OCORA

Open CCS On-board Reference Architecture

Train Display System (TDS)

Specification

Document ID: OCORA-TWS01-202

Version: 1.00

Date: 31.01.2025

Revision history

Version	Change Description	Initial	Date of change
1.00	▪ First version	NB	31.01.2025

Author: Nicolas Bied-Charreton (SNCF)

Contributors: Jérôme Lalouette (SNCF), Laurent Pinori (SNCF), Albert Ledermann (SBB), Martin Lindenmaier (SBB), Cirillo Ghielmetti (SBB)

Table of contents

References

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

[1]
[2] OCORA-BWS01-010 – Release Notes
[3] OCORA-BWS01-020 – Glossary
[4]
[5] OCORA-BWS01-030 – Question and Answers
[6] OCORA-BWS01-040 – Feedback Form
[7] OCORA-TWS01-201 – Train Display System – Concept
[8]
[9] OCORA-TWS01-221 - Train Display System – PoC Results
OCORA-BWS03-010 – Introduction to OCORA
OCORA-BWS03-020 – Guiding Principles
OCORA-BWS04-010 – Problem Statements

1 Introduction

1.1 Purpose of the Document

This document identifies the requirements for the “Train display system” based on the PoC results [6].

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

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

If you are an organization interested in developing CCS on-board building blocks according to the OCORA design principles, the 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.

1.3 Context of the document

This document is published as part of an OCORA Release, together with the documents listed in the Release Notes [1]. If you are interested in the context and the motivation that drives OCORA we recommend reading the Introduction to OCORA [7], the Guiding Principles [8], and the Problem Statements [9]. The reader should also be aware of the Glossary [2] and the Question and Answers [3].

2 Capabilities

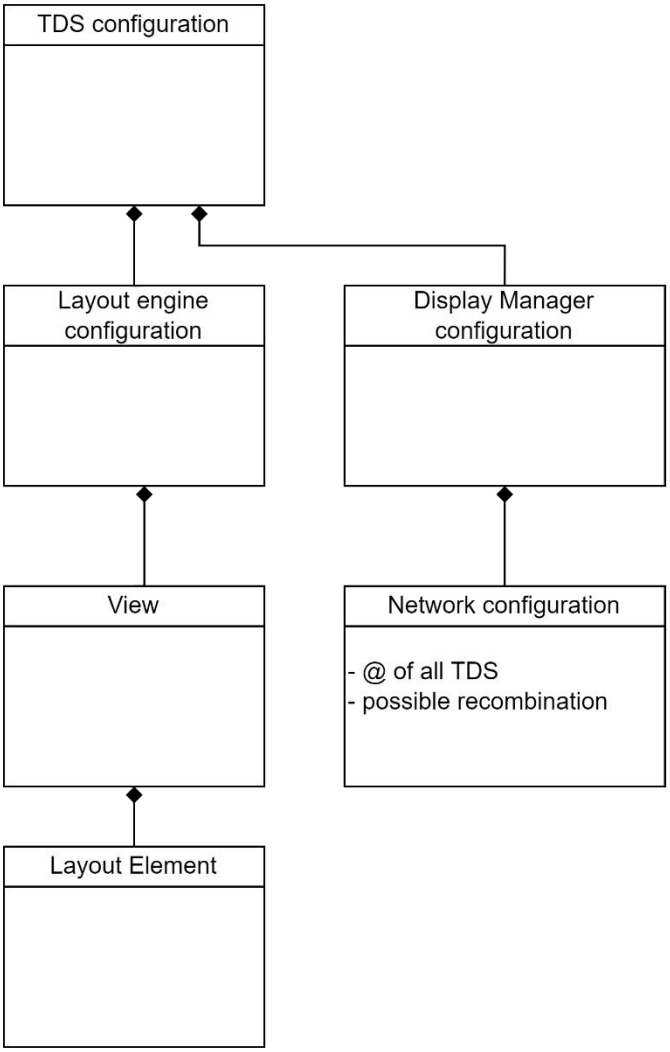
The capabilities of TDS are expressed in the TDS Concept [5] as high level requirements. Concerning the configuration,

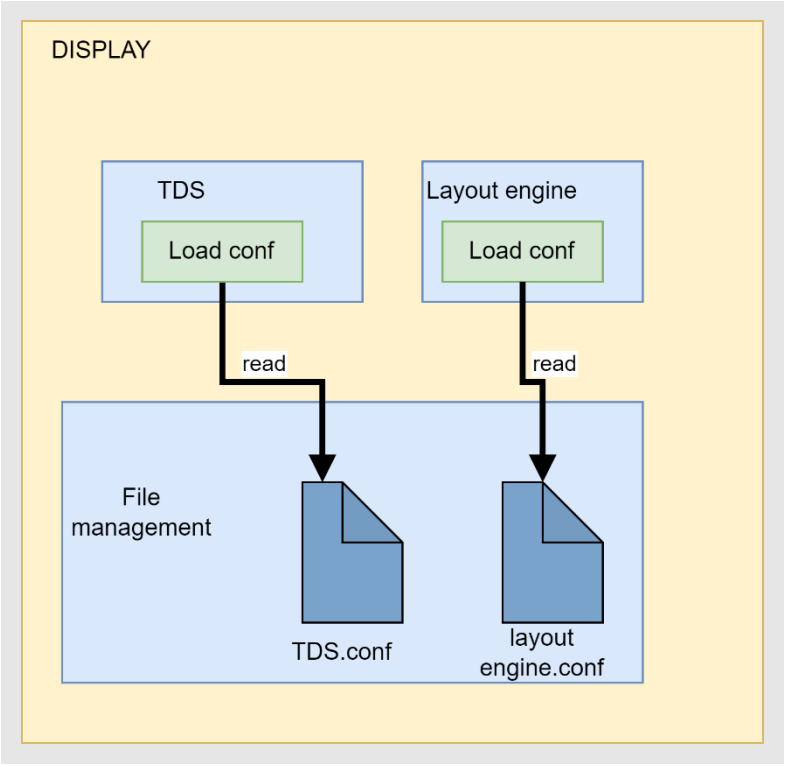
- TDS shall reconfigure displays if one display fails
- TDS shall reconfigure displays if one system fails or starts.
- TDS shall switch the view on a display on driver request

To handle such capabilities, the TDS shall manage communication between functional components, configuration.

3 Architecture and Configuration files

To support TDS principles, configuration files shall be built and shared to all TDS units. These files shall describe the possible configuration of the cabin and contain the structure of the view and layout elements.


TDS configuration
Layout engine configuration
Display Manager configuration
View
Network configuration
- @ of all TDS
- possible recombination
Layout Element


DISPLAY
TDS
Load conf
Layout engine
Load conf
read
read
File management
TDS.conf
layout engine.conf

3.1 Display Manager configuration

The Display Manager configuration file shall contain all information relative to System Presentation Logic, Display Manager and Layout Engine available on the network. So, one Display Manager can determine its role (master or slave Display Manager) and communicate to other components when master.

