



DPC: 22 / 30427187 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 22 June 2022

Origin: International

Latest date for receipt of comments: 19 July 2022

Project No. 2020/02560

Responsible committee: GEL/9/-/4 Railway applications - Train communication network and multimedia systems

Interested committees:

Title: Draft BS EN 61375-2-6 Ed.2.0 Electronic railway equipment - Train communication network (TCN)

Part 2-6: On-board to ground communication

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 19 July 2022**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **Ms Louise Delaney (BSI)**Direct tel: **020 3142 5596**E-mail: louise.delaney@rssb.co.uk

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

PROJECT NUMBER: IEC 61375-2-6 ED2	
DATE OF CIRCULATION: 2022-05-27	CLOSING DATE FOR COMMENTS: 2022-08-19
SUPERSEDES DOCUMENTS: 9/2629/RR	

IEC TC 9 : ELECTRICAL EQUIPMENT AND SYSTEMS FOR RAILWAYS	
SECRETARIAT: France	SECRETARY: Mr Denis MIGLIANICO
OF INTEREST TO THE FOLLOWING COMMITTEES:	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE: Electronic railway equipment – Train communication network (TCN) – Part 2-6: On-board to ground communication
--

NOTE FROM TC/SC OFFICERS:

CONTENTS

FOREWORD.....	9
INTRODUCTION.....	11
1 Scope.....	12
1.1 Specifications within the scope of this document.....	12
2 Normative references	13
3 Terms, definitions, symbols, abbreviated terms and conventions	14
3.1 Terms and definitions.....	14
3.2 Symbols and abbreviated terms	20
3.3 State diagram conventions.....	23
4 Board to Ground Communication system architecture.....	23
4.1 General.....	23
4.2 Requirements	23
4.3 Mobile communication network architecture	26
4.3.1 General	26
4.3.2 On-board network interface	26
4.4 System breakdown structure	27
4.4.1 General	27
4.4.2 System breakdown structure at board-to-ground system level.....	28
4.4.3 System breakdown structure at MCG sub-system level	28
4.4.4 System breakdown structure at GCG sub-system level	28
4.5 Functional breakdown structure	28
4.6 Mobile Communication Gateway	29
4.6.1 Architecture	29
4.6.2 Mobile communication gateway	31
4.7 Mobile communication redundancy	33
4.7.1 General	33
4.7.2 Full performance redundancy	34
4.7.3 Reduced performance redundancy	34
4.8 Train composition changes	34
4.9 Security	35
4.9.1 Security zones.....	35
4.9.2 Security measures	37
4.9.3 Authentication authorization accounting model	37
4.9.4 Network and MCG classification	41
5 Communication framework	43
5.1 General.....	43
5.2 MCG broker service architecture.....	43
5.3 Addressing concept	44
5.3.1 Use cases.....	44
5.3.2 Consist and train Identification.....	45
5.3.3 T2G Network Borders	45
5.3.4 T2G basic minimum network.....	45
5.3.5 T2G addressing	46
5.3.6 HTTP-URI.....	48

5.4	Data classes for T2G communication	49
5.4.1	General	49
5.4.2	Communication channel establishment	49
5.4.3	Message data	50
5.4.4	Process data	50
5.4.5	Stream Data	51
5.4.6	Best effort data	51
5.5	Communication protocol.....	52
5.5.1	General	52
5.5.2	HTTP(S)	52
5.5.3	MQTT (Option)	55
5.6	Communication services	55
5.6.1	General	55
5.6.2	Message data communication service.....	56
5.6.3	File transfer communication service	59
6	Services and interfaces (MCG)	80
6.1	Overview.....	80
6.1.1	MCG system service architecture	80
6.1.2	MCG / GCG system service interfaces	81
6.1.3	MCG / GCG communication relationship	81
6.2	Service provisioning.....	82
6.3	MCG / GCG system service description	82
6.3.1	Communication Services	82
6.3.2	Train Location Service (Option)	93
6.3.3	Train Information Service.....	98
6.3.4	MCG Network Selector Service	102
6.3.5	Train telemetry service (Option).....	104
6.3.6	MCG Train Wake-up Service (Option)	114
6.3.7	MCG Poll Command Set Service (Option)	122
7	Services and interfaces (GCG)	126
7.1	GCG Overview	126
7.2	GCG Addressing	128
7.2.1	Wireless MCG Interface	128
7.2.2	Ground GCG Interface	128
7.3	GCG Implementation	129
7.3.1	General (informative)	129
7.3.2	GCG Availability	129
7.3.3	GCG Workload	129
7.3.4	GCG Security	129
7.4	GCG services	129
7.4.1	GCG services protocol.....	129
7.4.2	GCG Fleet Database	129
7.4.3	MCG-GCG services	130
7.4.4	File transfer communication service	130
7.4.5	Local Ground GCG Interface.....	130
7.4.6	Home GCG – Foreign GCG services.....	131
7.4.7	Public Ground GCG services	131

Annex A (normative) Message presentation	133
A.1 General.....	133
A.2 Transmission rules.....	133
A.3 Generic message	133
Annex B (normative) Telemetry data coding and ordering	134
B.1 General.....	134
B.2 MQTT payload coding	134
B.3 Variables grouping and ordering criterion	135
Annex C (descriptive) Changelog for IEC 61375-2-6	138
C.1 Purpose	138
C.2 General Changes	138
C.2.1 Security	138
C.2.2 DNS Usage.....	138
C.2.3 ComID Harmonization.....	138
C.2.4 Communication Service	141
C.3 Changes to Train-to-Ground (T2G) Services	141
C.3.1 Changes for the Capability Exchange (CAP)	141
C.3.2 Changes for the Network Selector Service (NSS)	141
C.3.3 Changes for the File Transfer Service (FTS)	141
C.3.4 Changes to the Train Location Service (TLS)	141
C.3.5 Changes to the Train Telemetry Service (TTS)	141
Bibliography.....	142
Figure 1 – Train on-board communication system (example).....	26
Figure 2 – Ground communication system (example)	27
Figure 3 – Option 1: End device board to ground communication via MCG	30
Figure 4 – Option 2: End Device board to ground communication via dedicated interface	31
Figure 5 – MCG abstract model block diagram	32
Figure 6 – MCG configured as ALG	33
Figure 7 – Architectural example of redundant Board to Ground communication	33
Figure 8 – Security zones (simplified)	36
Figure 9 – Authentication, authorization and accounting model	38
Figure 9 – MCG connecting open and closed transmission systems.....	42
Figure 10 – MCG broker service architecture	44
Figure 11 – Minimum Train to Ground Network Setup	45
Figure 12 – A train consisting of four vehicles	46
Figure 13 – Communication stacks	53
Figure 14 – HTTP(S) MD communication pattern	54
Figure 15 – HTTP(S) request/event.....	54
Figure 16 – HTTP(S) response	54
Figure 17 – Message Data exchange (example).....	56
Figure 18 – Message Data telegram structure	57
Figure 19 – File upload example	61

Figure 20 – File download example	69
Figure 21 – Service architecture	80
Figure 22 – Service interfaces	81
Figure 23 – Procedure to establish the radio link from MCG	83
Figure 24 – Procedure to establish the radio link from GCG	83
Figure 25 – Procedure to update the ground DNS server	84
Figure 26 – Example architecture to provide the train location	93
Figure 27 – Example procedure to notify about current train location	94
Figure 28 – Example architecture to notify about train information	98
Figure 29 – Example procedure to notify about train information	99
Figure 30 – Illustration of network selector	103
Figure 31 – Architecture to provide telemetry data	104
Figure 32 – Procedure to notify about current train location	105
Figure 11 – Example Procedure to wake-up the train	115
Figure 12 – Example procedure to get Wake-Up process status	118
Figure 33 – MCG Poll Command Set Service	123
Figure 34 – Train to Ground interfaces	127
Figure B.1 – MQTT notification payload format	134
Figure B.2 – Example of ordering criteria	136
Figure B.3 – Example of values grouping	136
Table 1 – Board to ground requirements	24
Table 2 – Board-to-ground system breakdown	28
Table 3 – MCG sub-system breakdown	28
Table 4 – GCG sub-system breakdown	28
Table 5 – An example of the MCG function breakdown	29
Table 6 – An example of the GCG function breakdown	29
Table 7 – Device – status of implementation of the TIS	35
Table 8 – Composition – status of implementation of the TIS	35
Table 9 – Security measures	40
Table 10 – MCG categories	41
Table 11 – Security requirements	42
Table 12 – TCN-URI global DNS zone	48
Table 13 – Recommended service parameters for message data	50
Table 14 – Recommended service parameters for process data	51
Table 15 – Recommended service parameters for stream data	51
Table 16 – Recommended service parameters for best effort data	52
Table 17 – HTTP(S) parameters request/response pattern	54
Table 18 – General MD Header	58
Table 19 – General MD Body	58
Table 20 – Message types	59
Table 21 – Message representation	59

Table 22 – File transfer terminology	59
Table 23 – ComID 202: MD header telegram values	62
Table 24 – ComID 202: MD body telegram values	62
Table 25 – ComID 202: MD body: mdPayload object	63
Table 26 – ComID 203: MD header telegram values	63
Table 27 – ComID 203: MD body telegram values	64
Table 28 – ComID 203: MD body: mdPayload object	64
Table 29 – ComID 204: MD header telegram values	64
Table 30 – ComID 203: MD body telegram values	64
Table 31 – ComID 203: MD body: mdPayload object	65
Table 32 – ComID 205: MD header telegram values	65
Table 33 – ComID 203: MD body telegram values	65
Table 34 – ComID 203: MD body: mdPayload object	65
Table 35 – ComID 206: MD header telegram values	66
Table 36 – ComID 206: MD body telegram values	66
Table 37 – ComID 206: MD body: mdPayload object	67
Table 38 – ComID 207: MD header telegram values	67
Table 39 – ComID 207: MD body telegram values	68
Table 40 – ComID 207: MD body: mdPayload object	68
Table 41 – ComID 208: MD header telegram values	70
Table 42 – ComID 208: MD Body telegram values	71
Table 43 – ComID 208: MD Body: mdPayload object	72
Table 44 – ComID 209: MD header telegram values	72
Table 45 – ComID 209: MD Body telegram values	73
Table 46 – ComID 209: MD Body: mdPayload object	73
Table 47 – ComID 210: MD header telegram values	73
Table 48 – ComID 210: MD Body telegram values	74
Table 49 – ComID 210: MD Body: mdPayload object	74
Table 50 – ComID 211: MD header telegram values	74
Table 51 – ComID 211: MD Body telegram values	75
Table 52 – ComID 211: MD Body: mdPayload object	75
Table 53 – ComID 212: MD header telegram values	75
Table 54 – ComID 212: MD Body telegram values	76
Table 55 – ComID 212: MD Body: mdPayload object	76
Table 56 – ComID 213: MD header telegram values	77
Table 57 – ComID 213: MD Body telegram values	77
Table 58 – ComID 213: MD Body: mdPayload object	77
Table 59 – ComID 214: MD header telegram values	78
Table 60 – ComID 214: MD Body telegram values	78
Table 61 – ComID 214: MD Body: mdPayload object	78
Table 62 – ComID 215: MD header telegram values	78
Table 63 – ComID 215: MD Body telegram values	79

