

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Matériel électronique ferroviaire – Réseau embarqué de train (TCN) –
Partie 2-6: Communication train-sol**

IECNORM.COM : Click to view the full PDF of IEC 61375-2-6:2018



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2018 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 21 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Matériel électronique ferroviaire – Réseau embarqué de train (TCN) –
Partie 2-6: Communication train-sol**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 45.060.01

ISBN 978-2-8322-5611-4

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	8
INTRODUCTION.....	10
1 Scope.....	11
2 Normative references	11
3 Terms, definitions, symbols, abbreviated terms and conventions	12
3.1 Terms and definitions.....	12
3.2 Symbols and abbreviated terms	19
3.3 State diagram conventions	21
4 Board to Ground Communication system architecture.....	21
4.1 General.....	21
4.2 Requirements	21
4.3 Mobile communication network architecture	23
4.3.1 General	23
4.3.2 On-board network interface	23
4.4 System breakdown structure	24
4.4.1 General	24
4.4.2 System breakdown structure at board-to-ground system level.....	25
4.4.3 System breakdown structure at MCG sub-system level	25
4.4.4 System breakdown structure at GCG sub-system level	25
4.5 Functional breakdown structure	25
4.6 Mobile Communication Gateway	26
4.6.1 Architecture	26
4.6.2 Mobile communication gateway	28
4.7 Mobile communication redundancy	30
4.7.1 General	30
4.7.2 Full performance redundancy	31
4.7.3 Reduced performance redundancy	31
4.8 Train composition changes	31
4.9 Security	32
4.9.1 Security zones.....	32
4.9.2 Security measures	33
4.9.3 Authentication authorization accounting model	35
4.9.4 Network and MCG classification	37
5 Communication framework	39
5.1 General.....	39
5.2 MCG broker service architecture.....	39
5.3 Addressing concept	40
5.3.1 Use cases.....	40
5.3.2 Consist and train Identification.....	41
5.3.3 T2G Network Borders	41
5.3.4 T2G basic minimum network	41
5.3.5 T2G addressing	42
5.3.6 HTTP-URI.....	44
5.4 Data classes for T2G communication	45
5.4.1 General	45
5.4.2 Communication channel establishment	45

5.4.3	Message data	45
5.4.4	Process data	46
5.4.5	Stream Data	47
5.4.6	Best effort data	47
5.5	Communication protocol	48
5.5.1	General	48
5.5.2	HTTP(S)	48
5.5.3	MQTT (Option)	50
5.6	Communication services	51
5.6.1	General	51
5.6.2	Message data communication service	51
5.6.3	File transfer communication service	55
6	Services and interfaces (MCG)	76
6.1	Overview	76
6.1.1	MCG system service architecture	76
6.1.2	MCG / GCG system service interfaces	77
6.1.3	MCG / GCG communication relationship	78
6.2	Service provisioning	78
6.3	MCG / GCG system service description	79
6.3.1	Communication Services	79
6.3.2	Train Location Service (Option)	82
6.3.3	Train Information Service	88
6.3.4	MCG Network Selector Service	92
6.3.5	Train telemetry service (Option)	94
6.3.6	MCG Train Wake-up Service (Option)	104
7	Services and interfaces (GCG)	105
7.1	GCG Overview	105
7.2	GCG Addressing	107
7.2.1	Wireless MCG Interface	107
7.2.2	Ground GCG Interface	107
7.3	GCG Implementation	108
7.3.1	General (informative)	108
7.3.2	GCG Availability	108
7.3.3	GCG Workload	108
7.3.4	GCG Security	108
7.4	GCG services	108
7.4.1	GCG services protocol	108
7.4.2	GCG Fleet Database	108
7.4.3	MCG-GCG services	109
7.4.4	File transfer communication service	109
7.4.5	Local Ground GCG Interface	109
7.4.6	Home GCG – Foreign GCG services	110
7.4.7	Public Ground GCG services	110
Annex A (normative)	Message presentation	111
A.1	General	111
A.2	Transmission rules	111
A.3	Generic message	111
Annex B (normative)	Telemetry data coding and ordering	112

B.1	General.....	112
B.2	MQTT payload coding	112
B.3	Variables grouping and ordering criterion.....	113
	Bibliography.....	116
	Figure 1 – Train on-board communication system (example).....	23
	Figure 2 – Ground communication system (example)	24
	Figure 3 – Option 1: End device board to ground communication via MCG.....	27
	Figure 4 – Option 2: End Device board to ground communication via dedicated interface	28
	Figure 5 – MCG abstract model block diagram.....	29
	Figure 6 – MCG configured as ALG	29
	Figure 7 – Architectural example of redundant Board to Ground communication	30
	Figure 8 – Security zones (simplified)	33
	Figure 9 – Authentication, authorization and accounting model	36
	Figure 10 – MCG connecting open and closed transmission systems.....	38
	Figure 11 – MCG broker service architecture	40
	Figure 12 – Minimum Train to Ground Network Setup	41
	Figure 13 – A train consisting of four vehicles.....	42
	Figure 14 – Communication stacks	49
	Figure 15 – HTTP(S) MD communication pattern	49
	Figure 16 – HTTP(S) request/event.....	50
	Figure 17 – HTTP(S) response	50
	Figure 18 – Message Data exchange (example).....	52
	Figure 19 – Message Data telegram structure.....	53
	Figure 20 – File upload example.....	56
	Figure 21 – Error case: No ComID 203 received	61
	Figure 22 – Error case: no ComID 206 received, no file uploaded to the wayside.....	62
	Figure 23 – Error Case: No ComID 206 received, file uploaded to the wayside	63
	Figure 24 – Error Case: No ComID 207 received	64
	Figure 25 – File download example.....	65
	Figure 26 – Error case: no ComID 209 received.....	71
	Figure 27 – Error case: no ComID 211 received.....	72
	Figure 28 – Error case: no ComID 210 received.....	73
	Figure 29 – Service architecture	77
	Figure 30 – Service interfaces	78
	Figure 31 – Procedure to establish the radio link from MCG.....	80
	Figure 32 – Procedure to establish the radio link from GCG.....	80
	Figure 33 – Procedure to update the ground DNS server	81
	Figure 34 – Example architecture to provide the train location	83
	Figure 35 – Example procedure to notify about current train location	84
	Figure 36 – Example architecture to notify about train information	88
	Figure 37 – Example procedure to notify about train information	89
	Figure 38 – Illustration of network selector.....	93

Figure 39 – Architecture to provide telemetry data	94
Figure 40 – Procedure to notify about current train location	95
Figure 41 – Example Procedure to wake up the train	104
Figure 42 – Train to Ground interfaces	106
Figure B.1 – MQTT notification payload format	112
Figure B.2 – Example of ordering criteria	114
Figure B.3 – Example of values grouping	114
Table 1 – Board to ground requirements	22
Table 2 – Board-to-ground system breakdown	25
Table 3 – MCG sub-system breakdown	25
Table 4 – GCG sub-system breakdown	25
Table 5 – An example of the MCG function breakdown	26
Table 6 – An example of the GCG function breakdown	26
Table 7 – Device – status of implementation of the TIS	31
Table 8 – Composition – status of implementation of the TIS	31
Table 9 – Security measures	34
Table 10 – MCG categories	37
Table 11 – Security requirements	38
Table 12 – TCN-URI global DNS zone	44
Table 13 – Recommended service parameters for message data	46
Table 14 – Recommended service parameters for process data	47
Table 15 – Recommended service parameters for stream data	47
Table 16 – Recommended service parameters for best effort data	48
Table 17 – HTTP(S) parameters request/response pattern	50
Table 18 – General MD Header	53
Table 19 – General MD Body	54
Table 20 – MD Checksum	54
Table 21 – Message types	54
Table 22 – Message representation	55
Table 23 – File transfer terminology	55
Table 24 – ComID 202: MD header telegram values	57
Table 25 – ComID 202: MD body telegram values	57
Table 26 – ComID 202: MD body: mdPayload object	58
Table 27 – ComID 203: MD header telegram values	58
Table 28 – ComID 203: MD body telegram values	58
Table 29 – ComID 203: MD body: mdPayload object	59
Table 30 – ComID 206: MD header telegram values	59
Table 31 – ComID 206: MD body telegram values	59
Table 32 – ComID 206: MD body: mdPayload object	60
Table 33 – ComID 207: MD header telegram values	60
Table 34 – ComID 207: MD body telegram values	60
Table 35 – ComID 207: MD body: mdPayload object	61

Table 36 – ComID 208: MD header telegram values	66
Table 37 – ComID 208: MD Body telegram values	66
Table 38 – ComID 208: MD Body: mdPayload object	67
Table 39 – ComID 209: MD header telegram values	67
Table 40 – ComID 209: MD Body telegram values	68
Table 41 – ComID 209: MD Body: mdPayload object	68
Table 42 – ComID 210: MD header telegram values	68
Table 43 – ComID 210: MD Body telegram values	69
Table 44 – ComID 210: MD Body: mdPayload object	69
Table 45 – ComID 211: MD header telegram values	69
Table 46 – ComID 211: MD Body telegram values	69
Table 47 – ComID 211: MD Body: mdPayload object	70
Table 48 – Main parts of dITarget URI	74
Table 49 – Main parts of host element	74
Table 50 – Valid “device” label values	75
Table 51 – Valid “vehicle” label values	75
Table 52 – Valid “consist” label values	75
Table 53 – Valid “closed train” label values	76
Table 54 – Valid “train” label values	76
Table 55 – Exemplary dITarget values	76
Table 56 – ComID 240: Capability message	81
Table 57 – ComID 240: MD event body telegram values	82
Table 58 – ComID 240: MD event body: mdPayload object	82
Table 59 – ComID 230: MD request header telegram values	85
Table 60 – ComID 230: MD request body telegram values	85
Table 61 – ComID 230: MD request body: mdPayload object	85
Table 62 – ComID 230: MD reply header telegram values	86
Table 63 – ComID 230: MD reply body telegram values	86
Table 64 – ComID 230/232: MD reply/notification body: mdPayload object	86
Table 65 – Example of latitude/longitude with proposed fixed point notation	87
Table 66 – ComID 232: MD header telegram values	87
Table 67 – ComID 232: MD Body telegram values	87
Table 68 – ComID 234: MD request header telegram values	90
Table 69 – ComID 234: MD request body telegram values	90
Table 70 – ComID 234: MD request body: mdPayload object	90
Table 71 – ComID 234: MD reply header telegram values	90
Table 72 – ComID 234: MD reply body telegram values	91
Table 73 – ComID 234: MD reply body: mdPayload object	91
Table 74 – ComID 236: MD header telegram values	92
Table 75 – ComID 236: MD Body telegram values	92
Table 76 – ComID 240: MD request header telegram values	96
Table 77 – ComID 240: MD request Body telegram values	96
Table 78 – ComID 240: MD reply header telegram values	97

Table 79 – ComID 240: MD reply body telegram values	97
Table 80 – ComID 240: MD reply body: mdPayload object	97
Table 81 – ComID 242: MD request header telegram values	98
Table 82 – ComID 242: MD request Body telegram values	98
Table 83 – ComID 242: MD request body: mdPayload object	99
Table 84 – ComID 242: MD reply header telegram values	99
Table 85 – ComID 242: MD reply body telegram values	100
Table 86 – ComID 242: MD reply body: mdPayload object	100
Table 87 – ComID 243: MD request header telegram values	101
Table 88 – ComID 243: MD request Body telegram values	101
Table 89 – ComID 243: MD request body: mdPayload object	101
Table 90 – ComID 244: MD request header telegram values	102
Table 91 – ComID 244: MD request Body telegram values	102
Table 92 – ComID 244: MD request body: mdPayload object	102
Table 93 – ComID 244: MD reply header telegram values	102
Table 94 – ComID 244: MD reply body telegram values	102
Table 95 – ComID 244: MD reply body: mdPayload object	103
Table 96 – ComID 245: MD request header telegram values	103
Table 97 – ComID 245: MD request Body telegram values	103
Table 98 – ComID 245: MD request body: mdPayload object	104
Table 99 – ComID 238: twsWakeUp MD event header	105
Table 100 – ComID 238: twsWakeUp MD event body	105
Table 101 – ComID 238: twsWakeUp MD event body: mdPayload object	105
Table B.1 – Example of values decoding	115

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.

IECNORM.COM : Click to view the full PDF of IEC 61375-2-6:2018

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

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.

The communication of safety related data between on-board applications and ground applications are out of the scope of this International Standard as well as Internet connectivity service for passengers.

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 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

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

3.1.34

network device

components used to set up Consist Networks and Train Networks

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

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

3.1.35

network layer

layer in the OSI model responsible for routing between different busses

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

3.1.36

network management

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

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

3.1.37

node, <in a train communication network>

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

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

3.1.38**octet
byte**

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

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

3.1.39**open train**

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

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

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

3.1.40**railway undertaking**

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
ALG	Application Layer Gateway
ARP	Address Resolution Protocol
ASCII	American Standard Code For Information Interchange
BER	Bit Error Rate
CCTV	Closed Circuit Television
ComID	Communication Identifier
CRC	Cyclic Redundancy Check, a data integrity check based on polynomial division
DDNS	Dynamic Domain Name Server
DHCP	Dynamic Host Configuration Protocol
DIN	Deutsches Institut für Normung, the German national standardization body
DNS	Domain Name Server
DoS	Denial of Service
ECM	Entity in Charge of Maintenance
ECN	Ethernet Consist Network
ED	End Device
EDGE	Enhanced Data Rates for GSM Evolution
ERA	European Railways Agency, in 2017 became European Union Agency for Railways which replaces and succeeds the European Railway Agency (ERA)
EMS	Energy Metering System
ETB	Ethernet Train Backbone
ETSI	European Telecommunications Standards Institute
EVN	European Vehicle Number
FBS	Function Breakdown Structure
FCS	Frame Check Sequence
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
G2T	Ground to Train
GCG	Ground Communication Gateway
GNSS	Global Navigation Satellite System
GSM	Global System for Mobile Communications
GSM-R	Global System for Mobile Communications – Railway
GPRS	General Packet Radio Service
HSCSD	High Speed Circuit Switched Data
HSPA	High Speed Packet Access
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ID	Identifier
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers, New York
IETF	Internet Engineering Task Force

IP	Internet Protocol
JSON	Java Script Object Notation
LTE	Long Term Evolution
MAC	Medium Access Control, a sub-layer within the Link Layer ruling which device is entitled to send on the bus
MAR	Mobile Access Router
MCG	Mobile Communication Gateway
MD	Message Data
MQTT	Message Queuing Telemetry Transport
MVB	Multifunction Vehicle Bus
N/A	Not Applicable
NSS	Network Selection Service
OMTS	On-board Multimedia and Telematic Services
OSI	Open System Interconnection [SOURCE: IEC 60050-716:1995, 716-01-20]
OTIF	Intergovernmental Organisation for International Carriage by Rail
PAM	Pluggable Authentication Module
PCG	Partner Communication Gateway
PNAT	Port Network Address Translation
QoS	Quality of Service
RFC	Request For Comments, Internet Standard published by the Internet Task Force (IETF)
RTP	Real-Time Transport Protocol
RTCP	RealTime Control Protocol
RU	Railway Undertaking
SBS	System Breakdown Structure
SCP	Secure Copy
SDT	Safe Data Transmission
SFTP	SSH File Transfer Protocol
SSH	Secure Shell
T2G	Train to Ground
TBN	Train Backbone Node, generic name of a node connect to the train backbone independently of technology used.
TCMS	Train Control and Monitoring System
TCN	Train Communication Network, a set of communicating vehicle and Train Backbones
TCP	Transmission Control Protocol
TIS	Train Information Service
TLOS	Train Location Service
TLS	Transport Layer Security
TRDP	Train Real Time Data Protocol
TTDB	Train Topology DataBase
TWS	Train Wake-up Service
TTS	Train Telemetry Service
UDP	User Datagram Protocol

UMTS	Universal Mobile Telecommunications System
UIC	International Union of Railways, the international railways operators association
UID	Unique IDentifier
URI	Uniform Resource Identifier
UML	Unified Modelling Language
VPN	Virtual Private Network
XML	eXtensible Markup Language
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WTB	Wire Train Bus

3.3 State diagram conventions

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

4 Board to Ground Communication system architecture

4.1 General

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

- a) Railway undertaking.
- b) Infrastructure Manager.
- c) Fleet Control Centre Operator.
- d) Traffic Manager.
- e) ECM (Entity in Charge of Maintenance).
- f) Fleet owner.
- g) Train manufacturer.
- h) Train subsystem supplier.
- i) Authorised Third Parties (e.g. multimedia contents providers, energy data user)

for the transferring of the related data.

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

4.2 Requirements

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

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

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	The MCG shall be connected to internet directly or connected to internet via a GCG	Only Authorised Users can reach the train using an Internet connection
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 itself to the GCG. The DDNS shall match the consist symbolic name to the IP address (see Requirement 6)	
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	There shall be different connectivity modes: 1: communication strictly limited between the MCG and only one GCG 2: communication where the MCG can connect to more than one GCG	In mode1 the MCG and GCG have a private link with private IP addresses. Any ground application needs to reach the MCG only through its specific GCG In mode 2 the MCG has a public dynamic IP address which can be used by multiple GCG

Requirement number	Requirement	Additional information
16	End devices on ground are reachable by unique symbolic name/IP and are addressable by a unique symbolic name /IP address.	
17	MCGs on trains shall be reachable from ground by the unique symbolic name/IP and are addressable by a unique symbolic name/IP address. This address can be statically defined or dynamically assigned, e.g. by a DHCP server at ground	See also Requirement 10
18	The ground network infrastructure takes care of the mobility of the MCG IP address	
19	The ground network infrastructure takes care about the security measures necessary on ground to protect against cyber-attacks.	
20	The ground network infrastructure provides a DNS server for resolving TCN-URI addresses to IP addresses.	
21	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

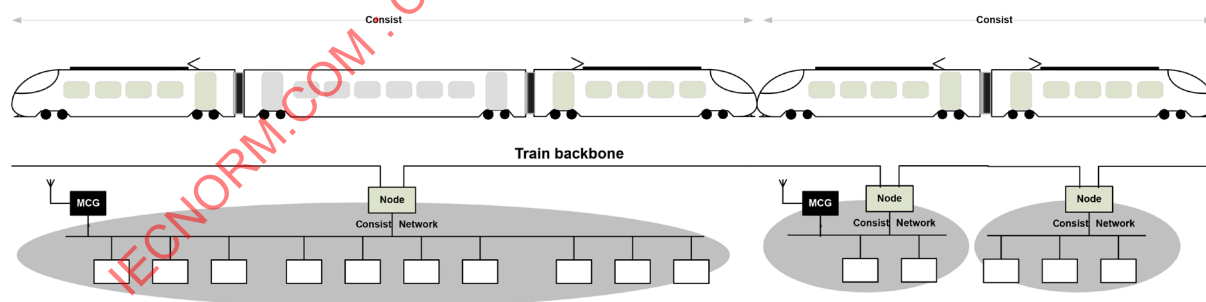
4.3 Mobile communication network architecture

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

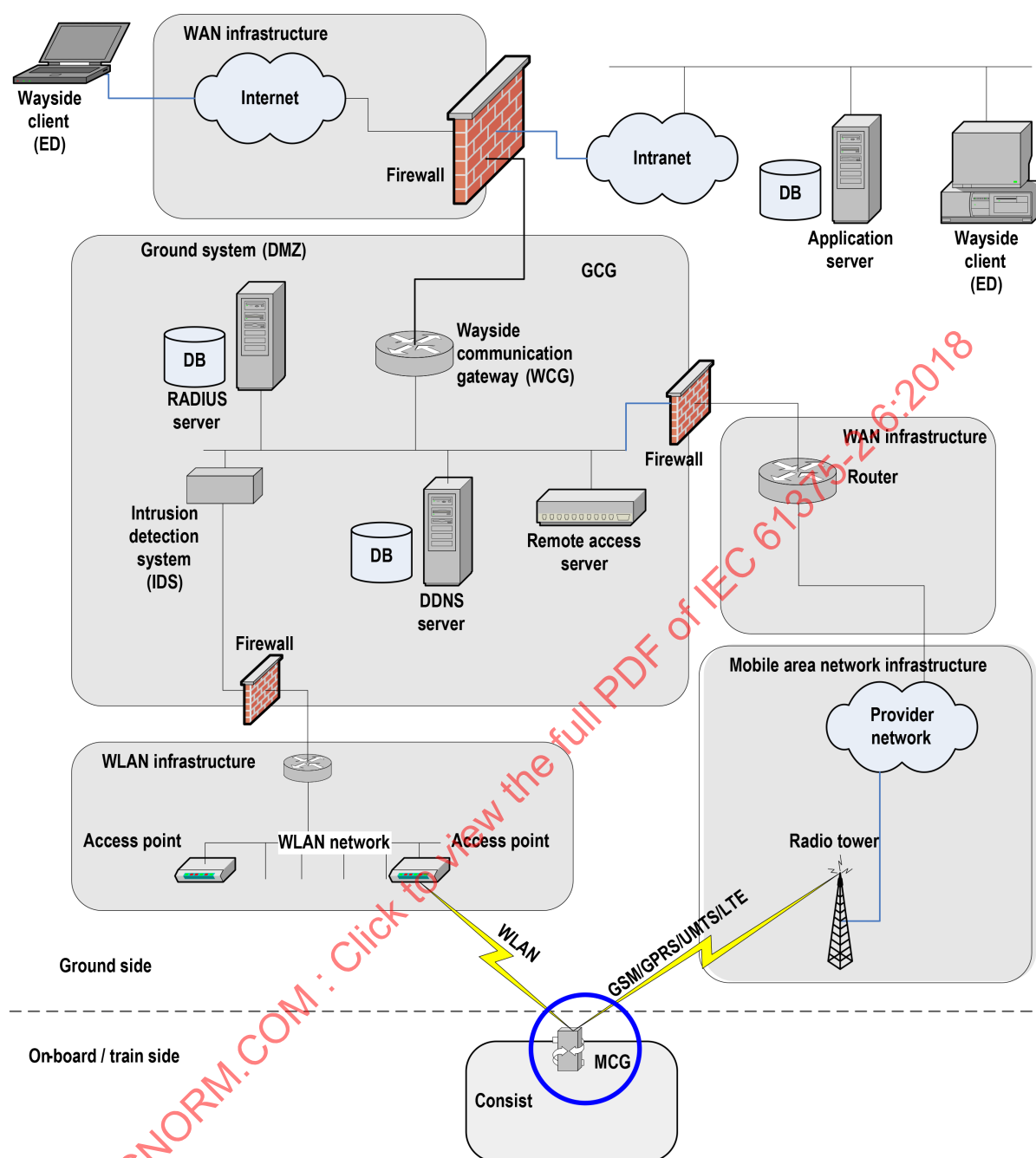


IEC

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.



IEC

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

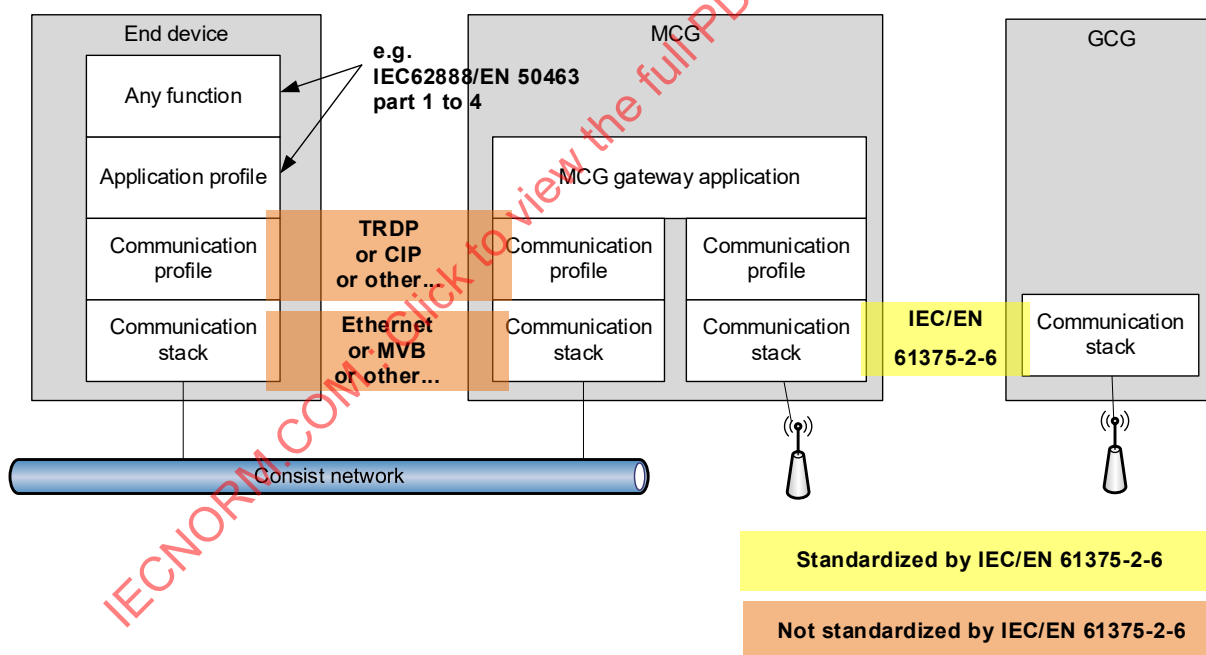
When this option is chosen, the function carried by the on-board device communicates, using an end device interface on the consist network, with the MCG which offers board-to-ground communication services as a router or as a gateway.

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.



IEC

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.

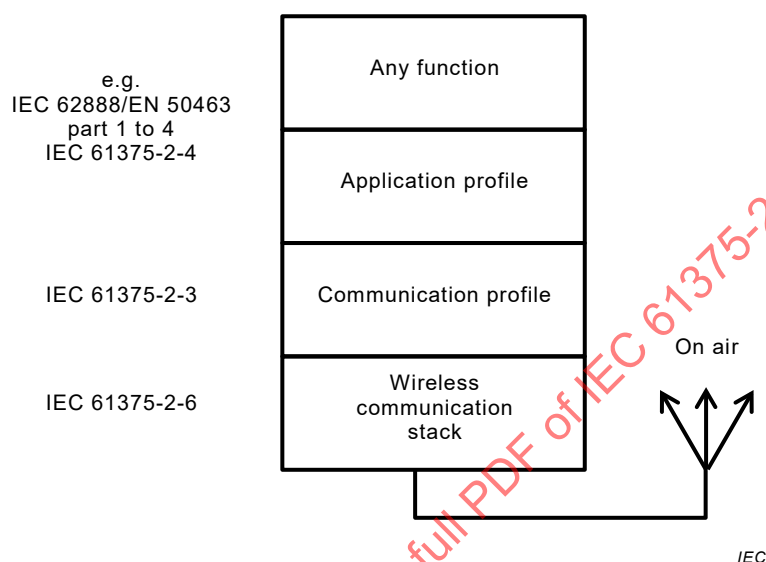


Figure 4 – Option 2: End Device board to ground communication via dedicated interface

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

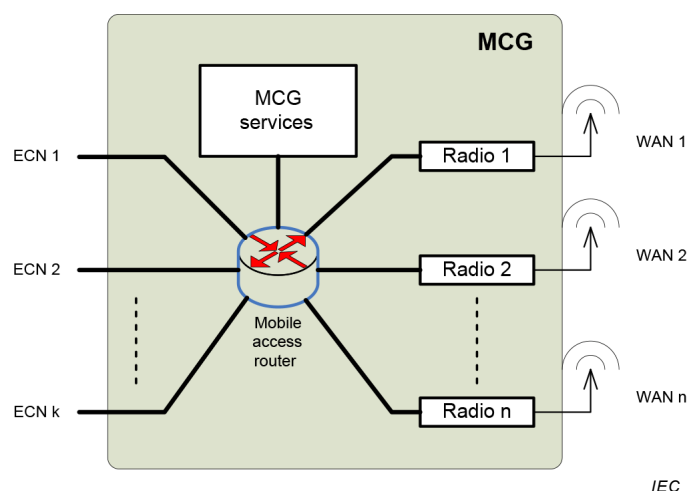


Figure 5 – MCG abstract model block diagram

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.

