PD CLC/TR 50542-1:2014

BSI Standards Publication

Railway applications — Driver's cab train display controller (TDC)

Part 1: General architecture

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CLC/TR 50542-1:2014. It supersedes PD CLC/TR 50542:2010 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee GEL/9, Railway Electrotechnical Applications.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2014

ISBN 978 0 580 79030 0
ICS 35.240.60; 45.020; 93.100

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 October 2014.

Amendments issued since publication

Date	Text affected

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CLC/TR 50542-1

October 2014

ICS 35.240.60; 45.020

Supersedes CLC/TR 50542:2010

English Version

Railway applications - Driver's cab train display controller (TDC) - Part 1: General architecture

This Technical Report was approved by CENELEC on 2014-06-30.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword

This document (CLC/TR 50542-1:2014) has been prepared by CLC/TC 9X "Electrical and electronic applications for railways".

This document supersedes CLC/TR 50542:2010.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association.

Introduction

The purpose of this Technical Report is to propose harmonisation for communication between the DMIs and the train systems on the driver's desk.

The need for this harmonisation has grown out of several trends.

One trend is that the rolling stock is being computerised more and more, enabling sophisticated functions within the rolling stock and various subsystems of the train.

Furthermore, the driver's desk of such rolling stock is built around one or several computer screens[1]. These allow the driver to interact with the computerised rolling stock functions. The user interfaces are typically user friendly, featuring e.g. graphics and colours.

In case of degraded situation (screen failure) and with several screens available on the desk, it should be possible to relocate important information to a screen that is still working. This improves operational availability.

Another trend is the harmonisation of onboard signalling safety equipment.

For ERTMS/ETCS onboard, the driver-machine interface is also based on computerised screen(s).

The ERTMS/ETCS defines the concept of Specific Transmission Module STM, allowing the integration of national control-command systems into the ERTMS/ETCS onboard system via a standardised interface.

Since desk space is a limited resource, the STM concept allows national onboard control-command systems to use the driver machine interface resources of ERTMS/ETCS. For this purpose the ERTMS/ETCS driver machine interface allows the driver to interact with any of the installed STMs connected by STMs specification or/and ERTMS/ETCS onboard.

A third trend is that a European market is opened for control-command and TCMS equipments as well as rolling stock.

Traditionally, control-command systems were generally linked to a country, and rolling stock was equipped with one or more national control-command systems. This has effectively limited the rolling stock to operate within a limited number of countries.

The ERTMS/ETCS, in combination with STMs enables cross-border traffic, freeing rolling stock from this barrier.

The combination of the above trends leads to the conclusion that during train operation, TCMS need to have access to the screens on the desk. Furthermore, it is desirable to maintain the advantages of multi-screen installations, allowing the ability to switch to another screen in case of screen failure for information to be still displayed. Thus a certain level of integration and harmonised communication is demanded.

Another motivation for this Technical Report is related to Life Cycle Cost. The recommendations written here simplify the replacement of screens and desk equipment through the lifetime of the vehicle, independent of the supplier.

---

[1] In this Introduction the term "screen" is used in a popular sense, implying e.g. touch screen or other means of input from driver.

This document is the first one of a series of three documents:

CLC/TR 50542-1 *Railway applications — Driver's cab Train Display Controller (TDC) — General architecture*

pr TR50542-2 *Railway applications — Driver's cab Train Display Controller (TDC) — Display systems FIS*

pr TR50542-3 *Railway applications — Driver's cab Train Display Controller (TDC) — Other systems FIS*

1 Scope

In accordance with the ERTMS/ETCS specifications, Subset 121, UIC 612 leaflet, ERA ERTMS-015560 3.3.0 document, EN 50126 and EN 61375 series requirements, this Technical Report describes the Train Display System (TDS) in the driver's cab, and the link between the TDS/TDC and some of its interfaces (Blue box and blue links only):