Table 64 – ComID 215: MD Body: mdPayload object	79
Table 65 – ComID 240: Capability message	86
Table 66 – ComID 240: MD event body telegram values	86
Table 67 – ComID 240: MD event body: mdPayload object	86
Table 68 – ComID 240: Capability message	89
Table 69 – ComID 240: MD event body telegram values	89
Table 70 – ComID 240: MD event body: mdPayload object	89
Table 71 – ComID 230: MD request header telegram values	95
Table 72 – ComID 230: MD request body telegram values	95
Table 73 – ComID 230: MD request body: mdPayload object	95
Table 74 – ComID 230: MD reply header telegram values	96
Table 75 – ComID 230: MD reply body telegram values	96
Table 76 – ComID 230/232: MD reply/notification body: mdPayload object	96
Table 77 – Example of latitude/longitude with proposed fixed-point notation	97
Table 78 – ComID 232: MD header telegram values	97
Table 79 – ComID 232: MD Body telegram values	97
Table 80 – ComID 234: MD request header telegram values	100
Table 81 – ComID 234: MD request body telegram values	100
Table 82 – ComID 234: MD request body: mdPayload object	100
Table 83 – ComID 234: MD reply header telegram values	101
Table 84 – ComID 234: MD reply body telegram values	101
Table 85 – ComID 234: MD reply body: mdPayload object	101
Table 86 – ComID 236: MD header telegram values	102
Table 87 – ComID 236: MD Body telegram values	102
Table 88 – ComID 240: MD request header telegram values	106
Table 89 – ComID 240: MD request Body telegram values	106
Table 90 – ComID 240: MD reply header telegram values	107
Table 91 – ComID 240: MD reply body telegram values	107
Table 92 – ComID 240: MD reply body: mdPayload object	107
Table 93 – ComID 242: MD request header telegram values	108
Table 94 – ComID 242: MD request Body telegram values	108
Table 95 – ComID 242: MD request body: mdPayload object	109
Table 96 – ComID 242: MD reply header telegram values	109
Table 97 – ComID 242: MD reply body telegram values	110
Table 98 – ComID 242: MD reply body: mdPayload object	110
Table 99 – ComID 243: MD request header telegram values	111
Table 100 – ComID 243: MD request Body telegram values	111
Table 101 – ComID 243: MD request body: mdPayload object	111
Table 102 – ComID 244: MD request header telegram values	112
Table 103 – ComID 244: MD request Body telegram values	112
Table 104 – ComID 244: MD request body: mdPayload object	112
Table 105 – ComID 244: MD reply header telegram values	113

Table 106 – ComID 244: MD reply body telegram values	113
Table 107 – ComID 244: MD reply body: mdPayload object	113
Table 108 – ComID 245: MD request header telegram values	113
Table 109 – ComID 245: MD request Body telegram values	114
Table 110 – ComID 245: MD request body: mdPayload object	114
Table 111 - ComID 238: twsWakeUp MD event header	116
Table 112 - ComID 238: twsWakeUp MD event body	116
Table 113 - ComID 238: twsWakeUp MD request body: mdPayload object.....	116
Table 114 – ComID 238: twsWakeUp MD response header.....	117
Table 115 – ComID 238: twsWakeUp MD response body	117
Table 116 – ComID 238: twsWakeUp MD response body – mdPayload object	117
Table 117 – ComID 239: twsStatus MDRequest header	119
Table 118 – ComID 239: twsStatus MDRequest body	119
Table 119 – ComID 239: twsWakeUp MD request body: mdPayload object	119
Table 120 – ComID 239: twsStatus MDResponse header.....	119
Table 121 – ComID 239: twsStatus MDResponse body	119
Table 122 – ComID 239: twsStatus MDResponse body: mdPayload object	120
Table 123 – ComID 238: twsWakeUp MD request body: mdPayload object Add-On	121
Table 124 – ComID 238: twsWakeUp MD response body: mdPayload object Add On.....	121
Table 125 – MCG Poll Command Set Service: mdCommandSet.....	122
Table 126 – ComID pcsCommandSetRequest: MD request header	125
Table 127 – ComID pcsCommandSetRequest: MD request body	125
Table 128 – ComID pcsCommandSetResponse: MD request header	125
Table 129 – ComID pcsCommandSetResponse: MD response body	125
Table B.1 – Example of values decoding.....	137
Table 130 – List of ComIDs from IEC 61375-2-6:2018.....	139
Table 131 – List of harmonized ComIDs for the next IEC 61375-2-6 revision	140

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**ELECTRONIC RAILWAY EQUIPMENT –
TRAIN COMMUNICATION NETWORK (TCN) –****Part 2-6: On-board to ground communication****FOREWORD**

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61375-2-6 has been prepared by IEC technical committee 9: Electrical equipment and systems for railways.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
9/2374/FDIS	9/2402/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 61375 series, published under the general title *Electronic railway equipment – Train communication network (TCN)*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Considering that the TCN series includes IEC 61375-2-3: *Electronic railway equipment – Train communication network (TCN) – Part 2-3: TCN communication profile*, references to this document are given when the case applies.

This document follows the ISO-OSI model.

This document does not cover the specification of the radio technologies and protocols relevant to the wireless communication between train and ground.

In the preparation of this document, the following main use cases, which the train to ground communication applies to, were considered:

a) Commissioning application

- 1) Operational Application.
- 2) Mission data application.
- 3) Driver Assistance Application.
- 4) Energy Meter Application.

b) Maintenance application

- 1) Configuration data application.
- 2) Monitoring train status (e.g. telemetry).
- 3) Diagnostic data application.
- 4) Event Recorder Application.

c) Multimedia application

- 1) Passenger information application.
- 2) Passenger entertainment application.
- 3) Electronic ticketing application.
- 4) CCTV and video-surveillance.

ELECTRONIC RAILWAY EQUIPMENT – TRAIN COMMUNICATION NETWORK (TCN) –

Part 2-6: On-board to ground communication

1 Scope

1.1 Specifications within the scope of this document

This part of IEC 61375 establishes the specification for the communication between the on-board subsystems and the ground subsystems.

The communication system, interfaces and protocols are specified as a mobile communication function, using any available wireless technology.

This document provides requirements in order to:

- a) select the wireless network on the basis of QoS parameters requested by the application;
- b) allow TCMS and/or OMTS applications, installed on-board and communicating on the on-board communication network, to have a remote access to applications running on ground installations;
- c) allow applications running on ground installations to have a remote access to the TCMS and/or OMTS applications installed on-board.

This document specifies further requirements which allow the applications running on-board and the applications running on ground to connect each other applying the virtual/functional addressing mechanism specified by IEC 61375-2-3 and exchanging application data sets produced or consumed by the on-board functions implemented in the devices attached to the TCN network.

Furthermore, this document covers the security requirements in order to grant the access only to authenticated and authorised applications and to allow encryption of exchanged data.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

IEC 61375-1:2012, *Electronic railway equipment – Train communication network (TCN) – Part 1: General architecture*

IEC 61375-2-3:2015, *Electronic railway equipment – Train communication network (TCN) – Part 2-3: TCN communication profile*

IEC 61375-3-4, *Electronic railway equipment – Train communication network (TCN) – Part 3-4: Ethernet Consist Network (ECN)*

IEC 62280, *Railway applications – Communication, signalling and processing systems – Safety related communication in transmission systems*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

IEC 62443-3-3, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

IEC 62580-1, *Electronic railway equipment – On-board multimedia and telematic subsystems for railways – Part 1: General architecture*

ISO/IEC 20922:2016, *Information technology – Message Queuing Telemetry Transport (MQTT) v3.1.1*

IEEE 802.3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access*

IEEE 802.11:2016, *IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*

IEEE 802.1X:2010, *IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control*

RFC 2136, *Dynamic Updates in the Domain Name System (DNS UPDATE)*

RFC 2616, *Hypertext Transfer Protocol – HTTP/1.1*

RFC 7233, *Hypertext Transfer Protocol (HTTP/1.1): Range Requests*

RFC 2818, *HTTP Over TLS*

RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*

RFC 4627, *The application/json Media Type for JavaScript Object Notation (JSON)*

RFC 7159, *The JavaScript Object Notation (JSON) Data Interchange Format*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1.1

Authentication Authorization Accounting

access control, policy enforcement and auditing framework for computing systems

3.1.2

Authentication Authorization Accounting service

security architecture for distributed systems, which enables control over which users are allowed access to which services, and how much of the resources they have used

3.1.3

Application Layer

upper layer in the OSI model, interfacing directly to the Application

[SOURCE: IEC 60050-811:2017, 811-37-03]

3.1.4

application process

element within a real open system which performs the information processing for a particular application

[SOURCE: IEC 60050-811:2017, 811-37-05]

3.1.5

Bit Error Rate

rate of bit errors in a data stream, mainly caused by noise (random bit errors), but also caused by memory defects in data storing devices (systematic bit errors)

3.1.6

bridge

device which stores and forwards frames from one bus to another on the base of their Link Layer addresses

[SOURCE: IEC 60050-811:2017, 811-37-09]

3.1.7

broadcast

nearly simultaneous transmission of the same information to several destinations

Note 1 to entry: Broadcast in the TCN is not considered reliable, i.e. some destinations can receive the information and others not.