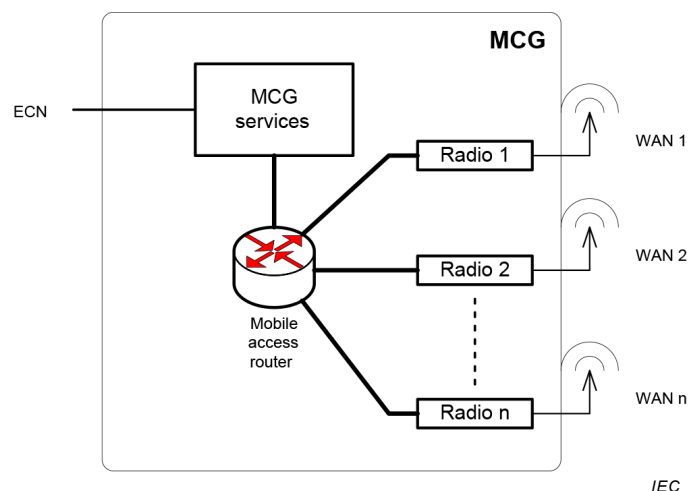


Figure 6 – MCG configured as ALG

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:

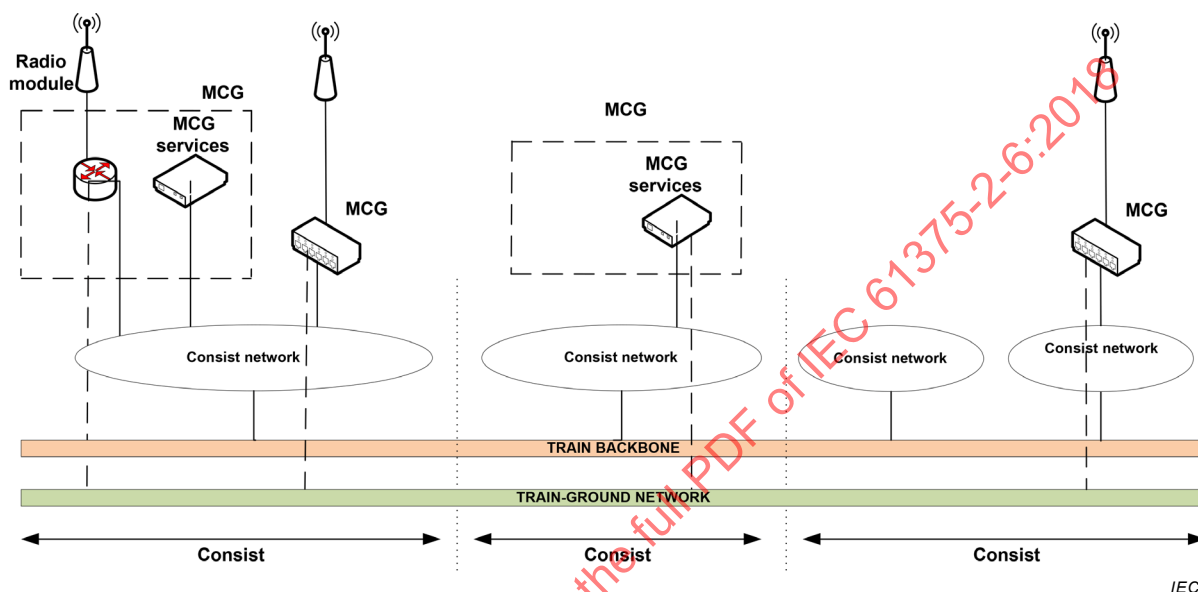


Figure 7 – Architectural example of redundant Board to Ground communication

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.

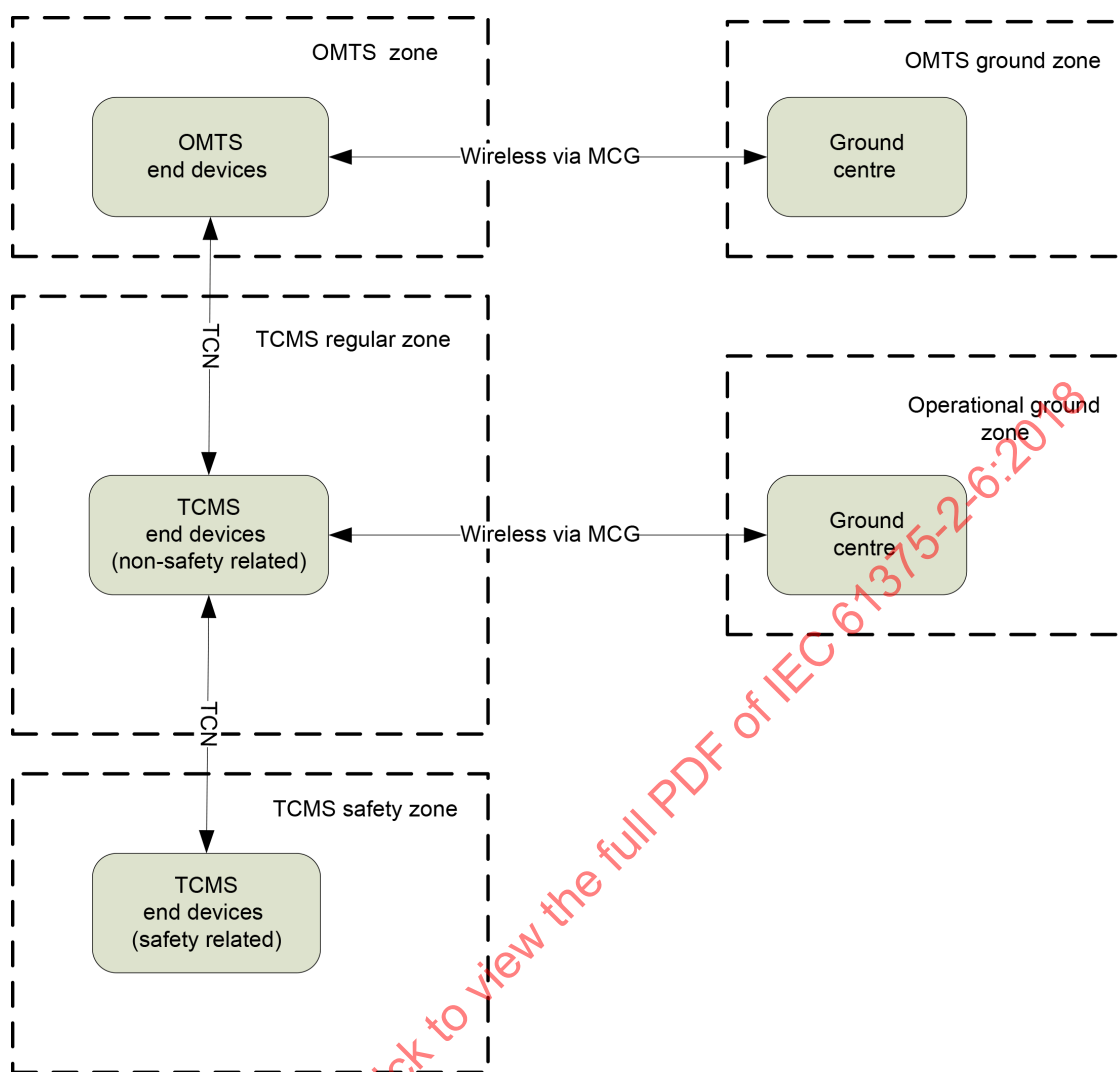
On-board of trains are identified the following zones:

- 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.



IEC

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.

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 measure	Supported by	Description
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.

4.9.3 Authentication authorization accounting model

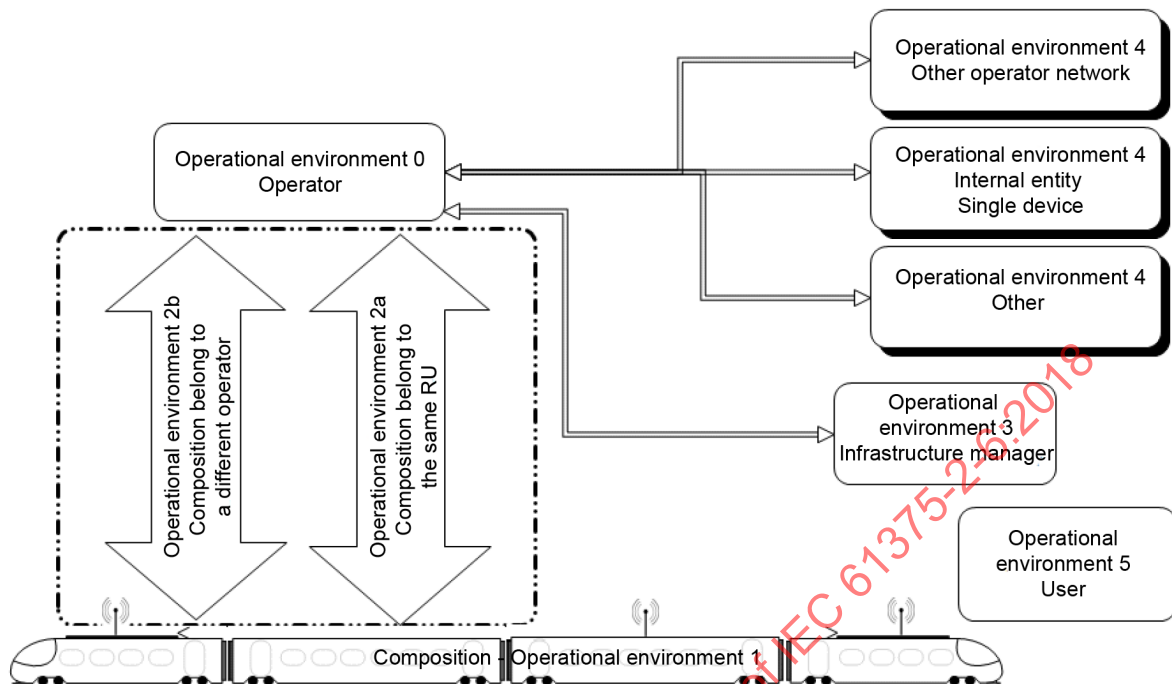
The model identifies the single components which are essential in a general system interaction:

- 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



IEC

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.

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

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

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

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 category 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:

- a) The number of pieces of connectable equipment – either safety-related or not – to the transmission system is known and fixed.

- b) 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.
- c) The risk of unauthorized access is considered negligible.

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

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.

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

4.9.4.3 MCG connecting both category 1 and category 2/3

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

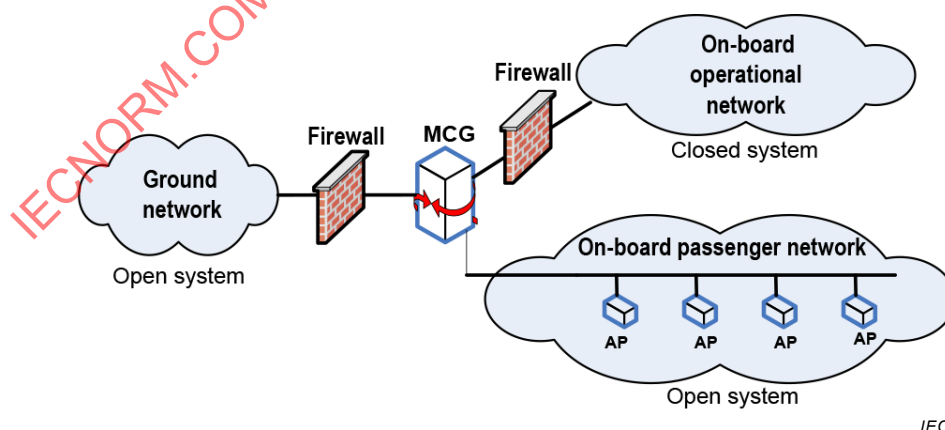


Figure 10 – MCG connecting open and closed transmission systems

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

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

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

5 Communication framework

5.1 General

The board-to-ground communication framework defines the basic functions and basic concepts which are necessary to establish and to maintain the secure and reliable communication between on-board end devices and devices (e.g. computer, servers) on ground.

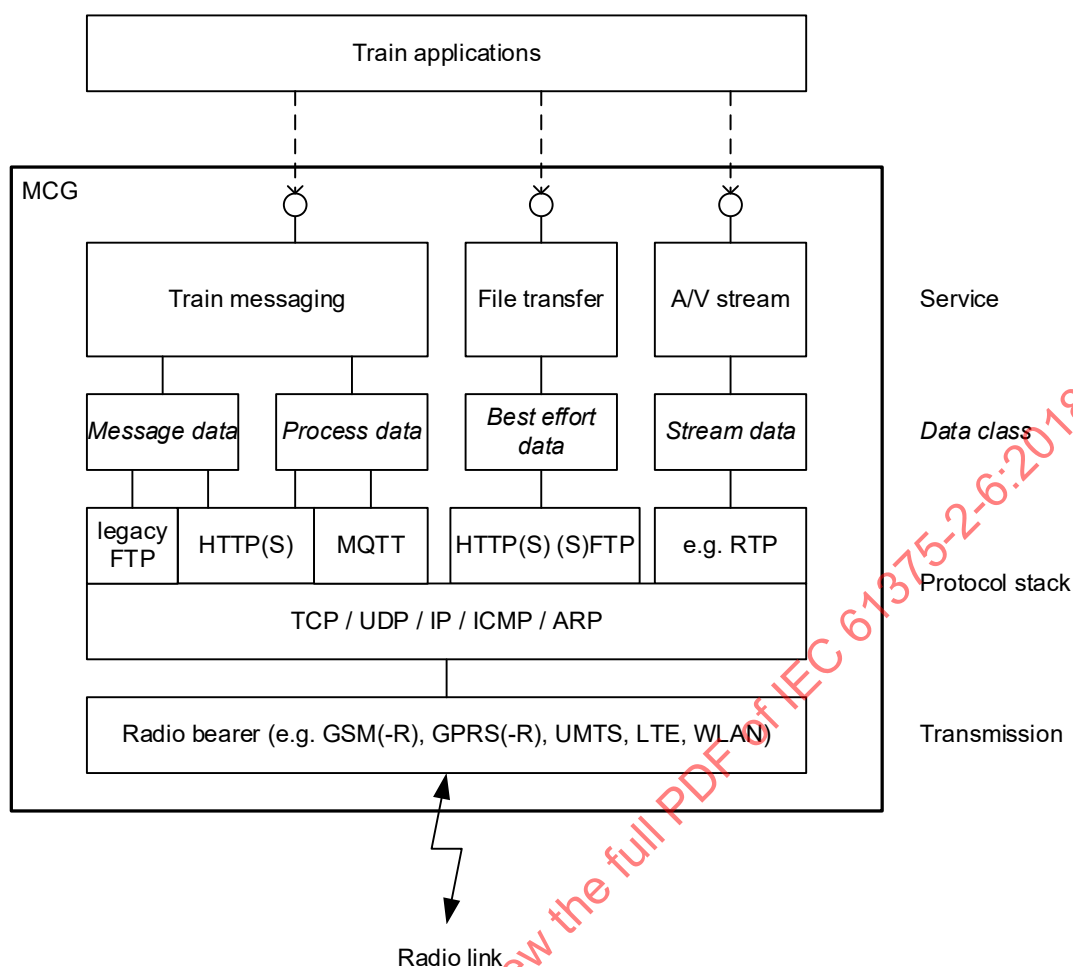
This addresses in particular the following aspects in the context of the mobile communication network architecture, see also 4.3:

- MCG as a broker service architecture, see 5.2.
- Addressing, see 5.3.
- Data classes, see 5.4.
- Communication protocols, see 5.5.
- Communication services, see 5.6.

As the MCG is the on-board device which is managing the on-board part of train to ground communication, all these aspects will be related to the MCG and the on-board communication system behind. The ground communication system is quite heterogeneous and mostly dependent on the infrastructure of railway operators and cellular network providers, hence these systems are only considered in an abstract manner.

5.2 MCG broker service architecture

Figure 11 shows an overview of the services the MCG provides for the train applications.



IEC

Figure 11 – MCG broker service architecture

Depending on the functional requirements, the train applications can use one or more of the following communication services:

- Train Messaging Service for event based or cyclic information exchange (e.g. diagnostic events or telemetry).
- File Transfer Service for complete data files (e.g. energy billing data).
- Audio/Video Streaming Service for continuous data (e.g. video or voice).

The used data classes depend on the application functional requirements.

The used protocols are based on standard internet protocols (e.g. IP, TCP, UDP, FTP, HTTP, DHCP, DDNS).

The used radio bearers (e.g. GSM, UMTS or others) are not in the scope of this document.

5.3 Addressing concept

5.3.1 Use cases

For addressing a train composition the following use cases shall be supported:

- Access to a specific consist regardless where the consist is located.

EXAMPLE: Request status information from consist with Consist ID '50 80 89 – 43 501 – 2'.

- Access to a specific train journey, regardless of the trains' consists and composition. This means that the train is declared ready for scheduled service and linked to a unique train journey ID.

EXAMPLE: Download time table information to the train with train journey ID 'ES9558'.

5.3.2 Consist and train Identification

Each consist is considered to have its own unique identifier, which in many cases will be derived from its Consist ID.

This unique identifier corresponds to the parameter '*cstId*' as defined in IEC 61375-2-3. Those identifiers are for instance allocated by ERA or OTIF.

A train composition, formed by connecting consists for a train journey, shall be identifiable by a unique train journey identifier.

This unique train journey identifier does not need to correspond to the parameter '*trnId*' as defined in IEC 61375-2-3.

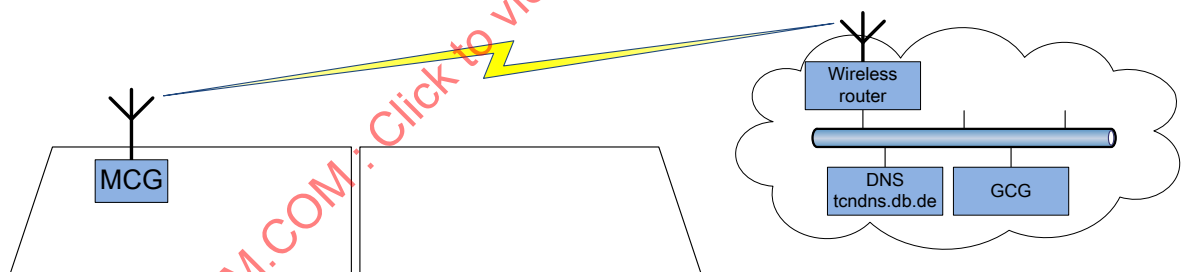
5.3.3 T2G Network Borders

The network between train (or better consists) and ground is formed basically out of the MCG as network border device of the train and the GCG as network border device of the ground network.

NOTE The exchange of structural network information would cause security risks.

5.3.4 T2G basic minimum network

The relevant entities are shown in Figure 12, simplified to an absolute minimum system:



IEC

Figure 12 – Minimum Train to Ground Network Setup

The wireless router is considered to be transparent and displayed for technical completeness, also the mobile IP handling is considered to be handled within this device – which may be any kind of WLAN infrastructure up to LTE provider.

Endpoint axiom:

Essentially the MCG forms the endpoint seen from the GCG attached network and vice versa as already stated in 5.3.3.

This separation serves basically a security purpose and also structures the train/ground network organization.

Applying the endpoint axiom implies another axiom:

Neither network exchanges any further DNS relevant information.

Combining these two axioms greatly reduce the naming variety, which would be imposed by IEC 61375-2-3.

This means that URIs like

```
mcg.anyVeh.UIC94910101123.anyClTr.anyTrn.tcndns.db.de
```

will not exist as they are ambiguous (the “any*” address parts) and TCP as transport layer for http does not support multi-/broadcasting.

5.3.5 T2G addressing

5.3.5.1 Consist addressing

The potential ambiguity presented in 5.3.4 is mitigated by moving to hostnames, which support http URL style addressing.

The simplification follows the latter reasoning:

- The only device seen from ground is an MCG – no need for “mcg.”
- Consist addressing via Consist ID does neither need “anyClTr.” nor “anyTrn.”
- Addressing a dedicated car via URI would always point to the same MCG

The application leads to the required move to a host identifier in the format:

```
<Consist ID>.tcndns.<operator domain>
```

e.g. UIC94806101123.tcndns.db.de

5.3.5.2 Train journey addressing

The desired feature to address a train journey (“train” in the sense of IEC 61375-2-3) requires to have a mapping of the train journey ID to the leading vehicle of the train.

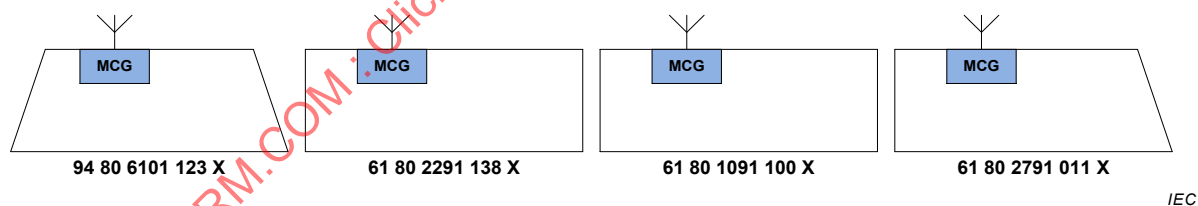


Figure 13 – A train consisting of four vehicles

A typical train composition is depicted in Figure 13.

The way of addressing a train (here EC41), as alias of the leading vehicle, would be the concise form, see 5.3.5.3:

```
EC41.tcndns.db.de
```

The pattern for the required host identifier is therefore:

```
<journey ID>.tcndns.<operator domain>
```

NOTE Though the <train: consists> relation remains important, it is not to be resolved in constructing the following host identifiers:

```
EC41.UIC94806101123.tcndns.db.de
```

EC41.UIC61802291138.tcndns.db.de

EC41.UIC61801091100.tcndns.db.de

EC41.UIC61802791011.tcndns.db.de

as the intrinsic information about the leading vehicle (consist) is not existent within this pattern.

5.3.5.3 Train inauguration, direction change

The event of train inauguration (which gets also triggered by a change of direction) will be needed to get evaluated by the MCGs in order to keep the DNS entries for the train journey ID based addressing consistent.

Each MCG within a train needs to evaluate whether it has to be in the leading consist in order to maintain the train journey ID based DNS entry.

The DNS entries for the train journey addressing point always to the leading MCG, the disappearance of an entry within an operators DNS cannot get covered here.

Assigning a train journey ID to the train depicted in Figure 13 will result in:

a) Locomotive leading:

EC41.tcndns.db.de and UIC94806101123.tcndns.db.de being identical concerning the IP address

b) Cab car leading:

EC41.tcndns.db.de and UIC61802791011.tcndns.db.de being identical concerning the IP address

The relation of train journey ID, consists within the train and the leading vehicle can get maintained via the mechanism described in 4.8 and 6.3.3.

5.3.5.4 The train journey ID as variable configuration item

The individual train journey ID is a configuration item for each train (in the sense of IEC 61375-2-3) which may change over time due to operational considerations of the RU.

The MCGs within the train will need to have access to this information, which in turn will need to get exchanged throughout the train.

The individual implementation of this mechanism is out of scope of IEC 61375-2-6.

5.3.5.5 Train journey ID uniqueness within the DNS

The Consist IDs are unique by their nature, the train journey ID in contrast is not unique per se among the various RU.

Essentially the train journey IDs used within the *tcndns* need to be unique.

5.3.5.6 Global DNS scope extension of the TCN-URI scheme

5.3.5.6.1 TCN-URI global DNS zone

For embedding TCN-URI in a global DNS, a suffix shall be added to the TCN-URI. This suffix shall start with a TCN-URI specific global DNS zone "tcndns" and end with the operators or maintainers sub-domain name in accordance with Table 12.

Table 12 – TCN-URI global DNS zone

<i>DNS zone name</i>	<i>DNS zone suffix</i>	<i>Definition</i>
tcndns	tcndns.railway.org	This DNS zone is used to embed all TCN-DNS host names inside the global DNS. Sub-domain name 'railway.org' to be replaced by the operators or maintainers real sub-domain name. EXAMPLE 'tcndns.sncf.fr'

5.3.5.6.2 T2G-DNS name resolution

The following rules shall be applied for the resolution of names in TCN-DNS:

- The DNS zone reserved by the railway operator for TCN-DNS, e.g. `tcndns.railway.org`, shall be delegated to TCN-DNS name server of the GCG.
- Due to the dynamic nature and availability of the connections between the GCG and MCGs, the DNS Resource Records (RR) of the `tcndns` DNS domain shall be configured with values to avoid caching in intermediary DNS servers and force queries to authoritative TCN-DNS or DNS servers.

5.3.6 HTTP-URI

5.3.6.1 HTTP-URI pattern

Train-to-ground communication as defined herein uses HTTP(S) for communication protocol. For addressing of resources HTTP uses an "http-URI" scheme as defined in RFC 3986 and RFC 2616.

The HTTP URI shall conform to the following pattern (employing the host identifier pattern from 5.3.5.1 and 5.3.5.2)

http-URI := "http://<authority>/<path>"

authority: is the host identifier, corresponding to the TCN-DNS name (see 5.3.5.1 and 5.3.5.2)

path: identifies a resource within the scope of the URI's scheme and naming authority.

EXAMPLE: A complete HTTP-URI may look like

"http://UIC94806101123.tcndns.db.de/mcgservice"

5.3.6.2 HTTP-URI on MCG side (option)

Based on the chosen addressing mode (consist or train journey ID) the host identifiers need to conform to the rules given in 5.3.5.1 and 5.3.5.2. The path to the communication services (described in 5.6.3 and 6) should be aligned to facilitate interoperability.

The latter is achieved by using the path "mcgservice".