3.1.1 Cabin configuration

In this section, the table below presents the TDS units available in cab A and cab B.

	CAB A		CAB B	
Nominal	TDS UNIT 1	IP@ X.X.1.1	TDS UNIT 1	IP@ X.X.2.1
	TDS UNIT 2	IP@ X.X.1.2	TDS UNIT 2	IP@ X.X.2.2
	TDS UNIT 3	IP@ X.X.1.3	TDS UNIT 3	IP@ X.X.2.3
TDS 1 failure				
	TDS UNIT 2	IP@ X.X.1.2	TDS UNIT 2	IP@ X.X.1.2
	TDS UNIT 3	IP@ X.X.1.3	TDS UNIT 3	IP@ X.X.1.3
TDS 2 failure	TDS UNIT 1	IP@ X.X.1.1	TDS UNIT 1	IP@ X.X.1.1
	TDS UNIT 3	IP@ X.X.1.3	TDS UNIT 3	IP@ X.X.1.3
TDS 3 failure	TDS UNIT 1	IP@ X.X.1.1	TDS UNIT 1	IP@ X.X.1.1
	TDS UNIT 2	IP@ X.X.1.2	TDS UNIT 2	IP@ X.X.1.2

Main principles:

- The Display Manager configuration file shall be the same in all TDS UNIT.
- TDS units are ordered by the length of IP address: X.X.X.1<X.X.X.2<X.X.X.3 in order to ease Master Display Manager determination.

```
<NETWORK_CONF>
	<CAB>
		<ID>A</ID>
		<CONFIGURATION>
			<NUMBER>1</NUMBER><!-- Nominal configuration -->
			<TDS_UNIT>
				<TDS_UNIT_IP_ADDRESS>X.X.1.1</TDS_UNIT_IP_ADDRESS>
			</TDS_UNIT>
			<TDS_UNIT>
				<TDS_UNIT_IP_ADDRESS>X.X.1.2</TDS_UNIT_IP_ADDRESS>
			</TDS_UNIT>
		</CONFIGURATION>

		<CONFIGURATION>
			<NUMBER>2</NUMBER><!-- Failure of TDS 2 @IP X.X.1.2 -->
			<TDS_UNIT>
				<TDS_UNIT_IP_ADDRESS>X.X.1.1</TDS_UNIT_IP_ADDRESS>
			</TDS_UNIT>
		</CONFIGURATION>
	</CAB>
	<CAB>
		<ID>B</ID>
		<CONFIGURATION>
			<NUMBER>1</NUMBER><!-- Nominal configuration -->
			<TDS_UNIT>
				<TDS_UNIT_IP_ADDRESS>X.X.2.1</TDS_UNIT_IP_ADDRESS>
			</TDS_UNIT>
			<TDS_UNIT>
				<TDS_UNIT_IP_ADDRESS>X.X.2.2</TDS_UNIT_IP_ADDRESS>
			</TDS_UNIT>
		</CONFIGURATION>
```

```
            <CONFIGURATION>
                  <NUMBER>2</NUMBER><!-- Failure of TDS 1 @IP X.X.2.1 -->
                  <TDS_UNIT>
                        <TDS_UNIT_IP_ADDRESS>X.X.2.2</TDS_UNIT_IP_ADDRESS>
                  </TDS_UNIT>
            </CONFIGURATION>
      </CAB>
</NETWORK_CONF>
```

3.1.2 Predefined configuration

This section presents in detail the configuration for cab A. More precisely, it makes the association between the System Presentation Logic and the Layout Engine. These data shall be added in the previous configuration file. So, only one configuration is used by the Display Manager.

The table below presents a suggestion of configuration between TDS units and systems. A human factor analysis shall be performed at the train level to validate the configuration file.

	TDS 1 X.X.X.1 (SIL2)		TDS 2 X.X.X.2 (SIL2)		TDS 3 X.X.X.3 (BASIC INTEGRITY)	
Nominal	ETCS	System IP@ Active channel Priority 1 Size: full screen Position: 0.0	TCMS	System IP@ Active channel Priority 1 Size: full screen Position: 0.0	CVR	
	RearView	System IP@ Active channel Priority 2 Size: full screen Position: 0.0				
TDS 1 failure			ETCS	Priority 1	CVR	Priority 1
			TCMS	Priority 2	RearView	Priority 2
TDS 2 failure	ETCS	System IP@ Active channel Priority 1 Size: full screen Position: 0.0			CVR	
	TCMS	System IP@ Active channel Priority 2 Size: full screen Position: 0.0				
	RearView	System IP@ Active channel Priority **3** Size: full screen Position: 0.0				
TDS 3 failure	ETCS	Priority 1	TCMS	Priority 1		
	RearView	Priority 2	CVR	Priority 2		
ETCS failure	RearView		TCMS	Priority 1	CVR	Priority 1
RearView failure	ETCS		TCMS		CVR	
TCMS failure	ETCS		RearView		CVR	
CVR failure	ETCS		TCMS		RearView	

Main principles:

- The Display Manager configuration file shall be the same in all TDS UNIT.
- The first configuration shall be the nominal, then configuration with a TDS unit failure (1>2>3), then configurations with a system failure (ETCS>TCMS>…).
- Configuration combinations are predefined.
- It is possible to allocate several systems' views to the same Layout Engine.
- It is possible to stack systems' view in the same display (low priority against system).
- It is possible to have trigger events that force to display a view (e.g standstill/in motion)
- The maintainer shall not associate a SIL2 Presentation Logic to a BASIC INTEGRITY Layout Engine.