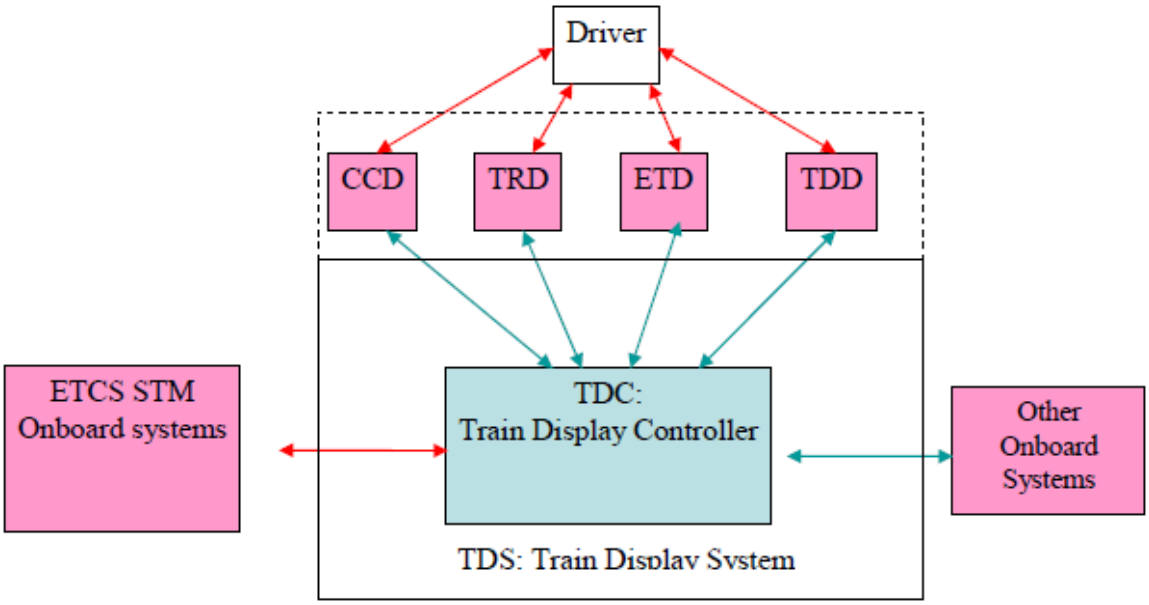


Figure 1 — Terms and definitions

The scope of the Train Display System (TDS) thus includes:

a) Functions, except functions defined in the ETCS Subset 121. These functions describe exchanges between TDC and the connected display systems;

b) Performance allocation (RAMS included as per EN 50126): for each function defined in item a), defining the performances needed and the degraded modes recovering;

c) Needs for certification: description of special requirements to avoid ETCS recertification after other display system modification;

d) Train Display Controller (TDC):

- Redundancy management;
- Architecture;

e) For each system connected (except those defined in ETCS Subset 121): the Functional Interface Specification (FIS).

This Technical Report excludes the following items:

- Communication protocols (e.g. EN 61375 series);
- Ergonomic aspects;
- Interface with ETCS (Subset 121);
- Train functions;
- GSMR EIRENE functions;

- Use of the displays as terminals for maintenance purpose.

2 Normative references

Not applicable.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
Driver Machine Interface
display used to give information to the driver. It contains the hardware and software means to support inform the driver

Note 1 to entry: Information is carried through this interface in the form of visual (light), acoustic and tactile (driver's pressing of buttons).

3.2
button event
pressing or releasing a button

3.3
button
operating element for interaction with the cab display (hard key, soft key, sensitive area)

3.4
cab display
hardware device or system that shows text and/or graphic information to the user

3.5
hard key
physical key with permanent marking and not part of the screen area

Note 1 to entry: This permanent marking may be alpha and/or numeric and/or a symbol.

3.6
indicator
element designed to draw attention to a cab system status which requires a response

3.7
sensitive area
enabled area on a touchscreen on which a physical action is possible in order to give input to the cab display

3.8
soft key
context-dependent key consisting of a combination of a hard key and an associated screen label (text or symbol)

Note 1 to entry: This key is for multifunctional use.

3.9
label
symbol or text indication on or close to an indicator or a button

3.10
Train Display Controller (TDC)
equipment used to manage information between displays on the driver's desk and the train

Note 1 to entry: TDC is called DCU (Display Control Unit) in UIC 612 leaflet series. See bibliography.

3.11
Train Display System (TDS)
TDS consists of the TDC and the related interfaces. Dotted line in Figure 1 — Terms and definitions, represents the limit between driver and the TDS

4 Symbols and abbreviations

CCD	Control Command Display
DMI	Driver Machine Interface
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
ETD	Electronic Timetable Display
EVC	European Vital Computer
FMEA	Failure Mode and Effects Analysis
FIS	Functional Interface Specification
FSV	Function/Task Supervision
HW	Hardware
LCC	Life Cycle Cost
MTBF	Mean Time Between Failures
RAM(S)	Reliability, Availability, Maintainability, (Safety)
SIL	Safety Integrity Level
STM	Specific Transmission Module
SW	Software
TCMS	Train Control and Monitoring System
TDC	Train Display Controller
TDD	Technical and Diagnostic Display

TDS Train Display System

THR Tolerable Hazard Rate

TRD Train Radio Display

5 Functions

5.1 Definitions

5.1.1 General

The functions described in this document are managed by the TDC and its connected systems. The following subclauses give the list of those functions.

The functions below should be implemented in the interface between the TDC and the connected systems. The interface may contain other functions not described in this document.

5.1.2 From TDC to connected systems

Button request: TDC request to connected system to give driver access to the related button.

Button deletion request: TDC request to connected system to remove driver access to the related button.