Therefore, an example for the resulting http-URIs will look like:

http://UIC94806101123.tcndns.db.de/mcgservice

http://EC41.tcndns.db.de/mcgservice

5.3.6.3 HTTP-URI on GCG side (option)

The GCG http-URI may get considered as configuration item, though it would prove to be highly beneficial to have the GCG host identifier also registered within the *tcndns* named according to the pattern

`gcg.tcndns.<operator domain>`

to have a uniform namespace.

NOTE Using plain IP addresses will put several constraints upon the wireless network infrastructure.

Similarly to 5.3.6.2, the path set to “gcgservice” will give an example for the http-URI

`http://gcg.tcndns.db.de/gcgservice`

5.4 Data classes for T2G communication

5.4.1 General

IEC 61375-1 defines four classes of data, each of them stemming from its own rich background in communication history with associated technologies, typical solutions and general mind-set of application developers.

These data classes are:

- a) Process Data
- b) Message Data
- c) Stream Data
- d) Best Effort Data

The MCG used for train to ground communication by the on-board End devices needs to support the data classes Message Data, Stream Data and Best Effort Data as set out in IEC 61375-1:2012, 7.5.3. Depending on the data class, appropriate communication protocols are used.

In case there is a need for Process Data communication between train and ground, the cyclic event communication pattern defined for Message Data could be used. However, there is the possibility of employing MQTT instead of HTTP (see Figure 12) as transport protocol and leverage the advantages of the former (see 5.5.3).

5.4.2 Communication channel establishment

The prime principle is that the MCG establishes the communication channel regardless of the data classes to be used.

The MCG will not accept requests from the ground side to establish a communication channel (e.g. from the GCG).

5.4.3 Message data

Where the MCG supports message data, the recommended service parameters are dependent on the application requirements and the properties of the available radio technology (see Table 13).

Table 13 – Recommended service parameters for message data

Service Parameter	Description
Data packet size	volume of the data to be transmitted with one data packet: ≤ 65507 octets NOTE The packet should fit in one UDP packet which has a maximal size of 65507 octets (65535 – 8 byte UDP header – 20 byte IP header). In praxis this size is often more limited, e.g. due to options in the IP header and constraints in the used protocol stacks.
Data packet rate	Number of sent data packets per second. Multiplied with the data packet size * 8, it equals the (net) data rate. $\leq (\text{Radio Bandwidth} / \text{Data Packet size}) * 20 \%$ (with available net Radio Bandwidth in octets per second).
Latency	Transmission time of the data packet from data source to data sink. ≤ 1 s NOTE The latency is application dependent.
Jitter	Variance in transmission time for subsequent data packet transmissions. ≤ 1 s NOTE The jitter is application dependent.
Data integrity	Application data packet received by the sink. bit error rate (BER) $\leq 10^{-6}$ Probability that the following failures will be detected: a) data corruption; b) sequencing error (unintended repetition, wrong sequence); c) timely delivery error; d) authentication error (wrong source, wrong destination). Probability P_{DU} of dangerous undetected failures 10^{-5} per hour

5.4.4 Process data

Where the MCG supports process data, the recommended service parameters are dependent on the application requirements and the properties of the available radio technology (see Table 14).

Table 14 – Recommended service parameters for process data

Service Parameter	Description
Data packet size	volume of the data to be transmitted with one data packet: ≤ 1436 octets NOTE The packet should fit in one unsegmented UDP packet.
Data packet rate	Number of sent data packets per second. Multiplied with the data packet size * 8, it equals the (net) data rate. $\leq (\text{Radio Bandwidth} / \text{Data Packet size}) * 20 \%$
Latency	Transmission time of the data packet from data source to data sink. ≤ 32 ms NOTE Latency from the application point of view. Obviously the network may introduce additional latencies of several orders of magnitude higher.
Jitter	Variance in transmission time for subsequent data packet transmissions. ≤ 32 ms
Data integrity	Application data packet received by the sink. bit error rate (BER) $\leq 10^{-6}$

5.4.5 Stream Data

Where the MCG supports stream data between train and ground, the recommended service parameters are dependent on the application requirements and the properties of the available radio technology (see Table 15).

Table 15 – Recommended service parameters for stream data

Service Parameter	Description
Data packet size	volume of the data to be transmitted with one data packet: depends on stream protocol
Data rate	Number of sent data per second. $\leq \text{Radio Bandwidth} * 50 \%$ (e.g. video over WLAN) $\leq 64 \text{ kbit/sec}$ (for audio) (with available netto Radio Bandwidth in octets per second)
Latency	Transmission time of the data packet from data source to data sink. $\leq 0,100$ s NOTE The latency is application dependent.
Jitter	Variance in transmission time for subsequent data packet transmissions. $\leq 0,030$ s (for audio) NOTE The jitter is application dependent.
Data integrity	Application data packet received by the sink. bit error rate (BER) $\leq 10^{-6}$

5.4.6 Best effort data

Where the MCG supports best effort data between train and ground, the recommended service parameters are dependent on the application requirements and the properties of the available radio technology (see Table 16).

Table 16 – Recommended service parameters for best effort data

Service Parameter	Description
Data rate	Number of sent data packets per second. Multiplied with the data packet size * 8, it equals the (netto) data rate. $\leq \text{Radio Bandwidth} * 20 \%$ (with available netto Radio Bandwidth in octets per second).
Latency	Transmission time of the data packet from data source to data sink. $\leq 5 \text{ s}$ NOTE The latency is application dependent.
Jitter	Variance in transmission time for subsequent data packet transmissions. $\leq 5 \text{ s}$ NOTE The jitter is application dependent.
Data integrity	Application data packet received by the sink. bit error rate (BER) $\leq 10^{-6}$

5.5 Communication protocol

5.5.1 General

The train to ground communication utilizes the following protocols:

- HTTP, for process data, message data and file transfer
- HTTPS, for secured process data, message data and file transfer

These protocols are described in the following subclauses.

As an option, the following protocols can be supported:

- FTP, alternatively for file transfer
- SFTP, alternatively for secured file transfer
- RTP, for audio and video live streams
- MQTT, for connections with remote locations where a "small code footprint" is required or the network bandwidth is limited

5.5.2 HTTP(S)

5.5.2.1 General

HTTP(S) shall be used as train-to-ground communication protocol for message data and file transfer. The principal communication stacking is shown in Figure 14.

HTTP(S) is the basic application level communication protocol, using the TCP/IP protocol stack for transport and network layer. HTTP(S) is then used to support the following application layer communication services:

- Message data (as defined in this document)
- File transfer (as defined in this document)
- Others (not defined in this document)

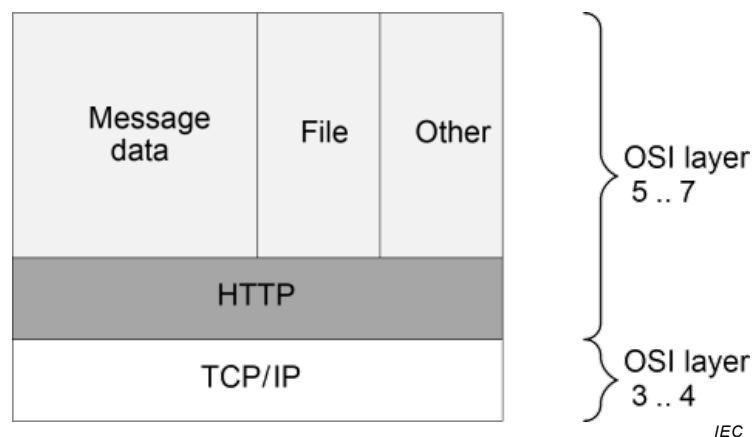


Figure 14 – Communication stacks

5.5.2.2 Basic protocol parameters

For data transfer using HTTP the following requirements shall be fulfilled according to RFC 2616:

- Protocol version shall be HTTP1.1
- Methods supported: POST
- Header properties supported:
 - “Host”
 - “Content-Type”
 - “Content-Length”

Secured version of HTTP as defined in RFC 2818. HTTPS shall be used instead of HTTP if security requirements demand it.

5.5.2.3 HTTP(S) exchange pattern

The basic HTTP(S) based MD communication pattern facilitates the standard request/response pattern as depicted in Figure 15.

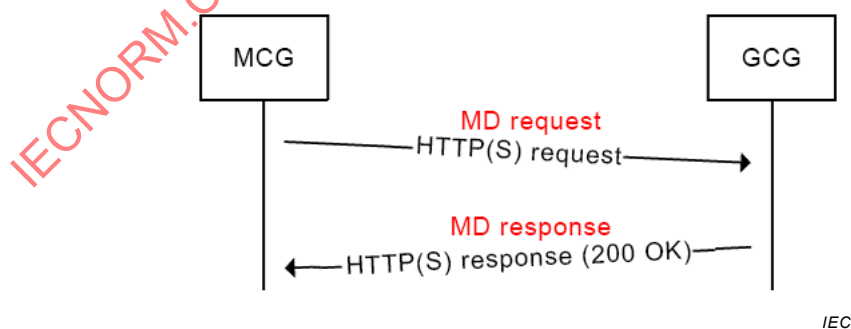


Figure 15 – HTTP(S) MD communication pattern

Figure 16 and Figure 17 illustrate the relevant HTTP(S) header information to be utilized by the train to ground MD communication.

```

POST /[authority/path] HTTP/1.1
User-Agent:      [see RFC 2616 sec. 14.43 for definition]
Host:            [see RFC 2616 sec. 14.23 for definition]
Content-type:    [packetType]
Content-length:  [length of packetBody in decimal number of octets]

[packetBody]

```

IEC

Figure 16 – HTTP(S) request/event

```

HTTP/1.1 [status code] [status phrase]
Content-type: [packetType]
Content-length: [length of packetBody in decimal number of octets]

[packetBody]

```

IEC

Figure 17 – HTTP(S) response

The HTTP(S) header fields for the HTTP(S) request/response pattern are referenced in Table 17.

Table 17 – HTTP(S) parameters request/response pattern

HTTP(S) request header (method POST)	
authority	See 5.3.6
path	See 5.3.6
packetType	At least the following “Content-Type” parameter values shall be supported: • “text/xml” • “text/html” • “application/octet-stream” • “application/json” (RFC 4627)
packetBody	Payload
HTTP(S) response	
status code	see RFC 2616,6.1.1
status phrase	see RFC 2616,6.1.1
packetBody	Payload

Beside the MDRequest/MDResponse pattern, there is the possibility to send sporadically or cyclically an MDEvent message, which has the same format shown in Table 17, but the HTTP response includes only a status code and status phrase. There is no packetBody.

5.5.3 MQTT (Option)

The MCG may optionally support the lightweight protocol Message Queue Telemetry Transport (MQTT) according to ISO/IEC 20922:2016, which has some advantages compared with HTTP(S).

- minimum header size to reduce data overhead;
- leverage of the same TCP connection for all the exchanged data with increased data rate and reduced latency;
- publish/subscribe paradigm for one to many communication relations;
- native QoS support to categorize the messages;
- client TCP connection heartbeat for communication supervision;

- no listening ports on end devices to increase the security;
- efficient data processing with compact binary data protocol.

5.6 Communication services

5.6.1 General

This subclause defines the communication services needed for the transfer of data between on-board ED and ground ED. Communication services are defined for the following data types:

- a) Message data
 - from train to ground
 - from ground to train
- b) Process data
 - from train to ground
- c) File transfer
 - from train to ground
 - from ground to train
- d) (Audio/video) stream
 - from train to ground
 - from ground to train

The communication services differentiate between the control of data transfer and the data transfer itself. Data transfer control is based on Messages data telegrams, which are exchanged between the stakeholders involved. The data transfer itself is mostly based on dedicated protocols, like HTTP(S) for file transfer and RTP/RTCP for streaming data.

5.6.2 Message data communication service

5.6.2.1 General

The Message Data communication service is one of the communication services which is based on HTTP as defined in 5.5. This subclause describes the supported uses cases and defines the related Message Data telegrams.

5.6.2.2 Message data exchange

The message data communication service is used to exchange message data once on demand.

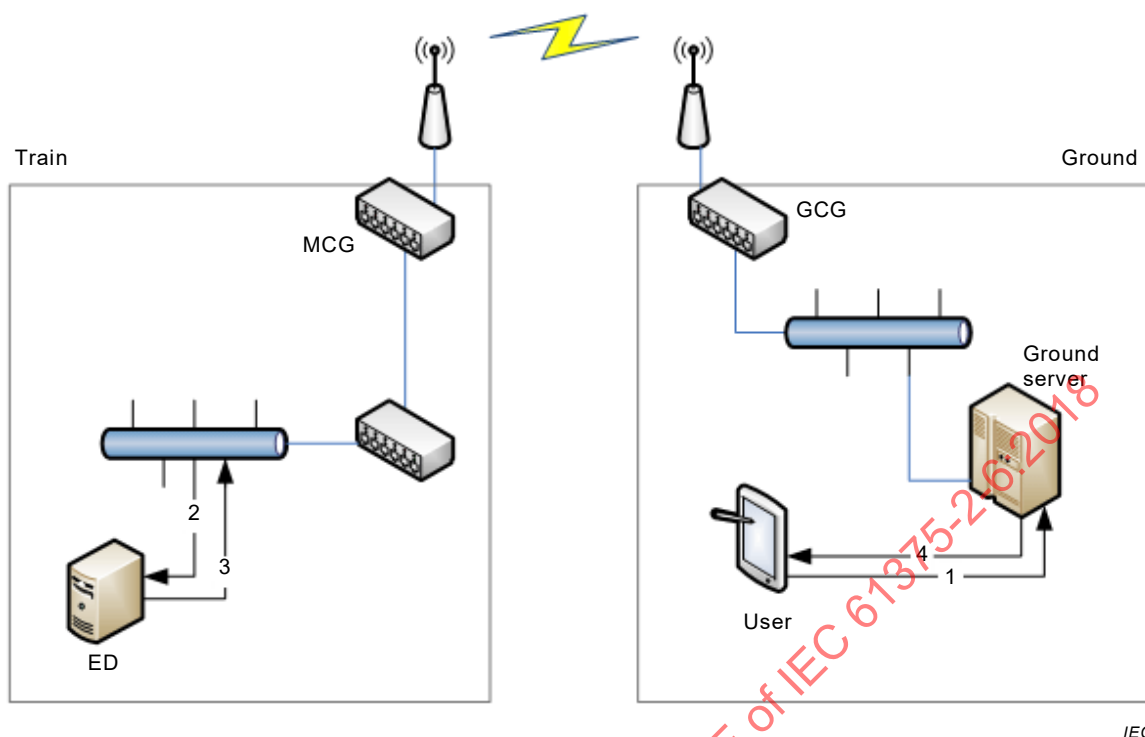


Figure 18 – Message Data exchange (example)

Message data transfer from train to ground initiated by a message data subscription requires the following steps as it is shown in the example of Figure 18. The user uses an application to send a message data request to the train. This application can e.g. be hosted by the ground server or another network device that can connect to the GCG.

- The data requested by the user (1) is forwarded to the ED (2) that provides the information.
- The ED prepares a response that contains the requested information and sends the information to ground (3).
- The information is then forwarded to the requesting user (4).

5.6.2.3 Telegram definitions

5.6.2.3.1 General

A Message Data telegram consists of a generic Message header and a service specific Message body. The parameters of the Message header and the parameters of Message bodies related to communication services defined herein are specified within this subclause. For data transmission, the complete message will be represented in the defined transmission format and placed into the payload of an HTTP(S) packet (Figure 19).

The transmission format of the Message shall be in JSON as defined in RFC 7159. A definition of the transmission format of the Message is given in Annex A.

Although the transmission format of the Message body is JSON, the body structure allows the embedding of information in other formats (see Annex A for details). Recommended formats are:

- JSON (same as Message)
- XML
- Base64 coded binaries

NOTE Standard IEC 62888/EN 50463 defines messages in XML format. In architectures where the energy metering system is connected to the on-board ECN and uses the MCG to ground communication (EMS consist

network connection based on the IEC 61375 series), the complete IEC 62888/EN 50463 message can be placed into the Message body and transferred between MCG and GCG.

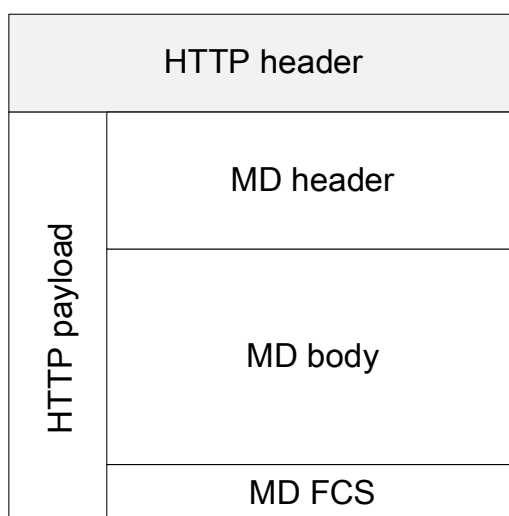


Figure 19 – Message Data telegram structure

5.6.2.3.2 General MD Telegram Format

5.6.2.3.2.1 General

The parameters of the MD-header shall be in accordance with Table 18:

Table 18 – General MD Header

Parameter	Description	Datatype	Value Range	Value
MDHeader	Message Header	JSON		
protocolVersion	The protocol-version of the MD-frame (pair of digits as version number). The protocol-version is annotated in two byte form, where the mapping is considered like: 0x10: protocol-version 1.0 value: 16 0x1A: protocol-version 1.10 value: 26 0xB5: protocol-version 11.5 value: 181	number	uint8	16
msgType	Message type	number	uint16	configured see Table 21
source	Specification of the train consist or train journey id	string	char[32]	Coming from the MCG or when the initial message is from the GCG: Configuration in the GCG
comID	Identifier for the message body (application dependant)	number	uint16	Configured
msgTimestamp	Timestamp indicating when the message has been sent	number	uint64	computed unix timestamp-format
msgTimeValidity	Indicating in milliseconds the validity (e.g. expected life duration) of the content sent in the message body.	number	uint32	configured 0: n.a. 1..'FFFFFFF'H

The data elements in the message body of the MD frame shall be in accordance with Table 19.

Table 19 – General MD Body

Data Element	Description	Datatype	Value Range	Value
mdPayloadType	Describes which type of content is embedded in message data body payload	string	char[16]	configured see Table 22
mdPayload	Contains application specific content (e.g. TRDP-frame, EMS-XML-frame, Octet-stream)	object	object	computed

The checksum of the MD frame shall be in accordance with Table 20.

Table 20 – MD Checksum

Data Element	Description	Datatype	Value Range	Value
mdFCS	Checksum calculated over MDHeader and MDBody. See 5.6.2.3.2.2	hex string	char[8]	0..'FFFFFFF'H Computed over complete MD Header and MD Body according to IEC 61375-2-3:2015, Clause A.3. Seed value: 0x0.

Since the MD Telegram is defined as an ASCII-based telegram format, it is necessary to enclose content in a manner that no control characters are included in the data to falsely indicate the end of the data-object.

The preferred method of encapsulation (e.g. base64-encoding) is in the scope of the application.

The message types which are defined for MD frames shall be in accordance with Table 21:

Table 21 – Message types

Value	Description
1	MDEvent-sporadic
2	MDEvent-cyclic
3	MDRequest
4	MDResponse

The message representation which is defined for MD frames shall be in accordance with Table 22.

Table 22 – Message representation

Value	Description
"JSON"	Content represented in JSON format, (see Annex A)
"XML"	Content represented in XML format (e.g. for EMS).
"Octet"	Content represented as octet-stream
"Base64"	Content represented as Base64 encoded octet-stream
...	others

5.6.2.3.2.2 Calculation of the mdFcs

The MD frame FCS shall be calculated as follows:

- The following JSON MD content shall be used in the calculation of the mdFCS:

```
"MDHeader":
{
    // all frame-header elements
},
"MDBody":
{
    // all frame-body elements
}
```

The checksum shall be computed over the whole MDHeader- and MDBody-tags of the JSON message, including the tag, colon, opening curly brace, all frame body elements to be transmitted (the checksum is calculated over the actual JSON text buffer), the closing brace as the last element.

- Since the mdFcs element is not an element of the MDHeader or MDBody, therefore there is no need to define a mandatory default value.
- For computing the mdFCS, the CRC32 according to IEEE 802.3 shall be used.
- The start value for the CRC32-calculation shall be: 0

5.6.3 File transfer communication service

5.6.3.1 General

When talking about file transfers, the following terms shall apply in accordance with Table 23:

Table 23 – File transfer terminology

Term	Description
Download	A file is transferred from the ground to the train
Upload	A file is transferred from the train to the ground

The file transfer communication service provides the means to transfer files from train to ground and vice versa. Due to security considerations, direct endpoint-to-endpoint file transfers are not allowed between End Devices on the train and the wayside.

Files are transferred using intermediate storage, i.e. files have to be temporarily put on a pre-defined storage location, from where the file can be uploaded or downloaded.

NOTE The exact definition and specification of a valid storage location is not in the scope of this document.

File retrieval during upload or download is always performed by the MCG. Therefore, the concepts for uploading and downloading a file are asymmetrical.

5.6.3.2 File upload

5.6.3.2.1 General

Figure 20 depicts an example of how a file is uploaded from an on-board end device (ED) to the ground side. The scope of the file upload pattern that is specified by this document is marked using pastel blue background colour.

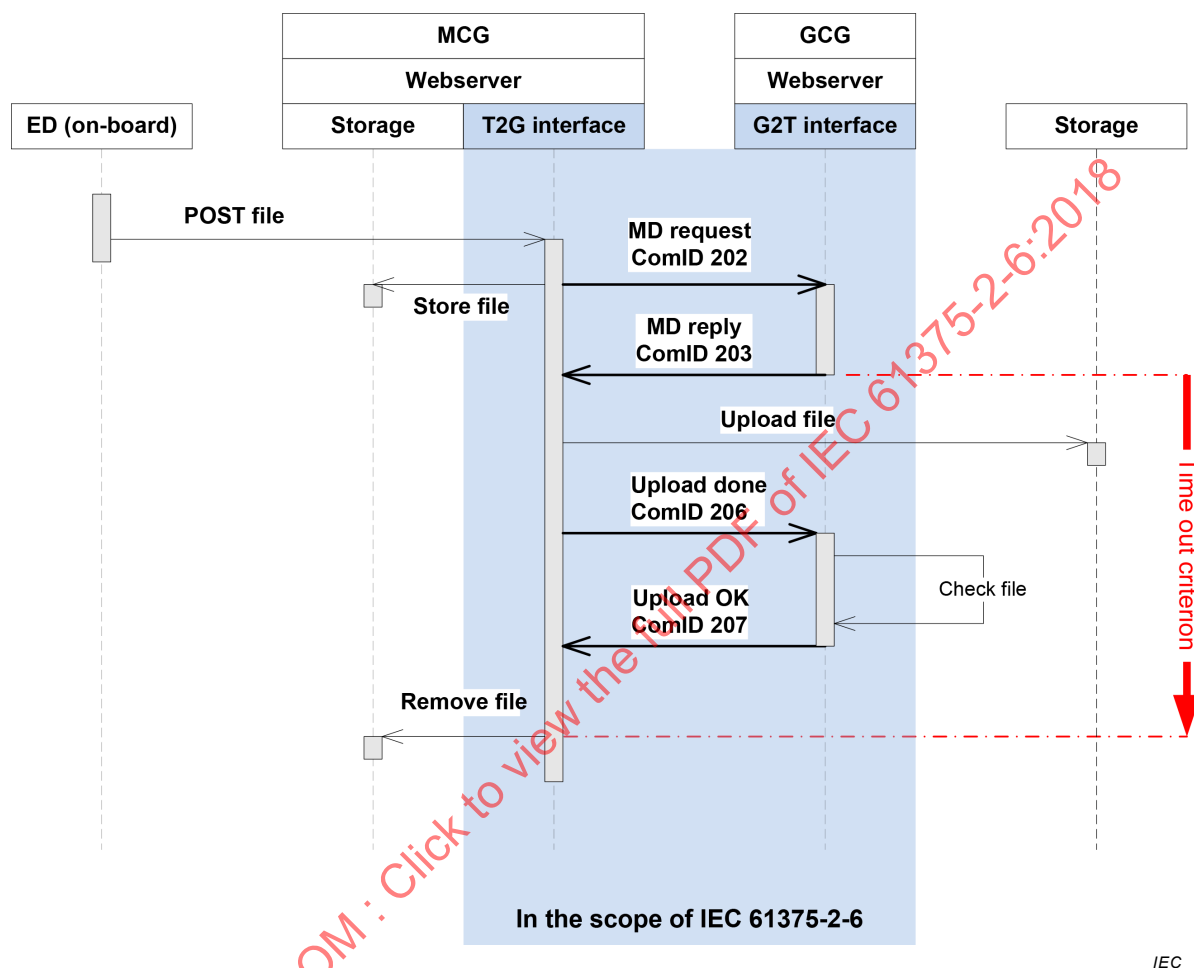


Figure 20 – File upload example

An on-board end device can upload a file to the ground side using a few steps, as described below:

- First, the End Device transfers the file to the MCG, e.g. by using a web server interface which is exposed by the MCG only to devices on the train.
- After the file has been successfully transferred to the MCG, the MCG automatically requests permission from the GCG to transfer the file to the wayside. The MCG sends a request message (ComID 202) to the web service interface exposed by the GCG.
- The GCG responds to the file transfer request by the MCG, indicating if the file transfer is allowed to take place. The GCG sends a reply message (ComID 203) to the web service interface exposed by the MCG, indicating to the MCG a storage location to be used for storing the file on the ground side.
- The MCG uploads the file to the indicated storage location.
- After the upload has been successfully performed, the MCG informs the GCG that the file transfer has been completed. The MCG sends an informative message (ComID 206) to the web service interface exposed by the GCG.

- f) The GCG uses a means of checking the integrity of the file that has been transferred to determine if the integrity of the file that has been transferred can be confirmed on the ground side.
- g) After checking the integrity of the file successfully on the ground side, the GCG sends a reply message to the web service interface exposed by the MCG. The GCG sends a reply message (ComID 207) to the web service interface exposed by the MCG, confirming the successful reception of the file.
- h) After receiving the confirmation from the GCG of the successful reception of the file, the MCG can discard the file from its internal storage.

NOTE The MCG can determine which radio bearer to use for uploading a file. Refer to 6.3.4 for more details.

5.6.3.2.2 Message Definition

5.6.3.2.2.1 Request permission for uploading (ComID 202)

The ComID 202 message is a MD telegram, which is sent from the MCG to the GCG. This message is used by the MCG to request permission for uploading a file to the wayside.

The MD request telegram ComID 202 shall be sent with the following header parameters in accordance with Table 24. Refer to Table 18 for general information about the MD header parameters.

Table 24 – ComID 202: MD header telegram values

Parameter	Value
msgType	3 (MD Request)
msgTimeValidity	0 (no timeout)
comID	202

The MD request telegram ComID 202 shall be sent with the following body parameters in accordance with Table 25. Refer to Table 19 for general information about the MD body parameters.

