



BSI Standards Publication

Railway applications — Communication means between safety equipment and man-machine interfaces (MMI)

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

raising standards worldwide™

Full document details: PD CLC/TR 50542:2010

National foreword

This Published Document is the UK implementation of CLC/TR 50542:2010.

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.

© BSI 2010

ISBN 978 0 580 69150 8

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 March 2010.

Amendments issued since publication

Amd. No.	Date	Text affected
----------	------	---------------

TECHNICAL REPORT
RAPPORT TECHNIQUE
TECHNISCHER BERICHT

CLC/TR 50542

February 2010

ICS 35.240.60, 45.020, 93.100

English version

**Railway applications -
Communication means between safety equipment
and man-machine interfaces (MMI)**

Applications ferroviaires -
Moyens de communication entre
l'équipement de sécurité et l'interface
homme-machine (IHM)

This Technical Report was approved by CENELEC on 2009-12-18.

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

CENELEC

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

Central Secretariat: Avenue Marnix 17, B - 1000 Brussels

© 2010 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Ref. No. CLC/TR 50542:2010 E

AVA Documents
Document Sharing Hub

Foreword

This Technical Report was prepared by the Technical Committee CENELEC TC 9X, Electrical and electronic applications for railways.

It was circulated for voting in accordance with the Internal Regulations, Part 2, Subclause 11.4.3.3 (simple majority).

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

This Technical Report has been prepared under a Mandate M/334 given to CENELEC by the European Commission and the European Free Trade Association.

Contents

1	Scope	8
2	Normative references.....	9
3	Terms and definitions	10
4	Symbols and abbreviations.....	12
5	Devices / modules of the systems	13
6	DMI functions for ERTMS/ETCS.....	13
6.1	Concepts	13
6.2	Delays	15
6.3	Object Controls analysis	15
7	DMI Safety targets	24
7.1	Difficulties to assign THR/SIL to ETCS Display display functions	24
7.2	Safety approach for DMI and communication system	27
8	Communication system requirements	28
8.1	Strategy	29
8.2	Connection to the DMI	29
8.3	Object Control Layer	30
8.4	Safety Layers	30
8.5	Implicit Layer	30
8.6	Objects Controls data format	31
8.7	Safe Time Layer	58
8.8	Safe Link Layer	81
8.9	Implicit Layer	101
8.10	Performances of HTI interface	102
8.11	RAM requirements on HTI interface	104
8.12	LCC requirements on HTI interface	105
Annex A (informative) Actions		106
Annex B (informative) Design rules		113
B.1	List of design rules	113
B.2	Function-specific rules	114
Annex C (informative) Services provided by the Safe Time Layer		115
Annex D (informative) Definition of notation.....		116
D.1	State machine	116
D.2	Sequence chart	117
Annex E (informative) Safety Link Layer telegram sequences examples		118
E.1	Telegram Sequences (SL 4 and SL 2 Point-to-Point Connections)	118
E.2	Telegram Sequences (SL 0 Point-to-Point logical connections).....	124
Annex F (normative) CRC Generator Polynomial and Application Rules.....		127
F.1	General.....	127
Annex G (informative) Calculation of the CRC Length.....		130
G.1	Safety target for the transmission (EN 50129).....	130
G.2	Calculation of the CRC length (SIL 2).....	133
Annex H (informative) Services provided by the Safe link layer.....		135
Bibliography		136

Figures

Figure 1 - Systems concerned by this document	8
Figure 2— Terms and definitions	10
Figure 3 — Fault tree model.....	25
Figure 4 — Methodology for THR allocations.....	27
Figure 5 — Communication system layers	29
Figure 6 — Data encapsulation	30
Figure 7 — Example for network architecture	60
Figure 8 — Reference Time Transfert.....	61
Figure 9 — Time stamp concepts.....	62
Figure 10 — Architecture.....	63
Figure 11 — Start up sequence.....	64
Figure 12 — Time stamping	69
Figure 13 — Reference clock transfer.....	71
Figure 14 — Reference Clock state machine.....	72
Figure 15 — Local Clock state machine.....	74
Figure 16 — Logical Connection Master connection state machine	76
Figure 17 — Logical Connection Slave state machine.....	78
Figure 18 — Content of Safe Link Layer	82
Figure 19 — General structure of a telegram	82
Figure 20 — Supervision of Idle Telegrams	92
Figure 21 — Example of the data flow for multicast messages	98
Figure D.1 — State machine notations.....	116
Figure D.2 — Sequence chart notation	117
Figure E.1 — Telegram sequence to establish a SL 4 logical connection (connection set-up and authentication)	121
Figure E.2 — Telegram sequence of a faulty authentication due to an authentication telegram error.....	122
Figure E.3 — Telegram sequence to establish a SL 2 logical connection (connection set-up and authentication)	123
Figure E.4 — Telegram sequence for data exchange (SL 4 logical connection).....	124
Figure E.5 — Telegram sequence to establish a SL 0 logical connection (connection set-up)	125
Figure E.6 — Telegram sequence for data exchange (SL 0 logical connection).....	126
Figure G.1 — Probability of undetected failures.....	132

Tables

Table 1 — Object Controls from HS to DMI	13
Table 2 — Object Controls from DMI to HS	14
Table 3 — OC definitions, part 1	14
Table 4 — OC definitions, part 2	14
Table 5 — Delays from HS to DMI	15
Table 6 — Delays from DMI to HS	15
Table 7 — Exchanges from driver to HS.....	16
Table 8 — Output exchanges from HS to driver	18
Table 9 — Failure modes, part 1	21
Table 10 — Failure modes, part 2	22
Table 11 — Defence techniques, part 1	23

Table 12 — Defence techniques, part 2	24
Table 13 — Human behaviour	26
Table 14 — THR allocation example	28
Table 15 — Packet structure	32
Table 16 — Message structure	33
Table 17 — Indicator Request	34
Table 18 — Button Request	35
Table 19 — Text Message Request	35
Table 20 — 8.6.5.4 Text Message Deletion	36
Table 21 — Sound Request	36
Table 22 — Data Entry Request	37
Table 23 — Data Confirmation Request	38
Table 24 — Dataview request	39
Table 25 — Continuous Dataview Request	40
Table 26 — Continuous Dataview Request for Announcement	40
Table 27 — Button Event Report	41
Table 28 — Text Ack	41
Table 29 — Data Entry Reply	42
Table 30 — Data Confirmation Reply	42
Table 31 — Packets numbering	43
Table 32 — Configuration Data	65
Table 33 — Disconnect Reason	65
Table 34 — Command number	66
Table 35 — Application Data	66
Table 36 — Sync and Reference Time	67
Table 37 — Ready to Run	67
Table 38 — Run	68
Table 39 — Safe Time Layer Startup for multicast	68
Table 40 — Constants for Safe Time Layer	80
Table 41 — Detailed protocol structure of a telegram	83
Table 42 — Structure of the Implicit Data	85
Table 43 — Connect Request telegram	86
Table 44 — Connect Confirm telegram	87
Table 45 — Authentication telegram	88
Table 46 — Authentication acknowledgement	88
Table 47 — Disconnect telegram	91
Table 48 — Idle telegram	93
Table 49 — Data telegram Table	93
Table 50 — Transition table, states	94
Table 51 — Transition table, events	94
Table 52 — Transition tables, actions (SL4 and SL2)	95
Table 53 — Transitions (SL2 and SL4 connections)	96
Table 54 — Transition table, actions (SL0)	97
Table 55 — Transitions (SL0)	97
Table 56 — Implicit Data format	99

Table 57 — Multicast example	100
Table 58 — Multicast telegram format.....	100
Table 59 — Structure of the implicit data telegram	101
Table 60 — List of services of lower layers services at HTI interface	103
Table 61 — Performances of lower layers services at HTI interface	104
Table A.1	106
Table A.2 — Actions for in-functions	107
Table A.3 — Actions for out-functions	110
Table B.1 — Design rules.....	113
Table B.2	114
Table C.1	115
Table E.1 — Example of CRC computation for SL4	119
Table E.2 — Example of CRC computation for SL 2	120
Table G.1	130
Table H.1 — Service provided by the Safe Link Layer.....	135

Introduction

The purpose of this Technical Report is to show how to harmonise the communication means between onboard signalling safety systems and the driver-machine interface in the driver's desk.

The need for this standardisation 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.

Further, 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, feature 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. The ERTMS/ETCS as defined by the directive 96/48/EC and the related Control-Command TSI defines a control-command signalling system on European level.

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 existing national control-command systems to be modified into an STM. This allows integration between national control-command systems and ERTMS/ETCS onboard equipment via a standardised interface (FFFIS STM).

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. This is one aspect of the integration of national equipment with ERTMS/ETCS onboard.

Therefore the ERTMS/ETCS driver machine interface allows the driver to interact with any of the installed STMs or/and ERTMS/ETCS onboard. The selection of the active system is a responsibility of ERTMS/ETCS.

A third trend is that a European market is opened for control-command equipment 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 signalling safety system. This has effectively limited the rolling stock to operate within a limited number of countries.

The ERTMS/ETCS, in combination with STMs makes available onboard signalling safety equipment that enables cross-border traffic, freeing rolling stock from this barrier.

There are indeed other barriers hindering cross-border traffic, being operational, technical or administrative. They are gradually being overcome. One example is the interoperable voice radio, EIRENE, based on GSM-R.

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.

