		**488**

With a final score of 564, "Functional Allocation 2" is the most promising architecture, particularly in terms of availability, integration effort and certification effort. Consequently, the functional requirements is based on this allocation.

The definition of TDS needs to be reconsidered with regard to the hardware and software allocation of this selection. In fact, TDS consists of one to n TDS units. And a TDS unit consists of hardware elements associated with a display panel and software elements (Display Manager and Layout Engine). These units communicate through CCN to systems (ETCS, TCMS, etc.) and between each other.

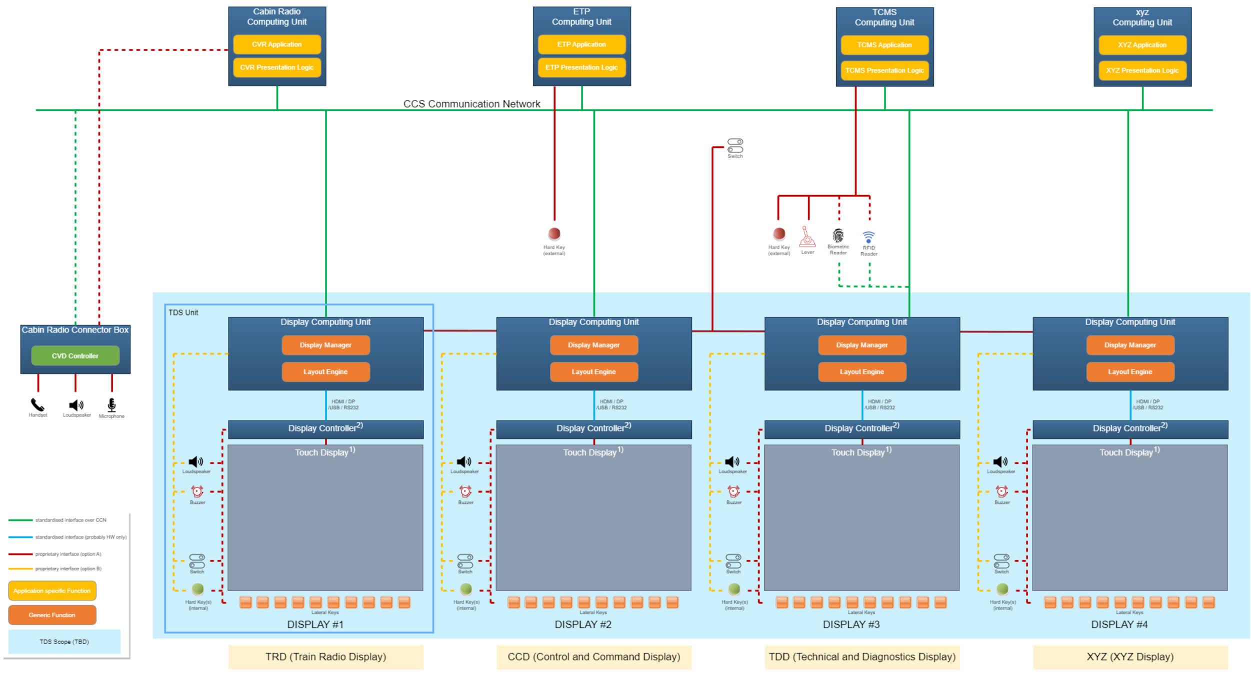


Figure 20 TDS consisting of several TDS units

This paradigm raises several questions for OCORA. Is TDS a complete solution provided by a single supplier? Could this situation lead to a vendor lock-in situation? If so, how is it possible to mix TDS units from different suppliers? To do so, an interface standardisation between the Display Manager is required. In order to give answers from the railway undertaking perspective, a short Pros/Cons analysis is provided below.

Complete TDS solution (TDS units provided by a single supplier)

Pros	Cons
One certification, one integration, one testing effort.	Spare part management, TDS units from only one single supplier could be used.
Standardisation limited, only data exchanged between systems and TDS are relevant.	Obsolescence management. If the supplier is changed, all TDS units have to be replaced.
Display manager update, one software version for all TDS units.	Lack of scalability of supplier solution.
	Competition among TDS units suppliers is not possible.

TDS units solution (TDS units may be provided by numerous suppliers)

Pros	Cons
Spare part management, TDS units from differents suppliers could be used.	Mutltiple certification, integration and increase of testing effort.
Obsolescence management, if the supplier is changed, no TDS units have to be replaced.	Display manager update, an upgrade of version impacts all TDS units suppliers.

