

© Copyright SEK. Reproduction in any form without permission is prohibited.

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

(CENELEC Technical Report 50542:2010)

ISSN 1651-1417

ICS 35.240.60, 45.020, 93.100

Upplysningar om **sakinnehållet** i rapporten lämnas av
SEK Svensk Elstandard.
Postadress: SEK, Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00. Telefax: 08 - 444 14 30
E-post: sek@elstandard.se. Internet: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard

Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

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

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.

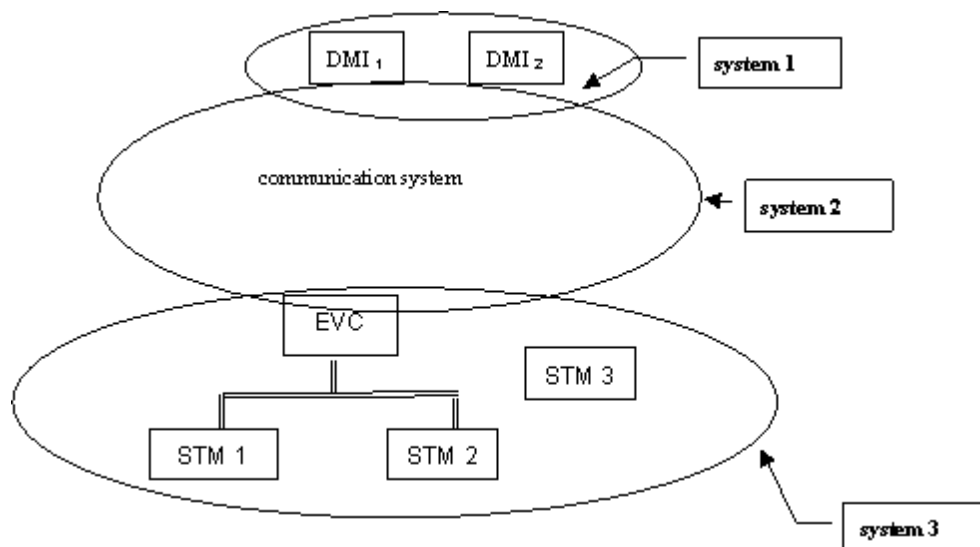


Figure 1 - Systems concerned by this document

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*