Below an example with the nominal configuration (two systems on Layout Engine 1 and one on Layout Engine 2) and a failure on TDS 2 of cab A.

```
<NETWORK_CONF>
	<CAB>
		<ID>A</ID>
		<CONFIGURATION>
			<NUMBER>1</NUMBER><!-- Nominal configuration -->
			<TDS_UNIT>
				<TDS_UNIT_IP_ADDRESS>X.X.1.1</TDS_UNIT_IP_ADDRESS>
				<SYSTEM>
					<TYPE>ETCS</TYPE>
					<CHANNEL>ACTIVE</CHANNEL>
					<SYSTEM_IP_ADDRESS>X.X.1.10</SYSTEM_IP_ADDRESS>
					<PRIORITY>1</PRIORITY>
					<SIZE>FULL SCREEN</SIZE>
					<POSITION>0,0</POSITION>
				</SYSTEM>
				<SYSTEM>
					<TYPE>RearView</TYPE>
					<CHANNEL>ACTIVE</CHANNEL>
					<SYSTEM_IP_ADDRESS>X.X.1.11</SYSTEM_IP_ADDRESS>
					<PRIORITY>2</PRIORITY>
					<SIZE>FULL SCREEN</SIZE>
					<POSITION>0,0</POSITION>
				</SYSTEM>
			</TDS_UNIT>
			<TDS_UNIT>
				<TDS UNIT IP ADDRESS>X.X.1.2</TDS UNIT IP ADDRESS>
				<SYSTEM>
					<TYPE>TCMS</TYPE>
					<CHANNEL>ACTIVE</CHANNEL>
					<SYSTEM_IP_ADDRESS>X.X.1.12</SYSTEM_IP_ADDRESS>
					<PRIORITY>1</PRIORITY>
					<SIZE>FULL SCREEN</SIZE>
					<POSITION>0,0</POSITION>
				</SYSTEM>
			</TDS_UNIT>
		</CONFIGURATION>

		<CONFIGURATION>
			<NUMBER>2</NUMBER> <!-- Failure of TDS 2 @IP X.X.1.2 -->
			<TDS_UNIT>
				<TDS_UNIT_IP_ADDRESS>X.X.1.1</TDS_UNIT_IP_ADDRESS>
				<SYSTEM>
					<TYPE>ETCS</TYPE>
					<CHANNEL>ACTIVE</CHANNEL>
					<SYSTEM_IP_ADDRESS>X.X.1.10</SYSTEM_IP_ADDRESS>
					<PRIORITY>1</PRIORITY>
					<SIZE>FULL SCREEN</SIZE>
					<POSITION>0,0</POSITION>
				</SYSTEM>
				<SYSTEM>
					<TYPE>TCMS</TYPE>
					<CHANNEL>ACTIVE</CHANNEL>
					<SYSTEM_IP_ADDRESS>X.X.1.12</SYSTEM_IP_ADDRESS>
					<PRIORITY>2</PRIORITY>
					<SIZE>FULL SCREEN</SIZE>
					<POSITION>0,0</POSITION>
				</SYSTEM>
				<SYSTEM>
					<TYPE>RearView</TYPE>
					<CHANNEL>ACTIVE</CHANNEL>
					<SYSTEM_IP_ADDRESS>X.X.1.11</SYSTEM_IP_ADDRESS>
					<PRIORITY>3</PRIORITY>
					<SIZE>FULL SCREEN</SIZE>
					<POSITION>0,0</POSITION>
				</SYSTEM>
			</TDS_UNIT>
		</CONFIGURATION>
	</CAB>
</NETWORK_CONF>
```

3.2 View configuration

In order to build a system view, each Layout Engine shall have access to: a view configuration containing the structure of the view requested by every system, the translation of the data received and the icons to be displayed.

For a system, it is recommended to use the same name for the value and icons.

It is recommended to use .png for icons to limit the quantity of format supported by Layout Engine.

For ETCS, the view shall comply with ERA DMI 15560.

For TCMS, the view shall comply with UIC-612-3 or EN16186-3.

For CVR, the view shall comply with UIC-612-4.

For Rear-View system, the view could be proprietary. So, it could be a video stream or a html page.

For other systems, the view could be a direct video stream or a html page.

To support the diversity of system configuration, the tree structure shall be the following one:

System/View -> contain the structure of each view of a System

System/data -> contain a configuration file with the translation of data received and the view, messages and icons to be displayed. (this is relevant for systems using subset 121 communication)

System/LayoutElement -> contains the collection of information of a System (icons, text messages, entry fields...).

4 TDS function

To ease the understanding of this functional specification, the subset 121 breakdown has been used. However, instead of describing requirements for ETCS, the requirements are now for systems using HMI. In addition, the TDS specification is split in two: one for Display Manager and one for Layout Engine (formerly called TDS in subset 121).

4.1 Cab Management

The aim of this function is to determine which TDS units are activated depending on the cab status.

Notes:

- Following chapter §7.4 of subset 121, ETCS shall inform the TDS if the cab is active or not (M_CAB_STATUS). However, as the TDS manages configurations for multiple systems, it would be worthwhile to change the transmitter of the information. Indeed, the ETCS could be isolated but other systems could use TDS units (e.g. maintenance, ETCS failure in operation…).
- The following chapter considers the activation of TDS units only when the cab is activated. It means, that configuration selection and application is done at this moment. To accelerate the awakening of the system, the operational state of the TDS could be considered when the train is powered on. So, configuration selection and activation could be performed even if the cab is not activated. These two solutions have to be analysed with regards to operational scenarios for the driver (change of direction of the train in case of end of mission with low time...).

4.1.1 Systems on-board requirements

When a System receives the information cab activation from the train, it shall wait for its configuration with a Layout Engine by the master Display Manager (see chapter 4.4).

4.1.2 Display Manager requirements

If a Display Manager receives the information cab activation from the train, it shall enter in operational state.

If the cab activation input is 0, the Display Manager shall be in sleeping state.

Note: It is assumed that for special train with two desks in the same cabin, one desk is considered cab A and the other cab B. TDS units integrated in a cab shall only receive the cab activation status of this cab. E.g.: TDS units integrated in the cab A shall receive cab activation status from cab A.

Cab activation input	Display Manager state
0	Sleeping
1	Operational

Note: A safety analysis shall be done on the cab activation input.

4.1.3 Layout Engine requirements

If the Display Manager is in a sleeping state, the Layout Engine shall not display any system object on the screen.

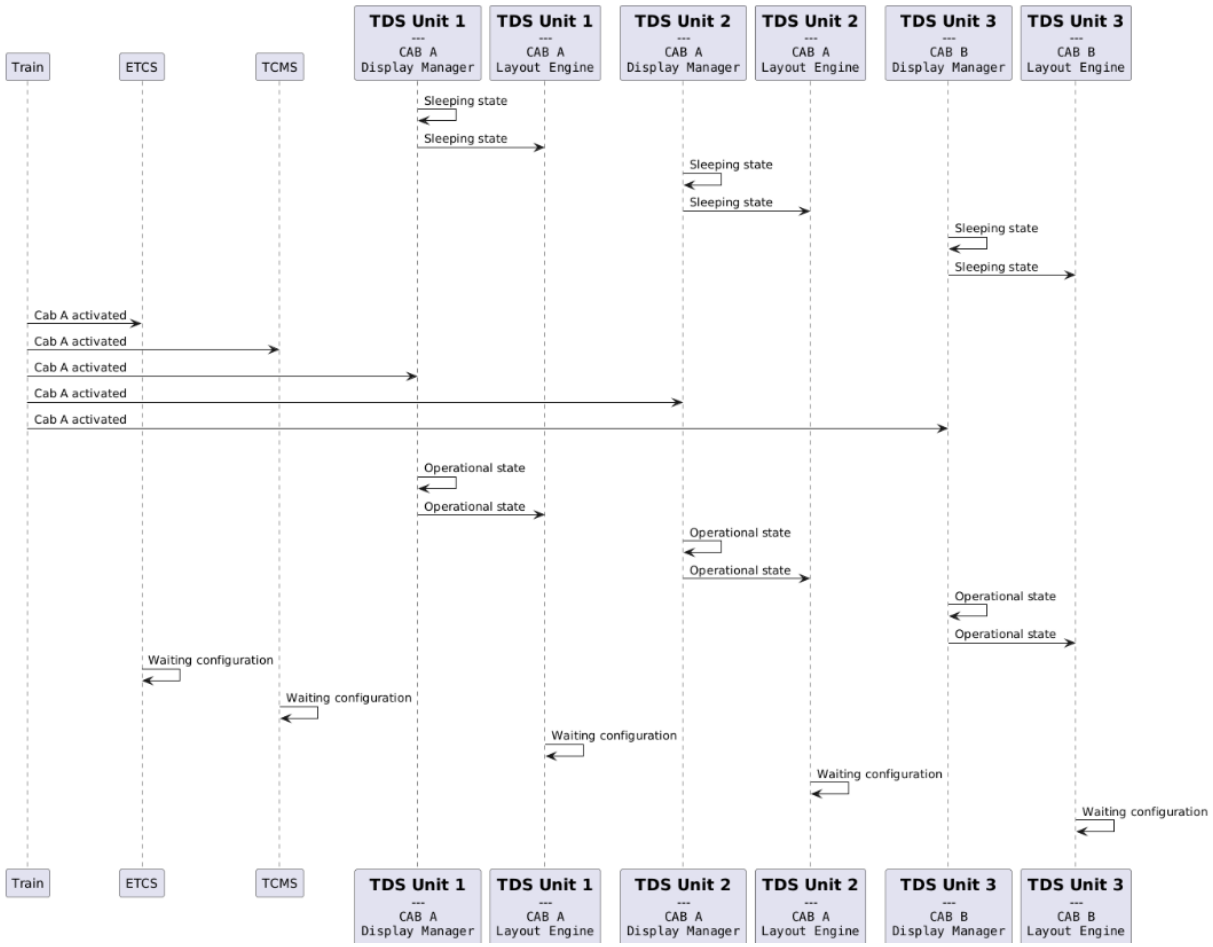
Rational: application of §7.2.3.7 of subset 121.