Pros	Cons
Competition among TDS units suppliers is possible.	More standardisation required, inteface between display/manager have also to be defined. This is limited to configuration management, master/slave mechanism and health monitoring between Display Manager. This effort is limited.
	Mechanical standardisation or constraints required, in case of replacing a TDS unit by another reference.

Although, the CAPEX and OPEX could be affected by the importance of certification/integration/testing effort and also the management of the Display Manager update, OCORA considers the standardisation as a low effort in the context of TDS. Under this assumption, the TDS units solution has a better pros/cons ratio than the complete TDS solution. Therefore, the TDS units solution seems to be the most promising solution. Furthermore, the TDS units solution covers the complete TDS solution when a single supplier is involved. In any case, a single tender should be issued for the train. Adding the requirement for the possibility to replace TDS units is up to the railway undertaking and should be considered by the supplier accordingly.

So, OCORA considers the TDS units solution in the rest of the document.

In order to improve the competitiveness and remove the vendor lock-in situation, OCORA also considered the possibility of standardising the interface between the hardware elements of the display and the Layout Engine. However, all members of the group agreed that this should not be done. In fact, it would make the requirements too detailed in terms of granularity.

7 Conclusion

In today's cab architecture, there are at least three main screens in a cab supporting three systems: European Train Protection (ETP), Train Control and Management System (TCMS) and Cabin Voice Radio (CVR). Each screen is usually dedicated to one system. The screen embeds only one business logic to enable data exchange with the corresponding system, and elaborates the associated view. This paradigm leads to some pitfalls. OCORA listed all these drawbacks in the problem statement. However, the main pain points are: a screen failure leads to a loss of the system (the availability of the screen is a key factor for the overall availability of the train and the line) and space in the cab is limited (the introduction of new display panels in both existing and new trains can be difficult for integrators due to the lack of space).

To solve these problems, OCORA proposes the introduction of a new building block in line with the ERA/European Commission vision for the future of the CCS-OB: the Train Display System (TDS). The main principle of the TDS is a collection of displays that can be used by any system or even shared by several systems according to a pre-approved configuration dynamically managed by the TDS. The needs covered by this new system are related to the Common Business Objectives of the ERJU. Following the operational analysis, the TDS system requirements have been written and allocated to three main logical components: Presentation Logic (controlling the flow of views and data), Display Manager (controlling the configuration of the HMI) and Layout Engine (displaying the view of a Presentation Logic and providing events based on driver input). The functional requirements of these three logical components have not yet been written, but will be for Release 7.

After the identification of the logical components, OCORA elaborated the TDS architecture with six functional allocations of the logical components distributed in different hardware components: systems, displays and a dedicated TDS computing unit. These allocations have been evaluated using a weighted decision matrix. As a result, OCORA concluded, that TDS could be defined as a collection of TDS units, where a TDS unit is a display that hosts a Display Manager and a Layout Engine.