Indicator request: TDC request to connected system to display the related indicator.

Indicator deletion request: TDC request to connected system to remove the related indicator.

Text message request: TDC request to connected system to display a text message. The request can consist of a reference to a text, or it can include the text itself.

Text message deletion: TDC request to connected system to remove a text message.

Sound on request: TDC request to connected system to start playing acoustic information to the driver.

Sound off request: TDC request to connected system to stop playing acoustic information to the driver.

Data entry request: TDC request to connected system to ask the driver to enter one or several data. The request can contain one or more data values (e.g. default or current values) that can be modified by the driver, and a text identifying the data for the driver.

Data confirmation request: TDC request to connected system to ask the driver to confirm one or several data. The request can contain one or more unconfirmed data values (e.g. recently given by the driver).

Dataview request: TDC request to connected system to display data to the driver.

Dataview deletion request: TDC request to connected system to remove data from the display.

Continuous dataview request: TDC request to connected system to display continuously changing data (e.g. speed, target distance).

Continuous dataview deletion request: TDC request to connected system to remove continuously changing data (e.g. speed, target distance) from the display.

Picture request: TDC request to connected system to display the related picture. The picture can consist of a reference to a pre-loaded picture in the connected system, or a description of the picture itself, or a file.

Picture deletion request: TDC request to connected system to remove the related picture.

Picture upload request: TDC request to connected system to upload a picture in a display memory.

Status Reqest: TDC request status to connected system.

5.1.3 From connected systems to TDC

Button event report: connected system reports button event to TDC.

Ack: connected system reports (driver) acknowledgement to TDC. Ack can be performed by means of acknowledgement of a text message, or by means of pressing a button, depending on the context.

General data input: connected system (train) provides data to TDC.

Data entry reply: connected system reports (driver) data entry to TDC.

Data confirmation reply: connected system reports (driver) confirmation or rejection of displayed data to TDC.

Status answer: connected system reports its status to TDC.

5.1.4 Delays

For each function, a maximum delay is recommended (Tables 1 and 2). The following delays are defined for the TDS (the time includes all the delays between displays and TDC external boundary, including displays and TDC inner delays).

Table 1 - Delays from TDC boundary to display

from TDC to display	Delay (ms)
button request	500
indicator request	250
text message request	500
text message deletion	1000
sound on request	250
sound off request	500
data entry request	500
data confirmation request	500
dataview request	1000
continuous dataview request	250
picture request	500
picture deletion request	500
status request	250

Table 2 - Delays from connected system to TDC boundary

from connected system to TDC	Delay (ms)
button event report	250
ack	250
general data input (from starting of data)	1000
data entry reply	1000
data confirmation reply	1000
status answer	250

NOTE For special data, the delays given in the previous tables can be exceeded.

5.2 Function analysis

5.2.1 Function failure modes and failure effects

5.2.1.1 General

The TDC is considered as category 2 system, according to EN 50159, due to the interaction with train systems.

TDC should guarantee separation of safety data and non safety data as explained in EN 50159:2010, 7.2.2.

The failures defined for the TDC functions are defined in EN 50159:2010, 7.4.2, Table 1:

— REP: repetition

— DEL: deletion

— INS: insertion

— RES: re-sequencing

— COR: corruption

— DYD: delayed

The details of the relevant failure effects are given in the documents *Railway applications — Driver's cab Train Display Controller (TDC) — Part 2: Display systems FIS* and *Railway applications — Driver's cab Train Display Controller (TDC) — Part 3: Other train systems FIS*. Those documents list the consequences of each of those effects on the interfaces.

5.2.1.2 General protection techniques

The reference for general protection techniques is EN 50159:2010, 7.4.

Applying Table B.1 of EN 50159:2010 to the TDC system leads to define it as a category 2 system. As a consequence, Table B.2 of EN 50159:2010 induces not to consider the "MASQUERADE" as a threat (failure mode). "CRYPTOGRAPHIC TECHNIQUES" and "IDENTIFICATION PROCEDURE" for defences are not considered because it is assumed that protection against outside attacks is made by other train systems.

If the customer or the supplier considers it as essential, it can be implemented at any convenient level, by mutual agreement.

It is recommended to use for the following threats the corresponding mitigation, implemented in low level communication protocols (the definition of these protocols is out of the scope of this Technical Report):

— REP: the protocol should indicate that the receiver's buffer or memory is going to be full;

— INS, RES, COR: data consistency checking. The protocol(s) should manage all the error conditions between the external systems and the TDC;

— DEL, DYD: repeating until timeout.

5.2.2 Failure modes and effects

5.2.2.1 List of failures

The general description of failure effects and degraded modes at TDC interfaces are listed in the following subclauses.

5.2.2.2 From TDC to external systems

5.2.2.2.1 Failure modes

The following table gives the failure modes, depending on each function (no = that failure mode of the function has no functional effect).