The combination of the above trends leads to the conclusion that during train operation, ERTMS/ETCS must have access to one of the screens in the desk. Further, it is desirable to maintain the advantages of multi-screen installations created by train system providers, allowing the ability to change screen for ERTMS/ETCS in case of screen failure. Thus a certain level of integration and harmonised communication is called for.

Another motivation for this Technical Report is related to Life Cycle Cost. The interface shown here helps replacement of screen and desk equipment through the lifetime of the vehicle, whatever is the supplier.

1 Scope

This Technical Report defines, in accordance with the ERTMS/ETCS requirements:

- a) for each DMI function to be exchanged to and from the driver, including ETCS, STM:
 - . performances needed;
 - . degraded modes recovering;
- b) DMI Safety targets;
- c) communication system requirements:
 - . real-time capability;
 - . performances (bandwidth, etc.);
 - . expansion capability;
 - . RAMS;
 - . applicable standards;
 - . degraded modes;
 - . degraded modes management;
 - . interface with other systems;
 - . LCC requirements.

Each item in the list above corresponds to one chapter of the present document.

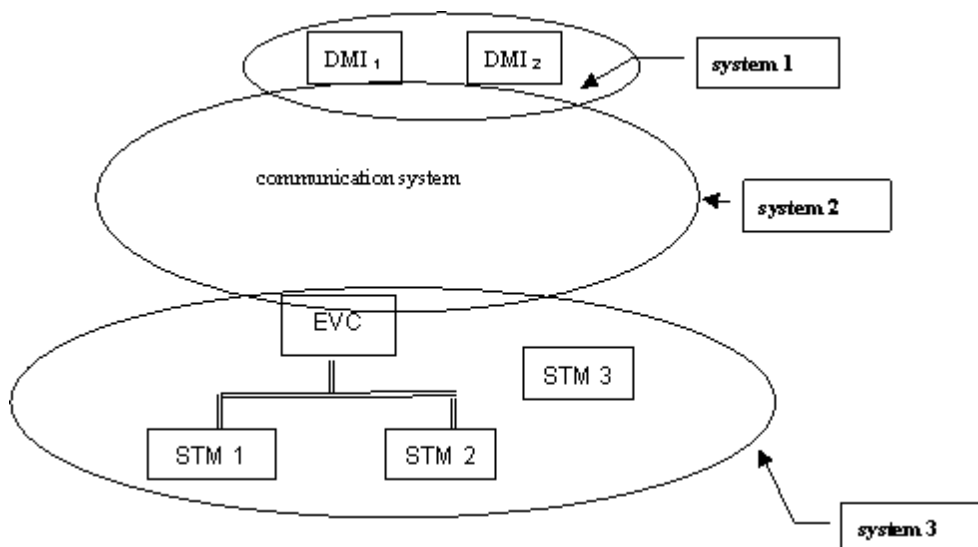


Figure 1 - Systems concerned by this document

This Technical Report does not cover the following items:

- . Train functions;
- . STM "Separate DMI" as defined in document [1] regarding DMI equipment that is part of the STM itself;
- . GSMR EIRENE functions;
- . Ergonomics;
- . Use of the ETCS DMI as a terminal server for maintenance purpose.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

96/48/EC, *Council Directive 96/48/EC of 23 July 1996 on the interoperability of the trans-European high-speed rail system*

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 50159-1, *Railway applications - Communication, signalling and processing systems - Part 1: Safety-related communication in closed transmission systems*

EN 50159-2:2001; *Railway applications - Communication, signalling and processing systems - Part 2: Safety-related communication in open transmission systems*

CLC/TS 50459-2, *Railway applications - Communication, signalling and processing systems - European Rail Traffic Management System - Driver-Machine Interface - Part 2: Ergonomic arrangements of ERTMS/ETCS information*

CLC/TS 50459-6, *Railway applications - Communication, signalling and processing systems - European Rail Traffic Management System - Driver-Machine Interface - Part 6: Audible information*

3 Terms and definitions

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

Figure 2 is given to illustrate the relationship between some definitions.

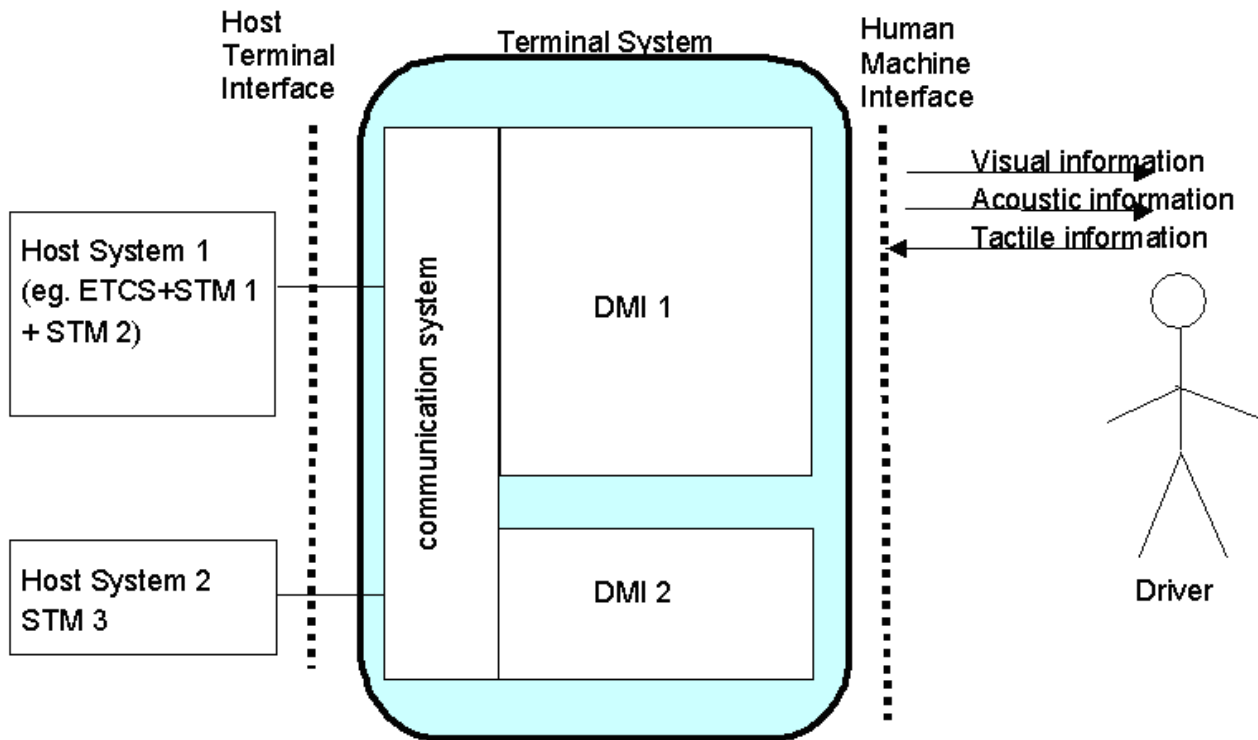


Figure 2— Terms and definitions

3.1

Human-Machine Interface

functional interface between the DMI(s) and the driver

NOTE Information is carried through this interface in the form of visual (light), acoustic and tactile (driver's pressing of buttons). One HMI is associated with one or more DMIs.

3.2

Driver Machine Interface

equipment to support one HMI. It contains the hardware and software means to support HMI

3.3

Host System

equipment communicating with the Driver via DMI

3.4

host application

functional service allocated in a Host System

3.5

terminal system

system comprising the communication system and at least one DMI in a desk

3.6**hard key**

physical key not part of the display area. This key can also have a text label or symbol

3.7**communication system**

system connecting one or more Host System to one or more DMIs and/or to other HS

3.8**softkey**

context-dependent key which consists of hard key with an associated label on the display area

3.9**in-function**

exchange of information (data) from the driver to the onboard system

3.10**out-function**

exchange of information (data) from the onboard system to the driver

3.11**button event**

pressing or releasing a button

3.12**button**

object shown to the driver through which the driver action is possible. It is composed of a label and the associated sensitive area

NOTE

The sensitive area of a button can be accessed via a touch screen area or via hardkey, depending on the chosen technology.

3.13**dimmed**

areas which appearance has been made less conspicuous than other areas

3.14**indicator**

object with a label shown to the driver for which no driver action is possible

3.15**sensitive area**

surface on which a driver can make a physical action to give input to the HS

3.16**Object Control**

data exchanged between Host System and DMI

3.17**label**

symbol or text indication on an indicator or a button

4 Symbols and abbreviations

ASIC	Application Specific Integrated Circuit
CRC	Cyclic Redundancy Code
DMI	Driver Machine Interface
EMC	Electromagnetic Compatibility
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EVC	European Vital Computer
FDL	Field Data Link
FMEA	Failure Mode and Effects Analysis
FRS	Functional Requirements Specification
FFFIS	Form Fits Functional Interface Specification
HMI	Human-Machine Interface
HTI	Host Terminal Interface
HW	Hardware
IL	Implicit Layer
LCC	Life Cycle Cost
MTBF	Mean Time Between Failures
OC	Object Control
Profibus	Process Field Bus
RAM(S)	Reliability, Availability, Maintainability, (Safety)
SAP	Service Access Point
SLL	Safe Link Layer
STL	Safe Time Layer
STM	Specific Transmission Module
SW	Software

5 Devices / modules of the systems

The different systems shown in Figure 1, are detailed hereafter:

- 1) the DMI(s). It can be constituted of (or it can be considered as the assembly of):
 - . input devices (from the driver to the system);
 - button(s). The button(s) can be hardkeys or softkeys or an area on a touch screen, the so-called "button event",
 - etc.;
 - . output devices (from the system to the driver);
 - visual devices,
 - acoustic devices,
 - etc.;
 - . a processing unit.
- 2) a communication system. It is constituted of:
 - . a hardware subsystem;
 - . a software subsystem.
 - . Each of those subsystems can be distributed on different devices.
- 3) the connected equipment (HS: for instance, EVC/STM system).