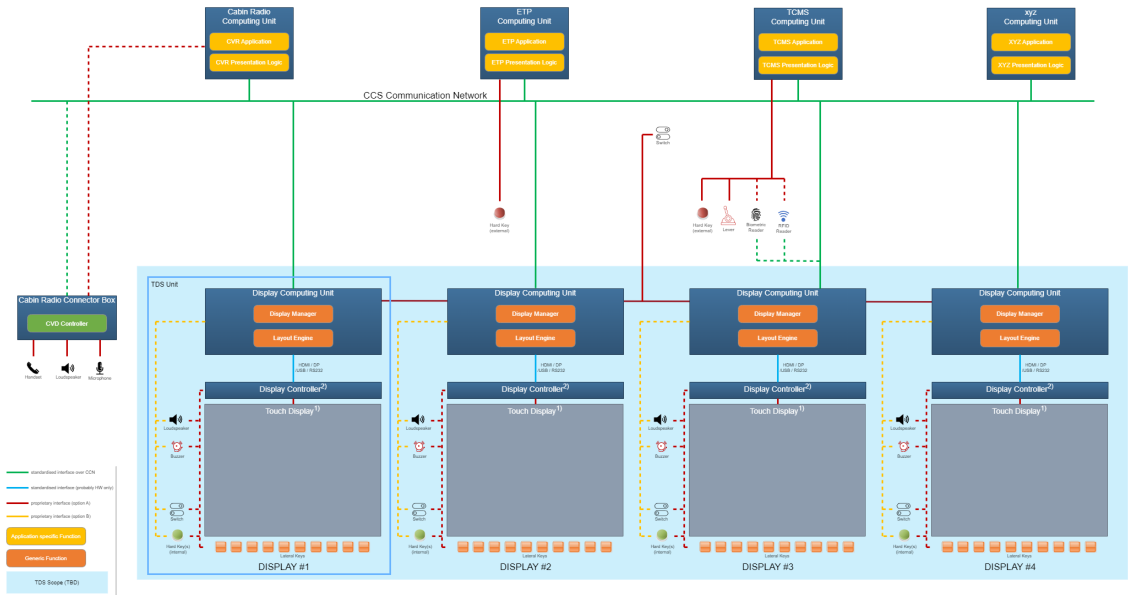


Figure 21 TDS architecture

At last, OCORA will develop the functional requirements of these logical components and define the data exchange between them and the systems (ETCS, TCMS, etc.). As a consequence, the TDS unit would be an independant and standardised building block which fulfils the modularity requirements. Therefore, TDS units could be provided by different vendors.

8 Annex : Cross-industry analysis of displays

This chapter gives an introduction of displays management among transport industries : railway, aeronautics, marine and cars.

Railway industry :

The railway industry has already published some standards to specify the Train Display System. The documents are:

- [CLC/TR 50542] Driver's cab train display controller, CENELEC, Mai 2018

This document introduces the concept of TDS. Chapter 9 supports a general description of TDS at a high level. Compared to other standards, the number of requirements for TDS is low. Chapter §9.2 presents how TDS should allow communication between systems and displays. Chapter §9.3 deals with a standard interface for TDS. Chapter §9.4 deals with compliance with EN50155 and EN50128. Chapter 9.5 presents safety and reliability requirements. Chapter 9.6 presents redundancy rules with extensive reference to UIC 612. Chapter 9.7 presents the architecture for the cab and the TDS. The architecture of the cab is limited to the management of 4 displays based on subset 121 and a local network. The physical architecture of the TDS requires a duplication of power supply, memory and CPU.

- [NF EN 1686] - Railway applications — Driver's cab — Part 1: Anthropometric data and visibility, AFNOR, February 2015

This document presents a set of rules for cab design in France. The main contributors are SNCF, RATP, EPSF and CERTIFER. Parts 2 and 3 contain interesting requirements for the OCORA analysis of TDS. It should be noted that rules are proposed for the existing configuration of the train : only ATP, TCMS, CVR are presented. In part 2, the characteristics of the display are presented. In particular, Table B1.1 describes the need to embed a system, if it has a mandatory location in the cab and the documents used as a reference. This could be useful for TDS configuration management. A deeper analysis should be done on part 3 where a concept close to TDS is specified. For instance, the management of mutltiple display and redundancy is described in §5.1.3. Chapters §5.1.4 and §5.1.5 present the need for simultaneous configuration of audible information and language between all systems.

- [UIC 612] - Driver Machine Interfaces for EMU/DMU, locomotives and driving coaches - Functional and system requirements associated with harmonised Driver Machine Interfaces, UIC, Mai 2011

The document UIC 612-01 is the document to be analysed in relation to TDS. It introduces the concept of a DDS (Driver Display system) which manages 4 displays for TRD, ETD, CCD and TDD. Although the configuration in the document is limited to a nominal configuration with one display for a system with only four systems, the concept of redundancy in chapter 5 is well described and should be taken as a reference for the OCORA analysis.

- [CLC/TS 50459] - Railway applications - Communication, signalling and processing systems - European Rail Traffic Management System - Driver-Machine Interface

The document CLC/TS 50459 is divided into 6 parts. The document CLC/TS TO459-1 describes the general principle for the presentation of ERTMS/ETCS/GSM-R information. Most of the chapters have cross-references to EN 16186. The document CLC/TS TO459-2 presents the ergonomic arrangements of GSM-R information. The document CLC/TS TO459-3 presents the ergonomic arrangements of non ETCS information. In other words, this is the arrangements of NTC systems: LZB/PZB, SCMT, etc. The document CLC/TS TO459-5 presents the symbols used by ETCS and GSM-R. The document CLC/TS TO459-6 presents the characteristics of the audible information. None of these parts are usefull in the context of Train Display System. In fact they are written for specific systems: ETCS, GSM-R, NTC.