Table 25 – ComID 202: MD body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 26

The MD request telegram ComID 202 shall be sent with the following payload object in accordance with Table 26.

Table 26 – ComID 202: MD body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter “mdPayload”	JSON		
fileTransferUID	Unique identifier. Defined by the MCG, used by the MCG and GCG to identify a file that is uploaded.	number	uint32	computed
filename	Name of the file to be transferred to the GCG. Used by the GCG later to enable access the uploaded file.	string	char[256]	predefined
fileType	Indicates the type of file that is uploaded.	number	uint8	0 = n.a. 1 = ASCII 2 = Binary 3 = Audio 4 = Video 5-255 not used
fileServiceFunction	Specifying the source service.	number	uint8	0 = not in the list 1 = EMS 2 = CCTV other values reserved
fileSize	Indicates the size of the file to be uploaded, in bytes. Determined by the MCG.	number	uint64	predefined

5.6.3.2.2.2 Answer a request for uploading (ComID 203)

The ComID 203 message is a MD telegram, which is sent from the GCG to the MCG. This telegram is used by the GCG to answer a request for uploading a file to the wayside.

The MD response telegram ComID 203 shall be sent with the following header parameters in accordance with Table 27. Refer to Table 18 for general information about the MD header parameters.

Table 27 – ComID 203: MD header telegram values

Parameter	Value
msgType	4 (MD response to received MD request)
msgTimeValidity	0 (no timeout)
comID	203

The MD response telegram ComID 203 shall be sent with the following body parameters in accordance with Table 28. Refer to Table 19 for general information about the MD body parameters.

Table 28 – ComID 203: MD body telegram values

Parameter	Value
mdPayloadType	“JSON”
mdPayload	see Table 29

The MD response telegram ComID 203 shall be sent with the following payload object in accordance with Table 29.

Table 29 – ComID 203: MD body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter "mdPayload"	JSON		
fileTransferUID	Unique identifier. Used by the MCG and GCG to identify a file that is uploaded.	number	uint32	predefined (taken from ComID 202 message)
storageURL	URL that indicates a storage location, to be used by the MCG for uploading a file.	string	char[512]	predefined

5.6.3.2.2.3 Successful upload (ComID 206)

The ComID 206 message is a MD telegram, which is sent from the MCG to the GCG. This message is used by the MCG to follow up on an earlier exchange of ComID 202 and ComID 203 messages. The MCG indicates to the GCG that it has successfully uploaded a file to the indicated storage location.

Refer to Table 18 for more information about the MD header parameters, and Table 19 for more information about the MD body.

The MD request telegram ComID 206 shall be sent with the following header parameters in accordance with Table 30. Refer to Table 18 for general information about the MD header parameters.

Table 30 – ComID 206: MD header telegram values

Parameter	Value
msgType	3 (MD Request)
msgTimeValidity	0 (no timeout)
comID	206

The MD request telegram ComID 206 shall be sent with the following body parameters in accordance with Table 31. Refer to Table 19 for general information about the MD body parameters.

Table 31 – ComID 206: MD body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 32

The MD request telegram ComID 206 shall be sent with the following payload object in accordance with Table 32.

Table 32 – ComID 206: MD body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter “mdPayload”	JSON		
fileTransferUID	Unique identifier. Used by the MCG and GCG to identify a file that is uploaded.	number	uint32	predefined (taken from ComID 202 message)
storageURL	URL that indicates a storage location where the MCG uploaded a file to.	string	char[512]	predefined
fileUploadResult	Indicates the results of the file upload, from the point of view of the MCG.	number	uint8	0 = n.a 1 = Upload OK 2 = Upload aborted 3 = Upload could not be started 4 – 254 currently not used 255 = Error
fileChecksum	MD5 checksum to enable verification on the ground side that the file upload has been successfully sent. The checksum mechanism used is in the scope of the application.	string	char[256]	computed

5.6.3.2.2.4 Integrity check of upload (ComID 207)

The ComID 207 message is a MD telegram, which is sent from the GCG to the MCG. This message is used by the GCG to respond to a ComID 206 message received from a MCG.

The GCG indicates to the MCG that the integrity check of the file it has uploaded to the wayside has been successful.

The MD response telegram ComID 207 shall be sent with the following header parameters in accordance with Table 33. Refer to Table 18 for general information about the MD header parameters.

Table 33 – ComID 207: MD header telegram values

Parameter	Value
msgType	4 (MD response to received MD request)
msgTimeValidity	0 (no timeout)
comID	207

The MD response telegram ComID 207 shall be sent with the following body parameters in accordance with Table 34. Refer to Table 19 for general information about the MD body parameters.

Table 34 – ComID 207: MD body telegram values

Parameter	Value
mdPayloadType	“JSON”
mdPayload	see table Table 35

The MD response telegram ComID 207 shall be sent with the following payload object in accordance with Table 35.

Table 35 – ComID 207: MD body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter “mdPayload”	JSON		
fileTransferUID	Unique identifier. Used by the MCG and GCG to identify a file that is uploaded.	number	uint32	predefined (taken from ComID 202 message)

5.6.3.2.2.5 Error handling

5.6.3.2.2.5.1 General

This subclause lists error cases that can occur when using the file transfer communication service. Each following subclause presents an error case, and outlines the underlying issue.

NOTE Error cases which are not in the scope of this document are not considered in this subclause.

5.6.3.2.2.5.2 Error case: No ComID 203 received

Figure 21 depicts a case where the ComID 203 message is not received by the MCG.

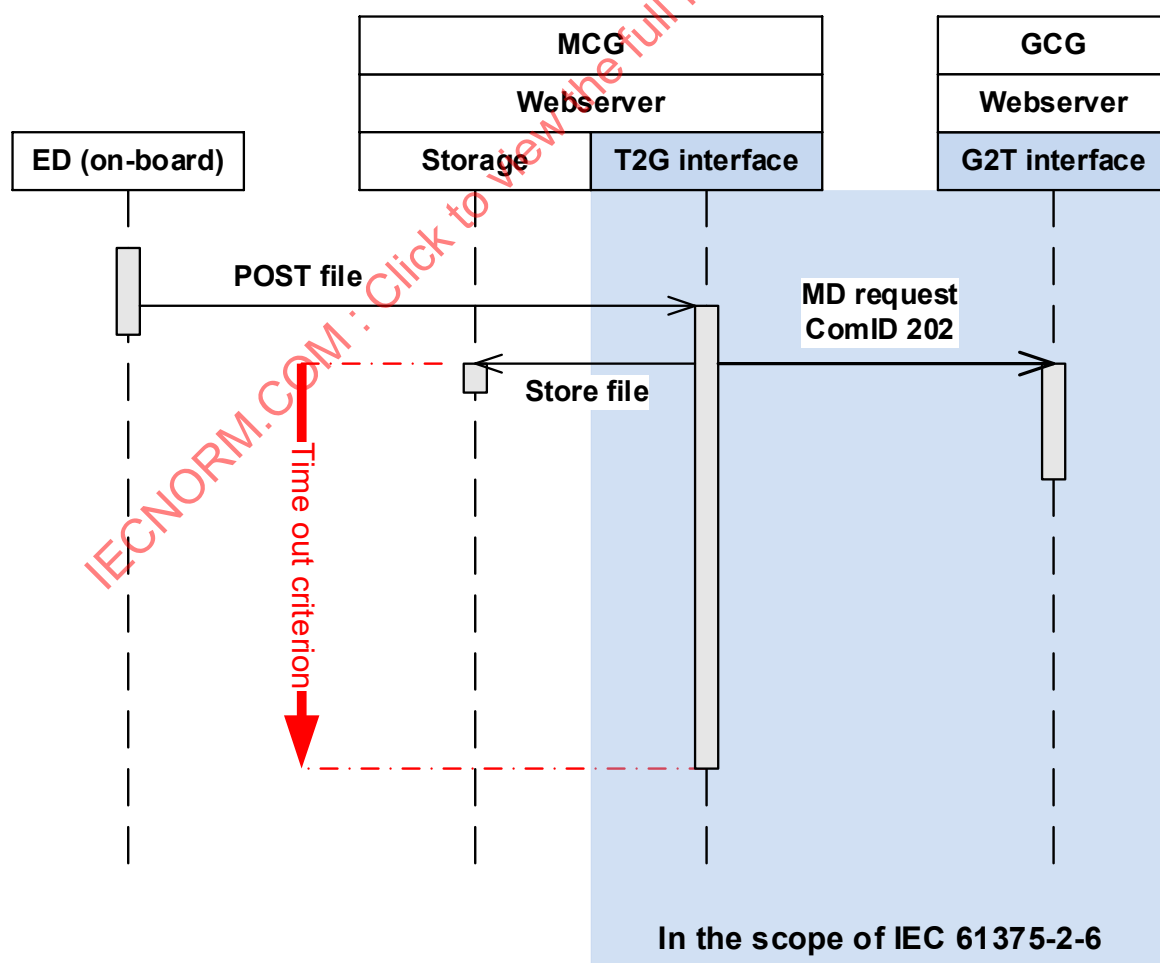


Figure 21 – Error case: No ComID 203 received

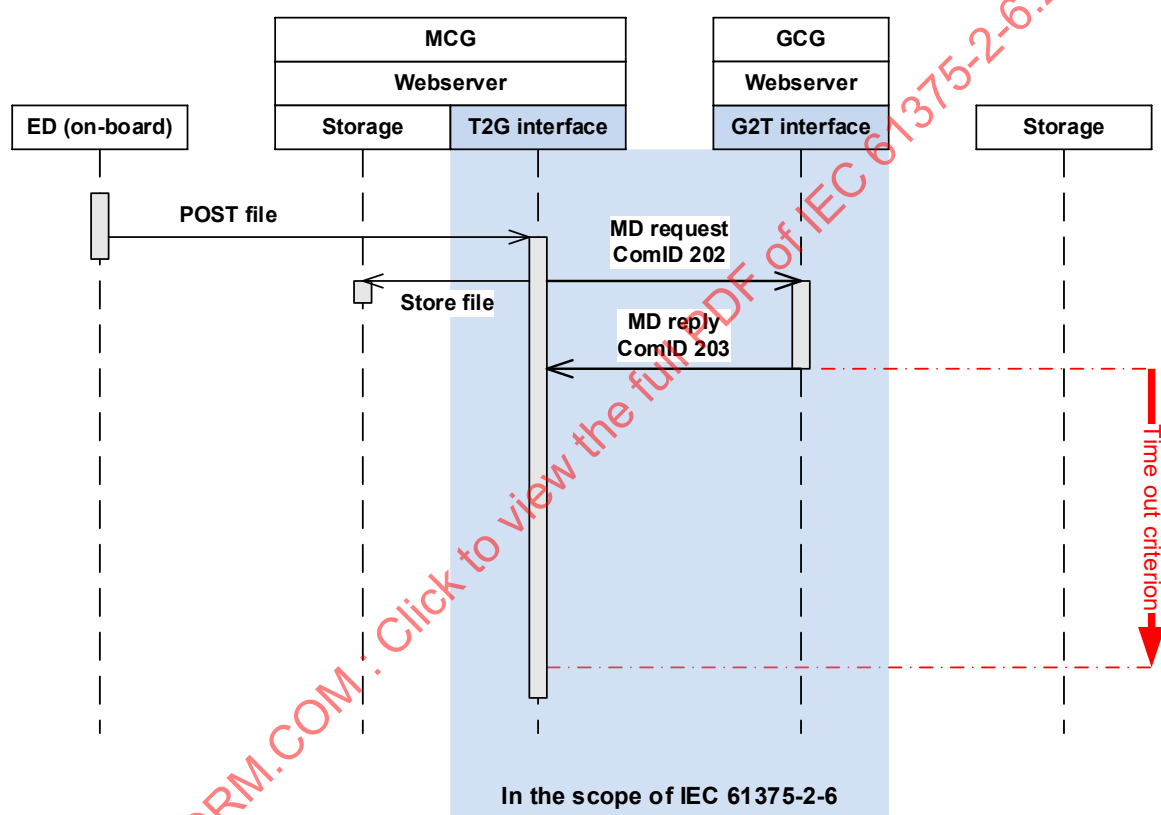
The ComID 202 message is sent from the MCG to the GCG. This message is used by the MCG to request permission for uploading a file to the wayside. The reply to this request, ComID 203, is not received by the MCG.

Problem description: The MCG shall detect that a sent ComID 202 request for uploading a file is not answered by the respective GCG.

Corrective action: It shall be ensured that no lingering upload requests are left in an undefined state, i.e. the request has to be renewed, or the upload request has to be aborted.

5.6.3.2.2.5.3 Error case: No ComID 206 received, no file uploaded to the wayside

Figure 22 depicts a case where the ComID message 206 is not received by the GCG, and no file has been uploaded to the wayside.



IEC

Figure 22 – Error case: no ComID 206 received, no file uploaded to the wayside

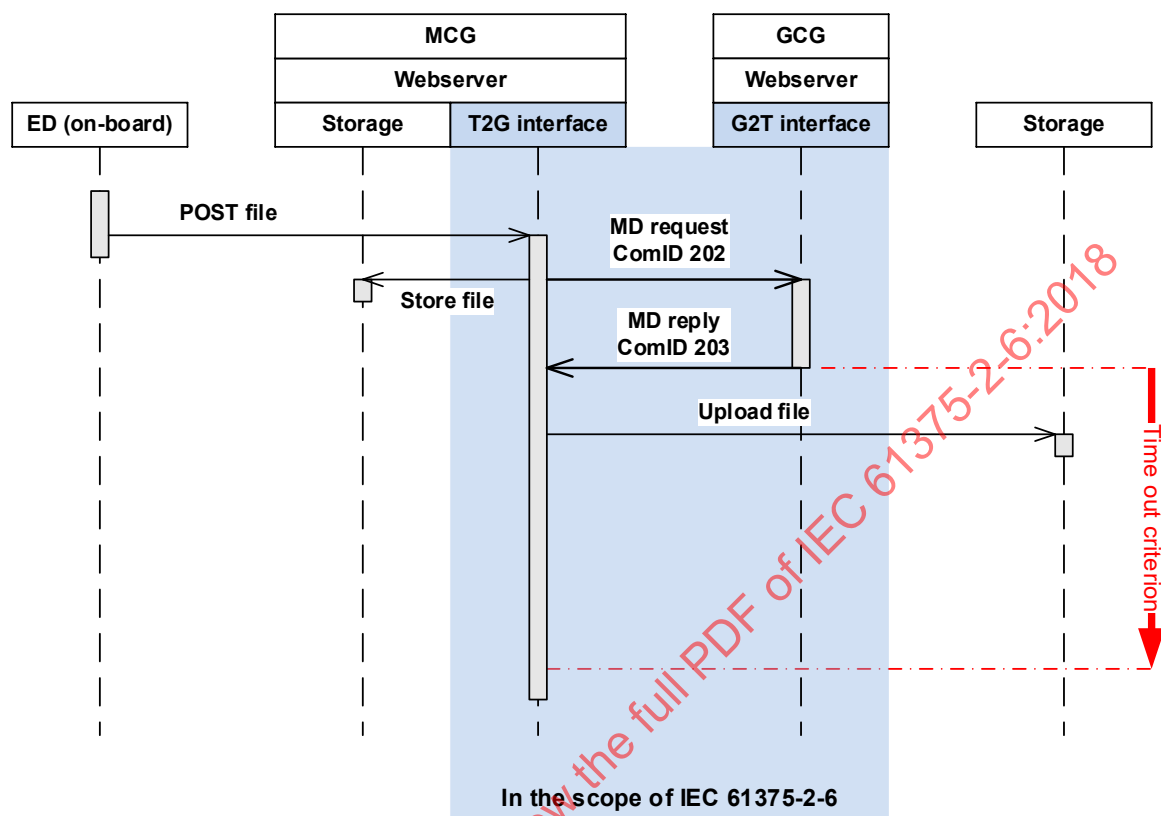
The ComID 206 message is sent from the MCG to the GCG. This message is used by the MCG to follow up on an earlier exchange of ComID 202 and ComID 203 messages, indicating a successful upload to the GCG.

Problem description: The MCG has not uploaded the file to the indicated storage, and never sends the ComID 206 message.

Corrective action: The GCG shall detect that after accepting the request for a file transfer, it is never followed up by a file upload, nor by confirmation. The MCG has to ensure that the upload request is not left in an undefined state, i.e. the request has to be renewed, or the upload request has to be aborted.

5.6.3.2.2.5.4 Error Case: No ComID 206 received, file uploaded to the wayside

Figure 23 depicts a case where the ComID message 206 is not received by the GCG, but the respective file has been uploaded to the wayside.



IEC

Figure 23 – Error Case: No ComID 206 received, file uploaded to the wayside

The ComID 206 message is sent from the MCG to the GCG. This message is used by the MCG to follow up on an earlier exchange of ComID 202 and ComID 203 messages, indicating a successful upload to the GCG.

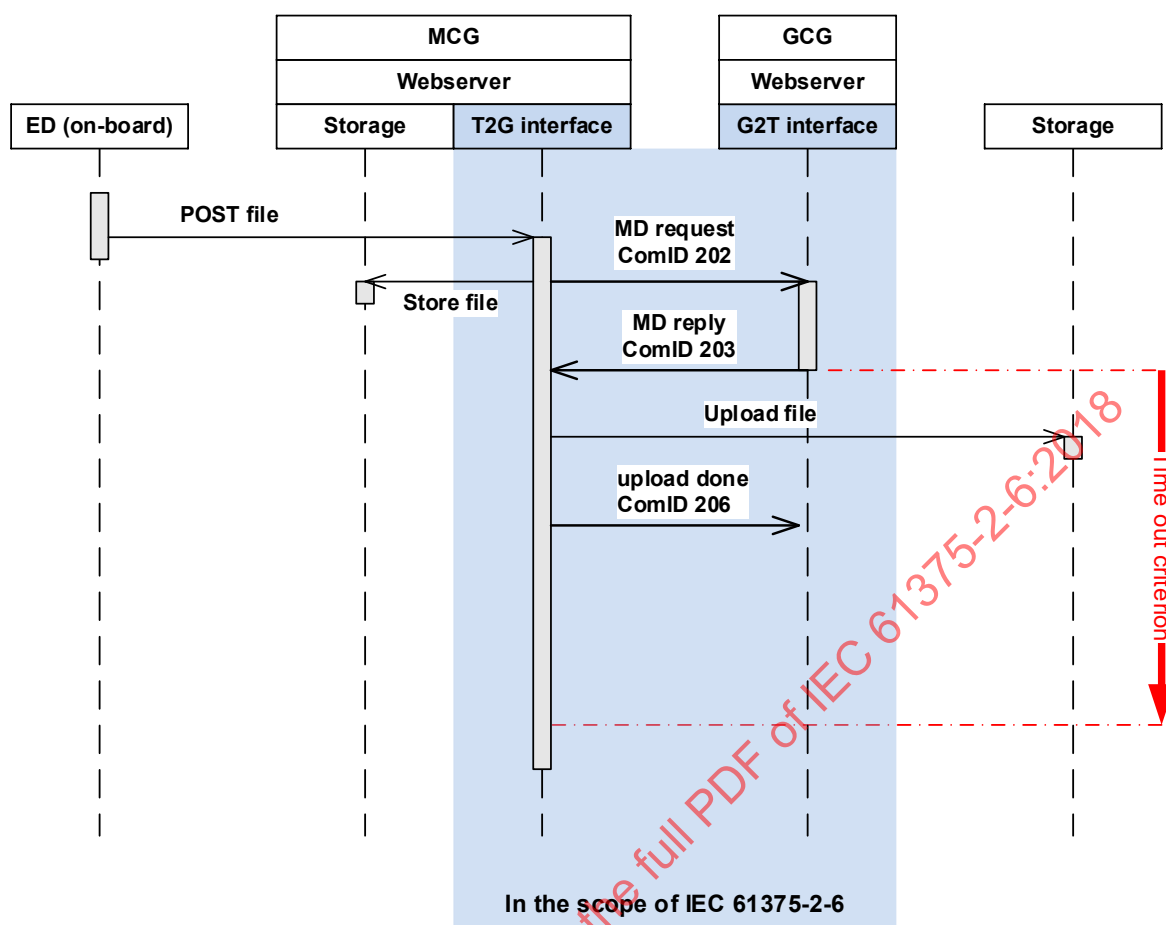
Problem description: The MCG has uploaded the file to the indicated storage, but the GCG never receives the ComID 206 message. The storage location, where the file is uploaded to, might not be internal to the GCG, i.e. the GCG cannot tell that the file has been uploaded.

Corrective action: The GCG shall detect that after accepting the request for a file transfer, it is never followed up by a file upload, nor by confirmation. The GCG might be able to determine if the file has been uploaded by using the information sent in the ComID 202 message, but this is out of scope of this document.

The MCG shall ensure that the upload request is not left in an undefined state, i.e. the request has to be renewed, or the upload request has to be aborted. The GCG has to ensure that no lingering files are left on the storage location indicated by the GCG.

5.6.3.2.2.5.5 Error Case: No ComID 207 received

Figure 24 depicts a case where the ComID message 207 is not received by the MCG.



IEC

Figure 24 – Error Case: No ComID 207 received

The ComID 207 message is sent from the GCG to the MCG. This message is used by the GCG to respond to a ComID 206 message received from a MCG, to indicate that the integrity check of the uploaded file has been successful.

Problem description: The MCG has uploaded the file to the indicated storage, and informed the GCG about the successful upload. The GCG never replies to the ComID 206 message.

Corrective action: The MCG shall detect that after uploading the file, and indicating the successful upload, the confirmation of the integrity check on the ground side is never received. The GCG has to ensure that the integrity of the uploaded file is confirmed on the ground side, and that the file is successfully uploaded to the wayside.

5.6.3.3 File download

5.6.3.3.1 General

Figure 25 depicts an example of how a file is downloaded from a ground end device to the train. The scope of the file download pattern that is specified by this document, will be marked in this subclause using pastel blue background colour.

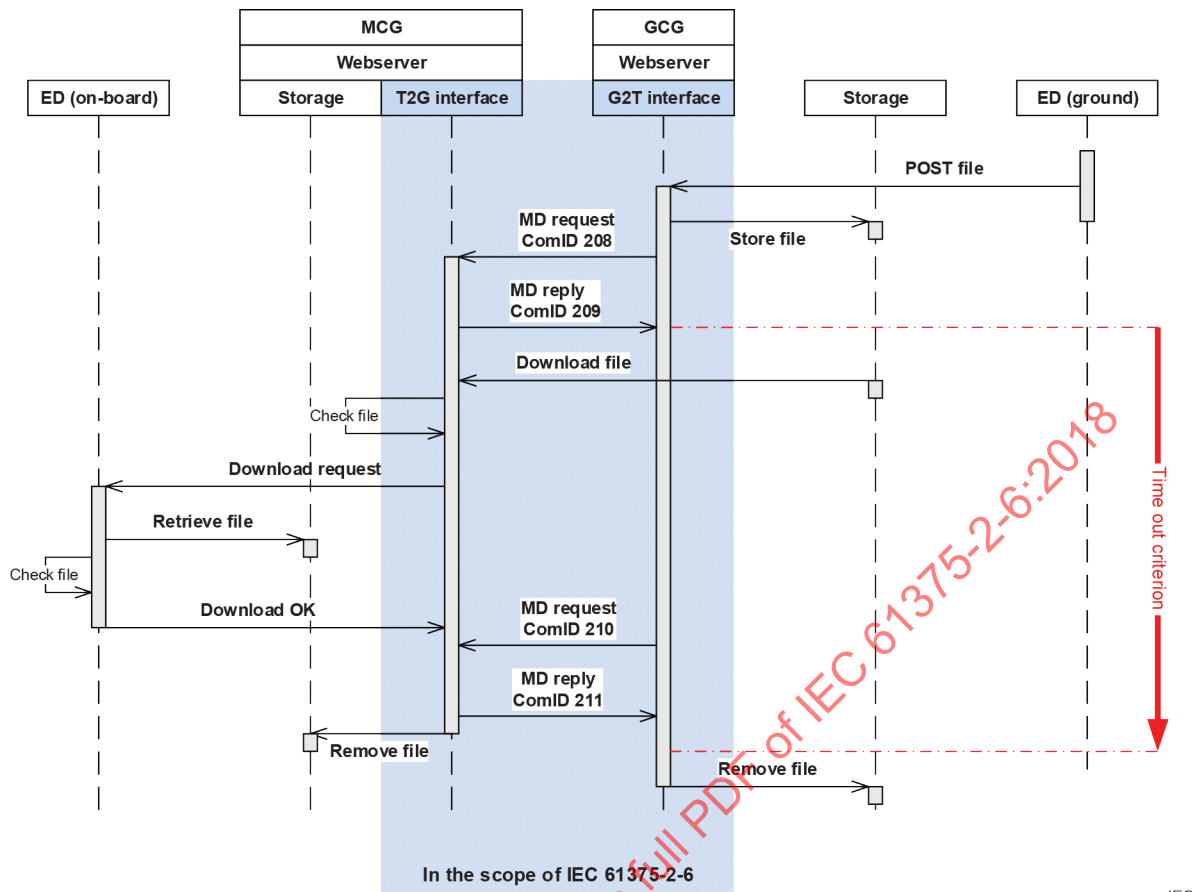


Figure 25 – File download example

A ground end device can download a file to the train using the following logical steps described below:

- The End Device transfers the file to the GCG first, e.g. by using a web server interface which is exposed by the GCG only to devices on the ground.
- After the file has been successfully transferred to the GCG, the GCG automatically asks the MCG to retrieve the file. To do so, the GCG sends a request message (ComID 208) to a web service interface exposed by the MCG, this message includes the storage location from where the MCG can retrieve the file from, and optionally a download **recipe** (see 5.6.3.3.5).
- The MCG acts on the file retrieval request by the GCG and sends a reply message (ComID 209), indicating whether it will download the file.
- After indicating that the file will be downloaded, the MCG retrieves the file from the storage location.
- The GCG checks cyclically (the used cycle time is a configuration item) the state of the download by contacting the MCG. The GCG sends a request message (ComID 210) to the MCG, and the MCG replies using a reply message (ComID 211) indicating the current state of the download.
- After the download has been successfully performed, the MCG uses a means of checking the integrity of the file that has been transferred to the train.
- After checking the integrity of the file successfully, the MCG will inform the GCG that the file transfer to the MCG has been successful the next time it receives a ComID 210 message (see step e).
- If a download recipe has been received in the request sent by the GCG, the MCG now uses this recipe to inform one (or more) End Device about the availability of the downloaded file.

- i) The MCG sends a download request message to each prospective file-receiving End Device.
- j) An End Device ready to receive files downloads the indicated file from the MCG e.g. by using a web server interface , exposed by the MCG to the train only.
- k) After the download has been successfully performed, the End Device uses a means of checking the integrity of the file that has been transferred, to determine if the integrity of the file can be confirmed.
- l) After successfully checking the integrity of the file, the End Device sends a reply message to the web service interface exposed by the MCG, confirming the successful download of the file.
- m) When the MCG receives the next ComID 210 message (see step e), it will inform the GCG about the successful reception and distribution of the file. Afterwards, the MCG and the GCG can discard the file from their storage locations.