6 DMI functions for ERTMS/ETCS

6.1 Concepts

6.1.1 Object Controls

The study of exchanges between the driver and the ERTMS/ETCS system has led to define the following generic Object Controls, that must be exchanged between Host System and DMI (see Table 1 to Table 4).

NOTE Those OCs must be usable by any HS connected to the communication system defined in this document.

Table 1 — Object Controls from HS to DMI

From Host System to DMI	Name
Button request	BR
Indicator request	IR
Text message request	TMR
Text message deletion	TMD
Sound request	SR
Data entry request	DER
Data confirmation request	DCR
Dataview request	DR
Continuous dataview request	CDR

Table 2 — Object Controls from DMI to HS

From DMI to Host System	Name
Button event report	BER
Ack	ACK
Data entry reply	DERy
Data confirmation reply	DCRy

6.1.2 Objects Controls from HS to DMI

Table 3 gives precisions about the concept of OC from HS to DMI.

Table 3 — OC definitions, Part 1

Name	Details
Button request	HS request DMI to give or remove driver access to the related button.
Indicator request	HS request DMI to display or remove the related indicator.
Text message request	HS request DMI to display the related text. The request can consist of a reference to the text, or it can include the text itself.
Text message deletion	HS request DMI to remove a text message.
Sound request	HS request DMI to play or stop playing a sound to the driver.
Data entry request	HS request DMI 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), and a text identifying the data for the driver.
Data confirmation request	HS request DMI 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), and a text identifying the data for the driver.
Dataview request	HS request DMI to display or remove data to the driver.
Continuous dataview request	HS request DMI to display or remove continuously changing data (e.g. speed, target distance).

6.1.3 Objects Controls from DMI to HS

Table 4 gives precisions about the concept of OC from DMI to HS.

Table 4 — OC definitions, Part 2

Name	Details
Button event report	DMI report to HS button event .
Ack	DMI report driver acknowledgement to HS.
Data entry reply	DMI report to HS driver data entry.
Data confirmation reply	DMI report to HS driver confirmation or rejection of data displayed.

6.2 Delays

For each OC, a maximum delay is defined and mandatory (Table 5 and Table 6). The following delays are defined for the complete system (i.e. DMI + communication system):

Table 5 — Delays from HS to DMI

From Host System to DMI	Name	Delay ms
Button request	BR	500
Indicator request	IR	500
Text message request	TMR	1 000
Text message deletion	TMD	500
Sound request	SR	500
Data entry request	DER	1 000
Data confirmation request	DCR	1 000
Dataview request	DR	1 000
Continuous dataview request	CDR	500

Table 6 — Delays from DMI to HS

From DMI to Host System	Name	Delay ms
Button event report	BER	500
Ack	ACK	500
Data entry reply	DERy	1 000
Data confirmation reply	DCRy	1 000

6.3 Object Controls analysis

6.3.1 Explanations

6.3.1.1 Object Controls and ERTMS/ETCS functions

The exchanges between the HS and the DMI have been analysed according to the documents [2], [3] and CLC/TS 50459. Table 7 and Table 8 demonstrate that the OCs defined in 6.1.1 are covering all the needs for all the functional exchanges between ERTMS/ETCS and the driver. Those Tables show one example of implementation for each function, other solutions are allowed, but only by using OCs defined in 6.1.1.

6.3.1.1.1 Exchanges from driver to HS**Table 7 — Exchanges from driver to HS**

ETCS Driver exchange	SRS [2], STM [3], CLC/TS 50459	Associated OCs
Data entry request	SRS 3.19, 4.7.2, 5.4	BR, BER
Train Data		
Maximum Train Speed	SRS 3.19, 4.7.2, 5.4, 5.14.2.2, 5.14.3.3	BR, BER, DER, DERy, DCR, DCRy
International Train category	SRS 3.19, 4.7.2, 5.4, 5.14.2.2, 5.14.3.3	BR, BER, DER, DERy, DCR, DCRy
Train length	SRS 3.19, 4.7.2, 5.4, 5.14.2.2, 5.14.3.3	BR, BER, DER, DERy, DCR, DCRy
Braking characteristics	SRS 3.19, 4.7.2, 5.4, 5.14.2.2, 5.14.3.3	BR, BER, DER, DERy, DCR, DCRy
Loading gauge	SRS 3.19, 4.7.2, 5.4, 5.14.2.2, 5.14.3.3	BR, BER, DER, DERy, DCR, DCRy
Axle load	SRS 3.19, 4.7.2, 5.4, 5.14.2.2, 5.14.3.3	BR, BER, DER, DERy, DCR, DCRy
Power supply	SRS 3.19, 4.7.2	BR, BER, DER, DERy, DCR, DCRy
Additional Data		
Driver Identity number	SRS 3.18.4.1, 4.7.2, 5.4	BR, BER, DER, DERy
Train Operational Identifier	SRS 3.18.3.2.1, 3.18.4.5.1, 4.7.2, 5.4	BR, BER, DER, DERy
ERTMS/ETCS Level	SRS 3.18.4.2, 4.7.2, 5.4, 5.10.2.9, 5.10.2.10	BR, BER, DER, DERy
RBC Identity	SRS 3.18.4.3.2, 4.7.2, 5.4	DER, DERy
RBC phone number	SRS 3.18.4.3.2, 4.7.2, 5.4	DER, DERy
Track adhesion factor	SRS 3.18.4.6, 4.7.2	BR, BER
Maximum Staff Responsible Speed	SRS 4.4.11.1.5, 4.7.2, 5.8.3.5	BR, BER, DER, DERy
Staff Responsible distance	SRS 4.4.11.1.5, 4.7.2, 5.8.3.5	BR, BER, DER, DERy
Additional STM data	SRS 3.15.6.3, 4.4.6.1.9, 4.4.15.1.7, 4.4.16, 4.4.17, 4.7.2, 5.4	BR, BER, DER, DERy, DCR, DCRy
STM selection	SRS 3.18.4.2, 4.7.2, 5.4, 5.10.2	BR, BER, DER, DERy
Driver confirmation		
Train Data Confirmation	SRS 4.7.2, 5.4	DCR, DCRy
Confirm «Continue without radio session»	SRS 5.4	DCR, DCRy
Mode change request		
Shunting Request	SRS 4.4.8.1, 4.4.14.5, 4.7.2, 5.4, 5.6	BR, BER
Exit of Shunting request	SRS 4.6.3, 4.7.2	BR, BER
Non-leading request	SRS 4.4.15.3.2, 4.6.3, 4.7.2, 5.5.12.3.4.1, 5.5.14.3.5	BR, BER
Exit of Non-leading request	SRS 4.6.3, 4.7.2, 5.4, 5.12.3.4.2, 5.14.2.4	BR, BER

Table 7 — Exchanges from driver to HS (continued)

ETCS Driver exchange	SRS [2], STM [3], CLC/TS 50459	Associated OCs
Acknowledgement		
Acknowledgement of train trip	SRS 3.14.1.3, 4.4.13.1.4, 4.6.3, 5.11.3	ACK
Acknowledgement of Staff Responsible mode	SRS 4.6.3, 4.7.2, 5.4	ACK
Acknowledgement of On Sight mode	SRS 4.6.3, 4.7.2, 5.4, 5.9.1.2, 5.9.2.3, 5.9.3	ACK
Acknowledgement of Unfitted mode	SRS 4.6.3, 4.7.2, 5.4	ACK
Acknowledgement of shunting ordered by trackside	SRS 4.4.8.1.9, 4.6.3, 5.4, 5.7.1.4, 5.7.3.2	ACK
Acknowledgement of reversing mode	SRS 4.6.3, 5.13	ACK
Acknowledgement of level transition to level	SRS 4.7.2, 5.10.4	ACK
Acknowledgement of Plain Text Information	SRS 3.12.3, 4.7.2	ACK
Acknowledgement of Fixed Text Information	SRS 3.12.3, 4.7.2	ACK
Acknowledgement of release emergency brake	SRS 3.14.1.8	ACK
Acknowledgement of release service brake	SRS 3.14.1.8	ACK
Other inputs		
Confirmation of Train Integrity	SRS 3.6.5.1.4, 3.6.5.2, 4.6.3, 4.7.2	BR, BER, DCR, DCRy
Track Ahead Free confirmation	SRS 3.15.5.2, 4.11.1.9, 4.4.12.1.5, 4.7.2, 5.9.6.3.3	BR, BER, DCR, DCRy
Override request	SRS 4.4.11.1.8, 4.6.3, 4.7.2, 5.4.3.2, 5.6.4.1.3, 5.8.1, 5.8.2	BR, BER, DCR, DCRy
Override route unsuitability	SRS 3.12.2.5, 3.12.2.6, 4.7.2	BR, BER, DCR, DCRy
Start	SRS 3.8.2.7, 4.4.11.1.6, 4.4.14.1, 4.6.3, 4.7.2, 5.4.1.1, 5.4.3.2, 5.14.2.5	BR, BER
Selection of language	SRS 3.12.3.3.2, 4.7.2	BR, BER, DER, DERy
Display request Supervision (including permitted speed and target distance, SR speed and distance)	SRS 2.6.3.1.6, 4.4.8.1.11, 4.4.11.1.7, 4.4.12.1.4	BR, BER
Display request geographical train position	SRS 3.6.6.1, 4.7.2	BR, BER, TMR, TMD
DMI input for STM	SRS 2.6.4.1, 3.15.6.3, 4.4.6.1.9, 4.4.15.1.7, 4.4.16, 4.4.17, 4.6.3, 4.7.2, 5.4	
Packet STM-30: Driver language transmission	STM 7.5.1	BR, BER, DER, DERy
Packet STM-32: Button Request	STM 7.5.2	BR
Packet STM-34: Button event report	STM 7.5.3	BER
Packet STM-40: Acknowledgement reply	STM 7.5.7	ACK