- **Displays suppliers :**

This section reports data collected from the websites of four display suppliers (Deuta, Centralp, Duagon and Eke-electronics).

The first observation is that no display supplier offers a display solution for the entire cab. They only sell individual displays. In other words, their customers may be CCS on-board suppliers who select the appropriate display for their needs. Then the train integrators have to install all these displays in their cabs. A different paradigm, where display suppliers offer a standard display solution for the cab to which CCS suppliers have to connect their system, is not yet available.

The second point to note is the range of display sizes available, from 6,5'' to 15,6''. To ensure the configuration management of TDS, views need to be built with relative size or the variety of display size for system need to be reduced.

The third observation is that display suppliers offer SIL capabilities up to SIL2. These solutions are optional and proprietary. Having standardised capabilities could improve interchangeability.

Fourth comment is that display suppliers offer touch key and soft key solutions but with a greater proportion of touch key solutions. The TDS approach could focus more on this type of display.

Fifth observation is the introduction of display solutions which increase availability. In fact, some redundant terminals are proposed with two adjacent portrait display panels. This solution implies two communication channels between this display and the system and the ability to compute a view spread in two screens.

The Last point concerns the connectivity supported by the displays. Most of them support ethernet interfaces (10BaseT, M12, etc.), USB interfaces, RS 422, MVB, CAN, Profibus and have an audio output. Given the need for connectivity and modularity, a selection of mandatory interfaces should be made.

Sources:

- https://www.deuta.com/en/deuta-multifunctional-terminals-dmi.aspx

- https://www.centralp.fr/k-vision-console-ihm-ferroviaire/

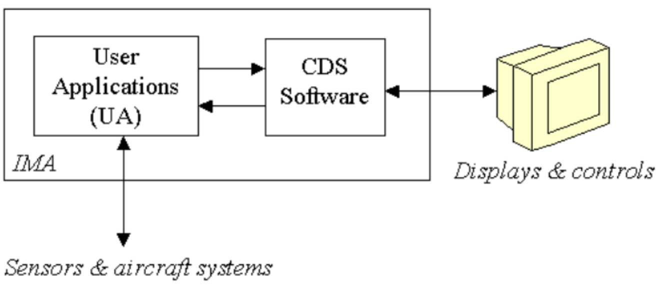
- https://www.duagon.com/products/#selectedCategory=122

- https://www.eke-electronics.com/products-and-solutions/eke-trainnet/human-machine-interfaces/

Aeronautics industry:

The aeronautics industry has already developed a Cockpit Display System (CDS) that is close to the Train Display System concept. The following paragraphs present it and its current integration on aircraft.

In the mid-1970s, aircraft manufacturers were confronted with the problem of the number of instruments and controls in the cockpit (more than one hundred), in particular the lack of space in the cockpit and the limitation of the pilot's attention. To overcome these problems, the industry has developed a CDS software which, thanks to Integrated Modular Avionics (IMA), allows the interface between user applications linked to sensors or aircraft systems and the displays and controls. This CDS provides the visible and audible part of the HMI for the aircrew, managing the glass cockpit (displays) and the interactions with the systems. The CDS provides separation between user applications and the displays and controls. The displays are not dedicated to one application. It is therefore possible to have more applications than displays. If a display fails, an automatic reconfiguration is done with the other displays. The pilot can organise his displays according to the priority associated with his flight phase.



This concept is based on standards such as ARINC 661, which specify the integration of the CDS and its interactions with the aircraft systems applications. However, the interaction between sensors and aircraft systems is not specified : ARINC 429, Ethernet protocol such as ARINC 664 could be used, but is not mandatory. In addition, the ARINC 661 standard has a fully defined graphical user interface (GUI), which allows a homogeneous presentation of data. With regards to these standards and concept, aeronautics suppliers can now offer a complete cockpit display solution. These products are compatible with other aircraft systems thanks to the IMA concept.

The introduction of the CDS and the glass cockpit has brought many benefits in terms of RAMS metrics. However, as the availability of displays has increased, so as the number of fatal crashes. In fact, the loss of the CDS leads to the loss of all displays. Therefore, crews need to be trained to deal with these failures and avoid consecutive accidents. To limit the impact of such a loss, some manufacturers have proposed an additional system (Integrated Standby Instrument System) that provides the minimum information necessary to complete a mission. This system is electronically separated from the main instruments and can run for several hours on a back-up battery.