Table 3 — Failure modes, part 1

Function	REP	DEL	INS	RES	COR	DYD
Button Request	no	no	yes	yes	yes	yes
Button deletion request	no	no	no	no	yes	yes
Indicator Request	no	yes	yes	yes	yes	yes
Indicator deletion request	no	yes	yes	yes	yes	yes
Text Message Request	no	no	no	no	yes	no
Text Message Deletion	no	yes	no	no	yes	no
Sound on Request	no	yes	yes	yes	yes	yes
Sound off Request	no	yes	yes	yes	yes	yes
Data Entry Request	no	no	yes	yes	yes	yes
Data Confirmation Request	no	no	yes	yes	yes	yes
Dataview request	no	no	no	no	no	no
Dataview deletion request	no	yes	yes	no	yes	no
Continuous Dataview Request	no	yes	yes	yes	yes	yes
Continuous Dataview deletion Request	no	yes	yes	yes	yes	yes
Picture request	no	yes	yes	yes	yes	yes
Picture deletion request	no	yes	yes	yes	yes	yes
Picture upload request	yes	yes	yes	yes	yes	yes
File upload request	yes	yes	yes	yes	yes	yes
Status request	no	no	no	no	no	no

Assumptions:

— text messages deletion and sounds are considered as non safety related;

— acknowledgement request is considered as a text message request.

5.2.2.2.2 Failure effects

The following subclauses give the consequences of each failure mode in Table 3.

5.2.2.2.2.1 Button Request

— INS, RES, COR, DYD: wrong button request, wrong train data confirmation.

5.2.2.2.2.2 Button deletion Request

— COR: a useful button cannot be accessed by the driver any more.

— DYD: depending on the context, can give the driver the ability to perform a dangerous action.

5.2.2.2.2.3 Indicator Request

— DEL, INS, RES, COR, DYD: wrong mode or level indication, missing indication.

5.2.2.2.2.4 Indicator deletion Request

— DEL, INS, RES, COR, DYD: wrong mode or level indication, missing indication.

5.2.2.2.2.5 Text Message Request

— COR: display of wrong text message (can lead to a hazard especially for acknowledgement request).

5.2.2.2.2.6 Text Message Deletion

— DEL: the previous text message is still displayed, and a new one at the same location could be not understandable.

— COR: delete the wrong text message.

5.2.2.2.2.7 Sound on Request

— DEL: no acoustic information given to the driver.

— INS, RES, COR: wrong acoustic information given to the driver.

— DYD: acoustic information given too late to the driver.

5.2.2.2.2.8 Sound off Request

— DEL: acoustic information does not stop.

— INS, RES, COR: wrong ending of the acoustic information.

— DYD: too long acoustic information duration. It can overlap a new acoustic information.

5.2.2.2.2.9 Data Entry Request

— INS, RES, COR, DYD: could hide train and track information.

5.2.2.2.2.10 Data Confirmation Request

— INS, RES, COR, DYD: same as Data Entry Request.

5.2.2.2.2.11 Dataview deletion request

— DEL; keep showing a data to the driver. That data can be no more valid, or system could need to display a new data in the area already occupied by the old data.

— INS, COR; wrong ending of data display.

5.2.2.2.2.12 Continuous Dataview Request

— DEL, INS, RES, COR, DYD: wrong value of train speed or target distance, brake pressure, line voltage etc.

5.2.2.2.2.13 Continuous Dataview deletion Request

— DEL, INS, RES, COR, DYD: non valid data can still be displayed.

5.2.2.2.2.14 Picture request

— DEL, INS, RES, COR, DYD: wrong picture describing train status, etc, or request to display non existing picture.

5.2.2.2.2.15 Picture deletion request

— DEL, INS, RES, COR, DYD: non valid picture describing train status can be displayed.

5.2.2.2.2.16 Picture upload request

— REP: risk to completely filling the memory of a DMI. The control program has to check the request to avoid that threat.

— DEL, DYD: no picture available when TDC asks to display it.

— INS, COR: see REP, or asking to upload a non existing picture.

— RES: for a multiple file picture, incorrect picture can be displayed (wrong picture reconstruction).

5.2.2.2.2.17 File upload request

— REP, DEL, INS, RES, COR, DYD: wrong new executable code on the DMI.

5.2.2.3 From external systems to TDC

5.2.2.3.1 Failure modes

The following table gives the failure modes, depending on each function (no = that failure mode of the function has no functional effect).

Table 4 — Failure modes, part 2

Function	REP	DEL	INS	RES	COR	DYD
Button Event Report	no	no	yes	yes	yes	yes
Ack	no	no	yes	yes	yes	yes
General data input	no	no	no	no	no	no
Data Entry Reply	no	no	yes	yes	yes	yes
Data Confirmation Reply	no	no	yes	yes	yes	yes
Status answer	no	yes	yes	no	yes	yes

5.2.2.3.2 Failure effects

The following subclauses give the consequences of each failure mode in Table 4.