5.6.3.3.2 Message definition

5.6.3.3.2.1 Request download of a file (ComID 208)

The ComID 208 message is a MD telegram, which is sent from the GCG to the MCG. This message is used by the GCG to request a download of a file to the train, and contains all the information for a file to be downloaded to the MCG.

The MD request telegram ComID 208 shall be sent with the following header parameters in accordance with Table 36. Refer to Table 18 for general information about the MD header parameters.

Table 36 – ComID 208: MD header telegram values

Parameter	Value
msgType	3 (MD Request)
msgTimeValidity	0 (no timeout)
comID	208

The MD request telegram ComID 208 shall be sent with the following body parameters in accordance with Table 37. Refer to Table 19 for general information about the MD body parameters.

Table 37 – ComID 208: MD Body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 38

The MD request telegram ComID 208 shall be sent with the following payload object in accordance with Table 38.

Table 38 – ComID 208: MD Body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter “mdPayload”	JSON		
fileTransferUID	Unique identifier. Defined by the GCG, used by the MCG and GCG to identify a file that is downloaded.	number	uint32	computed
filename	Name of the file to be transferred to the MCG and subsequently to a receiving ED.	string	char[256]	predefined
fileType	Indicates the type of file that is downloaded.	number	uint8	0 = n.a. 1 = ASCII 2 = Binary 3 = Audio 4 = Video 5-255 not used
fileSize	Indicates the size in bytes of the file.	number	uint64	predefined
fileChecksum	Checksum to enable verification on the train that the file download has been successfully performed. The checksum mechanism used is in the scope of the application.	string	char[256]	computed
storageURL	URL that indicates a location from where the file is to be downloaded by the MCG.	string	char[512]	predefined
dlTarget	Indicates the target ED(s) of the download. See 5.6.3.3.6 for more details.	string	char[128]	predefined
recipe	Indicates application specific handling of the downloaded file. Can be processed by the MCG, otherwise shall be ignored. See 5.6.3.3.5 for more details.	string	char[512]	predefined

5.6.3.3.2.2 Answer a request for downloading (ComID 209)

The ComID 209 message is a MD telegram, which is sent from the MCG to the GCG. This message is used by the MCG to reply to a download request sent by the GCG. The MCG indicates if the request for downloading a file to the train will be fulfilled by the MCG.

The MD response telegram ComID 209 shall be sent with the following header parameters in accordance with Table 39. Refer to Table 18 for general information about the MD header parameters.

Table 39 – ComID 209: MD header telegram values

Parameter	Value
msgType	4 (MD response to received MD request)
msgTimeValidity	0 (no timeout)
comID	209

The MD response telegram ComID 209 shall be sent with the following body parameters in accordance with Table 40. Refer to Table 19 for general information about the MD body parameters.

Table 40 – ComID 209: MD Body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 38

The MD response telegram ComID 209 shall be sent with the following payload object in accordance with Table 41.

Table 41 – ComID 209: MD Body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter "mdPayload"	JSON		
fileTransferUID	Unique identifier. Used by the MCG and GCG to identify and refer to a file that is downloaded.	number	uint32	predefined (taken from ComID 208 message)
reqResponse	Response of the MCG indicating whether the request will be fulfilled.	number	uint8	0 = n.a. 1 = will download file 2 = cannot download file 3..255 = to be defined
fileCheckResult	Indicates the result of the integrity check performed on the downloaded file.	number	bool	computed (true, false)

5.6.3.3.2.3 Request current download status (ComID 210)

The ComID 210 message is a MD telegram, which is sent from the GCG to the MCG. This message is used by the GCG to inquire about the current state of the download of a file to the train. This message can be sent cyclically by the GCG, the cycle time is a configuration item.

The MD request telegram ComID 210 shall be sent with the following header parameters in accordance with Table 42. Refer to Table 18 for general information about the MD header parameters.

Table 42 – ComID 210: MD header telegram values

Parameter	Value
msgType	3 (MD Request)
msgTimeValidity	0 (no timeout)
comID	210

The MD request telegram ComID 210 shall be sent with the following body parameters in accordance with Table 43. Refer to Table 19 for general information about the MD body parameters.

Table 43 – ComID 210: MD Body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 41

The MD request telegram ComID 210 shall be sent with the following payload object in accordance with Table 44.

Table 44 – ComID 210: MD Body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter "mdPayload"	JSON		
fileTransferUID	Unique identifier. Used by the MCG and GCG to identify and refer to a file that is downloaded.	number	uint32	predefined (taken from ComID 208 message)

5.6.3.3.3 Answer current download status (ComID 211)

The ComID 211 message is a MD telegram, which is sent from the MCG to the GCG. This message is used by the MCG to reply to the GCG and indicate to the GCG the current state of a requested file download.

The MD response telegram ComID 211 shall be sent with the following header parameters in accordance with Table 45. Refer to Table 18 for general information about the MD header parameters.

Table 45 – ComID 211: MD header telegram values

Parameter	Value
msgType	4 (MD response to received MD request)
msgTimeValidity	0 (no timeout)
comID	211

The MD response telegram ComID 211 shall be sent with the following body parameters in accordance with Table 46. Refer to Table 19 for general information about the MD body parameters.

Table 46 – ComID 211: MD Body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 44

The MD response telegram ComID 211 shall be sent with the following payload object in accordance with Table 47.

Table 47 – ComID 211: MD Body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter “mdPayload”	JSON		
fileTransferUID	Unique identifier. Used by the MCG and GCG to identify and refer to a file that is downloaded.	number	uint32	predefined (taken from ComID 208 message)
statFileTransfer	Indicates the current state of the file transfer to the MCG, as seen by the MCG.	number	uint8	0 = n.a. 1 = download to MCG not started 2 = download to MCG started 3 = download to MCG finished
statFileIntegrity	Indicates the current state of the file integrity check done by the MCG.	number	uint8	0 = n.a. 1 = integrity check by MCG not performed 2 = integrity check by MCG successful 3 = integrity check by MCG failed
statFileDistribution	Indicates the current state of the file distribution to the receiving ED(s).	number	uint8	0 = n.a. 1 = file transfer to ED not started 2 = file transfer to ED started 3 = file transfer to ED finished 4 = download to ED OK

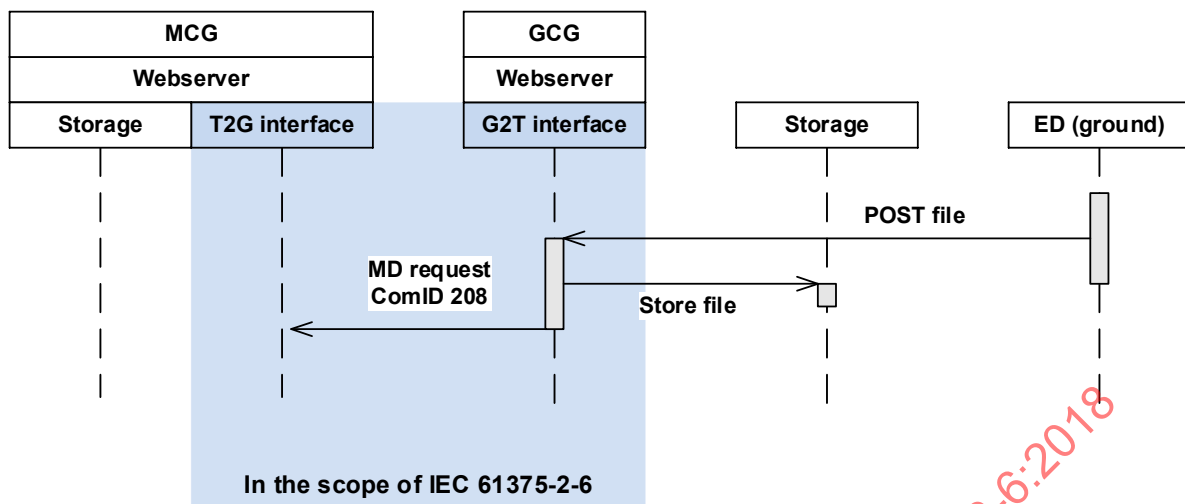
5.6.3.3.4 Error handling**5.6.3.3.4.1 General**

This subclause lists error cases that can occur when using the file transfer communication service. Each following subclause presents an error case, and outlines the underlying issue.

NOTE Error cases which are not in the scope of this document are not considered in this subclause.

5.6.3.3.4.2 Error case: no ComID 209 received

Figure 26 depicts a case where the ComID 209 message is not received by the GCG.



IEC

Figure 26 – Error case: no ComID 209 received

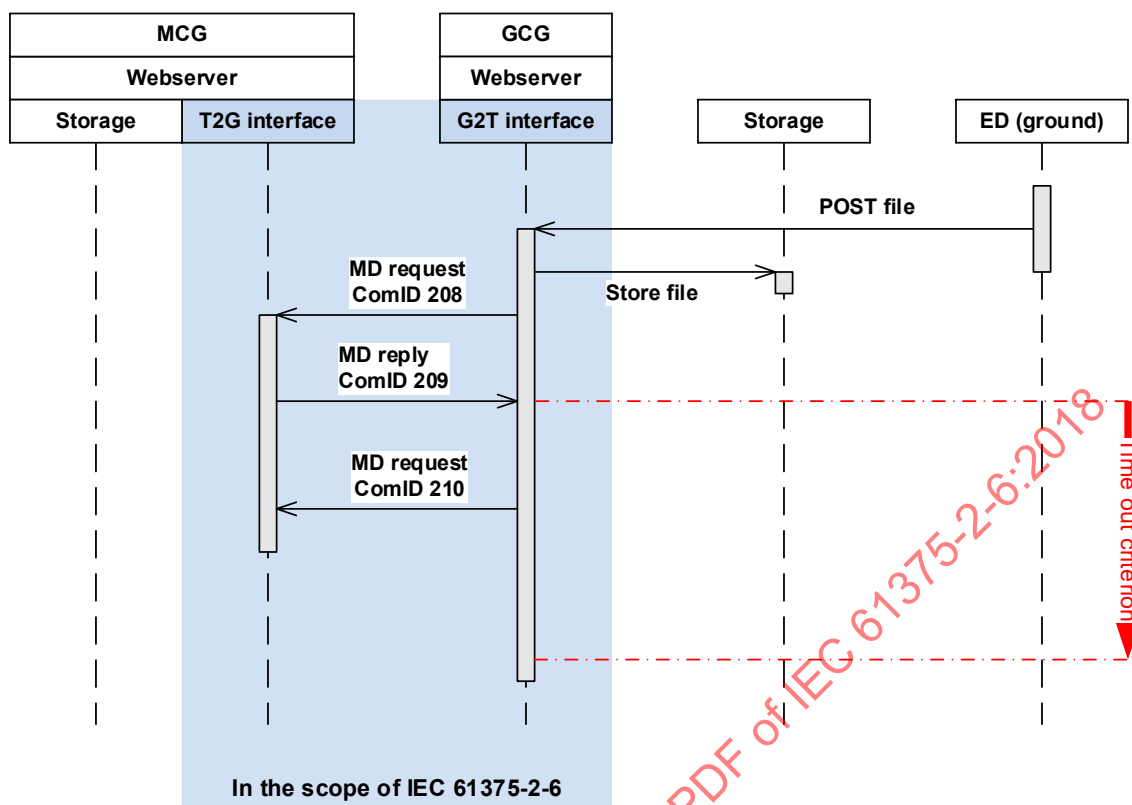
The ComID 208 message is sent from the GCG to the MCG. This message is used by the GCG to request a MCG to download a file to the train. The reply to this request, ComID 209, is not received by the GCG.

Problem description: The GCG has to detect that the MCG is not replying to the sent ComID 208 message. It has to be assumed that the MCG cannot download the file.

Corrective action: It shall be ensured that no lingering download requests are left in an undefined state, i.e. the request has to be renewed, or the request shall be aborted. Additionally, the file already under control of the GCG might still have to be uploaded, or deleted.

5.6.3.3.4.3 Error case: no ComID 211 received

Figure 27 depicts a case where the ComID 211 message is not received by the GCG.



IEC

Figure 27 – Error case: no ComID 211 received

Following up on an earlier exchange of ComID 208 and ComID 209 messages, the GCG sends a ComID 210 message to the MCG. This message is used by the GCG to check on the current state of the file download. The GCG never receives a reply from the MCG, a ComID 211 message.

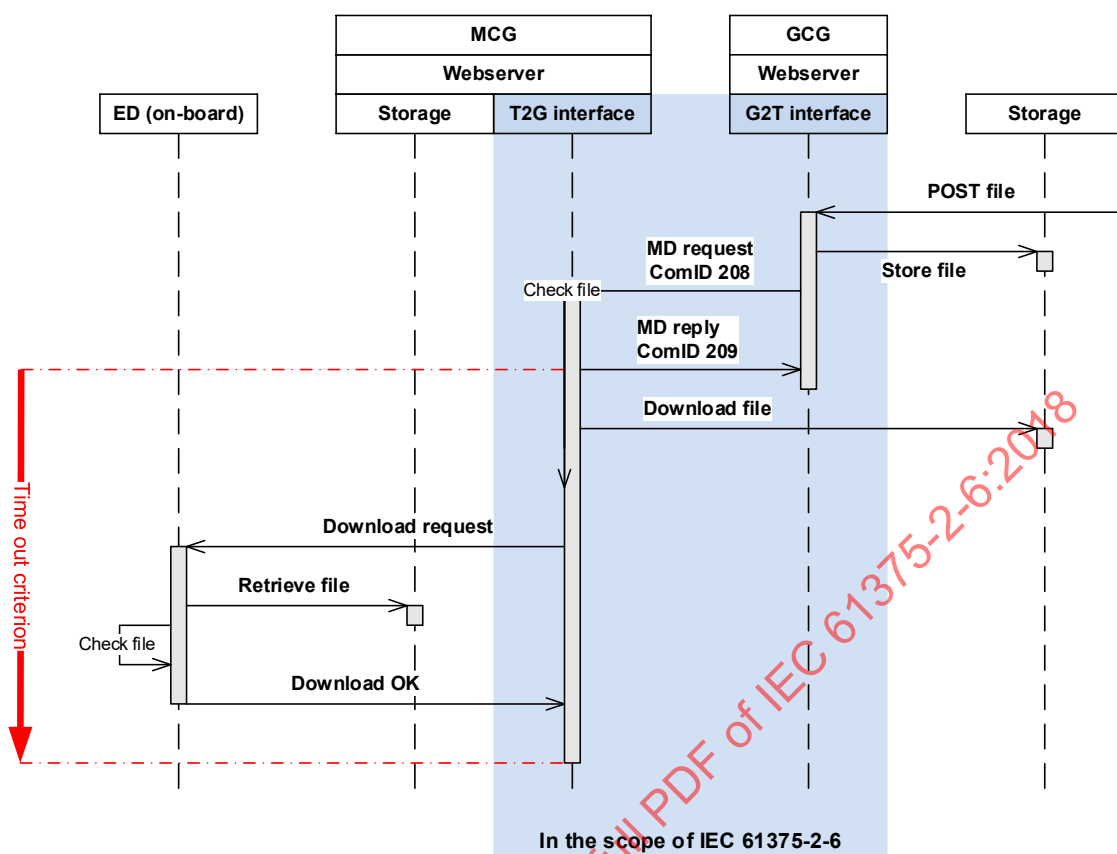
Problem description: The MCG does not send the ComID 211 message.

Corrective action: The GCG has to detect that the MCG, even though it indicated that it will download the file, never replies to inquiries about the current state of the download.

The GCG has to ensure that the download request is not left in an undefined state, i.e. either the request has to be renewed, or the download request has to be aborted.

5.6.3.3.4.4 Error case: no ComID 210 received

Figure 28 depicts a case where the MCG never receives a ComID 210 message sent by the GCG.



IEC

Figure 28 – Error case: no ComID 210 received

The ComID 210 message is sent from the GCG to the MCG. This message is used by the GCG to follow up on an earlier exchange of ComID 208 and ComID 209 messages, to determine whether a successful download of the file to the MCG, and subsequently the download to the target ED(s), took place.

Following up on an earlier exchange of ComID 208 and ComID 209 messages, the MCG downloads the file to the train. It checks the integrity of the file, and informs the target ED(s) about the availability of the file.

Even though the download successfully finished, it does not receive an inquiry from the GCG about the state of the download, and thus the MCG can never indicate the successful completion of the download request.

Problem description: The MCG does not receive the ComID 210 message. Since the file download can be successfully performed by the MCG, this issue might only be noticed after the file has successfully been distributed to the target ED(s).

Corrective action: The MCG can detect that after downloading a file to target ED(s), it is never receiving the ComID 210 message. From the point of view of the MCG, no action needs be taken to inform the GCG, instead the file can be removed from the MCG storage.

5.6.3.3.5 Download recipe

In the ComID 208 message (see 5.6.3.3.2.1), the “recipe”-field can be used to include an application specific string.

NOTE 1 This string is always Base64 encoded, in order not to violate the parsing of this message.

The contents of this string can be structured in such a way as to provide additional information for advanced download concepts, which go beyond the scope of the file transfer functionality described in this document.

NOTE 2 The definition of this string is out of the scope of this document.

5.6.3.3.6 Valid dITarget values

5.6.3.3.6.1 General

The dITarget field in the ComID 208 message basically contains a uniform resource identifier (URI) pointing at the target ED(s) where a file will be downloaded to. When it comes to addressing devices in the ECN, it is sensible to use values based on the TCN-URI Scheme defined in IEC 61375-2-3:2015, 5.4.4.

IEC 61375-2-3 presents a general schema syntax of a valid TCN-URI identifier. Table 48 to Table 54 list all the elements of a valid TCN-URI as defined by IEC 61375-2-3, indicate the “Applicability” as requested in IEC 61375-2-3, and also feature a “Handling” column, to indicate whether this part is allowed to be used as part of a valid dITarget value.

Table 48 lists the top-level parts of a TCN-URI, which can be used to create a valid dITarget value:

Table 48 – Main parts of dITarget URI

Element	Applicability	Handling	Reasoning
scheme	Optional	Not allowed	- Only the host part of the URI has to be interpreted by the MCG. - The message is to be processed by the MCG, so it is already established that it is a TCN-URI address.
user	Mandatory	Not allowed	Only the host part of the URI has to be interpreted by the MCG.
host	Mandatory	Allowed	see 5.6.3.3.6.2

5.6.3.3.6.2 Host element

Table 49 lists the elements of the host-part defined in IEC 61375-2-3, which are used to create a valid dITarget value:

Table 49 – Main parts of host element

Label	Applicability	Handling	Reasoning
device	Mandatory	Allowed	
vehicle	Optional	Allowed	
consist	Optional	Allowed	
cltrain	Optional	Allowed	Depends on usage of closed train concept
train	Optional	Allowed	Superfluous

5.6.3.3.6.3 Device label

Table 50 lists the labels of the host-part of the device, as defined in IEC 61375-2-3, which are used to create a valid dITarget value:

Table 50 – Valid “device” label values

Label part	Applicability	Handling	Reasoning
IDev	Optional	Allowed	
deviceName	Mandatory	Allowed	
grpDev	Mandatory	Allowed	
“grpAll”	Mandatory	Not allowed	A file shall not be downloaded to all devices
anyDev	Optional	Not allowed	A file shall not be downloaded to an unknown device, if it is not a well-defined group

5.6.3.3.6.4 Vehicle label

Table 51 lists the labels of the vehicle-part, as defined in IEC 61375-2-3, which are used to create a valid dITarget value:

Table 51 – Valid “vehicle” label values

Label part	Applicability	Handling	Reasoning
IVeh	Optional	Allowed	
aVeh	Mandatory	Allowed	
opVehNo	Mandatory	Not allowed	Label can only be used with label “anyCst”, which is not allowed (see Table 52)
cstVehNo	Mandatory	Allowed	
leadVeh	Mandatory	Allowed	
idVeh	Mandatory	Allowed	
anyVeh	Mandatory	Not allowed	A file shall not be downloaded to an unknown device, if it is not a well-defined group

5.6.3.3.6.5 Consist label

Table 52 lists the labels of the Consist-part, as defined in IEC 61375-2-3, which are used to create a valid dITarget value:

Table 52 – Valid “consist” label values

Label part	Applicability	Handling	Reasoning
ICst	Optional	Allowed	
cstNo	Mandatory	Allowed	
opCstNo	Optional	Not allowed	Label can only be used with label “anyVeh”, which is not allowed (see Table 51)
aCst	Mandatory	Allowed	
anyCst	Mandatory	Not allowed	Label can only be used with label “anyVeh” or “opVehNo”, which are not allowed (see Table 51)
idCst	Mandatory	Allowed	
leadCst	Mandatory	Allowed	

5.6.3.3.6.6 Closed train label

Table 53 lists the labels of the Closed train-part, as defined in IEC 61375-2-3, which are used to create a valid dITarget value:

Table 53 – Valid “closed train” label values

Label part	Applicability	Handling	Reasoning
ICITrn	Optional	Allowed	
anyCITrn	Mandatory	Not allowed	A file shall not be downloaded to an unknown device, if it is not a well-defined group
aCITrn	Mandatory	Not allowed	A file shall not be downloaded to an unknown device, if it is not a well-defined group

5.6.3.3.6.7 Train label

Table 54 lists the labels of the Train-part, as defined in IEC 61375-2-3, which are used to create a valid dITarget value:

Table 54 – Valid “train” label values

Label part	Applicability	Handling	Reasoning
ITrn	Mandatory	Allowed	

5.6.3.3.6.8 Examples of valid dITarget values

As an example, Table 55 lists valid dITarget strings that could be used as dITarget values:

Table 55 – Exemplary dITarget values

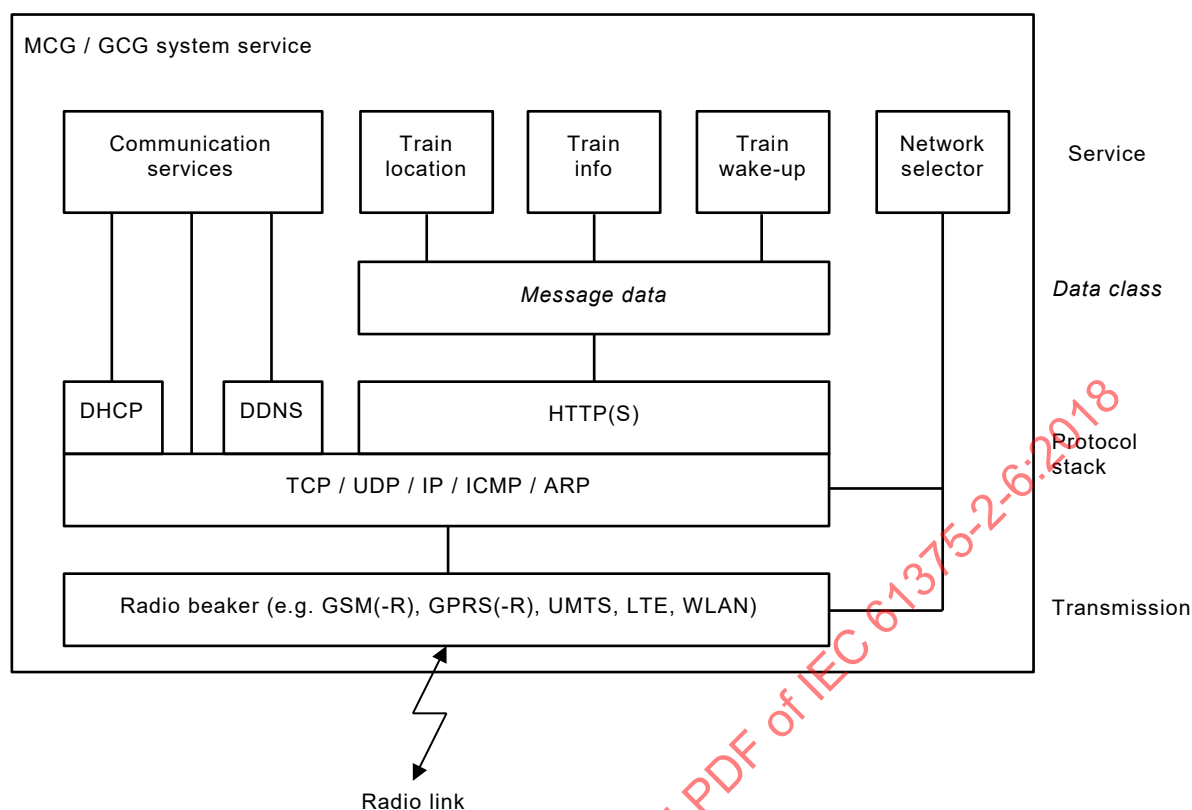
dITarget value	Comment
devHMI	
grpCCU	
grpHMI.aVeh	
fctHMI.UIC948002343044	
grpHMI.aVeh.UIC948002343045	- aVeh can only be used with a group label - group of HMIs is located in a car that is part of a consist

6 Services and interfaces (MCG)

6.1 Overview

6.1.1 MCG system service architecture

Figure 29 shows an overview of the services of the MCG system provided for the train and ground applications.



IEC

Figure 29 – Service architecture

The Communication Services provide functions for the organization of the communication channel between train and ground.

Furthermore the Train Info Service provides services for information about the train (e.g. train composition derived from the Train Topology Database (TTDB)).

The Train Location Service provides information about the train location.

Optionally a train wake-up service can be implemented by the MCG to power-up a train, which is in energy saving mode. This service is requested from ground side.

Optionally a telemetry service can be implemented by the MCG to provide telemetry information about the train with process data quality.