By the end of the 1990s, Liquid Cristal Display (LCD) panels were widly adopted for their efficiency, reliability and legibility. Today, glass cockpits are standard in commercial aircrafts, business jets, military aircrafts and spacecrafts. In the latest Airbus cockpits (A220, A350), the number of displays in the cockpit has been reduced. The aircrafts now have a maximum of 6 displays instead of 10 on the previous generation of aircrafts (A380). This reduction is made possible by the the use of very large screens that allow all informations to be displayed on fewer panels. These panels are also identical to ensure interchangeability and a significant reduction in maintenance costs. Most of the displays are touchscreens, resulting in a decrease in weight and Line Replaceable Units (LRUs).

The CDS functionalities integrated in a A220-300 were presented to an OCORA member. Five displays are integrated; they are not touch sensitive. Many applications can share the same display. One pre-approved configuration is displayed by default. However, pilots can change the configuration with other pre-approved by means of a multi-position switch. In the event of visible fault on a display panel, they can activate a two-position switch, one by display, to inform the CDS of a problem on a display panel. Then, a new pre-approved configuration is automatically applyed. Depending on the type of loss (mandatory informations lost, last acceptable configuration, etc.), an audible alarm is generated and an information message is provided.

Sources:

- https://en.wikipedia.org/wiki/Cockpit_display_system

- https://en.wikipedia.org/wiki/ARINC_661

- https://en.wikipedia.org/wiki/Glass_cockpit

- https://www.airbus.com/en/products-services/commercial-aircraft/cockpits

- https://aerospace.honeywell.com/us/en/products-and-services/product/hardware-and-systems/cockpit-systems-and-displays#4

- https://www.thalesgroup.com/en/markets/aerospace/flight-deck-avionics-equipment-functions/flytx-tactile-large-display-flight-deck

- https://www.einfochips.com/blog/electronic-flight-deck-systems-in-modern-aircrafts/

- https://www.astronautics.com/products/displays/

Marine industry:

Few information has been found on marine industry. A deeper investigation could be done in a next release.

The first observation is that display suppliers can sell a single display dedicated to a system or a set of displays for the whole cab. For the latter, several configurations are possible: integration of a single unit with many displays (2 to 7 display panels) or integration of several units (units with 2 or 3 display panels). A more detailed analysis could be made on how these displays are managed and the type of connectivity used between systems and these displays.

Source:

- https://seatronx.com/products/displays/marine-displays/

Automotive industry:

As the automotive industry considers displays as one of the key differentiators of modern vehicle interiors, suppliers are proposing new interesting solutions for driver-vehicle interaction.

The first observation is that most suppliers are offering display solutions that cover the whole "cockpit" from one ultra-wide display to four wide displays. These displays have dedicated areas that suppors functions: driver information (e.g. speed), control and information elements (e.g. cabin temperature), entertainment functions (e.g. radio), etc.

The second point to note is the quality of the displays. They are large, from 7'' to 15'' in a rectangular form, but the shape could be adapted to specific needs. They also have high resolution (OLED). Some of them have 3D capabilities to put focus on essential information. Other capabilities exist but seem less relevant in the context of train driving (privacy displays, providing images only visible to the passenger, etc.).

All these displays could be managed by a single platform. This platform allows space savings compared to the integration of distributed control units and gives flexibility in configuring the view in the cab. This solution is based on a system on a chip, a hypervisor and compliance with Autosar, an automotive norm defining, among others things, interfaces and data exchanged, that allows different runtime environments and softwares to be embedded on a single platform.

The final observation is the ability to give control of parts of the cockpit or displays to non-native applications. In fact, applications such as Android Auto can run on the displays. This means that they are either pre-configured as authorised applications, or have cybersecurity features that enable authorisation and authentication on the displays.

Sources:

- https://www.continental-automotive.com/en-gl/Passenger-Cars/User-Experience/Display-Solutions

- https://www.visteon.com/products/displays/

- https://www.bosch-mobility.com/en/solutions/infotainment/display-and-interaction-systems/

- https://www.faurecia.com/en/technologies/solutions-safe-advanced-personnalized-cockpit/display-technologies

- https://www.android.com/intl/en_en/auto/