6.3.1.2 Output Exchanges from HS to driver

Table 8 — Output exchanges from HS to driver

ETCS Driver exchange	SRS [2] ,STM [3], CLC/TS 50459	Associated OCs
Train Data	See input exchange	BR, BER, DR
Additional Data	See input exchange	BR, BER, DR
Train status		
Indication limit	SRS 3.14.4.8	CDR
Warning limit	SRS 3.14.4.5	CDR
Intervention limit	SRS 3.14.4.6, 3.14.4.7	CDR
Train Speed	SRS 2.6.3.1.6, 3.13.2.1, 4.4.8.1.10, 4.4.9.1.6, 4.4.10.1.4, 4.4.11.1.7, 4.4.12.1.4, 4.4.15.1.6, 4.4.18.1.5, 4.7.2	CDR
Service Brake Indication	SRS 3.13.4.6.5, 3.14.2.6, 3.14.3.4, 4.7.2	IR
Emergency Brake Indication	SRS 3.13.4.7.4, 3.14.2.6, 3.14.3.4, 4.7.2	IR
Mode and level indication		
ERTMS/ETCS Mode	SRS 4.4.2.1, 4.7.2	IR
current ERTMS/ETCS level	SRS 4.4.2.1, 4.7.2	IR
Ceiling Speed and Target Speed Monitoring		
Permitted Speed	SRS 2.6.3.1.6, 3.13.4.4.1, 3.13.7.3.6, 4.4.9.1.6, 4.4.12.1.5, 4.4.18.1.5, 4.7.2	CDR
Target Speed	SRS 3.13.2.2, 3.13.4.8.1, 4.4.9.1.6, 4.4.12.1.4, 4.7.2	CDR
Target Distance	SRS 3.13.2.2, 3.13.4.8.1, 4.4.9.1.6, 4.4.12.1.4, 4.4.18.1.5, 4.7.2	CDR
Release Speed	SRS 3.13.7.3.5, 4.4.9.1.6, 4.7.2	CDR
Intervention Speed	CLC/TS 50459-2	CDR
Supervised maximum speed	SRS 2.6.3.1.6, 4.4.8.1.11, 4.4.11.1.7	CDR
Warning time to intervention	CLC/TS 50459-2	CDR
Set Speed	CLC/TS 50459-2	CDR
Warnings and Text Messages		
Trip Alarm	SRS 4.4.13.1.3, 4.7.2	IR, SR, CDR
Text message: Fixed text message	SRS 3.12.3.1, 3.12.3.2, 3.12.3.3, 4.7.2, 4.8.3.1.1, 4.10.1.3	TMR, TMD
Text message to be acknowledged: Fixed text messages	SRS 3.12.3.1, 3.12.3.2, 3.12.3.3, 4.7.2, 4.8.3.1.1, 4.10.1.3	TMR, TMD
Plain Text Message	SRS 3.12.3, 4.7.2, 4.8.3.1.1, 4.10.1.3	TMR, TMD

Table 8 — Output exchanges from HS to driver (*continued*)

ETCS Driver exchange	SRS [2], STM [3], CLC/TS 50459	Associated OCs
Indications		
Emergency stop message received	SRS 3.10.2	IR
Local Time	SRS 3.18.5.1.2	CDR
Override status	SRS 4.4.11.1.7, 4.7.2	IR
SR mode proposed	SRS 4.6.3, 4.7.2, 5.4	TMR, TMD
Slippery track selected	SRS 3.18.4.6.2.3, 4.7.2	IR
Geographical train position	SRS 3.6.6.1, 4.7.2	TMR, TMD
Isolation status	SRS 4.4.2.1, 4.4.3.1.2, 4.7.2	IR
Track data and track condition	SRS 3.12.1.1, 3.12.1.4, 3.12.1.5	
Power control	SRS 3.12.1, 4.7.2	IR
Stopping control	SRS 3.12.1, 4.7.2	IR
Air tightness	SRS 3.12.1, 4.7.2	IR
Balise transmission control	SRS 3.12.1, 4.7.2	IR
Control radio transmission – Unchecked Area	SRS 3.12.1, 4.7.2 “Radio hole control”	IR
Brakes control	SRS 3.12.1, 4.7.2	IR
Route suitability	SRS 3.12.2.4	IR
TIU status	CLC/TS 50459-2	IR
Planning Area	CLC/TS 50459-2	
Distance Scale(D1)	CLC/TS 50459-2	CDR
Announcements area(D2/3/4)	SRS 3.12.1.1, 3.12.1.4, 3.12.1.5, CLC/TS 50459-2	IR
Gradient Profile(D5)	CLC/TS 50459-2	CDR
Speed Related Target(D6)	CLC/TS 50459-2	CDR
Speed Profile(D7)	CLC/TS 50459-2	CDR
Brake Curve Area Starting Point(D8)	CLC/TS 50459-2	CDR
Confirmation		
Train Data Confirmation	SRS 4.7.2, 5.4	DCR, DCRy
«Continue without radio session» confirmation	SRS 5.4	DCR, DCRy
DMI output for STM		
Packet STM-35: Indicator request	STM 7.5.4	IR
Packet STM-38: Text message	STM 7.5.5	TMR
Packet STM-39: Delete text message	STM 7.5.6	TMD
Packet STM-42: European ETCS DMI TBD	STM 7.5.8	CDR
Packet STM-43: National ETCS DMI	STM 7.5.9	CDR
Packet STM-46: Sound command	STM 7.5.10	SR
Packet STM-35: Indicator request	STM 7.5.4	IR
Packet STM-38: Text message	STM 7.5.5	TMR

Table 8 — Output exchanges from HS to driver (*continued*)

ETCS Driver exchange	SRS [2] ,STM [3], CLC/TS 50459	Associated OCs
Audible Information		
S info - Information on DMI	CLC/TS 50459-2, CLC/TS 50459-6	SR
S1 - Driving too fast	CLC/TS 50459-2, CLC/TS 50459-6	SR
S2 - Speed warning	CLC/TS 50459-2, CLC/TS 50459-6	SR
S3 - End of intervention	CLC/TS 50459-2, CLC/TS 50459-6	SR
S4 - Reserved	CLC/TS 50459-2, CLC/TS 50459-6	SR
S5 - Most Restrictive Target Changed	CLC/TS 50459-2, CLC/TS 50459-6	SR
S6 - Error occurred	CLC/TS 50459-2, CLC/TS 50459-6	SR
S7 - New text message	CLC/TS 50459-2, CLC/TS 50459-6	SR
S8 - New advisory	CLC/TS 50459-2, CLC/TS 50459-6	SR
S9 - Driver activity warning	CLC/TS 50459-2, CLC/TS 50459-6	SR
S10 - Release brake when applied by driver	CLC/TS 50459-2, CLC/TS 50459-6	SR
S11 - Brakes commanded by a system	CLC/TS 50459-2, CLC/TS 50459-6	SR
S12 - Acknowledgement required	CLC/TS 50459-2, CLC/TS 50459-6	SR

6.3.1.3 OCs failure modes and failure effects

The communication system is considered as a closed network system, according to EN 50159-1.

The failure modes definitions are given in 6.3.1.4 and adapted from EN 50159-2:2001.

Table 9 and Table 10 list for each OC the failure modes that could lead to an hazard. The details of the relevant failure effects are given in 6.3.2.2.2 and 6.3.2.3.2. For each of those effects, the ERTMS/ETCS functions impacted are listed.

6.3.1.4 Defence techniques

The reference for defence techniques is EN 50159-2:2001, Clause 7.

Applying EN 50159-2:2001, Table C.1 to the HS-DMI interface and communication system lead to define it as a class 2 system. As a consequence, Table C.2 of EN 50159-2:2001 induces not to consider the "MASCARADE" as a threat (failure mode), neither the "CRYPTOGRAPHIC TECHNIQUES" and "IDENTIFICATION PROC" for defences.

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

6.3.2 Failure modes and effects

6.3.2.1 List of failures

The following list gives the failures defined for the OC, with their definition.

- . Repeated OC (REP): OC error in which the same OC is received more than once in a short time;
- . deleted OC (DEL): OC error in which an OC is removed from the OC stream;
- . inserted OC (INS): OC error in which an additional OC is implanted in the OC stream;
- . resequenced OC (RES): OC error in which the order of OCs in the OC stream is changed;
- . corrupted OC (COR): OC error in which a data corruption occurs;
- . delayed OC (DYD): OC error in which a OC is received at a time later than intended.

6.3.2.2 From HS to DMI

6.3.2.2.1 Failure modes

Table 9 gives the failure modes, depending on each OC (no = that failure mode of the OC has no functional effect).