If the Display Manager is in operational state, the Layout Engine shall wait for its configuration with a/multiple System Presentation Logic by the master display manager (see chapter 4.4).

Rationale:

- Ensure displaying only the view of the configured system.
- Being aware of the priority of the different systems in case of stacked view.

4.1.4 Dialog sequence



PlantUML url:

//www.plantuml.com/plantuml/png/hPD1Qxj04CNlVeh1IquU_dhxGqkCoQsX1Iqzb1wcPYiBPhMw5W9--Begs7KY6KjFikFxlHcTjzjQOwMRS-viFCzpDl3K7MKgIrIw7chbL86aGgcioY69ObiI7Ut2NjPbZfSZAin41QyE0C1Tie_XMKaD__gpQMIUhXk5EmXTTpoDC8nqLt-pp1_mKZJwe3Afn4hh0OM1jOpfr3xnzlziRBxt-ha3uXrSyTxzQkwrtdJkCNAn-6o4IWNqMHogiz1uz_CO_OSu5wAKAZEO5fImXhsbzsaBdyDOJMuI0UqIi1ZxlnEYRLkdlvf6Qsva9udm7KB0LCklJdAQtfiBklYUpCTN-dnfS4LgFeApziTILAXbeJ3dRfuWZEKpCQiLXNWHu64q1HJgTpzbu0MbDYb92_KXisOGEoO0Kn0MH3zxpNkp8FftM1Zzq4NC16OhrAavvzy0

4.1.5 Data transmitted from Systems on-board

None

4.1.6 Data transmitted from Display Manager

Display Manager state: operational / sleeping

sporadic

4.1.7 Data transmitted from Layout Engine

None

4.1.8 Performance requirements for Systems on-board

None

4.1.9 Performance requirements for Display Manager

The Display Manager shall power up in less than 30s.

The Display Manager shall detect an evolution of cab status information in less than 0.4s.

The Display Manager shall apply a new state in less than 0.4s.

Rationale: 0.4s comes from the performance requirements of the TDS in the subset 121.

4.1.10 Performance requirements for Layout Engine

None

4.2 Master Display Manager determination

The aim of this function is to determine the role of each operational Display Manager: master or slave.

Note: The algorithm proposed below for the PoC has been chosen for its simplicity. Another protocol could be considered for the final specification of the TDS. To date, OCORA is aware about other protocols like EtherCat, VRRP, SDTv2. These protocols are adopted in the railway industry. The selection of the appropriate candidate shall be based on some criteria: compliance with subset 147, in-house knowledge, maturity, adoption in the industry, simplicity.

4.2.1 Systems on-board requirements

None.

4.2.2 Display Manager requirements

When the Display Manager enters in operational state, it shall consider itself as a slave.

All Display Manager have access to the same configuration file with the IP addresses of all Display Managers in the Cab activated (see chapter Display Manager configuration)

After 5s in operational state (time to consider all TDS units initialized), the Display Manager shall communicate with all the Display Managers in the Cab.

After 2s, if no Display Manager are already master, the Display Manager with the lowest TDS unit IP address is the master, the other Display Managers are slave.

When a Display Manager becomes master, it shall inform all slave Display Managers.

The master Display Manager shall initiate a cyclic communication (process data) with its first slave.

Note: First slave means the Display Manager with the next lowest IP after the master Display Manager [e.g. IP X.X.X.1 (master) > X.X.X.2 (first slave) > X.X.X.n (n-1 slave)].

If the master Display Manager fails, the first slave Display Manager becomes the master Display Manager.

If the first slave Display Manager communication fails, the master Display Manager shall initiate a communication with the next slave.

If no slave Display Manager is available, the master Display Manager remains operational and stops initiating communication with other Display Managers.

4.2.3 Layout Engine requirements

None.

4.2.4 Dialog sequence

PlantUML url:

//www.plantuml.com/plantuml/png/nPHHQ-9E5CNVvrCSV551fScy_2dqZowsq0T16WiBooBJU5k7JKPtPbG4F_pEQB3Rn3NZjcNn8UHmSi-T7yVf6okqNUKPQtQxNTR4sBtAL2w5ikQWBLyL3ALPPc8x4agyaCOt1W0tas62HoKjelsx_yW_6ut2ZiBVQ1Jw_RZ_jUT_aPE-dqc8An5nMCGn8Qv9u9K4Vc42toSK-1BwkIAL4lPS3se9MlV_CiPht3Tp99bOKyaSLztn6JklslaP--dX3ukC7lmnZAtryug_PljmVqW0lp20l_l4Ht_BUA3jO4A5Fu1Gk3yWW5yOmDz_OcV_GkaY9uo4iQI3aBgAXjhvM_jkjmjA60-doU3k5YshXJAvjExZQ_UddwwKjDEe0qqfoRKJSLJZ3aRJP3YP9fF1v1OtYDfCf5QkXQLI15CBfsdvChVC3u0VW0ZIFQItEoAvqr9XvK9X8-qSpr8RYprMb6uPj8upuZR3M2zICWOpOKK7XjGCv5RT8eh_omt3O2ra9fva9kqMwPpI7tWYko5Il-yYt6UlOtjuL5PcRvOrCEAPEXLycd8XbJdiscC-tv-tlfrrtEEJtACJt6Vq9_Ak0M7Nvfs3jD81M-E3rhvgiu0w_rqt-UTsKz4ci9_yS_h9m_l90_l9_rq_QsjGgUUPndnGOQu2Bl_IPTjtP5TvzWi0

4.2.5 Data transmitted from Systems on-board

None.