5.2.2.3.2.1 Button Event Report

— INS, RES, COR, DYD: wrong driver request, or wrong train data confirmation.

5.2.2.3.2.2 Ack

— INS, RES, COR, DYD: incorrect answer from driver.

5.2.2.3.2.3 General data input

Checking the General data input function is depending on the application, and not on the interface level.

5.2.2.3.2.4 Data Entry Reply

— INS, RES, COR, DYD: wrong train data, wrong additional data, wrong command received (e.g. voltage selection).

5.2.2.3.2.5 Data Confirmation Reply

— INS, RES, COR, DYD: same as Data Entry Reply.

5.2.2.3.2.6 Status Answer

— DEL: connected system is considered as out of service by TDC.

— INS, COR, DYD: TDC receives wrong status.

6 Safety targets

The TDC is a part of the TDS system. It uses information coming from the whole train. For instance, some data (alarms) are sent by other train systems to be displayed through TDC, needing to respect a given SIL or THR. Thus, safety studies respecting EN 50126 should be done to demonstrate that the TDC does not degrade the global safety level for each information.

In order to fulfil the safety targets induced by train data, it is recommended that the TDC almost uses the design rules given in Table 5.

Table 5 — Design rules recommendations

Ref	Design rules
DR1	Hardware Design according to EN 50155.
DR2	FMEA study with stuck-at fault model and calculation of hazard rate and/or probability of failure on demand.
DR3	Software development conformance to EN 50128 is highly recommended.
DR4	A FSV which is itself supervised by a hardware watchdog can be implemented. The FSV can start and supervise the timely execution of relevant tasks.
DR5	If the cyclic function of the TDC supervised by the FSV will be interrupted (e.g. caused by a malfunction of hardware or the FSV has stopped triggering the hardware watchdog) the TDC should be switched off through the hardware watchdog.
DR6	All information given to the driver should be based on actual input data transmitted via the TDC to the DMI.
DR7	A vital element is displayed on the screen in order to show to the driver that the DMI is still working. This vital element is also controlled via the FSV.
DR8	TDC requests to DMI are valid only during defined time slots.

7 Certification

This clause addresses the certification process by giving guidelines to minimise the effort and cost for ETCS recertification after TDC or DMI modification.

One way to minimise effort and cost is to limit the interactions between ETCS information and the other systems on the train information. In order to guarantee that ETCS information is not corrupted by other train information:

— TDC should use in nominal mode a dedicated channel for ETCS information to and from CCD;

— TDC should guarantee that no information of any other DMI can be displayed on CCD in any degraded mode of other DMIs;

— TDC software development and implementation should guarantee independence and modularity between ETCS information and the other DMIs information.

NOTE These guidelines allow using UIC 612 redundancy concepts. The recertifications when not following these guidelines are more complex and more expensive.

8 TDC general description

8.1 General

The target of this clause is to give general recommendations in order to help developing TDC answering to the following needs:

— give requirements for a second source for TDC and exchanging a device connected to the TDC without upgrading the TDC configuration;

— lower the maintenance cost of the TDC during its life cycle

— support the safety targets defined in Clause 6 studies.

The following subclauses describe the recommendations linked to each of the previous items. As a conclusion, some TDC architecture examples are shown.

8.2 Information destination

The external systems do not define the display destination of information. Sending information to the right display should be a task of the TDC.

TDC should only be a switch for information, the analysis of messages in order to display information is performed by the DMI equipment.

TDC should verify each DMI software level through "Status request" and "Status answer". Any DMI with a wrong status should be switched off, and TDS should enter a degraded mode, using DMI redundancy (see 8.6).

8.3 Second source

In order to help customers to use displays or TDCs from multiple suppliers, the TDS design should consider the following points:

a) TDC and its interfaces should comply with these documents and recommendation:

— *Railway applications — Driver's cab Train Display Controller (TDC) — Part 2: Display systems FIS*

— *Railway applications — Driver's cab Train Display Controller (TDC) — Part 3: Other train systems FIS*

— Following the ERA layout (see Bibliography: ERA_ERTMS_015560) for the total display area: minimum size 180 mm x 135 mm (w x h). Minimum resolution: 640 x 480 pixels. 24 bits RGB colors.

NOTE UIC 612-01 and prEN 16186-3 demand a screen size of 210 mm × 155 mm (w × h).

b) Following descriptions should be obtained from the suppliers as a minimum:

1) Descriptions of the TDC electrical interfaces including:

— Type of signals: electrical level, bias level,

— Type of network(s): protocols used, including the options used in the standards.

2) Descriptions of the TDC mechanical interfaces including:

— Display layout.