Table 9 — Failure modes, part 1

OC	Name	REP	DEL	INS	RES	COR	DYD
Button Request	BR	no	no	yes	yes	yes	yes
Indicator Request	IR	no	yes	yes	yes	yes	yes
Text Message Request	TMR	no	no	no	no	yes	no
Text Message Deletion	TMD	no	no	no	no	no	no
Sound Request	SR	no	no	no	no	no	no
Data Entry Request	DER	no	no	yes	yes	yes	yes
Data Confirmation Request	DCR	no	no	yes	yes	yes	yes
Dataview request	DR	no	no	no	no	no	no
Continuous Dataview Request	CDR	no	yes	yes	yes	yes	yes

Assumptions:

- . text messages deletion and sounds are considered as non safety related,
- . acknowledgement request is considered as a text message request,
- . dataview windows must not cover all the screen, as it can be requested while running.

6.3.2.2.2 Failure effects (related to safety)

6.3.2.2.2.1 to 6.3.2.2.2.6 give the consequences of each failure mode in Table 9.

6.3.2.2.2.1 Button Request

- . INS: wrong override activation, wrong override route unsuitability activation, wrong train data confirmation, wrong STM button request;
- . RES, COR, DYD: ditto.

6.3.2.2.2.2 Indicator Request

- . DEL: wrong ERTMS/ETCS mode indication, wrong ERTMS/ETCS level indication, missing (non) stopping area indication, wrong STM indication;
- . INS: wrong ERTMS/ETCS mode indication, wrong ERTMS/ETCS level indication, wrong (non) stopping area indication, wrong STM indication;
- . RES, COR, DYD: ditto.

6.3.2.2.2.3 Text Message Request

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

6.3.2.2.2.4 Data Entry Request

- INS: could hide ETCS/ERTMS mode and current level, speed information, stopping control, track adhesion factor;
- RES, COR, DYD: ditto.

6.3.2.2.2.5 Data Confirmation Request

INS, RES, COR, DYD: same as DER.

6.3.2.2.2.6 Continuous Dataview Request

- DEL: wrong value of train speed, permitted speed, target speed, target distance, release speed;
- INS, RES, COR, DYD: ditto.

6.3.2.3 From DMI to HS**6.3.2.3.1 Failure modes**

Table 10 gives the failure modes, depending on each OC (no = that failure mode of the OC has no functional effect).

Table 10 — Failure modes, Part 2

OC	Name	REP	DEL	INS	RES	COR	DYD
Button Event Report	BER	no	no	yes	yes	yes	yes
Ack	ACK	no	no	yes	yes	yes	yes
Data Entry Reply	DERy	no	no	yes	yes	yes	yes
Data Confirmation Reply	DCRy	no	no	yes	yes	yes	yes

6.3.2.3.2 Failure effects

6.3.2.3.2.1 to 6.3.2.3.2.4 give the consequences of each failure mode in Table 10.

6.3.2.3.2.1 Button Event Report

- INS: wrong override request, wrong override route unsuitability, wrong shunting request, wrong non-leading mode request, wrong train data confirmation, wrong train integrity, wrong track ahead free;
- RES, COR, DYD: ditto.

6.3.2.3.2.2 Ack

- INS: wrong staff responsible mode ack, wrong on sight mode ack, wrong unfitted mode ack, wrong level transition ack, wrong plain text message ack, wrong fixed text message ack;
- RES, COR, DYD: ditto.

6.3.2.3.2.3 Data Entry Reply

- INS: wrong train data, wrong additional data, wrong selection of language;
- RES, COR, DYD: ditto.

6.3.2.3.2.4 Data Confirmation Reply

- INS: same as DERy;
- RES, COR, DYD: ditto.

6.3.3 Defence techniques

Table 11 and Table 12 present for each failure mode of each OC the defence techniques that can be used, in accordance with 6.3.1.4.

NOTE The term "threat" in EN 50159-2:2001 is called "failure mode", as in the rest of the present document.

6.3.3.1 From HS to DMI

Table 11 — Defence techniques, Part 1

OC	Failure mode	Sequence Number	Time stamp	Time out	Source and destination Identifier	Feedback message	Safety code
Button Request	INS	X			X		
	RES	X	X				
	COR						X
	DYD		X				
Indicator Request	DEL	X					
	INS	X			X	X	
	RES	X	X				
	COR						X
	DYD		X				
Text Message Request	COR						X
Data Entry Request	INS	X			X		
	RES	X	X				
	COR						X
	DYD		X				
Data Confirmation Request	INS	X			X		
	RES	X	X				
	COR						X
	DYD		X				
Continuous Dataview Request	DEL	X		X			
	INS	X			X		
	RES	X	X				
	COR						X
	DYD		X	X			

Key:

"X" means same as in EN 50159-2:2001, Table 1 recommended.

Grey = useless defence.

Dashed means that there are differences with EN 50159-2:2001.

6.3.3.2 From DMI to HS

Table 12 — Defence techniques, Part 2

OC	Failure mode	Sequence Number	Time stamp	Time out	Source and destination Identifier	Feedback message	Safety code
Button Event Report	INS	X			X		
	RES	X	X				
	COR						X
	DYD		X				
Ack	INS	X			X	X	
	RES	X	X				
	COR						X
	DYD		X				
Data Entry Reply	INS	X			X		
	RES	X	X				
	COR						X
	DYD		X				
Data Confirmation Reply	INS	X			X		
	RES	X	X				
	COR						X
	DYD		X				
Key: "X" means same as in EN 50159-2:2001, Table 1 recommended. Grey = useless defence. Dashed means that there are differences with EN 50159-2:2001.							

7 DMI Safety targets

7.1 Difficulties to assign THR/SIL to ETCS Display display functions

It is quite a lot of effort to assign THRs/SILs to the DMI functions, as there are many unknown or vague factors.

The factors are explained in the following, simplified risk model given in Figure 3. This is done by means of a fault tree (lower part of the diagram) and an event tree (upper part of the diagram). This risk model describes in a simplified way the relationship between DMI failures/malfunctions and the other influencing factors up to an accident as a potential consequence of such failures.

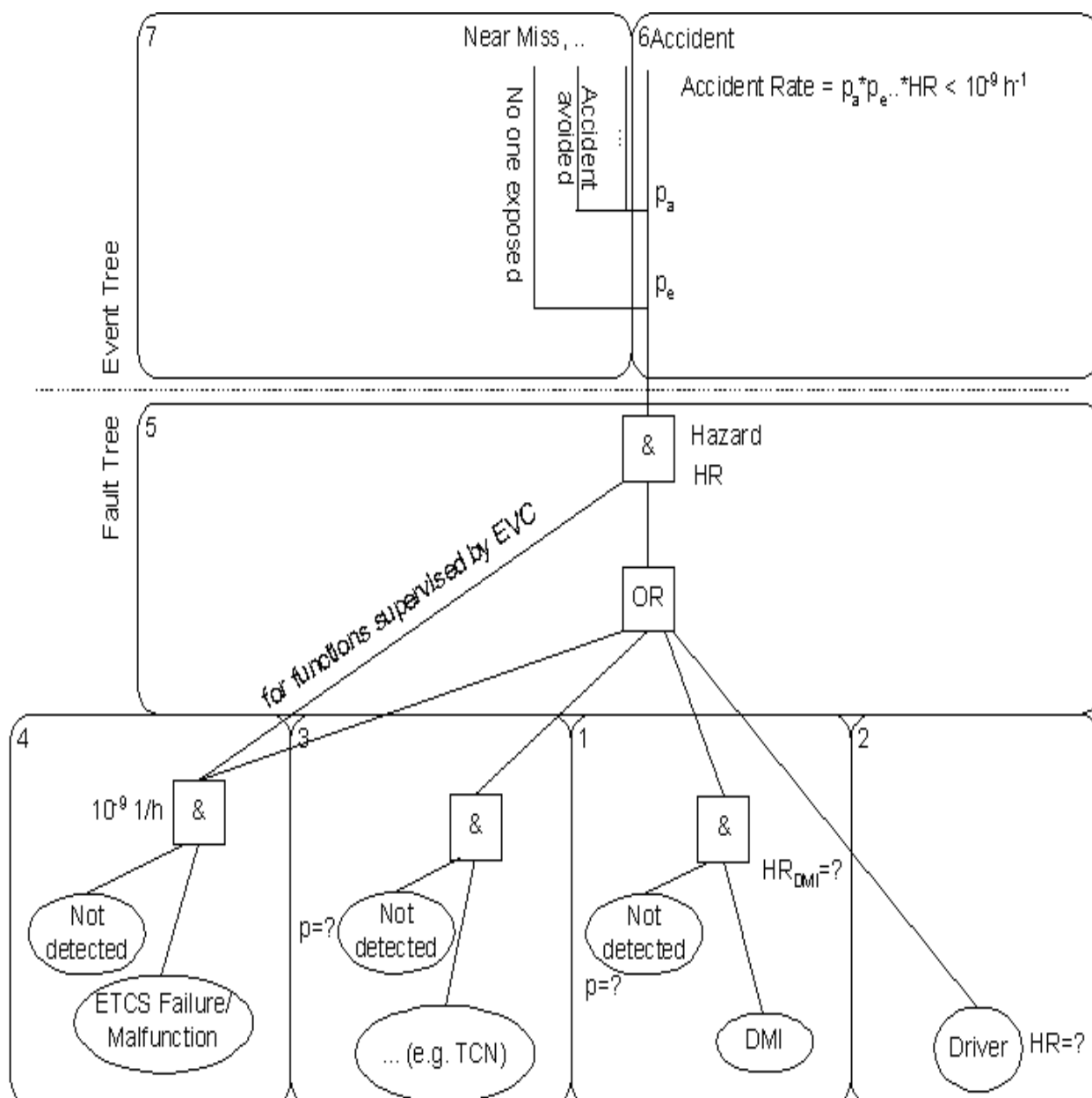


Figure 3 — Fault tree model

Box Nr 1: DMI failures/malfunctions are critical only if the driver does not detect it. The rate/probability of such a failure combined with the probability of not detecting such a failure will result in the hazard rate for the DMI.