4.2.6 Data transmitted from Display Manager

- RoleRequest
  Transmission type: sporadic
- Role (IP, master/slave).
  Transmission type: sporadic
- Availability of the master Display Manager.
  Transmission type: cyclic.

  Note: Structure of the Process Data could follow the structure of subset 121. In subset 121 the origin and destination are part of the name of the variable. As the number of transmitter/receiver increases, it is proposed to have a generic name for Safe communication with two new variables: transmitters and receivers. As example, PD_ETCS_TO_TDS_SAFE could become PD_SAFE(Transmitter:ETCS, Receiver:TDS).

  In the dialog sequence above, the following message could be sent PD_SAFE(transmitter:TDS_unit_1, receiver: TDS_unit_2, M_SDT_STATE).

4.2.7 Data transmitted from Layout Engine

None.

4.2.8 Performance requirements for Systems on-board

None.

4.2.9 Performance requirements for Display Manager

The Display Manager shall determine its role in less than 1s.

When the Display Manager become master, it shall inform other slave Display Managers in less than 0.4s.

When the master Display Manager fails (loss of safe data transmission), the first slave Display Manager shall become the master Display Manager in less than 64ms.

Rationale: Limit the reconfiguration time to 1 cycle of 128ms.

The master Display Manager shall initiate a new cyclic communication with its first slave Display Manager in less than 0.4 s.

Rationale: Ensure that a failure of the master Display Manager could be detected by the first slave Display Manager.

4.2.10 Performance requirements for Layout Engine

None.

4.3 Health Monitoring

The master Display Manager shall be aware of the availability of each Presentation logic and TDS units (slave Display Manager) activated in the cabin.

Note: In this section, it is proposed to extend the functionalities of subset 121 to every system and slave Display Manager with the master Display Manager.

The following chapters shall be applied:

5.1.3.2 In case of detection of a safety critical TDS internal fault (e.g. violation of system integrity), the TDS shall enter the 'Non-Operational Safe State' and shall be set powerless.
It shall be possible to recover from 'NOSS' by performing a system reset.

5.1.3.3 In case of detection of missing or invalid safety related data inputs for a TDS safety function (e.g. during start-up or due to intermittent failures of the incoming SDT channels), the TDS shall enter the 'Defined Operational Safe State' (DOSS) by setting the associated safety related data outputs invalid.
It shall be possible to (re-)enter 'Normal Operation' state from 'DOSS' (e.g. when safe communication is (re-)established).

5.2.7.4 In case the TDS indicates loss of safe communication for more than 5 seconds, the EVC shall enter ETCS mode System Failure.

Note: The 5 seconds requirement based on SUBSET-026-5 that defines the waiting time for a driver acknowledgement to be set to 5 seconds before commanding a service brake.

7.5 Failure/Degraded case management

7.5.1.1 In case of any internal TDS failure, the TDS shall disconnect from EVC.

Note: As a consequence, all ETCS/STM objects will be removed, see 7.2.3.6.

4.3.1 Systems on-board requirements

When the safe communication between the System and the master Display Manager is operational, the system shall send to the master Display Manager the indication that the communication is safe.

In case of detection of missing or invalid safety related data inputs for a System safety function, the system shall set the associated safety related data outputs as invalid to the Master Display Manager.

In case of any internal System failure, the System shall disconnect from the Master Display Manager.

4.3.2 Display Manager requirements

By configuration, the master Display Manager accesses a list of Systems and slave Display Manager in the activated cab.

The master Display Manager shall initiate a communication with the Systems and Slave Display Manager.

Rationale: This is in contradiction to §4.2.1.1 and §7.2.2.1 of subset 121 where EVC is the master of the connection and requests the connection with the TDS. However, to ensure the behaviour of TDS with multiple systems and TDS units, it is mandatory to modify the master as the master TDS unit.

A Display Manager shall monitor any internal failure of the TDS unit (e.g. temperature, power supply, Layout Engine Failure…).

In case of detection of a failure or missing/invalid data inputs, the Display Manager shall enter in the appropriate state: Defined Operational Safe State (DOSS) or Non-Operational Safe State (NOSS).

Note: the subset 121 doesn't specify clearly the link between the state of the system and the information sent to the EVC or the TDS. It is assumed that this information is sent with the M_SDT_STATE (REGULAR or SAFE) and by setting the safety associated data to invalid (§5.1.3.3 subset 121).

In case being in state DOSS for more than 5 seconds, the Display Manager shall enter the 'Non-operational safe state (NOSS)

Note: This requirement is consistent with §5.2.7.3 of subset 121.

If the Display Manager enters in DOSS or NOSS due to a failure, it shall inform its Layout Engine.

Note: these states are defined in the chapter 5.1.3 of subset 121 and the management of the failure by the TDS is described in chapter 7.5.1.1

The Master Display Manager should consider a system or slave Display Manager in failure state in case of an intermittent loss of the communication or in case of loss of safe communication for more than 5 seconds.

Note: the management of the intermittent loss is defined in chapter §5.1.3.3 of subset 121.

When a System Presentation Logic or slave Display Manager is detected as failed, the master Display Manager shall initiate the function "Configuration selection and application".

4.3.3 Layout Engine requirements

In case of detection of missing or invalid safety related data inputs for a Layout Engine safety function, the Layout Engine shall inform its Display Manager.

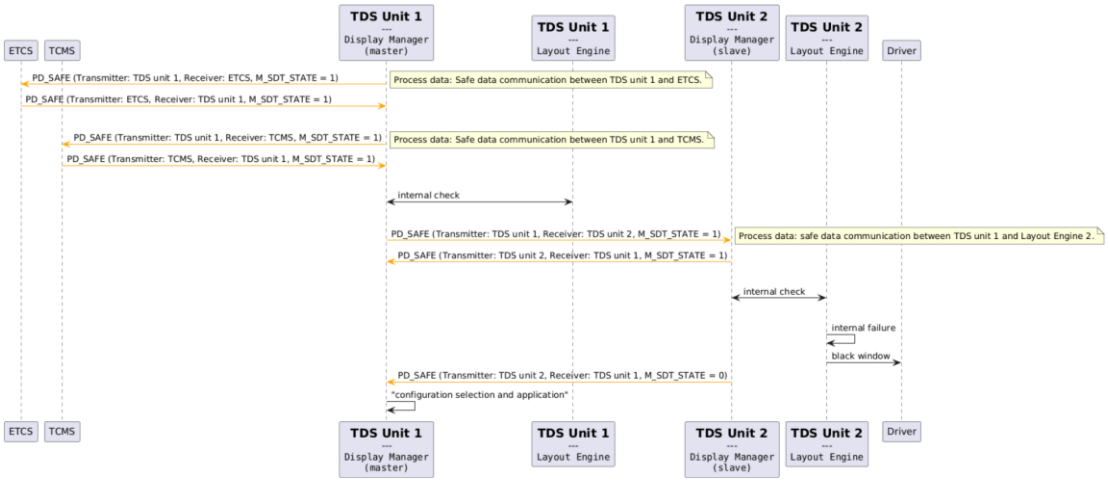
In case of any internal failure, the Layout Engine shall inform its Display Manager.