— Display mounting description (e.g. drawings).

— Connectors' description. When the connectors comply with a standard, the options used should be mentioned.

— TDC physical dimensions and mounting description (e.g. drawings).

3) Behavioural description of TDC and DMI

— High level document(s) (independent from technology) describing exchanges between TDC and DMI and other systems at application level (e.g. UML description). That description should permit to develop the applications on any new TDC or DMI.

8.4 TDC maintenance and LCC

— In order to reduce cost, hardware and software development of the TDC and DMI should follow the EN 50155 and EN 50128 principles, which tend to simplify the maintenance actions, from changing the lowest replaceable unit to the complete re-design of the TDC or DMI.

— The principles written in 8.3 are a key point to minimise the LCC of TDC and DMI system.

8.5 Safety and reliability targets

— Customer and supplier should agree on the method and result to calculate the expected TDC and DMI MTBF before the beginning of the studies. For example: see UIC 612-01.

— A single TDC hardware failure should not have any consequence on communication (e.g. the service should be maintained by the TDC in case of a single failure). Further using of this TDC after a single hardware failure is out of the scope of this Technical Report.

— TDC should manage some redundancies to achieve the target above:

1) TDC manages the information transmission to the displays in order to overcome any display failure. See 8.6.

2) Power supply: systems transforming train battery voltage to the voltage needed by the TDC should be doubled.

3) Interfaces TDC – DMI: it should not be necessary to double the interface between TDC and any display, because of information transmission management described above.

4) Interfaces TDC – Other systems and TDC – Subset 121: the performances for these interfaces are given by the respective external systems.

— There should be an indication for maintenance purposes (remotely and/or locally) that a redundancy has been activated.

— In order to improve ETCS availability, TDC uses a special process for CCD redundancy management when CCD is out of service: ETCS information is displayed on another DMI. TDD is then considered as in degraded mode, and TDC sends TDD information to the DMI defined in TDC database for TDD degraded mode.

8.6 TDC DMI redundancy management

It is recommended that TDC redundancy management follows the principles hereafter (see UIC 612-01, Clause 5 – Redundancy concept description):

— Redundancy should be provided by means of the identical interface and functional design of CCD, TDD, TRD, and ETD as well as the possible transfer of functions and screen contents/display images of CCD, TDD, TRD, and ETD to one of the other display unit.

— In redundancy mode two display images should be merged into one (in maximum redundancy mode two display images are assumed to be lost). It should not be permitted to use a reduced image for ETD.

One possible solution to fulfil these items is the use of a database implemented in the TDC describing information destination. For each information, that database should give the DMI destination in normal mode and the DMI destination for degraded mode (when the normal DMI destination is turned off).

8.7 TDC recommended architecture

8.7.1 Constraints

The recommendations of this Technical Report lead to the TDC architecture proposals in 8.7.2.

The recommended logical interfaces are at least:

— 4 DMIs;

— Subset 121 interface;

— Other systems: local network (MVB, Ethernet, CAN bus…), serial lines (synchronous/asynchronous), no direct logical or analogue signals;

— Service interface (e.g. USB - used to update DMIs software), for maintenance purpose only. For example new versions of executable software can be uploaded into DMI through the TDC service interface.

8.7.2 TDC architecture examples

The following figures are two possible examples for the TDC architecture, able to fulfil the recommendations of this Technical Report. They are functionally equivalent but not designed on the same SW and HW principles. Any other architecture functionally equivalent could be used.

The examples of Figure 2 and Figure 3 are based on the following complementary recommendations:

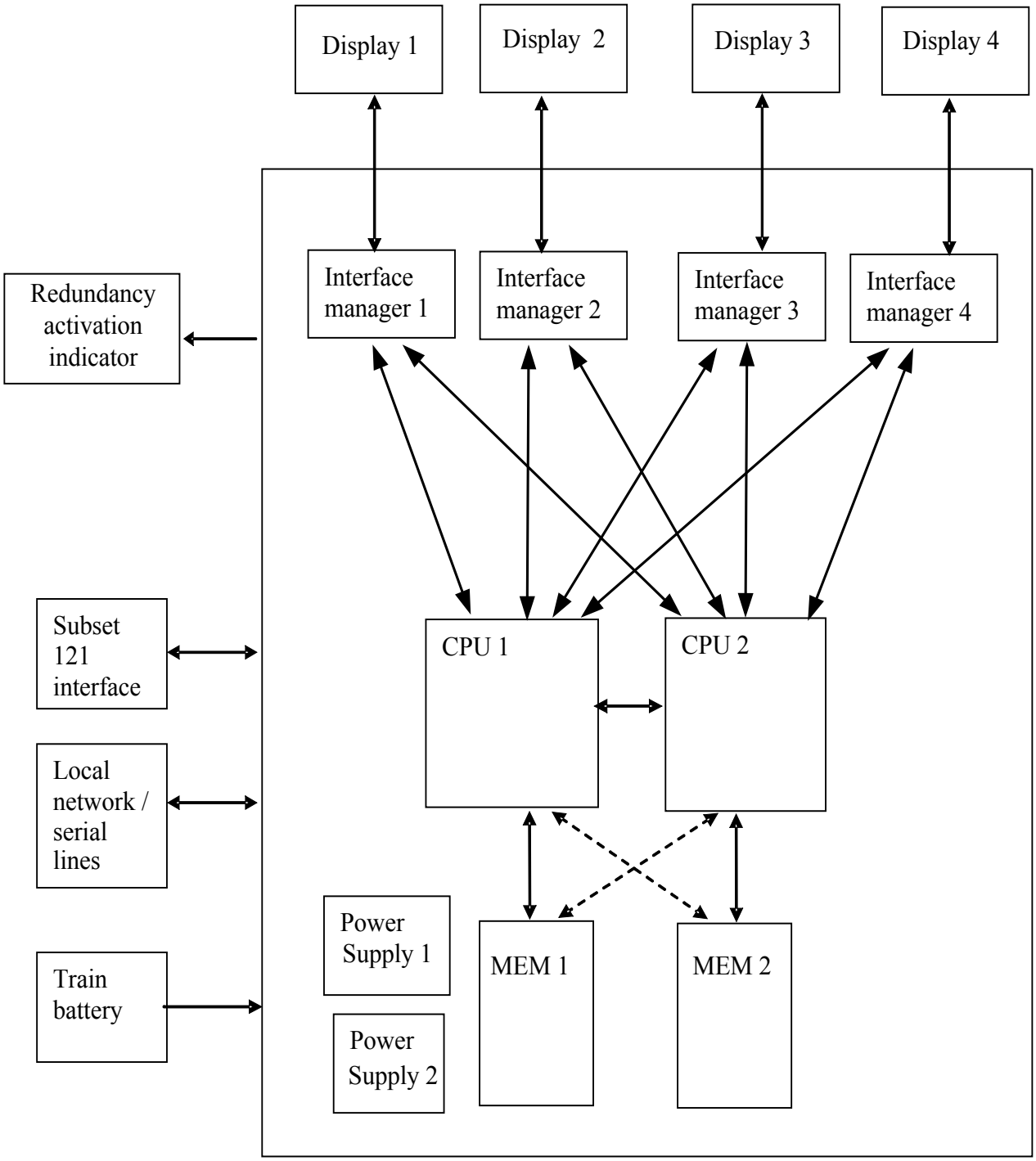
— Processing Unit/CPU: in order to keep communication in case of Processing Unit/CPU failure, the recommended action is to use two Processing Units/CPUs. If one Processing Unit/CPU fails, the other one takes over;

— Memory: at least one memory linked with each Processing Unit/CPU is recommended;

— Internal interfaces:

  — In Figure 2 each CPU has an interface internal to the TDC. For each internal interface, an interface manager switches the active internal interface to the respective external interface;

  — In Figure 3 the LAN is the link between Processing Units and DMIs.