Box Nr 2: a hazardous situation may also occur if the driver makes errors. However, the human error rate is dependent on the specific function. Available human error rates are questionable.

Table 13 may be useful in assessing the significance of human error probability when interacting with a vehicle system (like the DMI).

Table 13 — Human behaviour

Type of human behaviour	Human error probability
Extraordinary errors - those for which it is difficult to conceive how they could occur. Stress free, with powerful cues pointing to success.	10^{-5}
Errors in regularly performed, commonplace simple tasks with minimum stress.	10^{-4}
Errors of commission such as pressing the wrong button or reading the wrong display. Reasonably complex tasks, little time available, some cues necessary.	10^{-3}
Errors of omission where dependence is placed on situation and memory. Complex, unfamiliar task with little feedback and some distraction.	10^{-2}
Highly complex task, considerable stress, little time available.	10^{-1}
Process involving creative thinking, unfamiliar, complex operations where time is short and stress is high.	$1 - 10^{-1}$

Boxes Nr 3 and Nr 4: wrong data sent to the display due to failures in the ETCS (EVC) or corruption of data on communication media (e.g. MVB, FIP, etc.) may lead to hazardous situations, too.

Boxes Nr 5: hazards from failures/malfunctions of the display or driver errors are not critical as long as there is supervision by the EVC (not failed and in operation).

Boxes Nr 6 and Nr 7: remaining hazards do not necessarily lead to accidents. Depending on the function failed, some hazards do not lead to an accident. For instance, because nobody is exposed to the hazard or an accident could be avoided by some action taken from those exposed by the hazard or others. Consequently, the hazard rate is reduced by factor p_e and p_a . The factor p_e is the probability that somebody is exposed to the hazard. The factor p_a is the probability that an accident cannot be avoided. These factors are less or equal to 1 and depend on the specific hazard or function failed

From the risk model it is clear that we need to know the following factors to perform the risk analysis and hence to assign THR/SIL to ETCS display functions:

- probability for hazards leading to an accident (factors p_e and p_a) for each of the functions (Boxes Nr 6 and Nr 7);
- failure rates for other components like communication media (Box Nr 3);
- human error rates/probabilities for the actions of the driver related to any of the display functions.

Furthermore, an apportionment of a tolerable risk is not possible since other functions/hazards contribute to the overall system hazard rate (on railway level). Such functions/hazards are related for instance to braking, guidance. The contribution of these functions/hazard to the overall risk is not known.

Independent from this argumentation it is obvious that there are some safety relevant aspects given in operating the DMI.

NOTE To mitigate DMI safety relevant aspects, the design rules given in Annex B can be implemented.

Due to all unknown parameters to be taken into account, this document does not make any allocation of safety requirements.

7.2 Safety approach for DMI and communication system

This subclause gives a methodology based on OCs to demonstrate the safety of the ERTMS/ETCS driver interface functions. Figure 4 gives a summary of that methodology.

7.2.1 Methodology summary

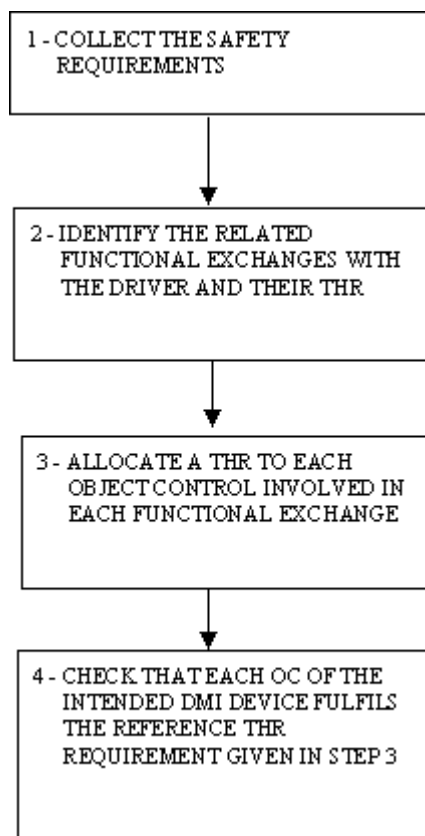


Figure 4 — Methodology for THR allocations

7.2.2 Explanations

- 1) Step 1: collect the safety requirements. That means identifying THR requirement and host system hazards.

NOTE It is recommended to consider the Technical Specifications for Interoperability, or any documents at the same level.

- 2) Identify all the functional exchanges with the driver involved in the HS hazards and the related THRs. The driver interface must be described as a collection of dialogues between a HS and the DMI. The data exchanged during dialogues must be OCs as defined in 6.1.1.
- 3) Step 3: allocate a THR to each OC involved in each functional exchange. The needed THR for each OC depends on the functional exchange and on the system architecture. As an OC is used for several functional exchanges, the reference THR associated with that OC must be the most restrictive one.
- 4) Step 4: check that each OC of the intended DMI device fulfils the reference THR requirement given in Step 3. Each OC of the intended DMI must fulfil its reference THR. The intended DMI can be a device from the market, or a new development. In both cases, the DMI supplier must demonstrate that the reference THRs allocated in Step 3 are fulfilled.

7.2.3 Informative example: false acknowledgement of mode change from Full Supervision

- 1) Steps 1 and 2 have identified that a functional exchange failure called "false acknowledgement of mode change from Full Supervision" is involved in one ERTMS/ETCS system hazard, and a related THR of 10-x h-1 had been allocated.
- 2) Step 3: the TMR and ACK are involved in that functional exchange. A THR is allocated to each of those OC (THRTMR and THRACK), depending on the system architecture. The result has to be filled in a table, to define the different reference THRs. A model of that table is given in Table 14.

Table 14 — THR allocation example

Functional exchange		BR	IR	TMR	TMD	SR	DER	DCR	DR	CDR	BER	ACK	DERy	DCRy
Nr	name													
1	False ack of mode change from full supervision	-	-	THR_TMR_1	-	-	-	-	-	-	-	THR_ACK_1	-	-
2	False ack of level transition	-	-	THR_TMR_2	-	-	-	-	-	-	-	THR_ACK_2	-	-
3	False ack of train trip	-	-	THR_TMR_3	-	-	-	-	-	-	-	THR_ACK_3	-	-
4	False ack of track ahead free	-	-	THR_TMR_4	-	-	-	-	-	-	-	THR_ACK_4	-	-
5														
6														
...	...	...	...	...										
Reference THRs				THR_TMR_3								THR_ACK_1		
NOTE In this example, after all the functional exchanges have been processed, the reference THRs for TMR are the most restrictive ones, e.g. THR_TMR=THR_TMR_3 and for ACK, THR_ACK=THR_ACK_1.														

- 3) Step 4: the DMI supplier demonstrates that all the THR of the OCs for his system fulfils the last line of the table in Step 3 (reference THRs).

8 Communication system requirements

The goal of this clause is to allow a purchaser to control the communication system between DMI and HS in order to:

- . give requirements to a second source for any device (DMI and/or HS) connected to the communication system;
- . adding a new device connected to the communication system while upgrading the network configuration;
- . add new functionalities to a HS or DMI connected to the communication system;
- . maintain the communication system during its life cycle.

Hence, this document shows the relevant parameters of the communication system listed in Clause 1.

8.1 Strategy

8.1.1 General

This document defines the following three upper layers shown in Figure 5: Object Control Layer, Safety Layers, Implicit Layer. This defines the communication system. The lower layers refer to the used protocol and the used bus, and are out of the scope of this document. The OCs defined in 6.1.1 are part of the Object Control Layer.

NOTE As those layers must use the same approach as the FFFIS STM (as defined within documents [1], [4], [5]), that FFFIS STM is considered as a basis for this document.

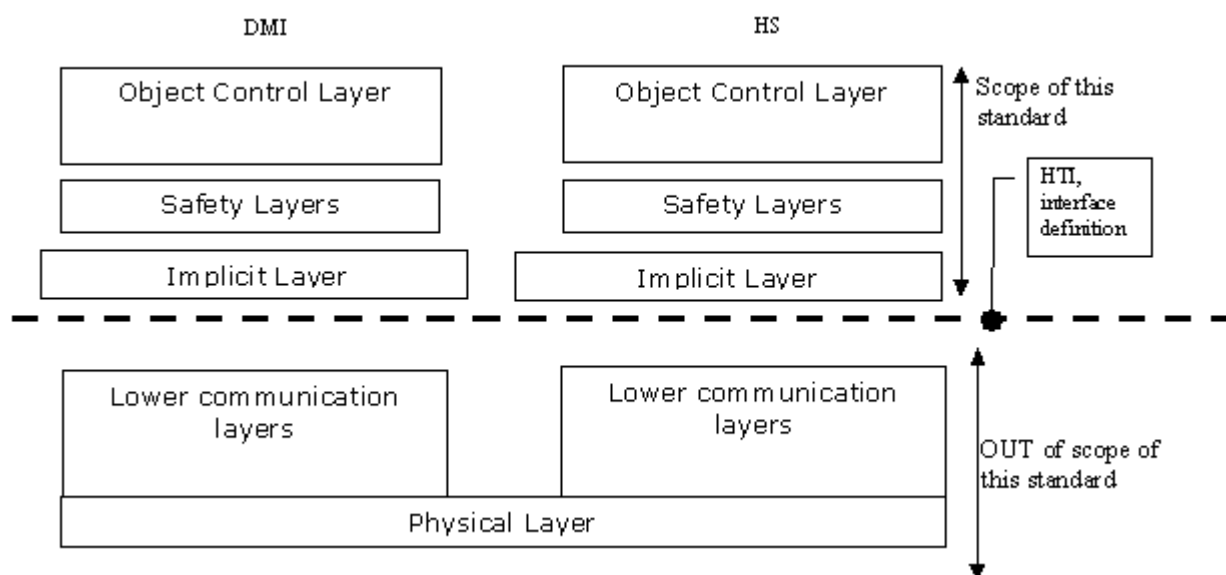


Figure 5 — Communication system layers

NOTE In the following paragraphs, the terms "logical connection" are used in an more extended manner than in the OSI model definition.