[SOURCE: IEC 60050-811:2017, 811-37-10]

3.1.8

bus

functional unit for the transfer of data between several participants, these being functional units for data processing, via a common transmission path, wherein participants are not involved in the transfer of data between other participants

Note 1 to entry: The logic and functional definition of a bus applies independently of the topological configuration and physical implementation of the bus. A bus may have a line or a ring configuration.

Note 2 to entry: In some cases, transmission rights are distributed by another participant, for example by a bus arbitrator.

[SOURCE: IEC 60050-351:2013, 351-56-10]

3.1.9

closed train

train composed of one or a set of consists, where the composition does not change during normal operation

EXAMPLE Metro, suburban train, or high-speed train unit.

Note 1 to entry: Consists are coupled in a workshop to establish a closed train for operation.

[SOURCE: IEC 60050-811:2017, 811-37-17]

3.1.10

communication device

device connected to the consist network or train backbone with the ability to transport, source or sink data

[SOURCE: IEC 60050-811:2017, 811-37-18]

3.1.11

communication channel

logical connection over a multiplexed medium such as a radio channel, or conceptual state in which a MCG has announced its presence to the GCG in a way that allows this latter to interact with the MCG

3.1.12

radio link

wireless link, that connects a device with a network, allowing the former to reach other devices through that network

3.1.13

composition

number and characteristics of the consists forming a train

[SOURCE: IEC 60050-811:2017, 811-37-19]

3.1.14

network configuration

definition of the topology of a network, the devices connected to it, their capabilities and the traffic they produce; by extension, the operation of loading the devices with the configuration information before going to regular operation

3.1.15**Consist**

single vehicle or a group of vehicles which are not separated during normal operation

Note 1 to entry: A consist can contain no, one or several consist networks.

[SOURCE: IEC 60050-811:2017, 811-37-20]

3.1.16**Consist Network**

bus connecting equipment within a consist, e.g. the MVB, and which conforms or adapts to the TCN real-time protocols

[SOURCE: IEC 60050-811:2017, 811-37-21]

3.1.17**end device**

unit connected to one Consist Network or to one set of Consist Networks prepared for redundancy reasons

[SOURCE: IEC 60050-811:2017, 811-37-33]

3.1.18**framework**

set of services and protocols to support board-to-ground communication

3.1.19**function**

application process which exchanges messages with another application process

3.1.20**gateway, <in a train communication network>**

connection between different busses at the application layer requiring application-dependent data analysis and protocol conversion

[SOURCE: IEC 60050-811:2017, 811-37-44]

3.1.21**group address**

address of a multicast group to which a device belongs

[SOURCE: IEC 60050-811:2017, 811-37-45]

3.1.22**host**

any addressable unit connected to the network: End Devices, Network Devices, etc.

3.1.23**inauguration**

operation executed in case of composition change, which gives all Nodes of the Train Backbone their Train Backbone address, their orientation and information about all named Nodes on the same backbone

[SOURCE: IEC 60050-811:2017, 811-37-48]

3.1.24**integrity**

state in which information is complete and not altered

[SOURCE: IEC 60050-821:2017, 821-11-26]

3.1.25**train journey**

scheduled railroad journey

3.1.26**journey train**

composition travelling on a scheduled train journey

3.1.27**Local Area Network**

part of a network characterized by a common medium access and address space

[SOURCE: IEC 60050-811:2017, 811-37-60]

3.1.28**Medium Access Control**

sublayer of the Link Layer, which controls the access to the medium (arbitration, mastership transfer, polling)

3.1.29**medium**

physical carrier of the signal

Note 1 to entry: Electrical wires, optical fibers, etc.

3.1.30**message, <in transmission systems>**

information which is transmitted in one or several packets from a sender to one or more receivers

[SOURCE: IEC 60050-821:2017, 821-11-29]

3.1.31**multicast**

transmission of the same message to a group of receivers, identified by their Group Address

Note 1 to entry: The term "multicast" is used even if the group includes all receivers.

[SOURCE: IEC 60050-811:2017, 811-37-66]

3.1.32**network**

set of possibly different communication systems which interchange information in a commonly agreed way

[SOURCE: IEC 60050-811:2017, 811-37-68]

3.1.33**network address**

address which identifies a communication device on network layer

248 [SOURCE: IEC 60050-811:2017, 811-37-69]

249 **3.1.34**

250 **network device**

251 components used to set up Consist Networks and Train Networks

252 Note 1 to entry: These components can be passive like cables or connectors, active unmanaged like repeaters,
253 media converters or (unmanaged) switches, or managed active like gateways, routers and (managed) switches.

254 [SOURCE: IEC 60050-811:2017, 811-37-70]

255 **3.1.35**

256 **network layer**

257 layer in the OSI model responsible for routing between different busses

258 [SOURCE: IEC 60050-811:2017, 811-37-72]

259 **3.1.36**

260 **network management**

261 operations necessary to remotely configure, monitor, diagnose and maintain the network

262 [SOURCE: IEC 60050-811:2017, 811-37-73]

263 **3.1.37**

264 **node, <in a train communication network>**

265 device on the train backbone, which can act as a gateway between the train backbone and
266 the consist network

267 [SOURCE: IEC 60050-811:2017, 811-37-74]

268 **3.1.38**

269 **octet**

270 **byte**

271 group of eight binary digits, or eight signal elements representing binary digits, operated on
272 as an entity

273 [SOURCE: IEC 60050-704:1993, 704-16-21]

274 **3.1.39**

275 **open train**

276 train composed of one or a set of consists, where the configuration can change during
277 operation

278 EXAMPLE Locomotive-hauled international UIC (International Union of Railways, the international railways
279 operators association) trains.

280 [SOURCE: IEC 60050-811:2017, 811-37-79]

281 **3.1.40**

282 **railway undertaking**

283 enterprise or organization which is operating trains

3.1.41**packet**

sequence of digital data representing a message or part of a message together with service digits including an address, organized to suit the transmission process and transmitted as a whole

[SOURCE: IEC 60050-721:1991, 721-09-02]

3.1.42**router**

functional unit that establishes a path through one or more computer networks and forwards packets

Note 1 to entry: In OSI conforming computer networks, a router operates at the network layer.

[SOURCE: IEC 60050-732:2010, 732-01-18]

3.1.43**safety related**

carries responsibility for safety

Note 1 to entry: A function, component, product, system or procedure is called safety-related if at least one of its properties is used in the safety argument for the system in which it is applied. These properties may be of functional or non-functional nature. The requirements attributed to the function may be systematic or random integrity requirements.

[SOURCE: IEC 60050-821:2017, 821-01-73, modified: note modified]

3.1.44**service <in a train communication network>**

capabilities and features of a subsystem (e.g. a communication layer) provided to a user

[SOURCE: IEC 60050-811:2017, 811-37-93]

3.1.45**service <in railways>**

service performs transportation of freight or passengers

3.1.46**job**

sequences of transactions

Note 1 to entry: The correctness of the job can be established by determining the correctness of each transaction it performs and the correctness of interactions between transactions.

3.1.47**transaction**

sequences of interactions between system components

3.1.48**switch <in a train communication network>**

MAC bridge as defined in IEEE 802.1D

Note 1 to entry: MAC means "Medium Access Control", a sublayer within the Link Layer ruling which device is entitled to send on the bus.

[SOURCE: IEC 60050-811:2017, 811-37-101]

3.1.49**topology**

possible cable interconnection and number of devices in a given network

[SOURCE: IEC 60050-811:2017, 811-37-106]

3.1.50**Train**

composition of one or a set of consists, which can be operated as an autonomous unit, e.g. containing drives and at least one driver's cab

Note 1 to entry: Trains can be categorized into open trains (see 3.1.39), closed trains (see 3.1.9).

3.1.51**Train Communication Network**

data communication network for connecting programmable electronic equipment on-board rail vehicles

[SOURCE: IEC 60050-811:2017, 811-37-108]

3.1.52**Train Backbone**

bus connecting the consists of a train, in particular the wire train bus, and which conforms to the TCN protocols

[SOURCE: IEC 60050-811:2017, 811-37-107]

3.1.53**Transport Layer**

layer of the OSI model responsible for end-to-end flow control and error recovery

[SOURCE: IEC 60050-811:2017, 811-37-113]

3.1.54**vertical handover**

refers to a network node changing the type of connectivity it uses to access a supporting infrastructure, usually to support node mobility

3.2 Symbols and abbreviated terms

AAA Authentication Authorization Accounting

ACS Adaptable Communication System

ALG Application Layer Gateway

APN Access Point Network

ARP Address Resolution Protocol

ASCII American Standard Code For Information Interchange

BER Bit Error Rate

CBTC Communication-Based Train Control

CCTV Closed Circuit Television

ComID Communication Identifier

CRC Cyclic Redundancy Check, a data integrity check based on polynomial division

DDNS Dynamic Domain Name Server

365	DHCP	Dynamic Host Configuration Protocol
366	DIN	Deutsches Institut für Normung, the German national standardization body
367	DNS	Domain Name Server
368	(D)DoS	(Distributed) Denial of Service
369	ECM	Entity in Charge of Maintenance
370	ECN	Ethernet Consist Network
371	ED	End Device
372	EDGE	Enhanced Data Rates for GSM Evolution
373	ERA	European Railways Agency, in 2017 became European Union Agency for
374		Railways which replaces and succeeds the European Railway Agency (ERA)
375	EMS	Energy Metering System
376	ETB	Ethernet Train Backbone
377	ETCS	European Train Control System
378	ETSI	European Telecommunications Standards Institute
379	EVN	European Vehicle Number
380	FBS	Function Breakdown Structure
381	FCS	Frame Check Sequence
382	FQDN	Fully Qualified Domain Name
383	FRMCS	Future Railway Mobile Communication System
384	FTP	File Transfer Protocol
385	G2T	Ground to Train
386	GCG	Ground Communication Gateway
387	GNSS	Global Navigation Satellite System
388	GSM	Global System for Mobile Communications
389	GSM-R	Global System for Mobile Communications – Railway
390	GPRS	General Packet Radio Service
391	HSCSD	High Speed Circuit Switched Data
392	HSPA	High Speed Packet Access
393	HTTP	HyperText Transfer Protocol
394	HTTPS	HyperText Transfer Protocol Secure
395	ICMP	Internet Control Message Protocol
396	ID	Identifier
397	IDS	Intrusion Detection System
398	IEEE	Institute of Electrical and Electronics Engineers, New York
399	IETF	Internet Engineering Task Force
400	IP	Internet Protocol
401	JSON	Java Script Object Notation
402	LTE	Long Term Evolution
403	MAC	Medium Access Control, a sub-layer within the Link Layer ruling which device is
404		entitled to send on the bus
405	MAR	Mobile Access Router
406	MCG	Mobile Communication Gateway