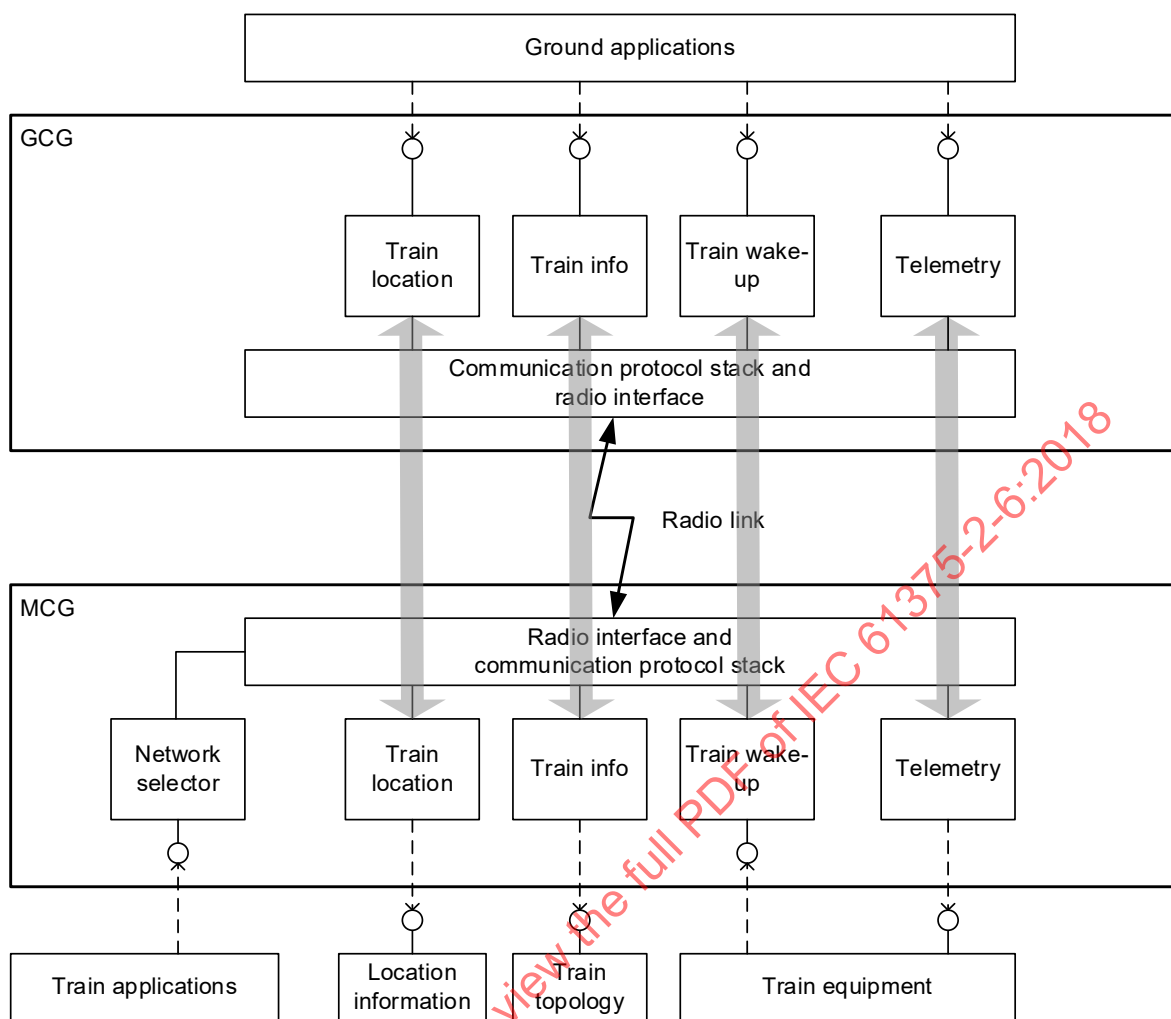
The Network Selector Service provides an interface for control of data transmission and radio bearer selection.

The communication stack protocols used are based on the standard internet protocols (e.g. IP, TCP, UDP, HTTP, MQTT).

The used radio bearers (e.g. GSM, UMTS or others) are not in the scope of this document.

6.1.2 MCG / GCG system service interfaces

Figure 30 shows an overview of the service interfaces between MCG and GCG system provided for the train and ground applications.



IEC

Figure 30 – Service interfaces

The application interfaces of the services are shown for completeness and comprehensibility only. The implementation of these interfaces is not in the scope of this document. This document defines only the communication interfaces between the parts of the services split between MCG and GCG, as illustrated by the light grey arrows in Figure 30.

6.1.3 MCG / GCG communication relationship

For the purpose of this document, the following terms are defined:

- a) communication channel;
- b) radio link.

A communication channel is a 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. This conceptual state is considered as a session between the two entities MCG and GCG.

A radio link is a wireless link, that connects a device with a network, allowing the former to reach other devices through that network (typically the Internet, but can be also a private network).

6.2 Service provisioning

The MCG shall provide the following services:

- a) Communication Services;

b) Train Information Service.

The MCG may provide the following optional services:

- c) Train Location Service;
- d) Telemetry Services;
- e) Train Wake-up Service.

If the MCG is equipped with several radio links, the MCG shall conditionally provide the following service:

f) Network Selector Service.

The GCG shall provide the following service:

- g) Communication Services;
- h) Train Location Service;
- i) Train Information Service;

The GCG may provide the following optional services:

- j) Telemetry Services;
- k) Train Wake-up Service.

6.3 MCG / GCG system service description

6.3.1 Communication Services

6.3.1.1 General

The Communication Services (CS) shall provide an interface for

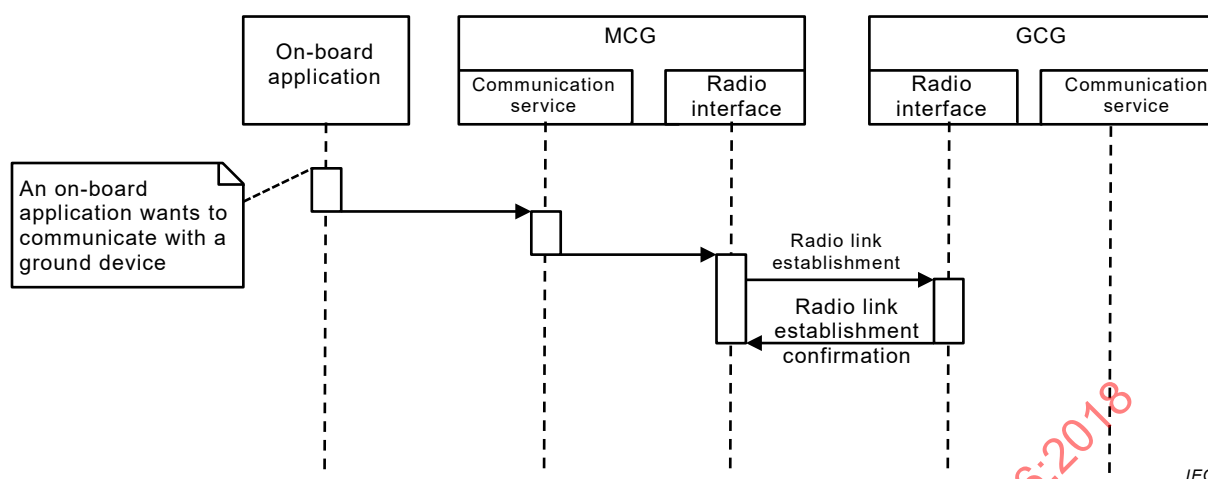
- a) radio link establishment (informative);
- b) IP address handling for the MCG for the communication to ground;
- c) registering the MCG on the ground DNS server, to resolve symbolic names to IP addresses using the DNS protocol;
- d) update of the ground DNS server for forwarding DNS requests to the MCG DNS server to resolve names in the train domain;
- e) Authentication service.

To facilitate radio link establishment, connection related parameters (e.g. to dial a call number) can be stored on the MCG and the GCG. The configuration and management of these parameters is not in the scope of this document.

6.3.1.2 Radio link establishment (informative)

Only the MCG shall establish the radio link to the GCG.

If the MCG is not linked to the GCG and a ground device wants to communicate with the MCG or a mobile device, the GCG shall indicate this request to the MCG. Then the MCG shall establish the radio link to the GCG.



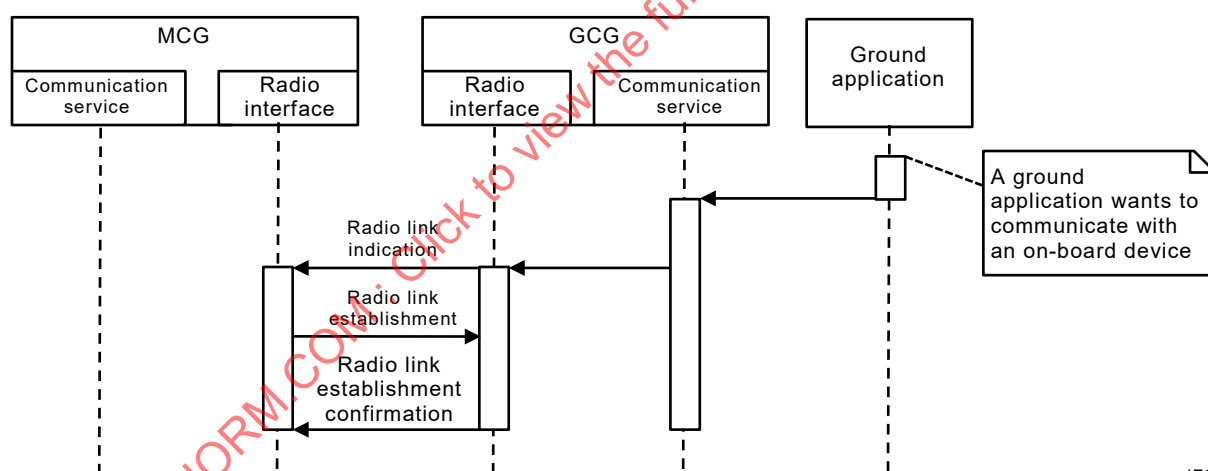
IEC

Figure 31 – Procedure to establish the radio link from MCG

NOTE Figure 31 is simplified to show the principle of link establishment and not the full communication sequence.

If the communication stack routes the IP communication to a radio interface of the MCG, the communication driver is instrumented to establish the radio link to the GCG. The implementation of the radio link establishment depends on the radio technology and is not in the scope of the document.

Figure 32 illustrates the procedure to establish the radio link from GCG to MCG.



IEC

Figure 32 – Procedure to establish the radio link from GCG

NOTE Figure 32 is simplified to show the principle of link establishment and not the full communication sequence.

If the communication stack routes the IP communication to a radio interface of the GCG, the communication driver is instrumented to indicate the radio link establishment to the MCG and the MCG establishes the radio link.

6.3.1.3 IP address handling

The MCG shall acquire an IP address for communication and addressing information of the DNS.

This process depends on the used radio technology. For example the during connection establishment with a telecommunication provider this address may assigned by the

telecommunication provider. When the MCG connects to a WLAN, for example DHCP can be used. The implementation to acquire the IP address is not in the scope of this document.

6.3.1.4 Register MCG on ground DNS

The GCG shall be accompanied by a dynamic updatable DNS (DDNS) server in the same network domain as the GCG.

The MCG shall register its IP address and the train identification at the ground DDNS, using the protocol according to RFC 2136.

Figure 33 illustrates the procedure to update the ground DNS server.

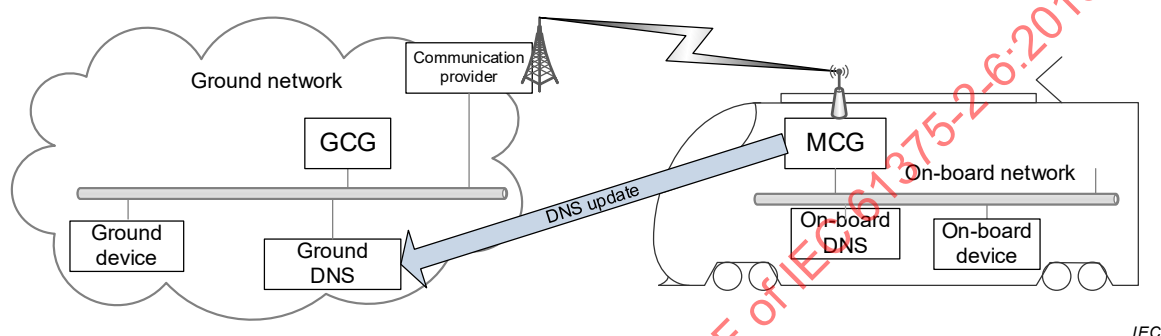


Figure 33 – Procedure to update the ground DNS server

The MCG sends the nsupdate telegram directly to the ground DNS server.

The nsupdate is made directly to a ground TCN-DNS instance, which is only responsible for managing the MCGs. Other security relevant information about the rest of the network cannot be accessed.

6.3.1.5 Capability detection

It is a prerequisite for all applications that the DDNS on the ground side is successfully updated. Moreover the MCG informs the GCG about the facilities of the train by sending a mandatory capabilities message right after the establishment of a connection. If the MCG detects a failure in the message transmission it has to be resent. The msgType is MDEvent. The MCG can easily evaluate the HTTP status code of the MDEvent. The following MD Header parameters according to Table 56 shall be used:

Table 56 – ComID 240: Capability message

Parameter	Value
msgType	1 (MD Event sporadic)
msgTimeValidity	0 (no timeout)
comID	240

The MD event telegram ComID 240 shall be sent with the following body parameters in accordance with Table 57. Refer to Table 19 for general information about the MD body parameters.

Table 57 – ComID 240: MD event body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 41

The MD event telegram ComID 240 shall be sent with the following payload object in accordance with Table 58.

Table 58 – ComID 240: MD event body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter "mdPayload"	JSON		
serviceList	List of IDs of supported services	array	uint8[]	0 = N/A 1 = File Transfer Service 2 = Train Location Service 3 = Train Information Service 4 = Network Selector Service 5 = Train Wake-up Service 6 .. 255 = sVendor specific services

6.3.1.6 Authentication service

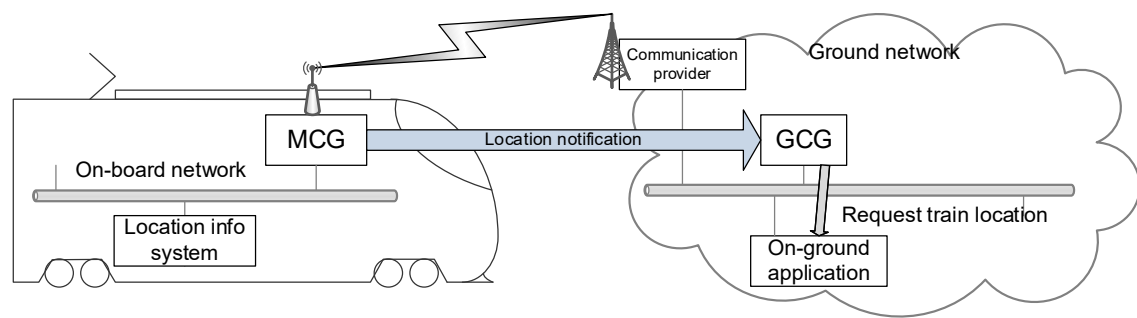
The authentication shall be provided by an authentication, authorization, accounting (AAA) system.

6.3.2 Train Location Service (Option)

6.3.2.1 General

The Train Location Service (TLOS) provides an interface to inform the GCG about the current train location and provide an interface for ground applications to request the current train location.

Figure 34 illustrates the architecture to provide the train location to an on-ground application.



IEC

Figure 34 – Example architecture to provide the train location

An on-ground application can request the train location from the GCG and the GCG requests it from the MCG. The request of the GCG can also be triggered for example when the MCG establishes the communication channel.

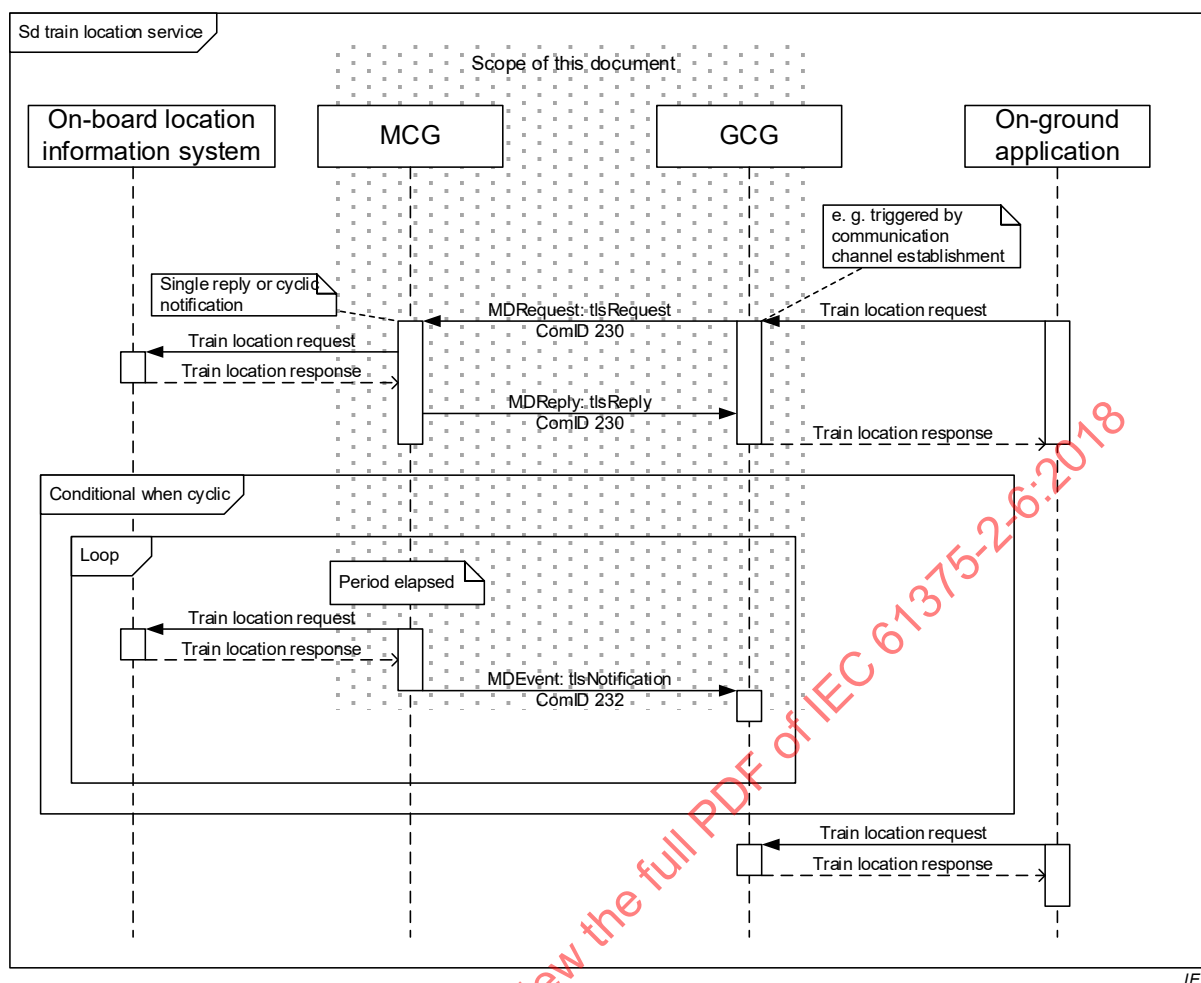
The TLOS of the MCG cyclically gets its information from a positioning system (e.g. GNSS receiver) and sends it with a location notification to the GCG.

NOTE The positioning system can be integrated in the MCG.

The GCG persists the received location information and provides it to the on-ground application. The persistence of the train location and the interface for the on-ground application is not in the scope of this document.

6.3.2.2 Procedure to notify about train location

Figure 35 illustrates the procedure for the MCG to notify the GCG about the current train location.



IEC

Figure 35 – Example procedure to notify about current train location

The GCG shall request the train location service TLOS with the MD request ComID 230 tlosRequest. The provisioning of information may be a single reply or cyclic update.

The MCG part of TLOS requests and gets the current location from an onboard location information source (for example Global Navigation Satellite System GNSS). The actual procedure of obtaining the location information is not in the scope of this document.

The MCG shall reply to the MD request ComID 230 with the MD reply ComID 230 tlosReply to the GCG.

When the train location is requested cyclically, then the MCG periodically acquires the train location notification and then the MCG shall send the MD event ComID 232 tlosNotification to the GCG.

The GCG persists the received train location information and provides it to ground applications. The ground interface and procedure to access the train location information is not in the scope of this document.

The request for train location from a ground application is not in the scope of this document. It can be implemented for example based on requests or with an application registration and notification by the GCG, when it receives a location notification from the MCG.

The behaviour of the TLOS on the GCG in case of loss of communication channel is not in the scope of this document. But it is recommended, that the GCG will inform the ground

application about the quality of the train location information, for example by a time stamp of the last received train location.

The trigger for deregistering the GCG is not in the scope of this document.

6.3.2.3 Request train location (ComID 230)

The ComID 230 message is a MD telegram, which is sent from the GCG to the MCG. This message is used by the GCG to inquire about the train location

The MD request telegram ComID 230 shall be sent with the following header parameters in accordance with Table 59. Refer to Table 18 for general information about the MD header parameters.

Table 59 – ComID 230: MD request header telegram values

Parameter	Value
msgType	3 (MD Request)
msgTimeValidity	0 (no timeout)
comID	230

The MD request telegram ComID 230 shall be sent with the following body parameters in accordance with Table 43. Refer to Table 19 for general information about the MD body parameters.

Table 60 – ComID 230: MD request body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 41

The MD request telegram ComID 230 shall be sent with the following payload object in accordance with Table 61.

Table 61 – ComID 230: MD request body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter "mdPayload"	JSON		
cyclic	Enable/disable cyclic location notification	number	uint8	0 = disable 1 = enable 2 = do not change other values reserved
cycleTime	Cycle time in units of seconds	number	uint16	application defined

The parameter cyclic switches on or off the cyclic notifications about the train location. With the parameter value 2 it is possible to request the train location from time to time without changing the enabled or disabled state of notification of a previous request.

6.3.2.4 Reply train location (ComID 230)

The ComID 230 message is a MD telegram, which is sent from the MCG to the GCG. This message is used by the MCG to reply to the GCG and indicate to the GCG the requested train location.

The MD response telegram ComID 230 shall be sent with the following header parameters in accordance with Table 45. Refer to Table 18 for general information about the MD header parameters.

Table 62 – ComID 230: MD reply header telegram values

Parameter	Value
msgType	4 (MD response to received MD request)
msgTimeValidity	0 (no timeout)
comID	230

The MD response telegram ComID 230 shall be sent with the following body parameters in accordance with Table 63. Refer to Table 19 for general information about the MD body parameters.

Table 63 – ComID 230: MD reply body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 64

The MD response telegram ComID 230 shall be sent with the following payload object in accordance with Table 64.

Table 64 – ComID 230/232: MD reply/notification body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter "mdPayload"	JSON		
result	Result of the request	number	0 .. 255	0 = N/A 1 = Ok 2 = Internal error 255 = Error Other values reserved
timeStamp	Current time UTC in seconds since the epoch	number	uint32	computed
latitude	Latitude of current position in decimal degrees	number	uint32	computed Fixed point notation: 1 bit – Sign 8 bits – Integer part 23 bits – Decimal part
longitude	Longitude of current position in decimal degrees	number	uint32	computed Fixed point notation: 1 bit – Sign 8 bits – Integer part 23 bits – Decimal part
altitude	Altitude of current position in metres over the sea level	number	uint32	computed

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter “mdPayload”	JSON		
orientation	Orientation at the current position in decimal degrees	number	0 .. 359	computed for example: 0 = North 90 = East 180 = South 270 = West
directionOfTravel	Orientation of the train on the route	number	uint8	0 = N/A 1 = Same direction 2 = Reverse direction Other values reserved
kilometricPoint	Current point on the track of the route in kilometres	number	int16	computed, “0”, if not available

Table 65 – Example of latitude/longitude with proposed fixed point notation

	Decimal	Binary	Hexadecimal
Latitude	40,405131	0 00101000 11000101110100010110000	142E8B0
Longitude	–3,698273	1 00000011 10101010011110100001000	81D53D08

6.3.2.5 Train location notification message (ComID 232)

The TLOS MD event telegram ComID 232 `tlosNotification` shall be sent with the following header parameters in accordance with Table 66. Refer to Table 18 for general information about the MD header parameters.

Table 66 – ComID 232: MD header telegram values

Parameter	Value
msgType	2 (MD Event-cyclic)
msgTimeValidity	0 (no timeout)
comId	232

The MD notification telegram ComID 232 shall be sent with the following body parameters in accordance with Table 67. Refer to Table 19 for general information about the MD body parameters.

Table 67 – ComID 232: MD Body telegram values

Parameter	Value
mdPayloadType	“JSON”
mdPayload	see Table 64

The MD notification telegram ComID 232 shall be sent with the payload object in accordance with Table 64.

6.3.3 Train Information Service

6.3.3.1 General

The Train Information Service (TIS) provides an interface to inform the GCG about the current train information and about changes in the current train information.

The TIS is an optional service at device level, but mandatory at train level, see 4.8:

- a) It is mandatory to ensure the presence of at least one device performing the TIS at train level. For a "fully functional real train" at least one device shall be available on-board, which performs the TIS. It is the responsibility of the manufacturer of the train to ensure the presence of the TIS;
- b) It is optional at device level, so that special applications, for example energy metering with dedicated T2G communication hardware can conform to this document without implementing TIS.

Figure 36 illustrates the architecture to provide the train information to an on-ground application.

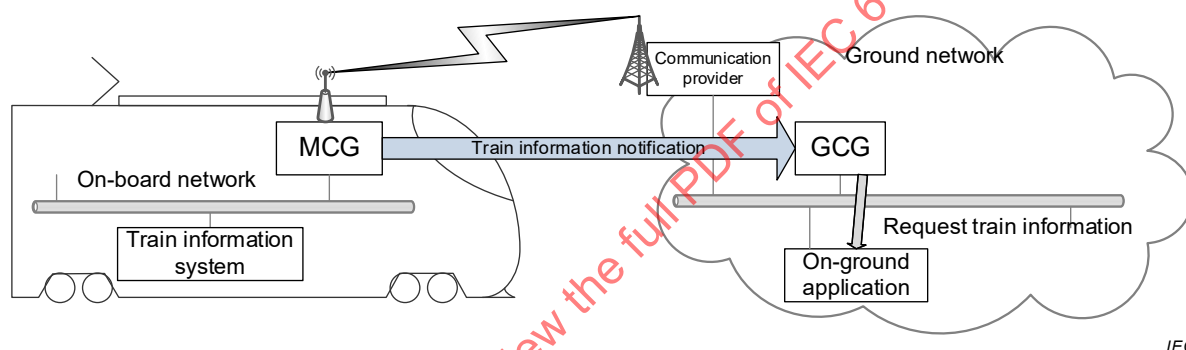


Figure 36 – Example architecture to notify about train information

The TIS gets its information from information sources in the train (e.g. the Train Topology Database of the ETB Control Services or the Node Address and Attribute Directory according to UIC leaflet 556). The actual procedure, how to obtain this information (for example according to IEC 61375-2-3) is not in the scope of this document.

6.3.3.2 Procedure to notify about train information

Figure 37 illustrates the procedure for the MCG TIS to inform the GCG TIS about the train information and a change of the train information.