In case of DOSS or NOSS state, the Layout Engine shall remove any object on the view.

Rationale: This is compliant with chapter 7.5.1.1 of subset 121.

Note: There is an open point on subset 121 concerning when to remove object on the view. Chapter 7.5.1.1 doesn't provide the link between DOSS and NOSS. Chapter 5.2.7.3 seems to request the removal of information only when in NOSS state.

4.3.4 Dialog sequence



Note: This diagram sequence represents only two systems (ETCS and TCMS) and two Layout Engines (TDS1 and TDS2). The mechanism shall be adopted for every System and Layout Engine using display in the activated cabin.

Note2: sporadic messages are shown with dotted lines and cyclic messages are shown with solid lines.

PlantUML:

//www.plantuml.com/plantuml/png/nLHHQzim47xNhpYyXpPGZzMFPWqjJVQqG9YzfrB2LRcuehBiIN938Jz-ikonA5xhcJ7w5Dt7tNUVli_AjR6eRLDATXR7CJk3jIi55pKgQpgi_et0Ch_D0Y2_NON0GfXQuiiA5HQauOu105pbYmo-As7XqjUErlz6KTyEVNyKzVXvYSQIdZdWFk3_YYzLOvUg48f6sRjcwBe7LA7KPC2M_ArM8_6PtfOwpZwYLOjdqhz2okX7GueJ-FGwzCJu-Ev3fL4LT3_tgK4AwyKck_coXFDSepAbi9Pq2gsWnfjt0T-8KxidzICNiDfaYtoJvJVv4gxWSiPKPGcqA1ujWxMkE1a3MxIOGeOxyaVWLLawGevML0eUoEw9rD4QGBNr_1yPkLDBoTeoa1pUvXNjdkL8TN2NWVR3uS3USCb_oXDTSYF_rIN7V-nIMqvtoRFyaqkVutduxb8Gob4hbC0VYJ-DUNlwr2RO7A399BFDDBE31mZ9aUydwYT64DvWIX2dYmT197zE8co9vw-Ex538HjDWeF-xSQqF4laJx8NQLljtyE7JRFXP3NT5l58xKJIwozUG9EvFRQnOrx9FFcBNBjEcb3y1

4.3.5 Data transmitted from Systems on-board

Safe communication state (M_SDT_STATE)

Transmission type: cyclic.

Note: Structure of the Process Data could follow the structure of subset 121. In subset 121 the origin and destination are part of the name of the variable. As the number of transmitter/receiver increase, it is proposed to modify the name of PD_ETCS_TO_TDS_SAFE and PD_TDS_TO_ETCS_SAFE to have a generic name for Safe communication with more variables: transmitters and receivers. As example, PD_ETCS_TO_TDS_SAFE could become PD_SAFE(Transmitter:ETCS, Receiver:TDS).

In our configuration, the following message could be sent PD_SAFE(transmitter:system X, receiver: Master Display Manager, M_SDT_STATE).

4.3.6 Data transmitted from Display Manager

Safe communication state (M_SDT_STATE)

Transmission type: cyclic.

Following the proposition in the chapter above, in our configuration, the following message could be sent PD_SAFE(transmitter:Master Display Manager, receiver: System X, M_SDT_STATE) or PD_SAFE(transmitter:Master Display Manager, receiver: Slave Display Manager, M_SDT_STATE)

PD_SAFE(transmitter:Slave Display Manager, receiver: Master Display Manager, M_SDT_STATE)

4.3.7 Data transmitted from Layout Engine

Safe state

Transmission type: cyclic.

This data could be proprietary.

4.3.8 Performance requirements for Systems on-board

None.

4.3.9 Performance requirements for Display Manager

None.

4.3.10 Performance requirements for Layout Engine

None.

4.4 Configuration selection and application

This chapter describes how the master Display Manager selects and shares the configuration to be set by Systems and TDS units (Display manager). This action is performed at the initialisation or after a failure detection (see chapter Health Monitoring).

So far, two options have been considered:

- Option 1: The Master Display Manager selects the configuration and sends all configuration information to the Systems and Slave Display Managers. The Systems and Slave Display Managers apply the received data directly.

- Option 2: The Master Display Manager selects the configuration and sends the identification number of the configuration to be applied to the Systems and Slave Display Managers. The systems and slave Display Managers check their configuration files and apply the appropriate data from the identification number of the configuration received.

The following chapter presents the requirements for both options and then the requirements for each of them.

4.4.1 Systems on-board requirements

The System Presentation logic shall only receive the configuration data from the Master Display Manager.

Note: The System Presentation logic requires the following data for its configuration: Number of Channels (max 2) to Layout Engine and for each of them the IP address of the TDS unit and their type of channel (active or redundant). See chapter 7.4 of subset 121.

When all configuration data is received and is coherent, the System Presentation logic sends a configuration acknowledgment to the master Display Manager.

If some configuration data is inconsistent, the System Presentation logic shall inform the master Display Manager. Suitable diagnostic information shall be made available.

Option 1:

If some configuration data is missing, the System Presentation logic shall inform the master Display Manager. Suitable diagnostic information shall be made available.

Option 2:

When the system receives a new configuration to be applied, first, it shall compare the version of its configuration file with the configuration file of the master Display Manager (e.g. Checksum...). In case of differences, it shall enter failure state.

4.4.2 Display Manager requirements

The Display Manager shall contain only a list of pre-approved configurations (see chapter Display Manager Configuration).

Depending on the availability of Systems Presentation Logic and TDS units (Health Monitoring), the master Display Manager shall select only one configuration.

When the configuration is selected, the master Display Manager shall send configuration data to the Systems Presentation Logic and the Display Manager.

When the master Display Manager has received all configuration acknowledgments, it shall send a start communication order to the systems and slaves Display Managers.

If the master Display Manager hasn't received at least one configuration acknowledgment after a configuration timer (2 configuration attempts), it shall resolve that the system/slave Display Manager, which didn't answer, has failed and select another configuration accordingly.

If the availability of a System presentation Logic or slave Display Manager evolves, the master Display

Manager shall reevaluate the configuration.

When the master Display Manager receives a message concerning missing or inconsistent data, it shall send again all the configuration data to the transmitter of the message.

In case of a second missing or inconsistent data, the master Display Manager shall consider the transmitter of the data failed. Suitable diagnostic information shall be made available.

When a new configuration is applied due to a failure, the master Display Manager shall send to all Layout Engines the trigger reason for the new configuration.