407	MD	Message Data
408	MQTT	Message Queuing Telemetry Transport
409	MVB	Multifunction Vehicle Bus
410	N/A	Not Applicable
411	NSS	Network Selection Service
412	OMTS	On-board Multimedia and Telematic Services
413	OSI	Open System Interconnection [SOURCE: IEC 60050-716:1995, 716-01-20]
414	OTIF	Intergovernmental Organisation for International Carriage by Rail
415	PAM	Pluggable Authentication Module
416	PCG	Partner Communication Gateway
417	PNAT	Port Network Address Translation
418	QoS	Quality of Service
419	RFC	Request For Comments, Internet Standard published by the Internet Task Force
420		(IETF)
421	RTP	Real-Time Transport Protocol
422	RTCP	RealTime Control Protocol
423	RU	Railway Undertaking
424	SBS	System Breakdown Structure
425	SCP	Secure Copy
426	SDT	Safe Data Transmission
427	SFTP	SSH File Transfer Protocol
428	SSH	Secure Shell
429	T2G	Train to Ground
430	TBN	Train Backbone Node, generic name of a node connected to the train backbone
431		independently of technology used.
432	TCMS	Train Control and Monitoring System
433	TCN	Train Communication Network, a set of communicating vehicle and Train
434		Backbones
435	TCP	Transmission Control Protocol
436	TIS	Train Information Service
437	TLOS	Train Location Service
438	TLS	Transport Layer Security
439	TRDP	Train Real Time Data Protocol
440	TTDB	Train Topology DataBase
441	TWS	Train Wake-up Service
442	TTS	Train Telemetry Service
443	UDP	User Datagram Protocol
444	UMTS	Universal Mobile Telecommunications System
445	UIC	International Union of Railways, the international railways operators association
446	UID	Unique Identifier
447	URI	Uniform Resource Identifier
448	UML	Unified Modelling Language
449	VoIP	Voice over IP

450	VPN	Virtual Private Network
451	XML	eXtensible Markup Language
452	WiFi	Wireless Fidelity
453	WLAN	Wireless Local Area Network
454	WTB	Wire Train Bus

455 **3.3 State diagram conventions**

456 State diagrams are defined following the notation of UML state machines.

457 **4 Board to Ground Communication system architecture**

458 **4.1 General**

459 This document addresses the train to ground communication of the related data which is
460 produced and/or consumer by users. Examples of such users include:

- 461 a) Railway undertaking.
- 462 b) Infrastructure Manager.
- 463 c) Fleet Control Centre Operator.
- 464 d) Traffic Manager.
- 465 e) ECM (Entity in Charge of Maintenance).
- 466 f) Fleet owner.
- 467 g) Train manufacturer.
- 468 h) Train subsystem supplier.
- 469 i) Authorised Third Parties (e.g. multimedia contents providers, energy data user)
- 470 for the transferring of the related data.

471 NOTE Some of the users listed above can be part of the same organization.

472 **4.2 Requirements**

473 The requirements for Board to Ground communication are set out in Table 1.

474 To aid understanding of these requirements, an example of Board and Ground architecture is
475 illustrated in Figure 1 and in Figure 2.

476

Table 1 – Board to ground requirements

Requirement number	Requirement	Additional information
1	The interoperable board-to-ground communication system shall fulfil the user needs related to non-safety related applications	Safety related communication is not in the scope of this document.
2	The communication system shall include a communication part on-board (MCG) and a part on ground (GCG)	MCG = Mobile Communication Gateway GCG = Ground Communication Gateway
3	The board-to-ground communication system shall use any available wireless IP link (bearer)	The wireless IP link connects the MCG and the GCG. The switching and selection of wireless links to be used is application dependent. A private radio link can also be used, e.g. GSM-R
4	MCG shall be connected to ground applications via the GCG. Ground applications can reach the MCG via the GCG.	
5	It shall be possible to have multiple MCGs in the same consist	Multiple MCGs can be used either for redundancy management or for load balancing.
6	In order to provide redundancy of the board to ground communication function, the system shall allow the use of a MCG located in another consist of the same train.	
7	It shall be possible to have multiple GCGs on ground serving the same train. The default GCG shall be unique, as requested by the registration process. It is allowed to have a unique GCG for each fleet.	
8	The MCG shall be able to act as an application gateway or as a router. The router can be part of the MCG. The IP addresses on-board shall be consistent with the IP addresses on ground in case that MCG is a router.	
9	Train composition changes resulting from consist coupling and uncoupling shall be managed.	
10	A consist shall be identified by a unique symbolic name	e.g. EVN + n where n is the identification of the MCG within the consist. EVN may be OTIF at international level
11	A consist shall announce and register itself to the GCG. The GCG shall be addressable by a unique symbolic name/IP address. MCG shall provide identification information about the composition to allow the GCG to match this for addressing.	
12	An application can request a job. A job can be started both by on-board applications and by ground applications	
13	A job can result in a number of transactions	
14	A transaction shall be initiated either by the MCG or by the GCG. A transaction shall be initiated either by on-board applications or by ground applications.	
15	End devices on ground are reachable by unique symbolic name and are addressable by a unique symbolic name.	

Requirement number	Requirement	Additional information
16	MCGs on trains shall be reachable from ground by the unique symbolic name and are addressable by a unique symbolic name. This address can be statically defined or dynamically assigned, e.g. by a DHCP server at ground	See also Requirement 10
17	T2G network infrastructure shall offer a means to ensure secure MCG reachability by GCG and vice versa.	
18	The ground network infrastructure shall take care about the security measures necessary on ground to protect against cyber-attacks.	
19	The ground network infrastructure shall provide a DNS server for resolving TCN-URI addresses to IP addresses.	
20	The MCG shall not accept the request to establish a communication channel from the GCG	Communication at application level can be initiated either by on-board applications or by ground applications

4.3 Mobile communication network architecture

4.3.1 General

The overall communication infrastructure can be separated into the train on-board communication network and the off-board (ground) communication system.

The train on-board communication network is defined in IEC 61375-1 as a hierarchical structure with a train backbone for the communication along the train and subordinated consist networks for inner-consist communication (see Figure 1).

4.3.2 On-board network interface

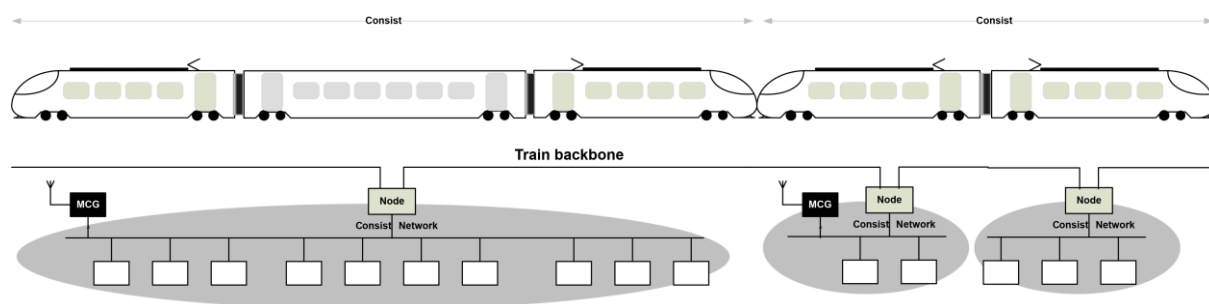


Figure 1 – Train on-board communication system (example)

The MCG connects the on-board communication network to the ground communication system, the Figure 2 illustrates an example of the architecture.

For the specification of the on-board to ground communication, the architecture of the ground communication system is irrelevant as long as the requirements of 4.2 are fulfilled.