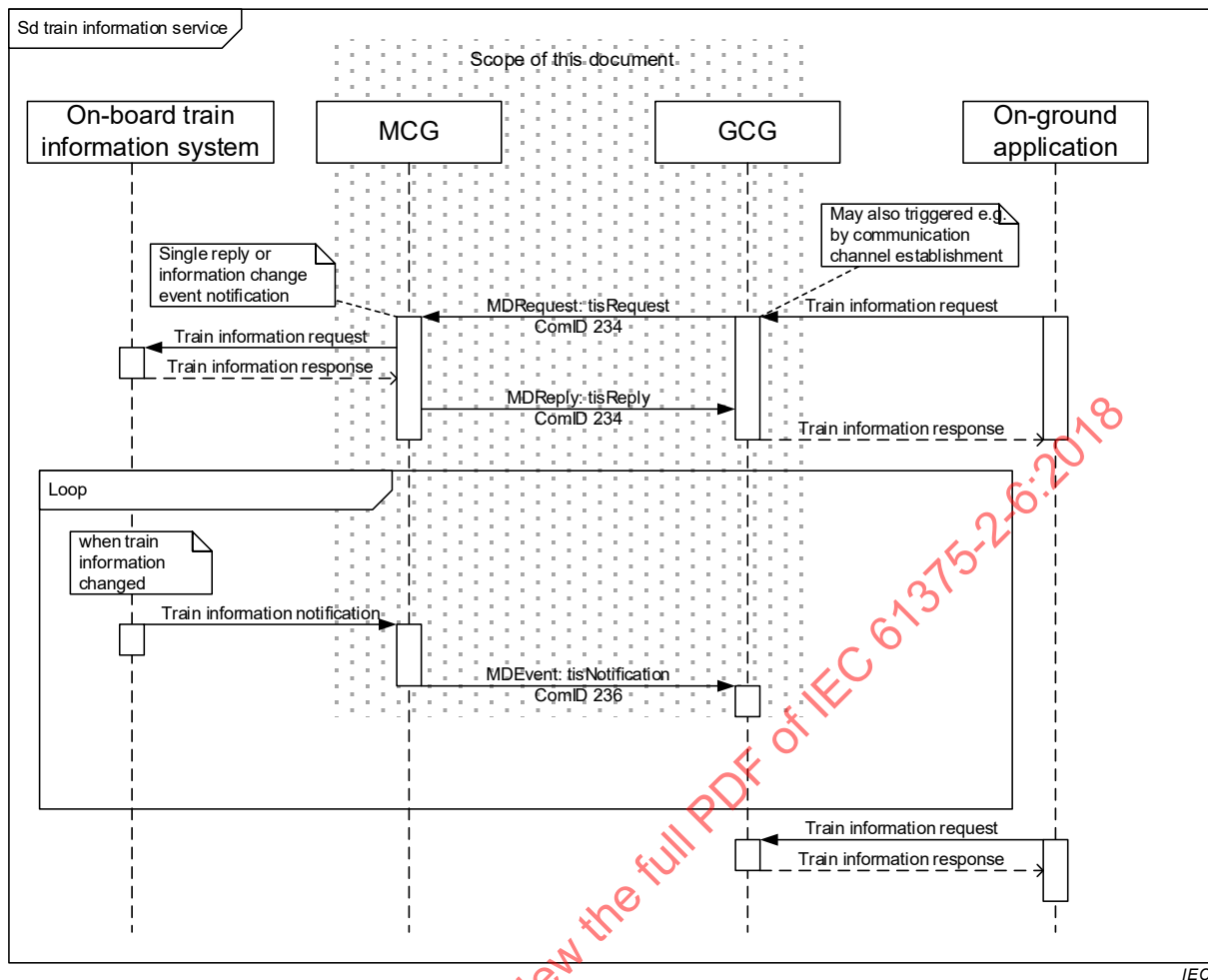


Figure 37 – Example procedure to notify about train information

The GCG shall request the train information from the MCG service TIS with the MD request ComID 234 *tisRequest*. The provisioning of information may be a single reply or by notification based on train information change.

The MCG retrieves the train topology information from the on-board train information system.

The MCG shall reply to the MD request ComID 234 with the MD reply ComID 234 *tisReply* to the GCG.

When the MCG receives the indication about a change of the train topology (for example coupling or change of driver's cab), then the MCG TIS notifies the GCG TIS with the MD event ComID 236 *tisNotification*, if the notification is enabled.

The GCG stores the received train topology information and provides it to ground applications. The on-ground interface and procedure to access the train topology information are not in the scope of this document.

6.3.3.3 Request train information (ComID 234)

The ComID 234 message is a MD telegram, which is sent from the GCG to the MCG. This message is used by the GCG to inquire about the train information.

The MD request telegram ComID 234 shall be sent with the following header parameters in accordance with Table 68. Refer to Table 18 for general information about the MD header parameters.

Table 68 – ComID 234: MD request header telegram values

Parameter	Value
msgType	3 (MD Request)
msgTimeValidity	0 (no timeout)
comID	234

The MD request telegram ComID 234 shall be sent with the following body parameters in accordance with Table 69. Refer to Table 19 for general information about the MD body parameters.

Table 69 – ComID 234: MD request body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 70

The MD request telegram ComID 234 shall be sent with the following payload object in accordance with Table 70.

Table 70 – ComID 234: MD request body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter "mdPayload"	JSON		
onChange	Enable/disable notification event on change train information change	number	uint8	0 = disable 1 = enable 2 = do not change other values reserved

The parameter onChange switches on or off the notifications about the train information in the case of change. With the parameter value 2 it is possible to request the train information from time to time without changing the enabled or disabled state of notification of a previous request.

6.3.3.4 Reply train information (ComID 234)

The ComID 234 message is a MD telegram, which is sent from the MCG to the GCG. This message is used by the MCG to reply to the GCG and indicate to the GCG the requested train information.

The MD response telegram ComID 234 shall be sent with the following header parameters in accordance with Table 71. Refer to Table 18 for general information about the MD header parameters.

Table 71 – ComID 234: MD reply header telegram values

Parameter	Value
msgType	4 (MD response to received MD request)
msgTimeValidity	0 (no timeout)
comID	234

The MD response telegram ComID 234 shall be sent with the following body parameters in accordance with Table 72. Refer to Table 19 for general information about the MD body parameters.

Table 72 – ComID 234: MD reply body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 73

The MD response telegram ComID 234 shall be sent with the following payload object in accordance with Table 73.

Table 73 – ComID 234: MD reply body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter "mdPayload"	JSON		
result	Result of the request	number	0 .. 255	0 = N/A 1 = Ok 2 = Internal error 255 = Error Other values reserved
backboneId	Identification of the backbone for which the train information is requested	number	0 .. 3	0 = ETB0 (operational network), or WTB 1 = ETB1 (multimedia network) 2 = ETB2 (other network) 3 = ETB3 (other network)
trnTopoCnt	Train topography counter	number	uint32	computed
opTrnTopoCnt	Operational train topography counter	number	uint32	computed
trnDirState	Confirmation status of operation train directory	number	1 .. 2	1 = UNCONFIRMED 2 = CONFIRMED
opTrnDirState	Operational train directory status	number	1 .. 4	1 = INVALID 2 = VALID 3 = reserved 4 = SHARED
opTrnOrient	Operational train orientation	number	0 .. 3	0 = unknown 1 = same as train direction 2 = inverse to train direction
trnJournId	Train journey ID	string	char[16]	"": no ID assigned "[a-z,A-Z,0-9]"
leadFlag	Flag for indication that sender is the leading consist	number	0 .. 1	0: not leading vehicle 1: leading vehicle
consistCnt	Amount of consist ID trailing (Consist IDs)	number	uint8	1..n: count of Consist IDs trailing 0: reserved
consistIDs	UIC IDs stored as array	array	char[16][]	e.g. ["UIC94806101123", "UIC61802791011"]

6.3.3.5 Train information notification message (ComID 236)

The TIS MD event telegram ComID 236 `tisNotification` shall be sent with the following header parameters in accordance with Table 74. Refer to Table 18 for general information about the MD header parameters.

Table 74 – ComID 236: MD header telegram values

Parameter	Value
msgType	1 (MDEvent-sporadic)
msgTimeValidity	0 (no timeout)
comId	236

The MD notification telegram ComID 236 shall be sent with the following body parameters in accordance with Table 75. Refer to Table 19 for general information about the MD body parameters.

Table 75 – ComID 236: MD Body telegram values

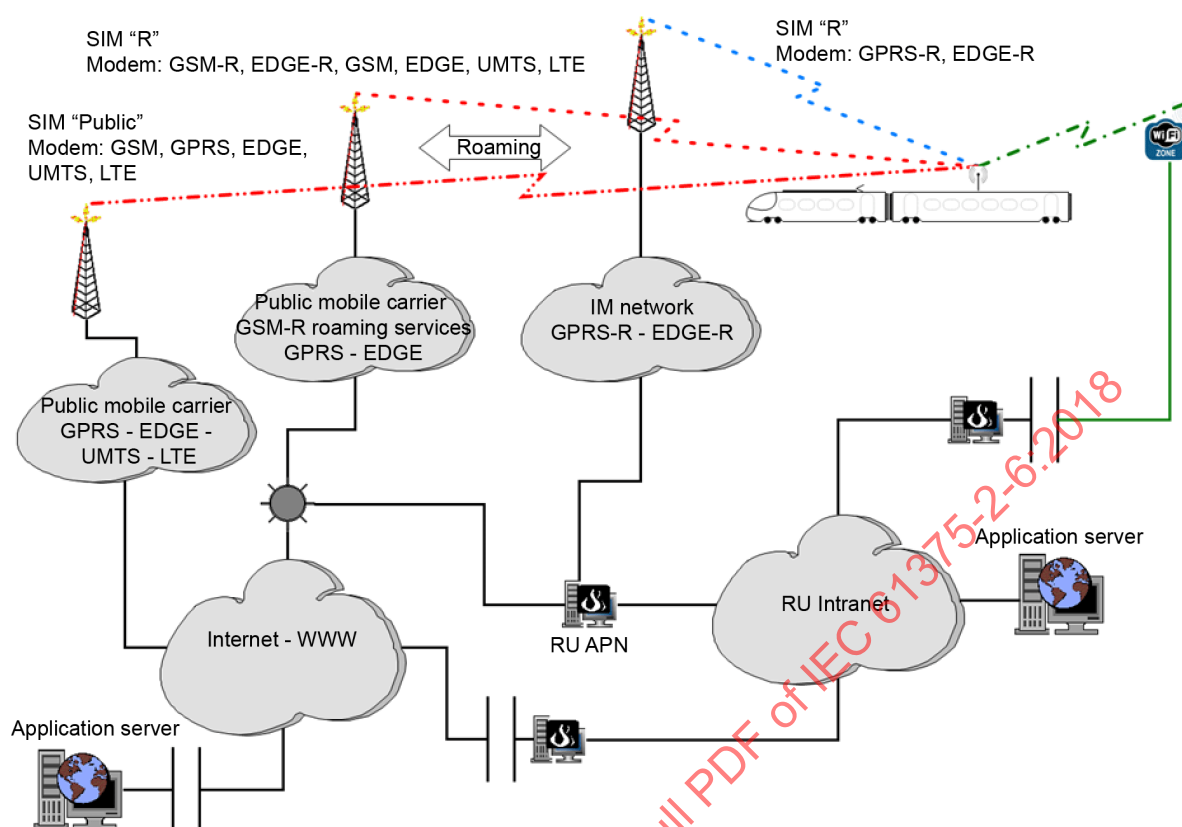
Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 73

The MD notification telegram ComID 236 shall be sent with the following payload object in accordance with Table 73.

6.3.4 MCG Network Selector Service

6.3.4.1 General

The MCG Network Selector Service (NSS) is applicable, when a MCG has more than one radio interface or to handle MCG redundancy. Network selection means the process to dynamically select an appropriate radio interface for the board-to-ground communication as illustrated in Figure 38. Typically, the radio selector is a protocol layer / entity located between the link layer (OSI layer 2) and the network layer (OSI layer 3). The selection of radio is based on link quality metric information, reported by the radio link layer to the network layer, and on the user policy in using radio bearers.



IEC

Figure 38 – Illustration of network selector

6.3.4.2 Radio selection

If the MCG provides more than one radio interface, the MCG Network Selection Service (NSS) shall support automatic radio selection by using suitable vertical handover technologies.

NOTE An example of vertical handover technologies is defined in IEEE 802.21.

The radio interface can be selected based on QoS parameters and cost criteria.

Related QoS parameters can be:

- a) Data rate provided (up-/downlink).
- b) Signal strength.

As both QoS and cost depend on the license contract between the MCG operator and the radio bearer, the MCG shall allow users to define a policy for the selection of radio interfaces. Examples for such a policy are:

- c) Using a specific radio interface for a specific communication services, e.g. a user who wants that video data transfer is only executed if WLAN access is available.
- d) Define that if a given access network provider charges users based on their traffic volume, then the radio selector should not consider the corresponding access when a high-bitrate service, such as CCTV streaming, is active.

The actual policy provided by the MCG is implementation specific and not in the scope of this document.

When a radio interface goes down (e.g. pre-detected by dramatic negative changes in the link characteristics) a seamless handover to another radio interface, in accordance with the agreed policy, should occur. Seamless here means that for instance existing TCP sessions will not be disrupted. In case of TCP, this means also lossless, because this is ensured by the transport protocol. In case of UDP a lossless service cannot be ensured by the transport protocol.

6.3.4.3 Radio selection control

The following operations shall be possible within the Network Selector Service:

- Request information about the network links: connection status, data rate, signal strength, cost.
- Set the details of the automatic selection criteria: preferred network link, minimum data rate, minimum signal strength.
- Force the MCG to use a specific network link, regardless of the automatic selection criteria.
- Release the MCG network link forcing.

6.3.5 Train telemetry service (Option)

6.3.5.1 General

The Train Telemetry Service (TTS) provides an interface to cyclically inform the GCG about the current state of process variables.

Figure 39 illustrates the architecture to provide the telemetry to an on-ground application.

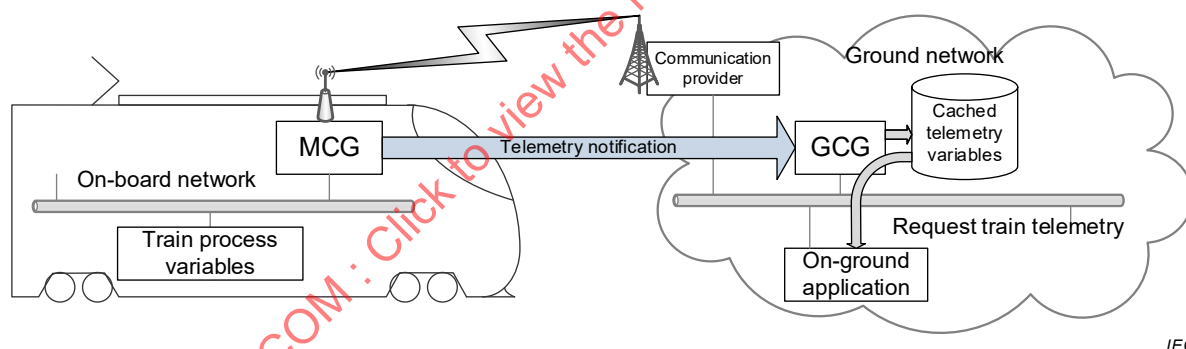


Figure 39 – Architecture to provide telemetry data

An on-ground application can request the telemetry data from the GCG. The GCG requests at the MCG the available process variables of the TTS. This registration can be triggered for example when the MCG establishes the communication channel or when an on-ground application requests information about the telemetry data. Then the GCG subscribes for telemetry notifications from the MCG.

The TTS of the MCG cyclically gets its information from the train process variables and sends it with a telemetry notification to the GCG.

The GCG caches the received telemetry data to decouple the provision to the on-ground application from the train to ground communication. The caching of the train location and the interface for the on-ground application are not in the scope of this document.

6.3.5.2 Procedure to notify about telemetry data

Figure 40 illustrates the procedure for the MCG to notify the GCG about the train telemetry data.

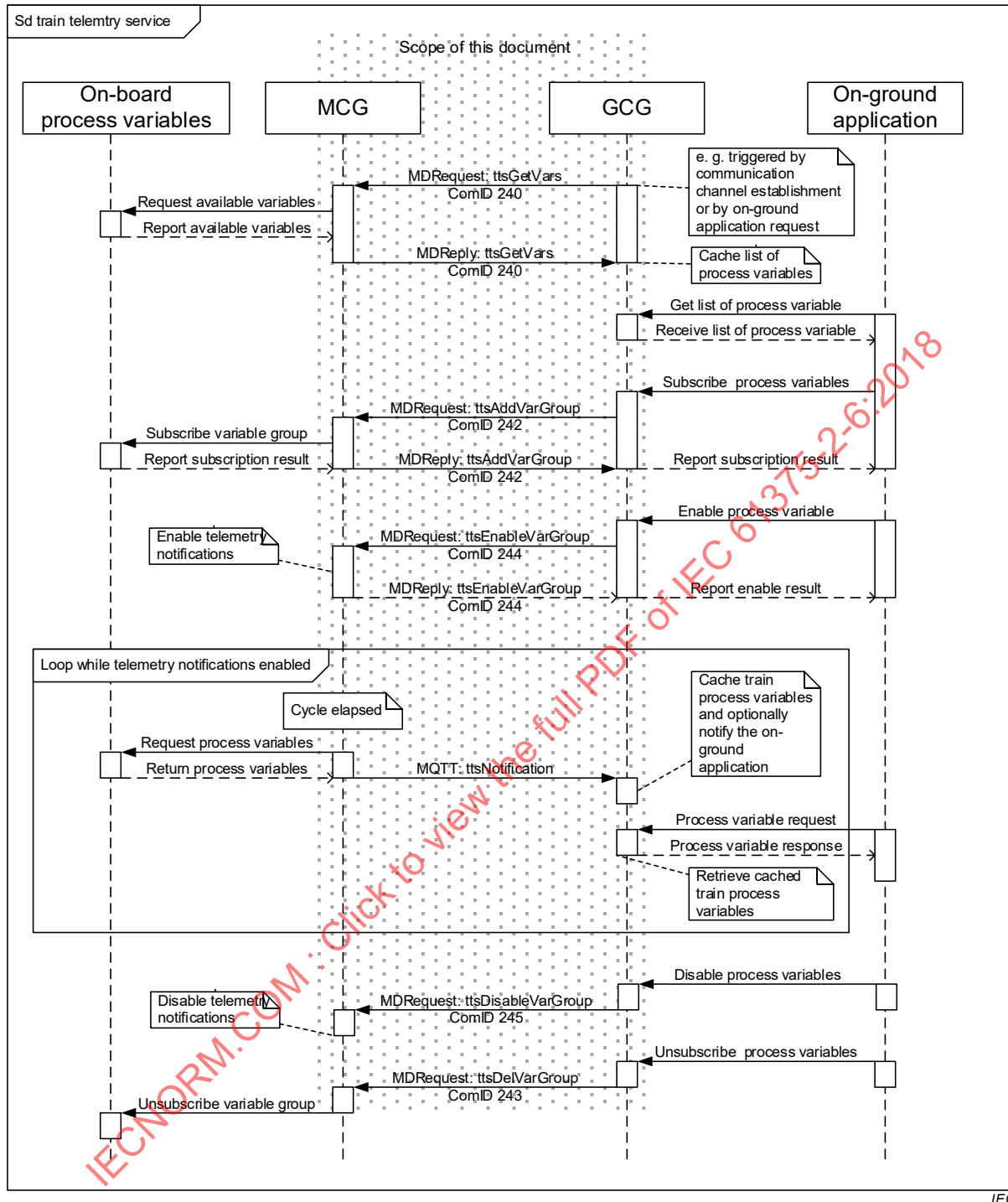


Figure 40 – Procedure to notify about current train location

The GCG shall request the list of available process variables of the train telemetry service TTS with the MD request ComID 240 ttsGetVars.

The MCG shall reply to the MD request ComID 240 with the MD reply 240 ttsGetVars to the GCG.

The GCG shall subscribe to the requested process variables of the train telemetry service TTS with the MD request ComID 242 ttsAddVarGroup. The MCG shall reply with the subscription success to the GCG with the MD reply ComID 242 ttsAddVarGroup.

The GCG shall enable the notification of to the requested process variables of the train telemetry service TTS with the MD request ComID 244 ttsEnableVarGroup.

When the train telemetry is enabled, then the MCG periodically acquires the train process variables and then the MCG shall send the MD event ComID 246 ttsNotification to the GCG. The actual procedure of obtaining the process variables is not in the scope of this document.

The GCG caches the received train telemetry data to decouple the provisioning to ground applications from the train to ground communication. The on-ground interface and procedure to access the train telemetry data are not in the scope of this document.

When the telemetry data is not longer required, the GCG shall disable or unsubscribe from the MCG TTS with the MD request ComID 245 ttsDisableVarGroup or with the MD request ComID 243 ttsDelVarGroup.

The behaviour of the TTS on the GCG in case of loss of communication to the MCG is not in the scope of this document. But it is recommended, that the GCG will inform the on-ground application about the quality of the telemetry data, for example by a time stamp of the last received telemetry data.

The trigger for disabling the TTS or unsubscribing the TTS from the GCG is not in the scope of this document.

6.3.5.3 Request list of available process variables (ComID 240)

The ComID 240 message is a MD telegram, which is sent from the GCG to the MCG. This message is used by the GCG to inquire about the list of available process variables.

The MD request telegram ComID 240 shall be sent with the following header parameters in accordance with Table 76. Refer to Table 18 for general information about the MD header parameters.

Table 76 – ComID 240: MD request header telegram values

Parameter	Value
msgType	3 (MD Request)
msgTimeValidity	0 (no timeout)
comID	240

The MD request telegram ComID 240 shall be sent with the following body parameters in accordance with Table 77. Refer to Table 19 for general information about the MD body parameters.

Table 77 – ComID 240: MD request Body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	none

The MD reply telegram ComID 240 shall be sent with the following header parameters in accordance with Table 78. Refer to Table 18 for general information about the MD header parameters.

Table 78 – ComID 240: MD reply header telegram values

Parameter	Value
msgType	3 (MD Reply)
msgTimeValidity	0 (no timeout)
comID	240

The MD reply telegram ComID 240 shall be sent with the following body parameters in accordance with Table 79. Refer to Table 19 for general information about the MD body parameters.

Table 79 – ComID 240: MD reply body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 80

The MD reply telegram ComID 240 shall be sent with the following payload object in accordance with Table 80.

Table 80 – ComID 240: MD reply body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter "mdPayload"	JSON		
varList	List of variables to be monitored			JSON array of elements
vars				
varId	Variable Id	string	char *	computed
varType	Variable type	number	0 .. 255	computed 0 = N/A 1 = BOOL8 2 = CHAR8 3 = UTF16 4 = INT8 5 = INT16 6 = INT32 7 = INT64 8 = UINT8 9 = UINT16 10 = UINT32 11 = UINT64 12 = REAL32 13 = REAL64 14 = TIMEDATE32 15 = TIMEDATE48 16 = TIMEDATE 64 17 = BITSET8 18 = ANTIVALENT8 other values reserved
varLength	Number of elements of a variable (to support arrays)	number	uint16	computed

EXAMPLE: JSON notation for a ComID 240 MD reply:

```
{
  "varsList": [
    {
      "varId": "varID0",
      "varType": 2,
      "varLength": 5
    },
    {
      "varId": "varID1",
      "varType": 1
    },
    {
      "varId": "varID2",
      "varType": 10,
      "varLength": 8
    }
  ]
}
```

6.3.5.4 Subscribe process variables (ComID 242)

The ComID 242 message is a MD telegram, which is sent from the GCG to the MCG. This message is used by the GCG to subscribe a group of process variables for notification.

The MD request telegram ComID 242 shall be sent with the following header parameters in accordance with Table 81. Refer to Table 18 for general information about the MD header parameters.

Table 81 – ComID 242: MD request header telegram values

Parameter	Value
msgType	3 (MD Request)
msgTimeValidity	0 (no timeout)
comID	242

The MD request telegram ComID 242 shall be sent with the following body parameters in accordance with Table 82. Refer to Table 19 for general information about the MD body parameters.

Table 82 – ComID 242: MD request Body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 83

The MD request telegram ComID 242 shall be sent with the following payload object in accordance with Table 83.

Table 83 – ComID 242: MD request body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter “mdPayload”	JSON		
groupTopic	Topic assigned for current group of variables	string	char *	Computed
qos	QoS to be used on notifications publications	number	uint8	0 = QoS 0 (default) 1 = QoS 1 2 = QoS 2 Other values reserved
monFreq	Monitoring frequency	number	uint32	In milliseconds
buffSize	Size of the buffer to be used in connection cuts	number	uint16	Number of notifications
varsList	List with the IDs of variables to be monitored	number	uint8 *	Computed

The parameter qos is optional and, if not provided by the GCG, the telemetry system of the MCG shall use a default value. The MQTT retain flag shall always be set to false since it is considered that a notification with changes from previous notifications does not have enough information to be retained for new subscribers to receive it.

The parameter buffSize sets the size of the buffer to be used in order to temporarily cache notifications generated during connection interruptions between MCG and GCG.

EXAMPLE: JSON notation for a ComID 242 MD request:

```
{
  "groupTopic": "group_a",
  "qos": 0,
  "monFreq": 1000,
  "varsList": ["varID0", "varID1", "varID9", "varID12"]
}
```

The MD reply telegram ComID 242 shall be sent with the following header parameters in accordance with Table 84. Refer to Table 18 for general information about the MD header parameters.

Table 84 – ComID 242: MD reply header telegram values

Parameter	Value
msgType	4 (MD Reply)
msgTimeValidity	0 (no timeout)
comID	242

The MD reply telegram ComID 242 shall be sent with the following body parameters in accordance with Table 85. Refer to Table 19 for general information about the MD body parameters.

Table 85 – ComID 242: MD reply body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 86

The MD request telegram ComID 242 shall be sent with the following payload object in accordance with Table 86.

Table 86 – ComID 242: MD reply body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter "mdPayload"	JSON		
result	Result of group creation process	number	0 .. 255	0 = N/A 1 = Group already exists 2 = Error on variable list 3 = Error on buffer size 255 = Error Other values reserved
resultList	List of results for each variable. Only present if result equal to 2	number	0 .. 255	0 = N/A 1 = OK 2 = Unknown variable 3 = Bad monitoring freq. 255 = Error Other values reserved

The parameter resultList shall only be present in case of error associated to a single variables (result with value 2) and it shall maintain the variables order provided in the request by the GCG, so that each element of the list can be linked with a variable.

Any error in result or in resultList shall imply that the group of variables is not created in the MCG telemetry service. The handling of reported errors is not in the scope of this document.

EXAMPLE 1: JSON notation for a ComID 242 MD reply in case of success:

```
{
  "result": 0
}
```

EXAMPLE 2: JSON notation for a ComID 242 MD reply in case of failure:

```
{
  "result": 2,
  "resultList": [1, 1, 1, 2, 1, 1, 3, 1, 1, 1]
}
```

6.3.5.5 Unsubscribe process variables (ComID 243)

The ComID 243 message is a MD telegram, which is sent from the GCG to the MCG. This message is used by the GCG to unsubscribe a group of process variables for notification.

The MD request telegram ComID 243 shall be sent with the following header parameters in accordance with Table 87. Refer to Table 18 for general information about the MD header parameters.

Table 87 – ComID 243: MD request header telegram values

Parameter	Value
msgType	3 (MD Request)
msgTimeValidity	0 (no timeout)
comID	243

The MD request telegram ComID 243 shall be sent with the following body parameters in accordance with Table 88. Refer to Table 19 for general information about the MD body parameters.