8.1.2 STM management

Communication between STM and DMI is defined in FFFIS STM (as defined within documents [1], [4], [5]).

The FFFIS STM documents are mandatory for STMs, so the information is not repeated in the present document.

The DMI must be able to make the difference between logical connections belonging to STM and those belonging to other HS.

8.2 Connection to the DMI

8.2.1 Requirements for the HS

Any HS that has to access the DMI must initiate a logical connection. The HS is the master of the logical connection as defined in 8.7.1.1.

The Receiver_address, Sender_address, DSAP, SSAP as defined in 8.8.2.1.2 must be configurable and easy to change. They must be compatible with the specifications of the FFFIS STM.

8.2.2 Requirements for the DMI

The DMI must only be implied in a logical connection as a connection slave as defined in 8.7.1.1.

The Receiver_address, Sender_address, DSAP, SSAP as defined in 8.8.2.1.2 must be configurable and easy to change. They must be compatible with the specifications of the FFFIS STM.

8.3 Object Control Layer

See 6.1.1 for OCs definition.

The Object Control Layer definition specifies data formats that must be used in the communication between HS and DMI.

The boundary to lower layers are the Safety Layers.

The boundary to higher layer are the applications processed within the HS and the DMI respectively.

The transmitted message to lower layers must be embedded in a safety protocol structure as defined by the Safety Layers and the Implicit Layer.

Figure 6 shows the mechanism for data encapsulation in the communication system layers.

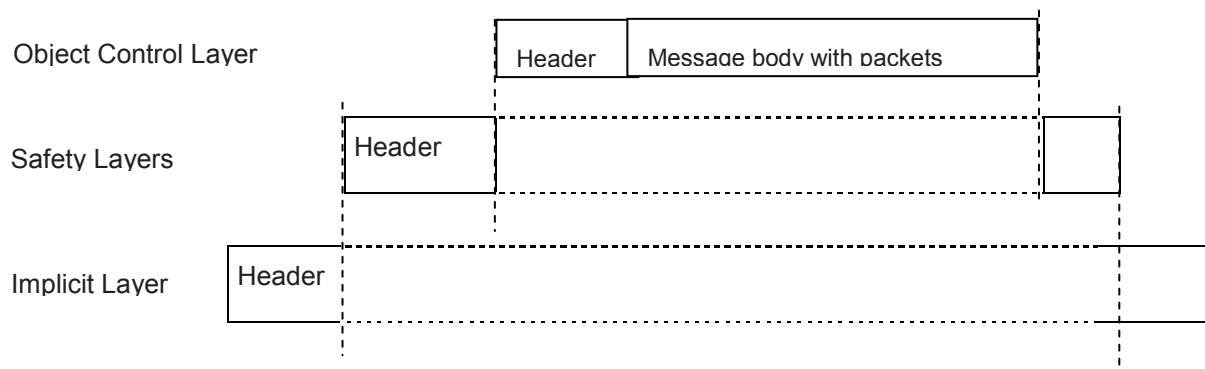


Figure 6 — Data encapsulation

8.4 Safety Layers

The Safety Layers must provide safe communication with protection against the top hazards of communication (see 6.3.1.3).

The boundary to lower layers is the Implicit Layer.

The boundary to higher layers is the Object Control Layer.

The transmitted message to lower layers must be embedded within the Implicit Layer message.

8.5 Implicit Layer

Implicit Data are data used by the Safety Layers for CRC and/or checksum computation. The Implicit Data are not contained into the Safety Layers messages.

NOTE This is made to keep compatibility with FFFIS STM (as defined within documents [1], [4], [5]).

The boundary to higher layers is the Safety Layers.

8.6 Objects Controls data format

8.6.1 Rules of the language

The language is based on variables, packets, and messages.

Variables must be used to encode single data values. Variables must not be split in minor units. The whole variable must have only one type (meaning).

Variables can have special values, which are related to the basic meaning of the variable.

Special values must have always the highest values in a variable (e.g. 11...111 = "unknown").

Spare values must be located between the normal and special values in the variable range.

Names of variables must be unique. A variable must be used in context with the meaning as described in the variable definition. Variables with different meanings must have different names.

Signed values must be encoded as 2's complement.

One bit variables (Boolean) must always use 0 for false and 1 for true.

Offsets for numerical values must be avoided (0 must be used for value zero, 1 for value one, etc.) except where justified.

All Variables must have one of the following prefixes:

- . D_ Distance
- . L_ Length
- . M_ Miscellaneous
- . N_ Number
- . NID_ Identity Number
- . Q_ Qualifier
- . T_ Time/Date
- . V_ Speed
- . X_ Text

Length of variables is given in bits, unless otherwise stated.

Reserved values and spare values for variables must not be used for implementation.

8.6.2 Definition of Packets and rules for packets handling

Packets are multiple variables grouped into a single unit, with a defined internal structure.

This structure must consist in a unique packet number, the length of the packet in bits and an information section containing a defined set of variables. The packet structure is defined as in Table 15.

Table 15 — Packet structure

Name	Name of the packet		
Content	Variable	Length	Comment
	NID_PACKET	8	Packet identifier
	L_PACKET	13	Packet length
	Q_SCALE	2	Specifies which distance scale is used for all distance information within the packet. There must be no Q_SCALE variable in packets, which do not contain distance information in a variable, which requires the information in Q_SCALE.
	Other variables in packet if any	N	

The data element transmission order must respect the order of data elements listed in the packet definition (from top to bottom).

The packet length (number of bits) must be the length in bits of the whole packet. It must take into account the following variables NID_PACKET and L_PACKET plus all other packet variables length as well as iterations for its value computation.

All currently not defined packet identifiers are reserved for future use. All future packet definitions must follow the above-defined structure.

The sender of a packet must ensure that the packet length will fit within one message.

The variable N_ITER in a packet must specify the number of iterations of a variable or group of variables, which follow.

If N_ITER is 0 then no variable which belong to the iteration given by N_ITER must follow.

The variable L_CAPTION in a packet must specify the number of characters in a data label, button label, or indicator label.

The variable L_VALUE in a packet must specify the number of characters in a data value.

If L_VALUE is 0 then no variable for characters must follow.

The variable L_TEXT in a packet must specify the number of characters in a text string.

If L_TEXT is 0 then no variable for characters must follow.

If, depending on the value of a previous qualifier variable in the packet, a variable is optional, it is written indented in the packet definition.

8.6.3 Definition of a message and rules for messages handling

A message is the whole data transmitted at a given time on the interface between HS and DMI.

The message must have the format as defined in 8.6.4.

The data element transmission order must respect the order of data elements listed in the message format (from top to bottom).

The sender of messages must transmit the messages in a chronological way. The first transmitted message must be the oldest.

Messages belonging to the same HS must be treated by the receiver in the order of their reception.

The message header must be composed of the NID_HS and the L_MESSAGE variables.

The NID_HS in the message header must indicate the HS, which is the receiver or transmitter of the message.

The message header must be part of the message at every transmission.

The NID_HS in the message header must be the same for all connection sessions to a given HS in both directions (from DMI to HS and from HS to DMI).

The Message Body must consist of one or many packets.

The sender of a message must put the packet in the message in a chronological way. The first packet transmitted within the message must be the oldest one.

The receiver of a message must treat the packets of a message in the order of their reception.

The message must be completed by padding bits to have the whole message length to be byte aligned for transmission through the Safety Layers.

8.6.4 Message structure

The structure of messages between HS and DMI is described in Table 16.

Table 16 — Message structure

Application message	Message Header	NID_HS
		L_MESSAGE
	First Packet	NID_PACKET
		L_PACKET
		Other variables in First Packet
	Other packets in application message if any	
	Packet-N last data packet if different from First Packet	NID_PACKET
		L_PACKET
		Other variables in Packet
	Padding bits	0 to 7 bits

8.6.5 Objects Controls structure

This subclause defines which packet must be used for each OC.

One OC can be controlled by different packets, depending on the context (see 8.6.5.1 for example).