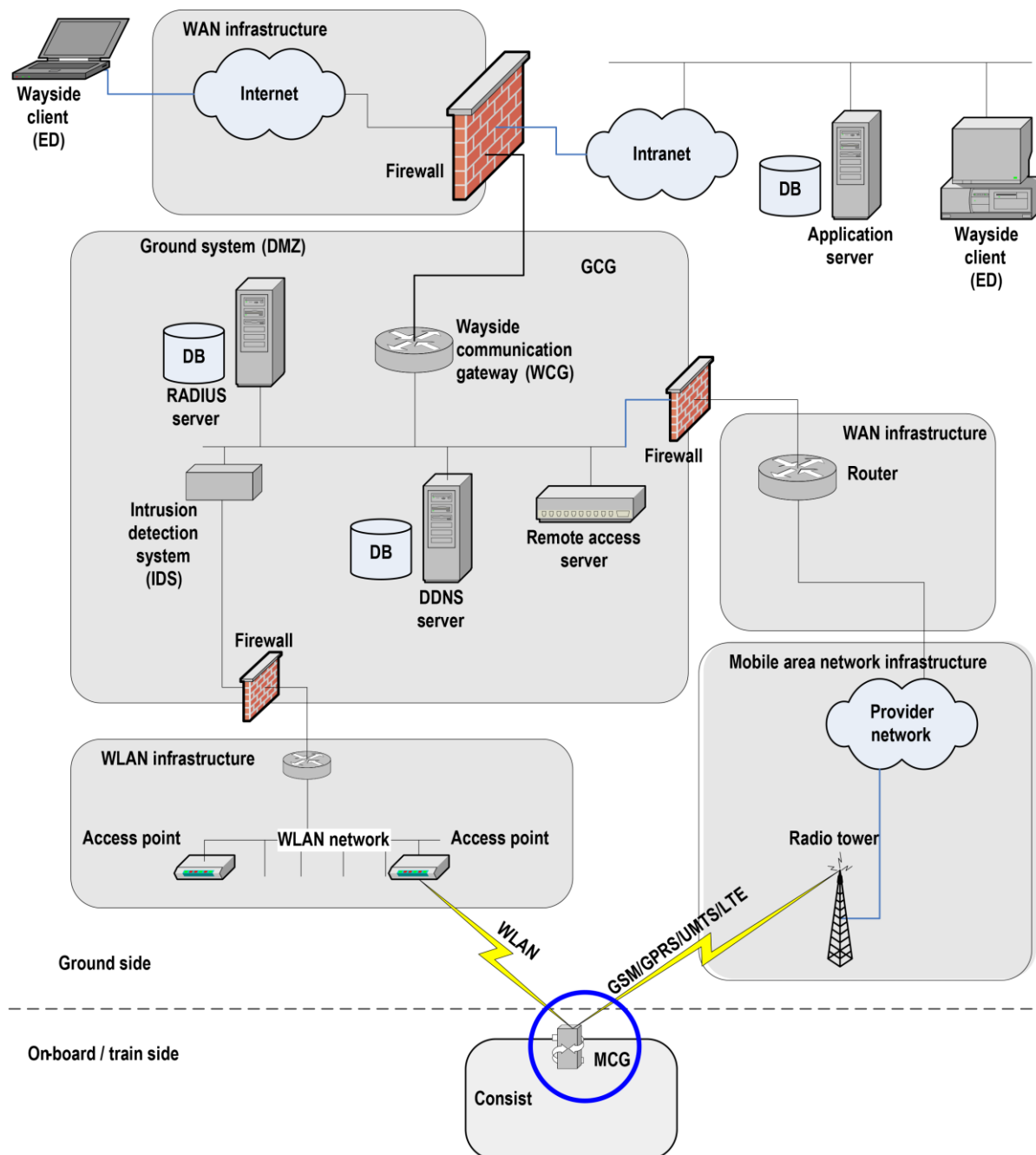


Figure 2 – Ground communication system (example)

4.4 System breakdown structure

4.4.1 General

According to the essential requirements specified by Table 1, the System Breakdown Structure and the Functional Breakdown Structure are specified by the following subclauses.

The system breakdown structure is limited to board-to-ground communication first level.

The second level is split between:

a) on-board sub-system level.

b) ground sub-system level.

4.4.2 System breakdown structure at board-to-ground system level

The Table 2 lists the elements relevant to the system breakdown structure (SBS) at first level.

Table 2 – Board-to-ground system breakdown

No.	System	Description
1	MCG	The Mobile Communication Gateway is specified by this document and is intended as a train-side sub-system providing board-to-ground services to the on-board end devices or as a communication function embedded into the on-board End device.
2	Wireless link	It includes bearers, intranet and internet which are not covered by the requirements specified by this document.
3	GCG	The Ground Communication Gateway is specified by this document in terms of its services and interfaces.

4.4.3 System breakdown structure at MCG sub-system level

The Table 3 lists the elements of the MCG which are relevant to the system breakdown structure at second level.

Table 3 – MCG sub-system breakdown

No.	Sub-system	Description
1	Radio technology	Multiple bearers based on available radio technologies are possible (e.g. GPRS, UMTS, LTE, WiFi)
2	Radio link interface	Any type specified by ITU, ETSI or IEEE
3	Consist/train network interface	ECN/ETB interface
4	Communication gateway/router	MCG behaves as a router or as an application gateway respecting the security access requirements and/or train mode which is the train active state (e.g. operation, maintenance, commissioning)
5	Communication/application profiles	The requirements for this element are specified taking into account IEC 61375-2-3 and IEC 62580-1

4.4.4 System breakdown structure at GCG sub-system level

The Table 4 lists the elements of the GCG which are relevant to the system breakdown structure at second level.

Table 4 – GCG sub-system breakdown

No.	Sub-system	Description
1	Communication/application profiles	
2	Consist/composition registration	
3	Identity management	

4.5 Functional breakdown structure

The functional breakdown structure (FBS) is specified only on the sub-systems MCG and GCG.

No functional breakdown structure of the wireless link is specified, in fact the specification of such element is not covered by this document, but it is assumed that the wireless link is provided by private or public wireless network specified by ITU, ETSI or IEEE, etc.

The Table 5 gives an example of the sub-functions which are relevant to the FBS of the MCG.

Table 5 – An example of the MCG function breakdown

No.	Function	Description
1	Radio link front-end	Interface for management of the physical radio bearer
2	Announcing function	It is the on-board function involved in the registration process to the ground infrastructure
3	AAA check function	Authentication, authorisation and accounting validation for applications
4	Firewall and NAT function	Network protection from unauthorized access
5	Network Selector function	Selection of suitable radio network
6	Session Manager function	Management of application context handling during a job
7	Message Data Handling Function	Management of data class Message Data
8	Bulk Data Handling function	Management of data class Bulk Data
9	Streaming Data Handling function	Management of data class Streaming Data

The Table 6 gives an example of the sub-functions which are relevant to the FBS of the GCG.

Table 6 – An example of the GCG function breakdown

No.	Function	Description
1	Radio link front-end	
2	Internet interface with Firewall	
3	AAA (Authentication, Authorisation, Accounting)	
4	DDNS (Dynamic Domain Name Server)	
5	Data encryption and decryption	Alternatively, this functionality can be provided at application level
6	IDS (Intrusion Detection System)	

4.6 Mobile Communication Gateway

4.6.1 Architecture

4.6.1.1 General

Any on-board device, carrying a function, which needs to communicate with a function hosted by a ground system, shall use one of two possible architectural options:

Option 1: Shared communication unit to be used by one or more on-board functions/devices

Option 2: Dedicated communication unit to be used by one specific function/devices

4.6.1.2 Option 1: Shared communication unit

When this option is chosen, the function carried by the on-board device communicates, using an end device interface on the consist network, with the MCG which offers board-to-ground communication services as a router or as a gateway.

Figure 3 shows the layered architecture of the on-board end device and the MCG, communicating on the consist network. The Figure 3 shows the references to the parts of the TCN series which specify the requirements of each layer.

Any function means any TCMS or OMTS function which is carried by the end device. One end device can carry more than one function; for clarity the layered architecture in Figure 3 shows only one function.

The gateway functionality shall be used when the on-board device wishes to establish a connection during the normal and/or automatic operational state of the train. In this case the ground system is not able to have a direct access to the on-board end device; the MCG gateway application provides the requested level of security by means of authentication, authorisation and encryption services.

The router functionality may be used when the state of the train is commissioning or maintenance, or where application communication requirements demand this (e.g. CCTV) and appropriate security access methods are deployed. In this case a direct access of the ground system to the on-board device is granted.

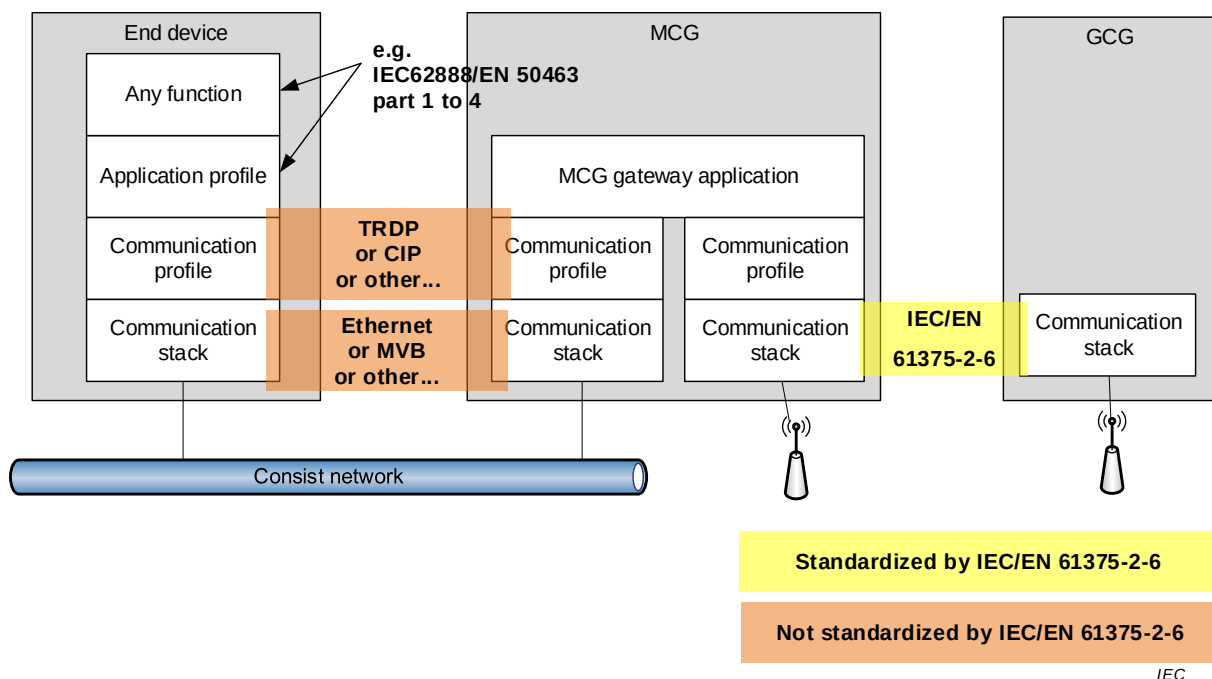


Figure 3 – Option 1: End device board to ground communication via MCG

4.6.1.3 Option 2: Dedicated communication unit

When this option is chosen, the function carried by the on-board device communicates, using an embedded wireless interface, with the function carried by the ground system.

The layered architecture of end device is shown in Figure 4.