Key

◄- - - - - ► Recommended link

Figure 2 — TDC architecture example 1

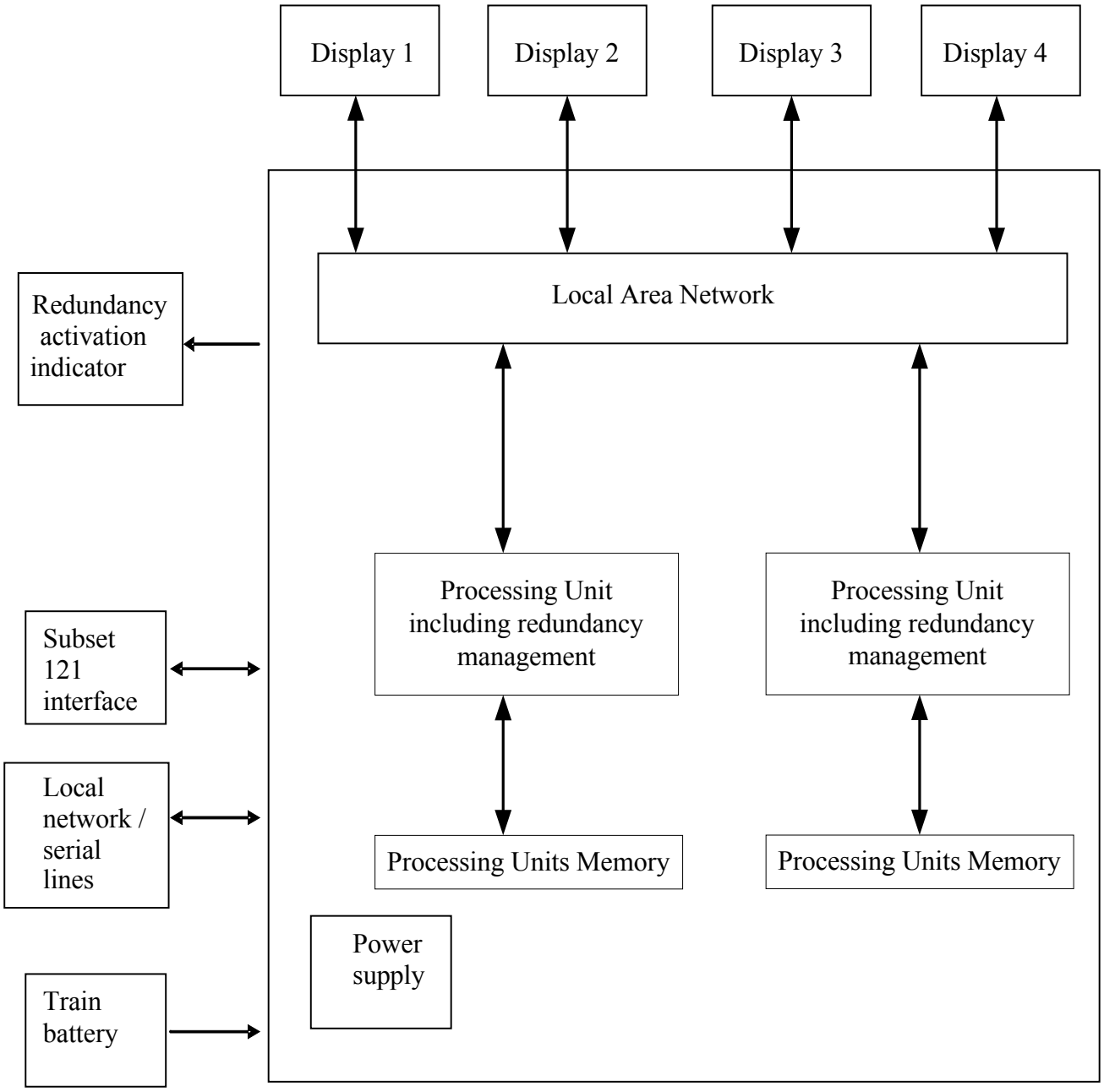


Figure 3 — TDC architecture example 2

Annex A
(informative)

Actions

A.1 Introduction

For some functions, this annex explains what action can be taken when a degraded mode is denoted.

Five actions are defined in the following table.

Action	Description	Remarks
1	Use of a second DMI	Can be switched on automatically or manually Exclusive work vs. principal DMI (one information present on only one DMI at the same time) Second DMI ergonomics and functionalities out of the scope (e.g. some information already displayed on the 2nd DMI should still be displayed)
2	Check of data consistency	Example of mechanism: the DMI sends data that are sent back by the EVC and displayed by the DMI.
3	Safe ack	Mechanism : no detailed mechanism defined
4	Cutting off the DMI	The DMI has to analyse: - that the data received on the medium are updated, complete and correct (e.g. a Cyclic Redundancy Code and a time related information given with the data and checked by the DMI). - its own functional status, including studying the problem of frozen image. If any problem, it switches off itself (a second DMI could be automatic or manually switched on. See action 1).
5	Repeat until timeout	

A.2 From TDC to connected systems

The detailed actions that can be done for each function are denoted in the following table.

Table A.1 — Actions for functions from TDC to connected systems

Function	Failure mode	Actions or comment
Button Request	INS, RES, COR	check data consistency by external receiver
Button Request	DYD	5
Button deletion request	COR	2
Button deletion request	DYD	5
Indicator Request	DEL, DYD	5
Indicator Request	INS, RES, COR,	2
Indicator deletion request	DEL, DYD	5
Indicator Request	INS, RES, COR,	2
Text Message Request	COR	2
Text Message Deletion	DEL	5
Text Message Deletion	COR	2
Sound on Request	DEL, DYD	5
Sound on Request	INS, RES, COR	2
Sound off Request	DEL, DYD	5
Sound off Request	INS, RES, COR	2

Bibliography

EN 50126/CLC/TR 50126 series, *Railway applications -— The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*

EN 50128, *Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems*

EN 50129, *Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling*

EN 50155, *Railway applications — Electronic equipment used on rolling stock*

EN 50159:2010, *Railway applications -— Communication, signalling and processing systems — Safety-related communication in transmission systems*

prEN 16186-3 *Railway Applications — Driver's Cab — Part 3: Design of Displays*

UIC 612-01 *Display System in driver cabs (DDS): General Requirements, Set Up and Technical Specifications*

ERA_ERTMS_015560 3.3.0 01/13/12 ETCS Driver Machine Interface

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™