Note: In case of system failure, TDS unit shall keep the configuration. Indeed, the layout engine shall present a black screen with a failure message (see chapter §4.4.3). In case of TDS unit failure, a reconfiguration shall occur without sending the trigger reason. The requirement above shall be evaluated in more detail and may be reworked in R7.

The slave Display Managers shall only receive the configuration data from the master Display Manager.

When all configuration data is received and is coherent, the slave Display Manager sends a configuration acknowledgment to the master Display Manager and the configuration to its Layout Engine.

If some configuration data is inconsistent, the slave Display Manager shall inform the master Display Manager. Suitable diagnostic information shall be made available.

Option 1:

If some configuration data is missing, the slave Display Manager shall inform the master Display Manager. Suitable diagnostic information shall be made available.

Option 2:

When the slave Display Managers receives a new configuration to be applied, first, it shall compare the version of its configuration file with the configuration file of the master Display Manager (e.g. Checksum...). In case of differences, it shall enter failure state.

4.4.3 Layout Engine requirements

Before receiving any configuration, the Layout Engine shall display an information to the driver:

At start up, it could be an initialisation message.

When initialisation is finished, a progress indicator could be displayed until the configuration is done.

The Layout Engine shall only receive the configuration data from its Display Manager.

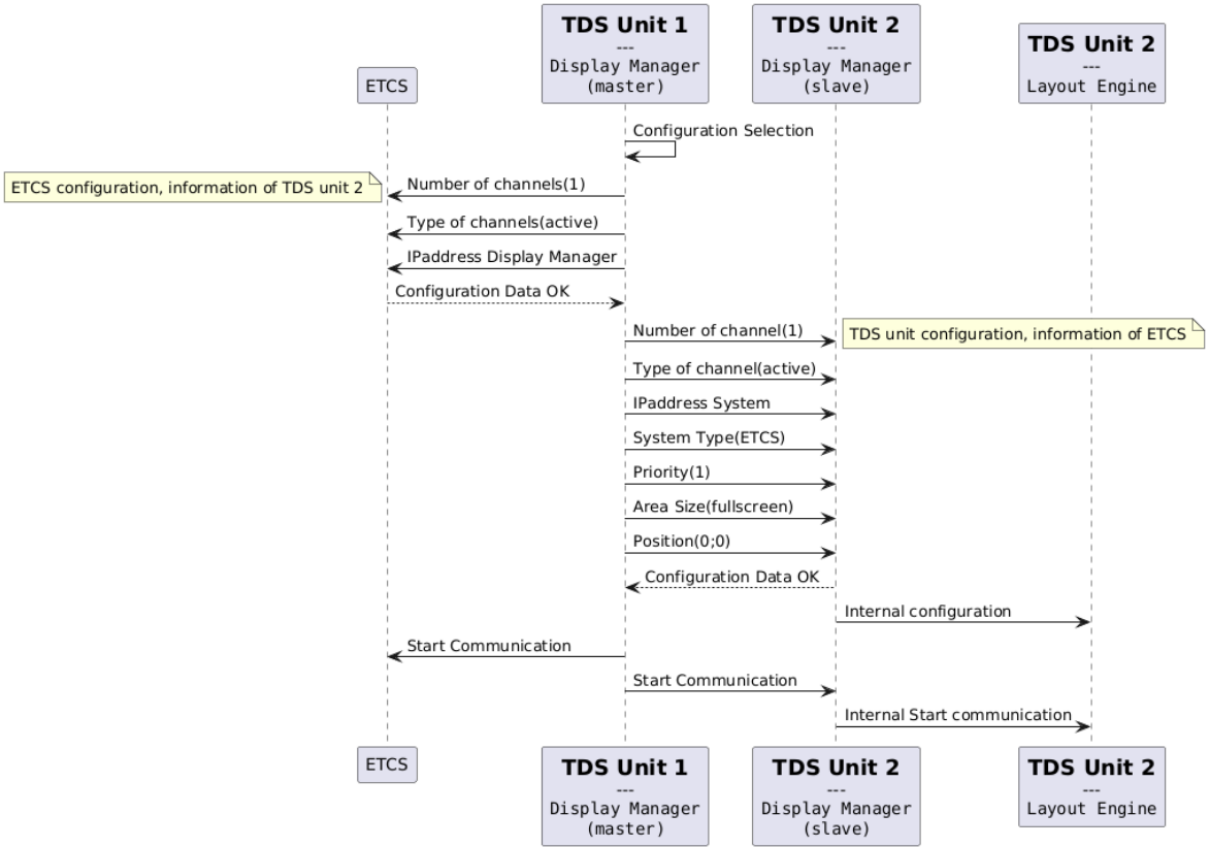
Note: The Layout Engine requires the following data for its configuration: Number of Channels and for each of them the IP address of the System Presentation Logic, the type of the system priority against other systems, the size of the area, the position of the area and its type of channel (active or redundant).

When a trigger reason of a reconfiguration is sent by the master Display Manager (e.g. TDS unit 1 failed), the Layout Engine shall display it.

Note: the trigger reason of the reconfiguration display is under discussion. This topic is linked to the reconfiguration management in case of system or TDS unit failure detection.