Any function means any TCMS or OMTS function which is carried by the end device. One end device can carry more than one function; for clarity the layered architecture in Figure 4 shows only one function.

The wireless stack shall provide communication services at the relevant security level according to the train state ensuring that no direct access to the on-board device is granted to the ground system when the train is in operational or automatic mode. The access shall be provided by communication services which ensure the requested level of security by means of authentication, authorisation and encryption.

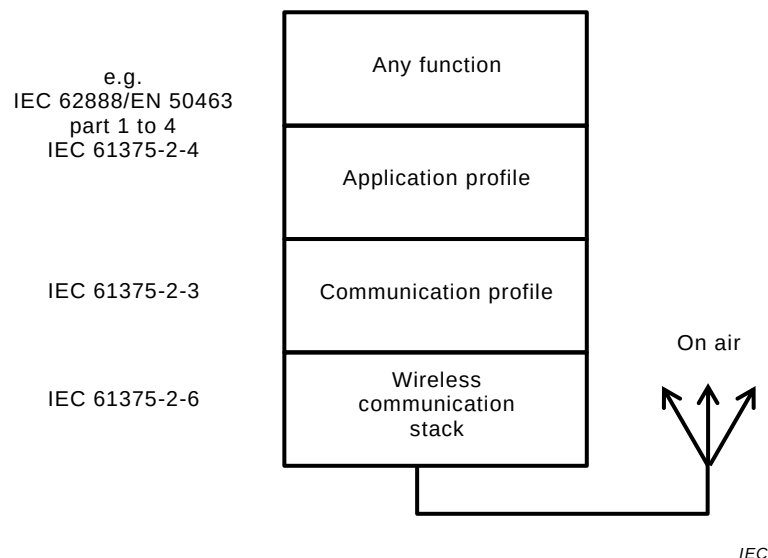


Figure 4 – Option 2: End Device board to ground communication via dedicated interface

4.6.2 Mobile communication gateway

An abstract model of a MCG is shown in Figure 5. The heart of the MCG is a mobile access router which interconnects on-board networks with ground networks. The abstract model can be implemented using multiple physical architectures (e.g. a separated processing unit plus a separate router or a fully integrated MCG device) as long as the required MCG services and interfaces are provided.

Towards ground, the MCG shall provide one or multiple radio interfaces, each is related to a specific radio technology and each connects to the ground network.

Examples of radio technologies are:

- GSM (and with its extensions HSCSD, GPRS, EDGE)
- UMTS (and with extensions like HSPA)
- LTE
- WLAN, as specified in IEEE 802.11

NOTE 1 Other suitable technologies may be added as they become available.

NOTE 2 The different mobile technologies may be implemented in a Mobile Access Router as part of the MCG. The MAR may be a separate unit.

The requirements to address the selection of radio interfaces for data communication are set out in 4.9.

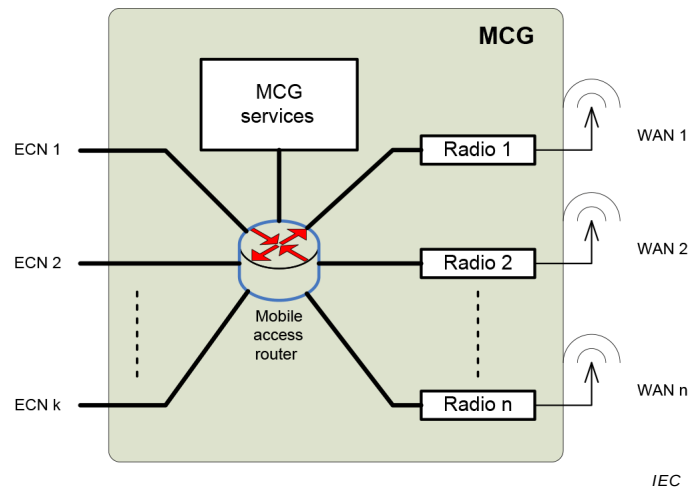


Figure 5 – MCG abstract model block diagram

Towards on-board, the MCG shall provide at least one interface which allows to connect to the on-board network, e.g. an ECN. In case of multiple consist networks in a consist, the MCG may support multiple interfaces, one for each consist network.

NOTE 3 A minimal implementation of a MCG provides one on-board interface and one radio interface, e.g. a WLAN.

Besides the mobile access router, the MCG supports MCG services, executed on a service platform which is connected to the mobile access router. These services are used to establish and to support the on-board to ground communication and are also important with respect to security aspects. Services provided by the MCG service platform are defined in 4.9.

To support security, the MCG provides a firewall between:

- radio interfaces (to control data flow between different radio carriers)
- radio interfaces and on-board interfaces (to control data flow between on-board and ground)
- on-board interfaces (to control data flow between on-board consist networks which belong to different security zones)

Details on the firewall and further security measures are defined in 4.9.

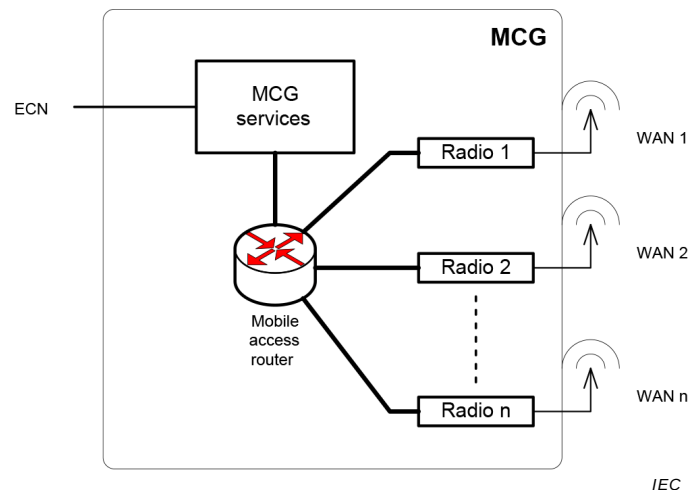


Figure 6 – MCG configured as ALG

Figure 6 shows an abstract model how the MCG can be acting as an ALG. The gateway functionality is handled in the scope of the MCG Services, the latter are acting as an intermediary between the ECN and the ground side.

4.7 Mobile communication redundancy

4.7.1 General

Figure 7 depicts an example for a board to ground architecture able to provide mobile communication redundancy:

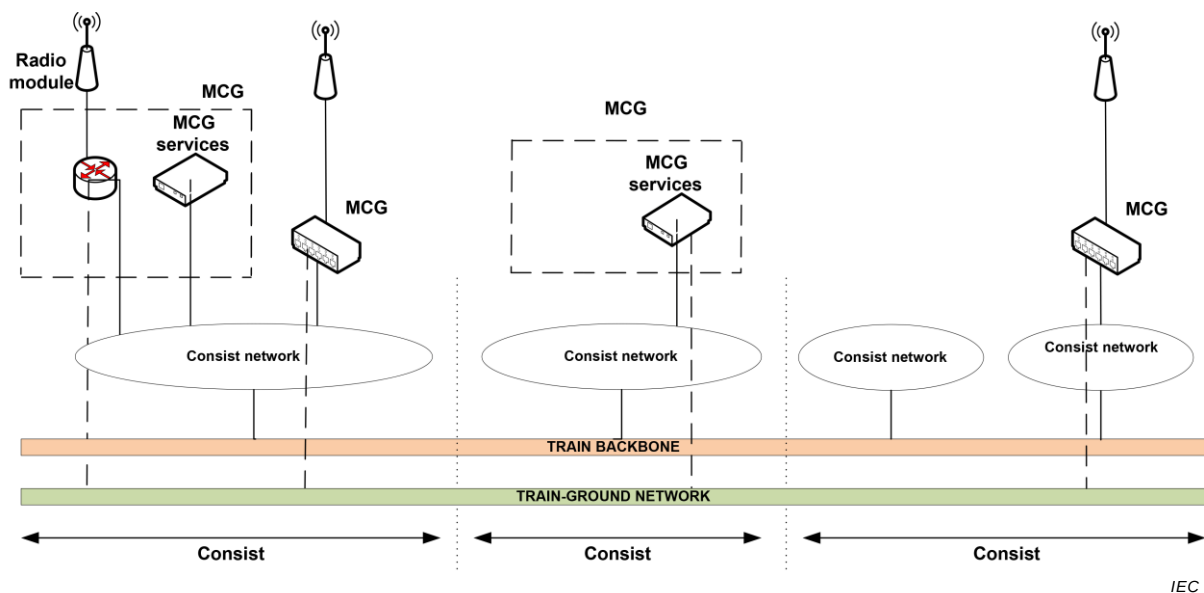


Figure 7 – Architectural example of redundant Board to Ground communication

The following features in this example can be identified:

- A consist contains one or more consist networks.
- A consist network can contain zero or more MCGs. In order to be able to use board to ground communication, it is necessary that there shall be at least one MCG per train.

- A MCG can be connected to the following networks in the train:
 - to a consist network
 - to a separate network (here called “Train-Ground Network”) that is separated from the TCMS network (e.g.: This could be an OMTS network)
- A MCG internally contains components as described in 4.6, e.g.
 - MCG Services
 - a Mobile Access Router (MAR)
 - a connection to a radio module

The board to ground communication redundancy requirements are dependent upon the needs of the applications which are to be supported. The two following approaches to redundancy may be used:

- Full performance redundancy, see 4.7.2
- Reduced performance redundancy, see 4.7.3

4.7.2 Full performance redundancy

The full functional redundancy is obtained by the duplication of the MCG.

Two architectures are suggested for the full performance redundancy:

a) Cold stand-by

This architecture provides two identical MCGs. One is active and one is switched off. When the active MCG fails, a manual intervention is necessary in order to switch off the failing unit and switch on the redundant unit. It is to be noted that such operation may require controlled conditions in order to be executed, e.g. train stopped in a station.

b) Warm stand-by

This architecture provides two identical MCGs. One is active and one is switched on and monitors the communication on the consist network without offering any service to the End devices. When the active MCG fails, a voting unit detects the failure, switches off the failing MCG and enables the redundant unit. This event should be detected by the application which is in charge to re-establish the communication link to the ground system.