8.6.5.1 Indicator Request, IR

Table 17 — Indicator Request

Packet Name	Indicator Request		
Content	Variable	Length	Comment
	NID_PACKET	8	Packet identifier Value = 01
	L_PACKET	13	Packet length
	N_ITER	5	Maximum value = 24
	NID_HS(k)	8	HS identity used to point to the corresponding palette for indicator and icon. This NID_HS can be different from the one in the message header as one HS is allowed to re-use indicators from another HS.
	NID_INDICATOR(k)	8	Functional identity of indicator from indicator palette selected by NID_HS
	NID_INDPOS(k)	8	Indicator position on DMI
	NID_ICON(k)	8	Identity of icon from palette selected by NID_HS
	M_IND_ATTRIB(k)	10	Attributes of the indicator
	L_CAPTION(k)	5	Length of X_CAPTION Maximum value = 12
	X_CAPTION(k,j)	8	Caption text bytestring
Packet Name	Indicator Request for Announcement		
Content	Variable	Length	Comment
	NID_PACKET	8	Packet identifier Value = 02
	L_PACKET	13	Packet length
	N_ITER	5	Maximum value = 24
	NID_HS(k)	8	HS identity used to point to the corresponding palette for indicator and icon. This NID_HS may be different from the one in the message header as the STM is allowed to re-use indicators from another HS.
	NID_INDICATOR(k)	8	Functional identity of indicator from indicator palette selected by NID_HS
	NID_INDPOS(k)	8	Indicator position on DMI
	NID_ICON(k)	8	Identity of icon from palette selected by NID_HS
	M_IND_ATTRIB(k)	10	Attributes of the indicator
	L_CAPTION(k)	5	Length of X_CAPTION Maximum value = 12
	X_CAPTION(k,j)	8	Caption text bytestring
	Q_SCALE	8	Scale for D_ANNOUNCEMENT
	D_ANNOUNCEMENT	15	Distance to the next announcement

NOTE Indicator request for Announcement is dedicated to Planning Area data.

8.6.5.2 Button Request, BR

Table 18 — Button Request

Packet Name	Button Request		
Content	Variable	Length	Comment
	NID_PACKET	8	Packet identifier Value = 10
	L_PACKET	13	Packet length
	N_ITER	5	Maximum value = 10
	NID_HS(k)	8	HS identity used to point to the corresponding palette for button and icon. This NID_HS may be different from the one in the message header as one HS is allowed to re-use buttons from another HS.
	NID_BUTTON(k)	8	Functional identity of button from button palette selected by NID_HS
	NID_BUTPOS(k)	8	Button position on DMI
	NID_ICON(k)	8	Identity of icon from palette selected by NID_HS
	M_BUT_ATTRIB (k)	10	Attributes of the button
	L_CAPTION(k)	5	Length of X_CAPTION Maximum value = 12
	X_CAPTION(k)	8	Caption text bytestring

8.6.5.3 Text Message Request

Table 19 — Text Message Request

Packet Name	Text Message Request		
Content	Variable	Length	Comment
	NID_PACKET	8	Packet identifier Value = 20
	L_PACKET	13	Packet length
	NID_XMESSAGE	8	Sequence number of given text messages
	NID_HS	8	HS identity used to point to the corresponding palette for text and icon. This NID_HS may be different from the one in the message header as one HS is allowed to re-use texts from another HS.
	NID_TEXT	8	Pointer to a selected text memorised in the DMI.
	NID_TEXTPOS	8	Position of the text
	M_XATTRIBUTE	10	Attributes of text
	Q_ACK	1	Acknowledgement qualifier
	L_TEXT	8	Number of characters in text string Maximum value = 40
	X_TEXT(k)	8	Text character

8.6.5.4 Text Message Deletion

Table 20 — 8.6.5.4 Text Message Deletion

Packet Name	Text Message Deletion		
Content	Variable	Length	Comment
	NID_PACKET	8	Packet identifier Value = 21
	L_PACKET	13	Packet length
	NID_XMESSAGE	8	Sequence number of text message to be deleted.

8.6.5.5 Sound Request

Table 21 — Sound Request

Packet Name	Sound Request		
Content	Variable	Length	Comment
	NID_PACKET	8	Packet identifier Value = 30
	L_PACKET	13	Packet length
	N_ITER	5	Number of sounds to be generated Maximum value = 2 The HS is able to request to the DMI to generate a maximum of two sounds at the same time.
	NID_HS(n)	8	HS identity used to point to the corresponding sound palette. This NID_HS may be different from the one in the message header as one HS is allowed to re-use sounds from another HS.
	NID_SOUND(n)	8	Functional identity of sound from sound palette selected by NID_HS
	Q_SOUND(n)	2	Continuous/ Not continuous/ Stopped
	N_ITER(n)	5	Number of segments of sound
	M_FREQ(n,k)	8	Frequency of a segment
	T_SOUND(n,k)	8	Duration of segment

8.6.5.6 Data Entry Request

Table 22 — Data Entry Request

Packet Name	Data Entry Request		
Content	Variable	Length	Comment
	NID_PACKET	8	Packet identifier Value = 40
	L_PACKET	13	Packet length
	Q_DRIVERINIT	1	Need for driver intervention or not.
	Q_FOLLOWING	1	Indicate a following request
	N_ITER	5	Maximum iteration data Minimum value = 1 Maximum value = 5
	NID_HS(j)	8	HS identity used to point to the corresponding palette of Specific HS Data variables. This NID_HS may be different from the one in the message header as one HS is allowed to re-use Specific STM data from another HS.
	NID_DATA(j)	8	Identifier of a Specific HS Data to be entered.
	M_XATTRIBUTE(j)	10	Attribute for text string of the data label
	L_CAPTION(j)	5	Length of X_CAPTION for data label Maximum value = 20
	X_CAPTION (j,q)	8	Data label caption text bytestring
	L_VALUE(j)	8	Length of X_VALUE for default value. Maximum value = 10
	X_VALUE(j,i)	8	Data value caption text bytestring
	N_ITER (j)	5	Maximum iteration data pick-up list values = 0 if there is no pick-up list value Maximum value = 16 if the maximum length has been used for all caption texts. Higher values are allowed, if a reduced size of caption text is used but limited by the maximum message length.
	L_VALUE (j,i)	8	Length of X_VALUE for pick-up list value Maximum value = 10
	X_VALUE (j,i,k)	8	Data for pick-up list value caption text bytestring

8.6.5.7 Data Confirmation Request

Table 23 — Data Confirmation Request

Packet Name	Data Confirmation Request		
Content	Variable	Length	Comment
	NID_PACKET	8	Packet identifier Value = 41
	L_PACKET	13	Packet length
	N_ITER	5	Maximum iteration data Minimum value = 1 Maximum value = ???
	NID_HS(j)	8	HS identity used to point to the corresponding palette of Specific HS Data variables. This NID_HS may be different from the one in the message header as one HS is allowed to re-use Specific HS data from another HS.
	NID_DATA(j)	8	Identifier of a Specific HS Data to be entered.
	M_XATTRIBUTE(j)	10	Attribute for text string of the data label
	L_CAPTION(j)	5	Length of X_CAPTION for data label Maximum value = 20
	X_CAPTION (j,q)	8	Data label caption text bytestring
	L_VALUE(j)	8	Length of X_VALUE for default value. Maximum value = 10
	X_VALUE(j,i)	8	Data value caption text bytestring

8.6.5.8 Dataview request

Table 24 — Dataview request

Packet Name	Dataview request		
Content	Variable	Length	Comment
	NID_PACKET	8	Packet identifier Value = 42
	L_PACKET	13	Packet length
	Q_FOLLOWING	1	Indicate following data to be viewed at the same time
	N_ITER	5	Maximum iteration data = 0 if there is "No Specific Data Values" Maximum value = 5
	NID_HS(j)	8	HS identity used to point to the corresponding palette of Specific HS Data variables. This NID_HS may be different from the one in the message header as one HS is allowed to re-use Specific HS data from another HS.
	NID_DATA(j)	8	Identifier of the Specific HS Data
	M_XATTRIBUTE(j)	10	Attribute for text string of the data label and its associated value(s)
	L_CAPTION(j)	5	Length of X_CAPTION for data label Maximum value = 20
	X_CAPTION (j,q)	8	Length of X_VALUE for current value. Maximum value = 10 = 0 if there is no current value
	X_VALUE(j,i)	8	Data value caption text bytestring

8.6.5.9 Continuous Dataview Request

Table 25 — Continuous Dataview Request

Packet Name	Continuous Dataview request		
Content	Variable	Length	Comment
	NID_PACKET	8	Packet identifier Value = 50
	L_PACKET	13	Packet length
	Q_SCALE	2	Qualifier for the distance scale.
	Q_INDICATE	12	Inhibition of ETCS DMI objects
	Q_WARNINGLIMIT	1	Warning limit status
	Q_INDICATIONLIMIT	1	Indication limit status
	V_PERMIT	10	Permitted speed
	V_TARGET	7	Target speed
	V_RELEASE	7	Release speed
	V_INTERV	7	Intervention speed
	D_TARGET	15	Target distance
	V_ACTUAL	10	Actual speed
	N_ITER	5	
	M_SUP(k)	32	HS-customised information

Table 26 — Continuous Dataview Request for Announcement

Packet Name	Continuous Dataview Request for Announcement		
Content	Variable	Length	Comment
	NID_PACKET	8	Packet identifier Value = 51
	L_PACKET	--	Packet length
	Q_DIMMED	1	Whether dimmed or not
	N_ITER	5	
	Q_SCALE(i)	2	Qualifier for the distance scale in planning area
	D_GRADIENT(i)	15	Incremental distance to next change of gradient.
	Q_GRAD(i)	1	Qualifier for gradient slope
	M_GRAD(i)	8	Absolute gradient value
	N_ITER	5	
	Q_SCALE(j)	2	Qualifier for the distance scale in planning area
	D_PLANNING(j)	15	Distance in planning area
	Q_WIDTH(j)	7	Width of the speed restriction

NOTE The three last data permit to draw the "speed profile" in the planning area.