4.4.4 Dialog sequence

Option 1: sending all configuration data

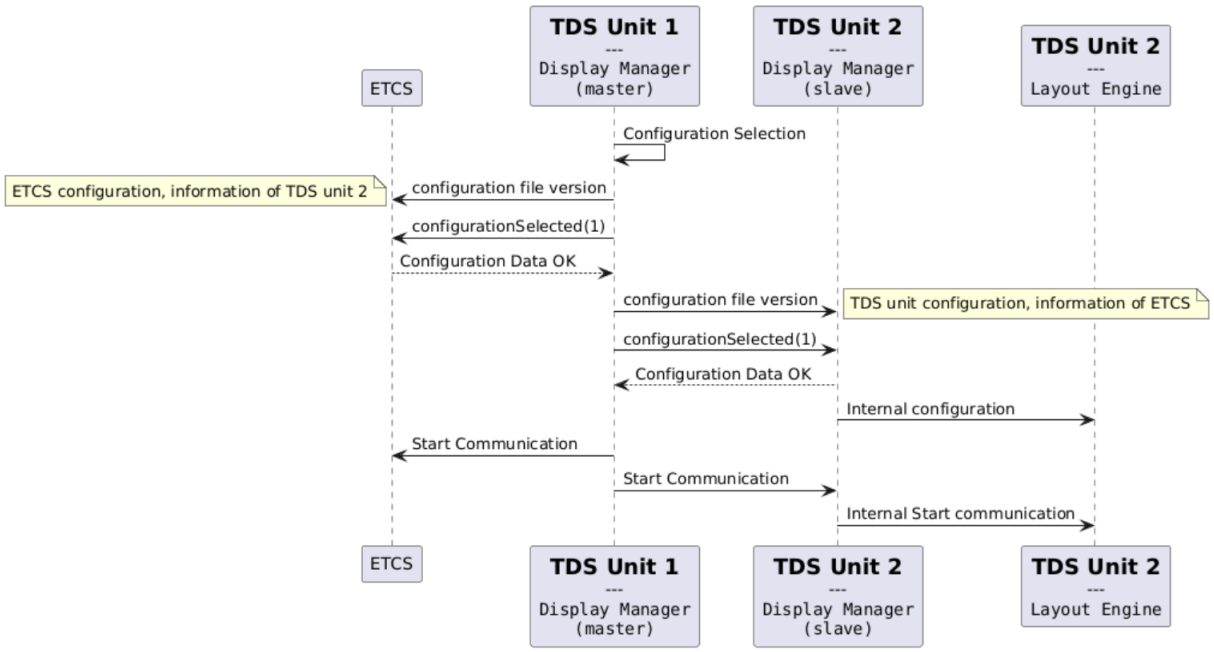


Note: This dialog sequence depicts an example of ETCS configuration with a TDS unit 2 when the master Display Manager (TDS unit 1) sends sporadic messages. The same configuration shall occur on any System Presentation Logic and TDS unit.

PlantUML :

//www.plantuml.com/plantuml/png/bPDBRnCn4CVl-ob6kNGhiLAJ8uYggEa1yI3IXXFYC3YpgILx7Fn0MZuzzZfGrcassroo7lqVzi_odVDeVT2gkcgQfhg2JLnA8G_8tkNPuMa23zlxTZHOItTGs7z2nZrP-5P1_BtThbluojB3SbYdbFI_M1pbSDGl5iTvhT5vijTny7qYVtLIi9fRu1J-ejFyZzYRu1zuBvakfsSrPFcGzHTRIpy3iI0OUEPfLS1fRajSh-7US2VtmQANXcEA8f6-dlCczj7nEUWVSM0w48_8JChLo-kAZITGrFaAib3y7_mA97V6wjmIhUc48P-GU0V9VRvnsnzer8V2omZplEFz1dSxIyv1SHzLDIYQooZMw16-VBWCSVKSatz8hDm_HYPF1vxcadPN49ckBk4KR2Qy8qnjxppfMQOi7NhhjDrvLHihZPM-hvVpzEyi8RJoDzLTKCe9IyGpcuoJ2MTzy-QcTAnUSlCdrjlYjKQ0xCaogl6jJZoUDhtEsATrO2coUXRqYxxf_MM_6FdlY7T1gpy0

Option 2: sending the number of the configuration



Note: This dialog sequence depicts an example of ETCS configuration with a TDS unit 2 when the master Display Manager (TDS unit 1) sends sporadic messages. The same configuration shall occur on any System Presentation Logic and TDS unit.

PlantUML :

//www.plantuml.com/plantuml/png/ZP9FQy904CNl-oc6N5He3deKAe9wA6rf8VPKUXZY95tOJEp-4VpspMOLoLgwEINxU6zcViEiZKLjNQF49CzpCO7txYbBUKIs9cZ7cmAx_QOO25jfZWhFhyXOauPF0G3mkDyMyC7Imhn_-oh-csKNErpyMNRHfmqQIthM2L__r5_SDLYCRM0KdkY-_WkUMsTtN4kcTFNWXc3lQrtNLj2F8ou9-dq6LKJBoLSGAKlOj5p9sccqicKeI57f__xA-jrtYNAGgAGYE94sFiIj9L1KMG71FV0-WEIgrKq8jXLuJ1SmYG_WqoFRXZdfC9tFXEWDUHfkYnRXxJczbiK8IYthRuzvPKYW-XaZoB43nBonTJpvVNGLtTyIdjYIPbIt_ebpAFozTVsQnh4iWpl9byobvmlvSf1V4nzSetu1

4.4.5 Data transmitted from Systems on-board

- Acknowledgment of configuration
  Transmission type: sporadic
- Missing data
  Transmission type: sporadic
- Inconsistent data
  Transmission type: sporadic

4.4.6 Data transmitted from Display Manager

For master Display Manager:

- Start communication
  Transmission type: sporadic
- Trigger reason of reconfiguration (failure)
  Transmission type: sporadic

Option 1:

When all configuration data is transmitted, the following sporadic message shall be considered:

For the Systems Presentation Logic

- Number of Channels (max 2)
- IP address of the Display Manager
- Type of the channel (active or redundant) of the Layout Engine

For the slave Display Manager

- Number of Channels
- IP address of the System Presentation Logic
- Type of the system Presentation Logic
- Priority against other systems (swap management)
- Size of the area allocated to the system Presentation Logic
- The position of the area allocated to the system Presentation Logic
- Type of the channel (active or redundant)

Option 2:

When the System Presentation Logic and slave Display Manager hosts the configuration file, the master Display Manager sends the version of the configuration and the identification number of the configuration to be applied.

- Version of the configuration file
- Transmission type: sporadic
- Identification number of the configuration to be applied
- Transmission type: sporadic

For slave Display Manager:

- Acknowledgment of configuration
- Transmission type: sporadic
- Missing data
- Transmission type: sporadic
- Inconsistent data
- Transmission type: sporadic

4.4.7 Data transmitted from Layout Engine

None

4.4.8 Performance requirements for Systems on-board

When receiving configuration data, the System Presentation Logic shall evaluate the consistency of the data and send the appropriate answer in less than 0.5s.

Rationale : Reconfiguration shall be applied in less than 5s to avoid System Failure (§5.2.7.4 of subset 121). 0.5s to manage a double missing/inconsistency of data and another configuration selection.

4.4.9 Performance requirements for Display Manager

The master Display Manager shall select the configuration in less than 0.4s.

Rationale: Reconfiguration shall be applied in less than 5s to avoid System Failure (§5.2.7.4 of subset 121). 0.4s to manage a double missing/inconsistency of data and another configuration selection.

When the configuration is selected, the master Display Manager shall send the configuration data in less than 0.4s.

Rationale: Reconfiguration shall be applied in less than 5s to avoid System Failure (§5.2.7.4 of subset 121). 0.4s to manage a double missing/inconsistency of data and another configuration selection.

The master Display Manager shall modify the configuration at most every 5s.

Rationale: avoid intermittent reconfiguration

When receiving configuration data, the slave Display Manager shall evaluate the consistency of the data and send the appropriate answer in less than 0.4s.

Rationale: Reconfiguration shall be applied in less than 5s to avoid System Failure (§5.2.7.4 of subset 121). 0.4s to manage a double missing/inconsistency of data and another configuration selection.

4.4.10 Performance requirements for Layout Engine

When receiving configuration data, the Layout Engine shall apply the configuration in less than 3s (worst case).

In nominal case, it is expected that the Layout Engine apply the configuration in 0.5s.

Rationale: 5s of the §5.2.7.4 of subset 121 – 2* configuration exchange (sending configuration > missing data > sending configuration > ack configuration) – start communication message = 5 – 2*(0.4+0.4)-0.4 = 3s.