4.7.3 Reduced performance redundancy

This architecture provides two identical MCGs located in two different consists/vehicles of the same train. Both MCGs are active. The on-board applications are using the services of the MCG which is attached to the same consist network.

When one MCG is failing, the application using such a MCG subscribes services on the second MCG, reaching such a MCG via the train backbone.

4.8 Train composition changes

The train composition changes are supervised by the Train Information Service (TIS). The TIS provides an interface to inform the GCG about the current train information and about changes in the current train information. The TIS may use the train topology database (TTDB) which is a repository for all the information related to the actual train composition and the actual ETB state.

It is necessary that there shall be at least one TIS active per train. The TIS redundancy requirements are dependent upon the needs of the applications which are to be supported.

The status of implementation of the TIS at device or composition level is summarised in the Table 7 and Table 8:

Table 7 – Device – status of implementation of the TIS

Device	Implementation
End device	optional
MCG	Mandatory

Table 8 – Composition – status of implementation of the TIS

Composition	Implementation
Consist	optional
Train	Mandatory

In a "fully functional real train", at least one device performing an instance of the TIS shall be available on-board. TIS Redundancy may be managed at train level.

The TTDB is specified by IEC 61375-2-3. Another example for train topology database is the Node Address and Attribute Directory NADI according to UIC leaflet 556.

The TIS allows GCG to retrieve information about the actual train composition.

Furthermore, the TIS provides, through the MCG, a service for the notification about a train composition change.

Detailed requirements of the TIS are in 6.3.3.

4.9 Security

4.9.1 Security zones

The security architecture of an on-board to ground communication system may be modelled with the concept of 'zones' and 'conduits' as defined in IEC 62443. A zone is defined as a grouping of logical or physical assets that share common security requirements. If equipment in the zone has a security level not equal or higher than the requirement level, extra security measures need to be taken. Each zone can be more exactly defined by a zone definition document which specifies the security requirements of a zone.

It is essential that communication between zones only occurs via defined conduits. Conduits implement those security measures which are needed to have controlled access to the zone, resist DoS attacks, prevent the transfer of malware and protect network traffic integrity and, if needed, confidentiality. Typically, the security measures implemented within conduits are intended to mitigate the difference between a zone's security level capability and its security requirements.

A security level (SL) shall be assigned to each zone and each consist. The security level shall be based on a security analysis and following the recommendations and the railway specific profiles given in IEC 62443-3-3, as for instance given in DIN VDE V 0831-104.

A simplified zone model of the on-board to ground architecture is shown in Figure 8.

On-board of trains are identified the following zones:

- TCMS safety zone, dealing with safety and operation critical data (e.g. brakes, doors). The safety zone is typically embedded in the operational on-board network as defined in IEC 61375-2-3.
- TCMS regular zone, dealing with non-safety related data (e.g. diagnostics, HVAC). The regular zone is typically embedded in the operational on-board network as defined in IEC 61375-2-3.
- OMTS zone, dealing with multimedia and telematics services-oriented data. The OMTS zone is typically embedded in the multimedia on-board network as defined in IEC 61375-2-3.

The counterparts on ground could be for example:

- Operational centre zone, dealing with operation control data
- OMTS centre zone, dealing with multimedia and telemetric services-oriented data

In most cases there will exist more zones on ground, e.g. zones for the centres but also a zone for the open internet. The on-ground zones are not within the scope of this document.

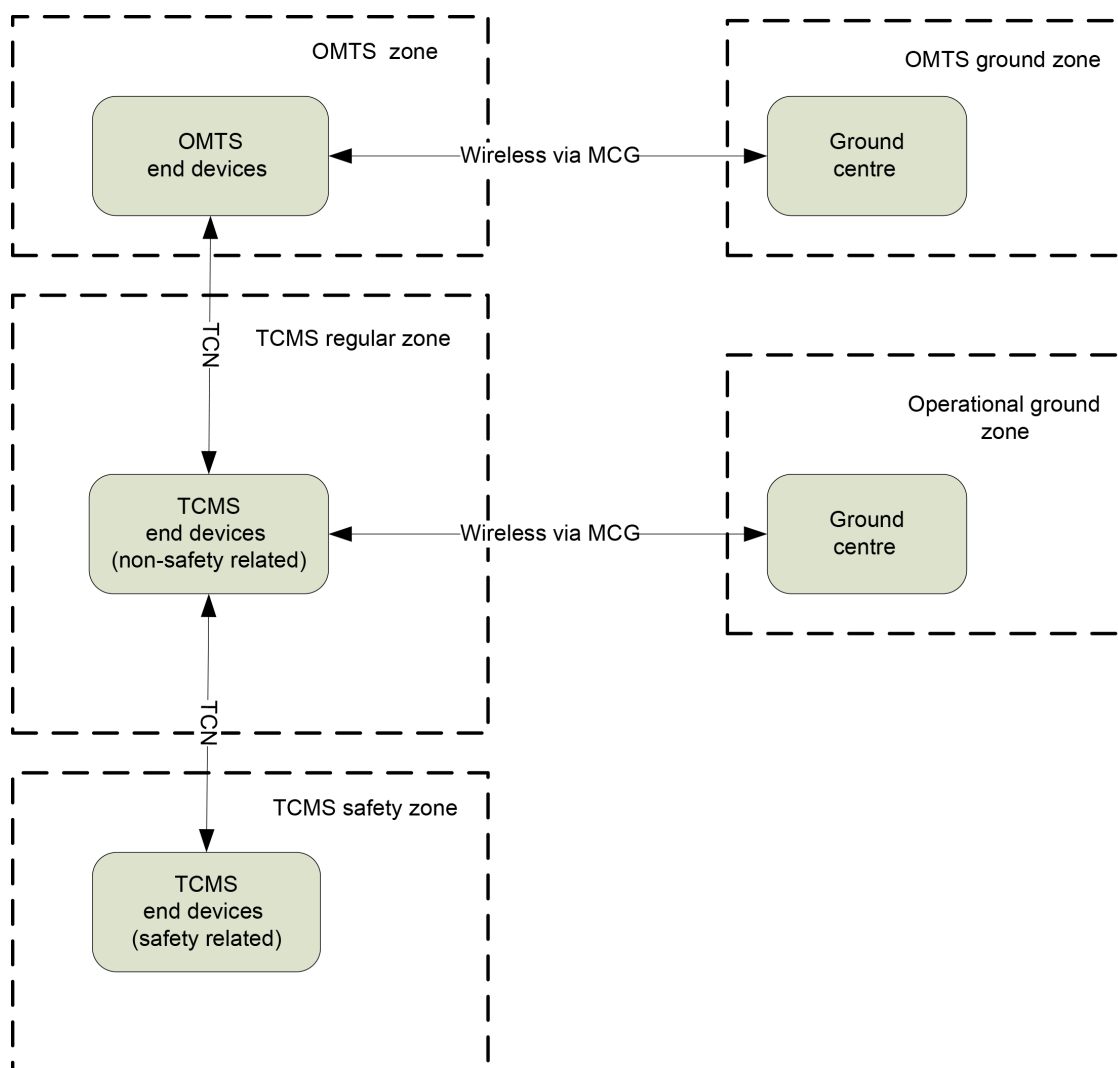


Figure 8 – Security zones (simplified)

NOTE There exists no conduit between the TCMS safety zone and ground, meaning that no direct exchange of safety related information can take place between train and ground.

IEC 61375-2-3 requires that the TCMS safety zone belongs to a closed system as defined in IEC 62280. Because TCMS safety zone and TCMS regular zone normally share the same consist network, the MCG connecting the TCMS regular zone with the operational ground zone shall be designed in a way that the closed system conditions are not violated.

4.9.2 Security measures

Security measures which are applicable for the conduits connecting train to ground are listed in Table 9.

4.9.3 Authentication authorization accounting model

The model identifies the single components which are essential in a general system interaction:

- the composition moving on the track
- the operator infrastructure, composed of its different single components
- the wayside infrastructure, except for the signalling system
- the user, who operates on the composition or in the depot. They could be a driver, a conductor, a maintenance operator, a commissioning operator, etc.
- the services active on-board and on ground.

The model considers the different communication channels that are supposed to be used in a typical communication scenario (e.g wireless or wired).

An identifier (1 to 5) is associated to each communication link that can be considered as an "operational environment", see Figure 9. Each operational environment in its turn is a basis for the identification of communication use cases and can be summarized as follow:

- Operational Environment 0 – Communication inside one operator central network using standard IT practices
- Operational Environment 1 – Inside train communication link – wireless or wired channel
- Operational Environment 2 – Composition to operator communication link – wireless channel
- Operational Environment 2a – Composition and ground infrastructure belongs to the same operator
- Operational Environment 2b – Composition and ground infrastructure belongs to different operators
- Operational Environment 3 – Wayside communication link – wireless or wired channel
- Operational Environment 4 – Operator to operator communication link – wired channel
- Operational Environment 5 – User communication link – wireless channel

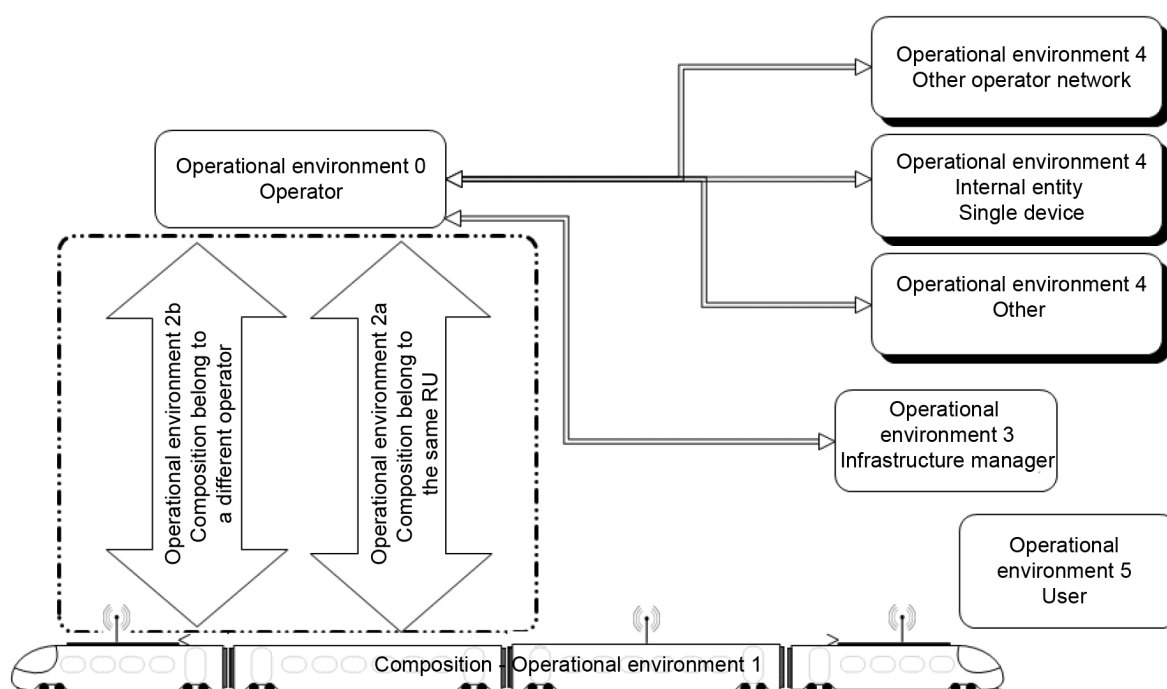


Figure 9 – Authentication, authorization and accounting model

Considering the whole integrated system, there is a need for each system component to be authenticated and authorized to be a part of the network. In order to control the constitution of the integrated system and the admitted components, it is important to recognize and authenticate the single nodes (e.g. composition or device), the single elements but also the provided applications in order to manage and evaluate what could be inside the system. In any case the model adopted for the system is also to grant the scalability of the security solution and in particular of the authentication model. Considering that nodes, applications, and users could be distributed, it is necessary to adopt and use an authentication solution that can support a distributed approach but also maximum flexibility.

The access to the internal resources of the composition is through the MCG.

Open trains, wide range of mission profiles and cross-border connections raise some questions about right access to information available on board. An example for maintenance data:

- RU shall have access to all equipment it bought, but not to the equipment it did not.
- Equipment manufacturers shall have access to the equipment it sold, if so allowed by the RU.
- Equipment manufacturers shall have no access to data of other manufacturers, except if has got the access rights.

Troubleshooting procedures need to be shared across several entities, but the reliability data are surely “private” information.

The provided model has to grant different levels of access rights per user and per maintained data or available functions/applications. For this reason, it is necessary to associate to each user a set of information related to the roles he/she can assume, the resources or functionalities that can be accessed and the level of operations that can be done on the requested access (e.g. read, execution, etc.). Also the data should be classified and maintained in order for the system to be able to state every time who has the right of access to these data.

772 Furthermore, it is possible to set-up ad hoc signature and/or cryptographic method that can be
773 invoked on user or application requests that can really protect transmitted data from external
774 modification or simple reading.

775 The devices and functional addressing requirements are detailed in Clause 8.

776 The AAA function manages locally for each user the several access profiles defined by the RU
777 general policy. The token-based AAA method allows to trust locally a user identity when the
778 composition is not connected to the RU network.

779

Table 9 – Security measures

Security measure	Supported by	Description
Firewall	MCG	A firewall between two networks permits the filtering of IP packets based on the content, as for example: • IP source address • IP destination address • UDP/TCP source port number • UDP/TCP destination port number • TRDP ComId The MCG firstly authenticates itself before providing a mechanism to filter IP packets based on the content, meaning that it supports connection tracking of for example TCP and UDP sessions. With connection tracking, it can for instance prevent the opening of a session from an untrusted network.
PNAT	MCG	Port and network address translation. This feature prevents real IP addresses and port numbers of ED devices within a trusted network from being seen in an untrusted network. This feature is often supported by firewall implementations.
Authentication and Authorization	MCG GCG	A ground device (e.g. GCG) trying to connect to the MCG shall first authenticate itself before access to MCG services are granted. The authentication procedure depends on the used radio technology (e.g. SIM, IEEE 802.1X). Authentication shall be enforced either by the application (e.g. through TLS 1.2 with mutual authentication) or on the network level (e.g. using an IPSEC/IKEv2- or SSL-VPN with mutual authentication).
Encryption	MCG GCG ED	Data exchanged should be encrypted and its integrity protected by using established standards like TLS 1.2 or HTTPS.
VPN	ED	A VPN between trusted ED includes authentication as well as encryption of transferred data. To establish a VPN between a ground ED and the MCG will in most cases be sufficient for board-to-ground communication
ALG	MCG	An ALG between any two networks provides full control of exchanged data. From each network, the ALG is seen as an ED, so the ALG takes the role of a proxy for each function which is executed on a 'hidden' ED. The MCG is acting as ALG for message data and file transfer communication services.
Security event logging	MCG GCG	Security related events are logged. Security related events should be: • Authentication attempts (positive and negative) • Credential modification • Firewall activation/deactivation/reconfiguration • Firewall events (e.g. access to blacklisted IP addresses, ports) • Unexpected incoming traffic • DHCP event (e.g. unknown host identifier) • System time event (e.g. update)
Security Updates	MCG GCG ED	Security vulnerability monitoring (SVM) and Security updates are key for keeping the components secure over time. Components shall be able to be updated with security patches in a timely manner (locally or over the air). Components shall check integrity and authenticity of software updates by evaluating cryptographic signatures.

4.9.4 Network and MCG classification

4.9.4.1 Categories

IEC 62280 defines three categories of transmission systems. Category 1 is defined as a closed transmission system, while category 2 and category 3 are open transmission systems.

Take into account that the IEC 61375-3-4 and IEC 61375-2-3 do not define special security measures (e.g. ED authentication and data encryption, to be used within the operational on-board network), the operational on-board network, if it is used for the transmission of safety related data, is considered as closed category 1 transmission system according to the IEC 62280.

The on-board multimedia network can be, depending on its offered services and security measures, be an open category 2 or category 3 transmission system.

Depending on the role of the MCG, e.g. whether it connects the on-board operational network or the on-board multimedia network to ground, it needs to ensure that the related categories are kept.

Following the definition of transmission system categories, the MCG can be classified the same way according the categories listed in Table 10:

Table 10 – MCG categories

Category 1 MCG	MCG which connects a closed transmission system to an open transmission system (Example: connecting an operational network or a combined operational/multimedia network to ground)
Category 2 MCG	MCG which connects an open category 2 transmission system to an open category 2/3 transmission system (Example: connecting a multimedia network to ground)
Category 3 MCG	MCG which interconnects category 3 transmission systems (Example: internet routers)

The following subclauses define security measures for a category 1 MCG.

MCG of categories 2 and 3 are out of the scope of this document.

4.9.4.2 MCG as closed system barrier (category 1 MCG)

The characteristics of a closed transmission system (category 1 transmission system), see Table 10, are defined as follows:

- The number of pieces of connectable equipment – either safety-related or not – to the transmission system is known and fixed.
- The physical characteristics of the transmission system (e.g. transmission media, environment according to the design hypothesis, etc.) are fixed and unchanged during the life cycle of the system.
- The risk of unauthorized access is considered negligible.

The security requirements for the MCG, derived from the listed characteristics, are listed in Table 11:

813

Table 11 – Security requirements

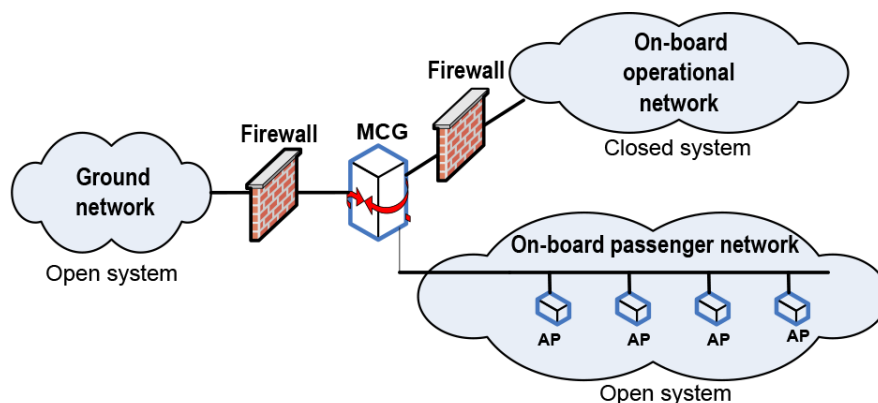
Requirement number	Requirement
S1	The MCG shall be the end point of the communications link between the train and the wayside
S2	The MCG shall also be the boundary of the train consist networks, e.g. MVB and Ethernet (ECN)
S3	The MCG shall provide a firewall function which protects the on-board operational network
S4	Once channel connection is established (according to requirement 21), the MCG shall only permit a connection to well defined ports (e.g. port 80) to be made from ground.
S5	In normal operation mode, it shall not be possible to get shell access to the MCG from ground. Shell access from ground may be blocked by the firewall.
S6	It shall only be possible for the MCG to communicate with a known set of authenticated and registered ground devices.
S7	The MCG shall not send safety related messages to ground.
S8	The MCG shall be able to receive security updates/patches.
S9	The MCG shall check the integrity and authenticity of software updates by evaluating cryptographic signatures.

814

815 NOTE Within the operational network, the MCGs are seen as end devices. From ground, the MCGs are the only
816 points of visibility for the on-board operational network.

817 4.9.4.3 MCG connecting both category 1 and categories 2/3

818 An MCG can be used to connect both category 1 and categories 2/3 transmission systems as
819 it is shown in the example of Figure 10.



820

IEC

821

Figure 10 – MCG connecting open and closed transmission systems

822 In this case, the MCG shall act as a category 1 MCG towards the closed system.

823 This also means in particular that there shall be no possibility to change the configuration of
824 the MCG from either open system.

825 EXAMPLE The firewall in the MCG is configured to block all direct traffic between the open systems and the
826 closed system (everything ending in the MCG services platform), but is more open for traffic between the open
827 systems.