Table 88 – ComID 243: MD request Body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 89

The MD request telegram ComID 243 shall be sent with the following payload object in accordance with Table 89.

Table 89 – ComID 243: MD request body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter "mdPayload"	JSON		
groupTopic	Topic assigned for current group of variables	string	char *	Computed

The ComID 243 message does not have a response message since the timeout mechanism allows to delete automatically monitoring groups of process variables in case of errors.

6.3.5.6 Enable process variables (ComID 244)

The ComID 244 message is a MD telegram, which is sent from the GCG to the MCG. This message is used by the GCG to enable a group of process variables for notification.

This message can also be used to ask the MCG to refresh an already enabled group of process variables to allow subscribers (that are not the first) getting values of all variables.

The MD request telegram ComID 244 shall be sent with the following header parameters in accordance with Table 90. Refer to Table 18 for general information about the MD header parameters.

Table 90 – ComID 244: MD request header telegram values

Parameter	Value
msgType	3 (MD Request)
msgTimeValidity	0 (no timeout)
comID	244

The MD request telegram ComID 244 shall be sent with the following body parameters in accordance with Table 91. Refer to Table 19 for general information about the MD body parameters.

Table 91 – ComID 244: MD request Body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 92

The MD request telegram ComID 244 shall be sent with the following payload object in accordance with Table 92.

Table 92 – ComID 244: MD request body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter "mdPayload"	JSON		
groupTopic	Topic assigned for current group of variables	string	char *	Computed

The MD reply telegram ComID 244 shall be sent with the following header parameters in accordance with Table 93. Refer to Table 18 for general information about the MD header parameters.

Table 93 – ComID 244: MD reply header telegram values

Parameter	Value
msgType	4 (MD Reply)
msgTimeValidity	0 (no timeout)
comID	244

The MD reply telegram ComID 244 shall be sent with the following body parameters in accordance with Table 94. Refer to Table 19 for general information about the MD body parameters.

Table 94 – ComID 244: MD reply body telegram values

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 95

The MD request telegram ComID 244 shall be sent with the following payload object in accordance with Table 95.

Table 95 – ComID 244: MD reply body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter “mdPayload”	JSON		
result	Result of group activation process	number	0 .. 255	0 = N/A 1 = OK 2 = Already enabled 3 = Unknown group 4 = Not enough resources 255 = Error Other values not used

6.3.5.7 Disable process variables (ComID 245)

The ComID 245 message is a MD telegram, which is sent from the GCG to the MCG. This message is used by the GCG to disable a group of process variables for notification.

The MD request telegram ComID 245 shall be sent with the following header parameters in accordance with Table 96. Refer to Table 18 for general information about the MD header parameters.

Table 96 – ComID 245: MD request header telegram values

Parameter	Value
msgType	3 (MD Request)
msgTimeValidity	0 (no timeout)
comID	245

The MD request telegram ComID 245 shall be sent with the following body parameters in accordance with Table 97. Refer to Table 19 for general information about the MD body parameters.

Table 97 – ComID 245: MD request Body telegram values

Parameter	Value
mdPayloadType	“JSON”
mdPayload	see Table 98

The MD request telegram ComID 245 shall be sent with the following payload object in accordance with Table 98.

Table 98 – ComID 245: MD request body: mdPayload object

Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter “mdPayload”	JSON		
groupTopic	Topic assigned for current group of variables	string	char *	Computed

6.3.5.8 Telemetry notification message

The MCG shall transfer the telemetry data with the MQTT protocol and the GCG shall receive the telemetry data with the MQTT protocol.

The telemetry data coding and ordering shall conform to Annex B.

6.3.6 MCG Train Wake-up Service (Option)

6.3.6.1 General

The MCG Train Wake-up Service (TWS) shall provide an interface for the train equipment to power-up the equipment from energy saving mode.

The MCG TWS shall be active in energy saving mode.

Figure 41 illustrates the procedure for a ground application to remotely wake up the train.

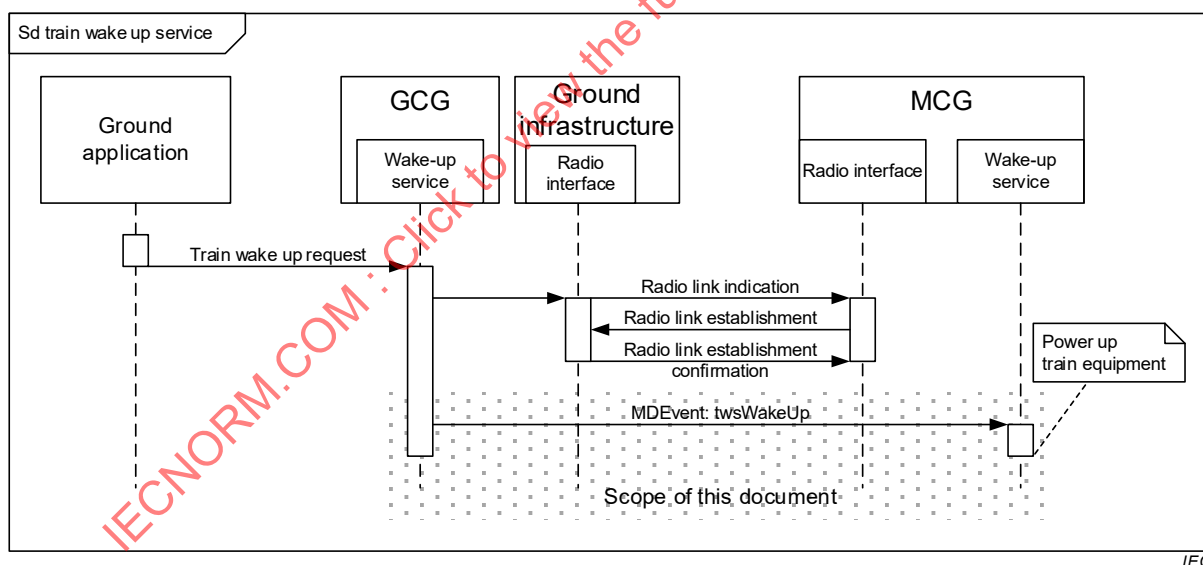


Figure 41 – Example Procedure to wake up the train

The ground application requests from the GCG TWS to wake up the train. The GCG initiates with the support of the ground infrastructure a radio link establishment from the MCG. When the radio link is set up, the GCG sends the MD event telegram `twsWakeUp` to the MCG. The MCG TWS actually wakes up the train equipment.

6.3.6.2 Train Wake-up Service event message

The TWS MD event telegram ComId 238 `twsWakeUp` shall be sent with the following header parameters in accordance with Table 99. Refer to Table 18 for general information about the MD header parameters.

Table 99 – ComID 238: twsWakeUp MD event header

Parameter	Value
msgType	1 (MDEvent-sporadic)
msgTimeValidity	0 (no timeout)
comId	238

The body parameters of the MD event telegram ComID 238 `twsWakeUp` shall be in accordance with Table 100:

Table 100 – ComID 238: twsWakeUp MD event body

Parameter	Value
mdPayloadType	"JSON"
mdPayload	see Table 101

The MD request telegram ComID 238 shall be sent with the following payload object in accordance with Table 101.

Table 101 – ComID 238: twsWakeUp MD event body: mdPayload object

Parameter	Description	type	Value
mdPayloadType			"JSON"
mdPayload			
magic	Magic number to reduce to probability to inadvertently wake up the train	number	'57616B65'H

7 Services and interfaces (GCG)

7.1 GCG Overview

A train fleet is comprised of a group of consists managed by the same operator. Generally all consists of a fleet have the same type or profile (fleet of locomotives, fleet of regional trains, fleet of high speed trains, etc.). The same operator can manage many fleets.

For each train fleet, a Ground Communication Gateway (GCG) is defined and initiated to manage fleet train to ground communication.

From ground side, this GCG is used as an IP gateway to speak with any consists (including a Mobile Communication Gateway, MCG) of the fleet.

GCG has two IP interfaces:

- Wireless GCG interface: exported by GCG this interface is used by MCG to call ground communication services (train authentication, train declaration, etc.)
- Ground GCG interface: with ground applications. This interface is used by ground applications to know train availability, communications status, etc.

To give access for a partner to train data, fleet owner should put in place a Partner Communication Gateway (PCG). This gateway exports a fleet public interface over Internet.

The following Figure 42 shows a synthetic view of these components and interfaces.

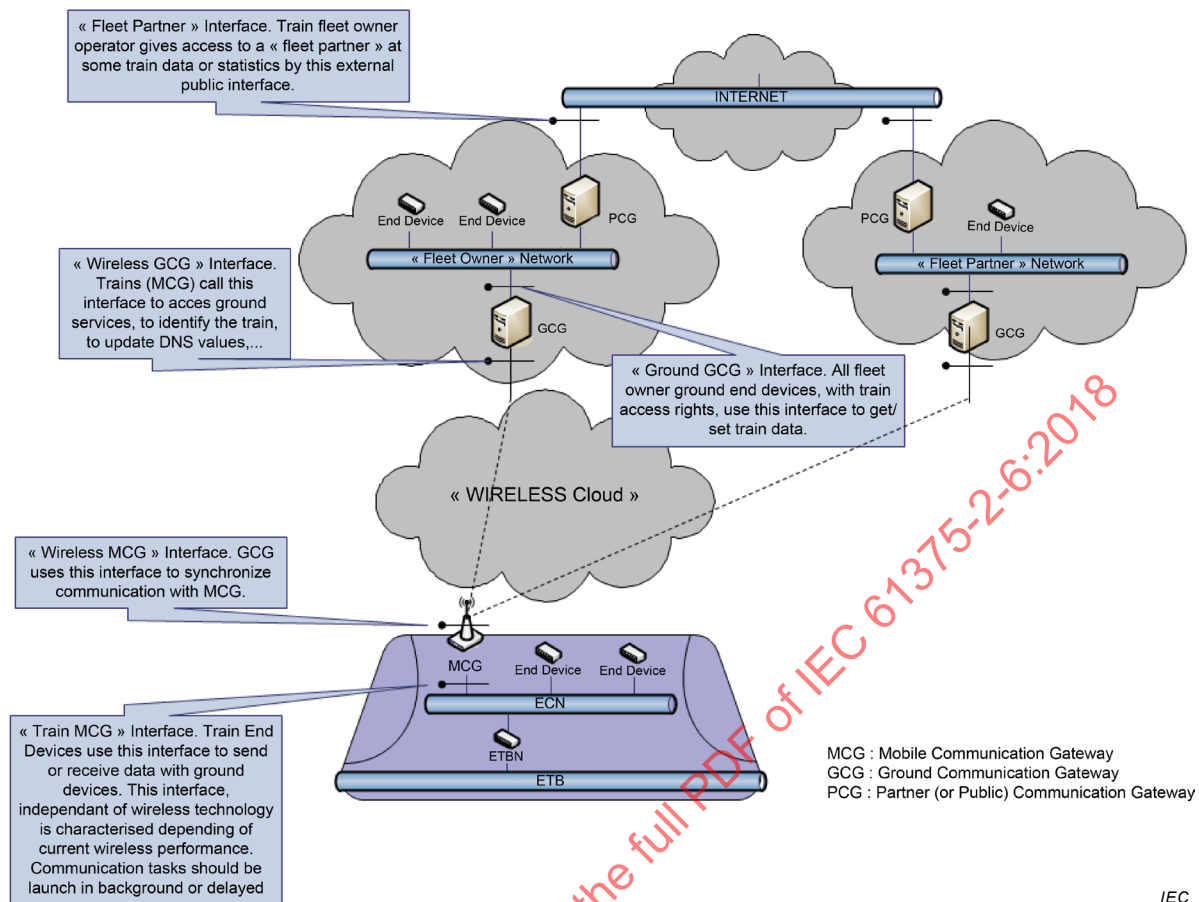


Figure 42 – Train to Ground interfaces

Home GCG:

As each consist is attached to a fleet, each MCG is attached to a specific Ground Communication Gateway (GCG). This particular GCG is named “Home GCG”.

All MCGs have a “Home GCG” and are able to join it by IP.

For a train, many MCGs should be available (one per consist for example). These MCGs use the same “Home GCG” at the same time.

MCG mode 1 is only able to exchange data with its “Home GCG”.

Foreign GCG:

By definition MCGs mode 2, are able to use many available GCG.

Foreign GCG are used to locally manage a train by a fleet owner partner. The list of Ground services offered by a Foreign GCG should be a subset of the list offered by the Home GCG (i.e. not all services should be implemented). For example, Foreign GCG should be used by an operator partner to see camera live video streaming from the train inside its railway stations locally covered by Wi-Fi.

Foreign GCG should also be used by the MCG to join its Home GCG.

Foreign GCG FQDNs are acquired dynamically by MCG from its Home GCG.

7.2 GCG Addressing

7.2.1 Wireless MCG Interface

7.2.1.1 General

From MCG, GCGs (Home or Foreign) shall be accessible via IP (currently using an IPv4 address).

7.2.1.2 Home GCG IP address

As “Home GCG” is unique for a fleet and not used by other trains outside the fleet (i.e. without interoperability constraint), “Home GCG” IP address should be set directly inside the MCG (by configuration or hard coded).

To avoid setting IP address inside MCG, GCG IP should be acquired by DNS resolution from a DNS server on ground side.

As “Home GCG” name is local and private, “Home GCG” name should be set by each train fleet owner without a specific rule.

“Home GCG” name should be set by configuration inside MCG.

7.2.1.3 Foreign GCG address

“Foreign GCG” IP address shall always be acquired by DNS resolution from a DNS server on ground side.

MCG shall acquire “Foreign GCG” URL name list from its “Home GCG” using a specific service (see 7.4.3.2). This list should be recorded inside MCG when “Home GCG” is unavailable.

“Foreign GCG” should be used:

- When “Home GCG” is not available, all “Foreign GCGs” should be called up one by one to find a connection.
- Or when Train application asks MCG mode 2 to use a dedicated “Foreign GCG”

7.2.2 Ground GCG Interface

7.2.2.1 General

For any ground application servers GCG (Home or Foreign) shall be available via IP.

7.2.2.2 Home GCG IP address

As “Home GCG” name is local and private to fleet owner network, “Home GCG” name should be set by fleet owner without specific rule.

7.2.2.3 Foreign GCG IP address

Foreign GCG names shall be resolved inside Internet using a DNS resolution.

As this interface shall be used by fleet partners, a specific and standard public domain definition shall be set and advertised over Internet.

7.3 GCG Implementation

7.3.1 General (informative)

GCG can be implemented on a specific machine, but GCG can be implemented as virtual machine inside a cluster of servers.

NOTE GCG is mainly defined by its IP interfaces and services.

7.3.2 GCG Availability

GCG shall provide the necessary service level to ensure availability.

GCG should be available all the time (24 h a day).

Cold (with a backup offline GCG), warm (with periodic replications on a backup GCG) or hot (with fine synchronization between master and backup GCG) redundancy can be used.

Active redundancy using virtual IP redundancy mechanism can also be used.

GCG redundancy shall be transparent for MCG.

7.3.3 GCG Workload

GCG shall provide mechanisms to manage the workload.

To accept many consists, a fleet can be split into many smaller fleets and so with many GCG instances. GCG workload can also be split between many virtual machines using workload balancing mechanism.

GCG workload shall be transparent for MCG.

7.3.4 GCG Security

GCG shall provide mechanisms to manage the security.

The fleet owner shall be responsible for the security of its GCG implementations. As any ground machine, security updates and patches should be monitored periodically.

GCG should be insulated by firewall where IP flows should be recorded, analysed and filtered.

7.4 GCG services

7.4.1 GCG services protocol

All GCG services called by MCG shall be available using HTTP protocol (see Clause 5).

NOTE This enables easy routing when using IP, NAT and firewalls.

7.4.2 GCG Fleet Database

GCG shall record train connectivity: which train is connected, by which wireless link. GCG should record and manage train description:

- Train Identification
- Train Composition (topology, number of consists, number of cars, etc.)
- Train Services Directory (services list exposed by the train)

MCG should send Train Database to ground side.

GCG should record and manage train geo-localization.

Home GCG shall record Foreign GCG names.

7.4.3 MCG-GCG services

7.4.3.1 GCG Communication service

The GCG communication service shall be used by any MCG to announce the train to ground.

This GCG communication service shall be available on any GCG (Home and Foreign).

The GCG communication shall be the first service called by MCG just after keeping a wireless IP address.

The GCG communication service shall be used to manage train authentication and authorization.

The GCG communication should also be used to manage wireless connection status:

- A connection session should be managed between MCG and GCG. This session should be cut, based on a communication timeout criterion.
- A periodic call by MCG should take place to keep alive the session. This periodic call should include:
 - Geo-localization of the train (optionally)
 - Wireless connection quality: average round trip delay for example

GCG communication service should be used also to upload the train description to ground. This train description should be used to update ground DNS and address the train.

The GCG communication service shall be used by MCG to download “Foreign GCG” name list.

See 6.3.1 for details.

7.4.3.2 Train Location service

This service is called by MCG to advise train geo-localization. See 6.3.2 for details.

7.4.3.3 Train Information service

This service is called by MCG to advise train composition and description. See 6.3.3 for details.

7.4.4 File transfer communication service

This service shared with MCG, helps to transfer files between ground and train. See 5.6.3 for details.

7.4.5 Local Ground GCG Interface

7.4.5.1 General

Ground interfaces are out of scope of this document, but the following descriptions could help to understand MCG-GCG interface usage.

By default the GCG services are available from local ground fleet network. By opposite Public Services are available also from Internet.

Only services exported by the Partner Communication Gateway (PCG) Internet interface are public (see 7.4.6).

7.4.5.2 Fleet Status service

The Fleet Status service is used to advertise train communication status.

For example, train connected/not connected status, wireless link quality, etc.

The Train status can be extracted from GCG database (see 7.4.2).

7.4.5.3 Train Localization service

The Train Localization service can be used to manage train geo-localization.

The train geo-localization can be extracted from GCG database (see 7.4.2).

7.4.5.4 Train File Transfer service

The Train File Transfer service can be a basic service used to transfer files from ground to train and train to ground.

The Train File Transfer service can move any types of file.

File transfers can be linked with date/time and/or wireless link quality.

7.4.5.5 Train Events service

The Train Events service can be used to get train recorded events data.

In an example, UIC 559 leaflet specifies the XML format for Diagnostic Data.

7.4.6 Home GCG – Foreign GCG services

The interface between GCG (Home and Foreign) can be used

- to manage authentication during train identification on “Foreign GCG”;
- to synchronize train geo-localization.

7.4.7 Public Ground GCG services

The public interface of GCG (also called PCG) can be used by any partner organization to access from Internet some train data: geo-localization for example, UIC 559 events files, etc.

Annex A (normative)

Message presentation

A.1 General

This annex defines the JSON representation of message data telegrams which are defined in this document for the message data exchange between MCG and GCG.

A.2 Transmission rules

JSON (JavaScript Object Notation) is a lightweight data-interchange format and is specified in RFC 7159.

A.3 Generic message

```
{
  "MDHeader":
  {
    "protocolVersion": 16,
    "msgType":         number,
    "comID":            number,
    "msgTimestamp":     number,
    "msgTimeValidity": number,
    "mcgFQDN":          string,
  },
  "MDBody":
  {
    "mdPayloadType": string,
    "mdPayload":     specific
  },
  "mdFCS":           number
}
```

Annex B (normative)

Telemetry data coding and ordering

B.1 General

Notifications of multiple process variables shall travel within a single MQTT message's payload. Moreover, and with the purpose of reducing the overhead introduced by different layers, only the value of those process variables of the group whose value or quality had changed shall be sent in the message, so a data coding and ordering algorithm needs to be defined.

B.2 MQTT payload coding

The MQTT message payload shall conform to the format as depicted in Figure B.1.

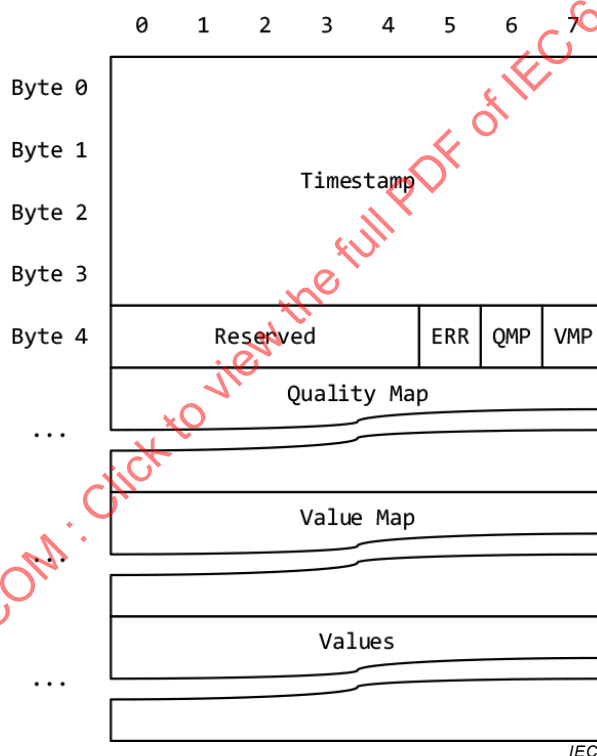


Figure B.1 – MQTT notification payload format

Where:

- **Timestamp:** Timestamp of the notification in seconds from epoch.
- **Flags:** Set of flags.
 - **Reserved:** Reserved bits for future use.
 - **ERR:** If this flag is set no extra fields shall be present in the frame. It indicates that error has occurred in the subscription.
 - **QMP:** Quality Map Present flag that indicates if Quality Map field is present. If set to 0 it indicates that the quality of the variables has not changed since the last notification.
 - **VMP:** Value Map Present flag that indicates if Value Map field is present. If set to 0 it indicates the values of all monitored elements are included in "Values" field.

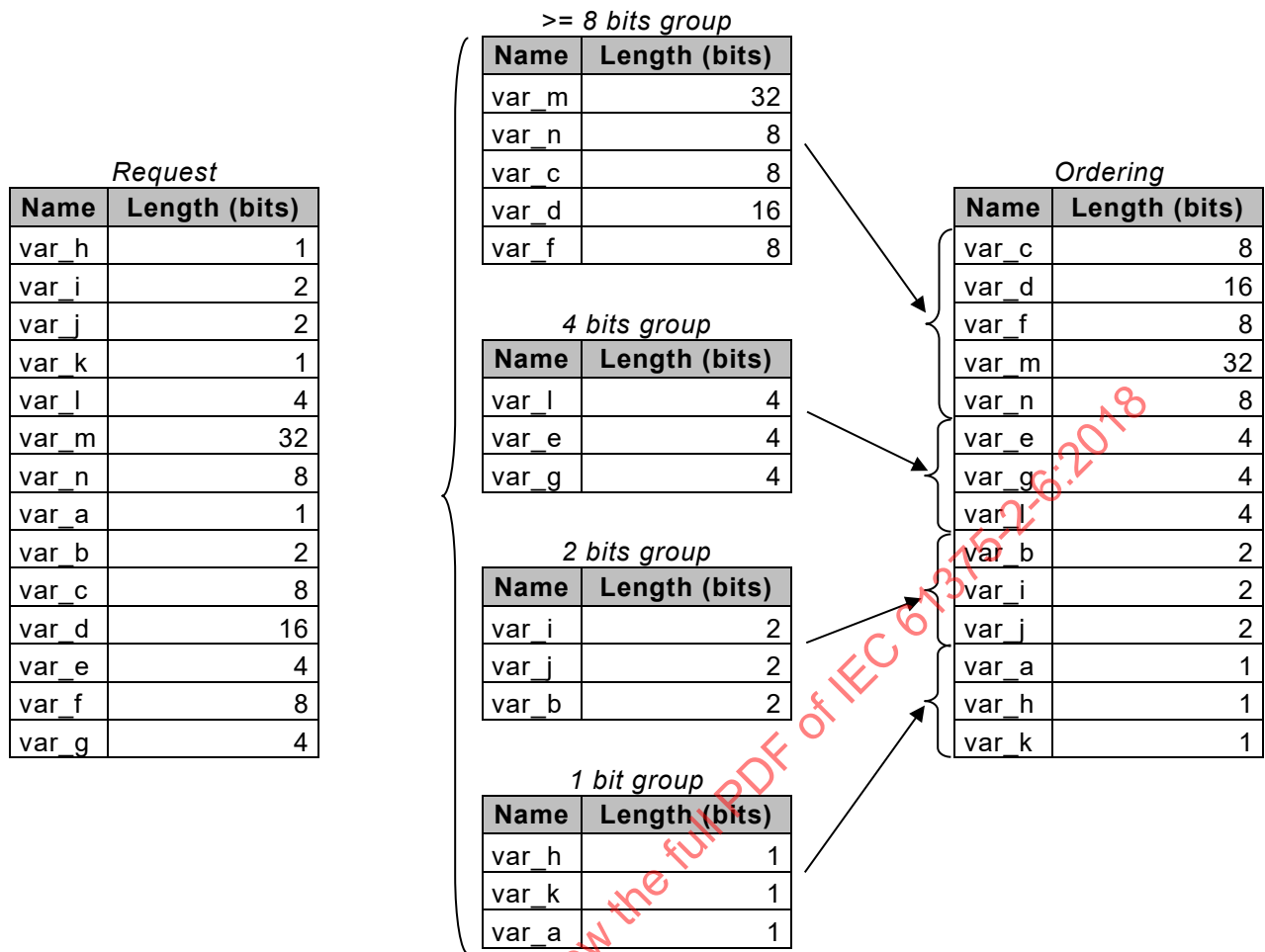
- Quality Map:** Bit map in which each bit indicates the quality of each variable of the group. If the bit representing a variable is set to 0 it indicates that the quality of the variable is incorrect while if the bit is set to 1 it indicates that the quality of the same variable is correct. Not used bits of the last byte are set to 0.
 The length of this field is dependent of the number of variables monitored within the same group. If N variables are monitored, the length shall be:
 $(N-1)/8+1$ bytes
 To decode this field it is mandatory that both ends of the communication use the same ordering criterion (see Clause B.3).
- Value Map:** Bit map in which each bit indicates if the value of the variable it represents is present in the Values field. If the bit representing a variable is set to 0 it indicates that the value of the variable is not present in the Values field while if the bit is set to 1 it indicates that the value of the same variable is present. Not used bits of the last byte are set to 0.
 The length of this field is dependent of the number of variables monitored within the same group. If N variables are monitored, the length shall be:
 $(N-1)/8+1$ bytes
 To decode this field it is mandatory that both ends of the communication use the same ordering criterion (see Clause B.3).
- Values:** Values of those variables for which their bit in Value Map field is set to 1. To decode this field it is mandatory that both ends of the communication use the same ordering criterion (see Clause B.3) and also to know the type (length) of each variable.

B.3 Variables grouping and ordering criterion

The ordering mechanism shall follow the rules below:

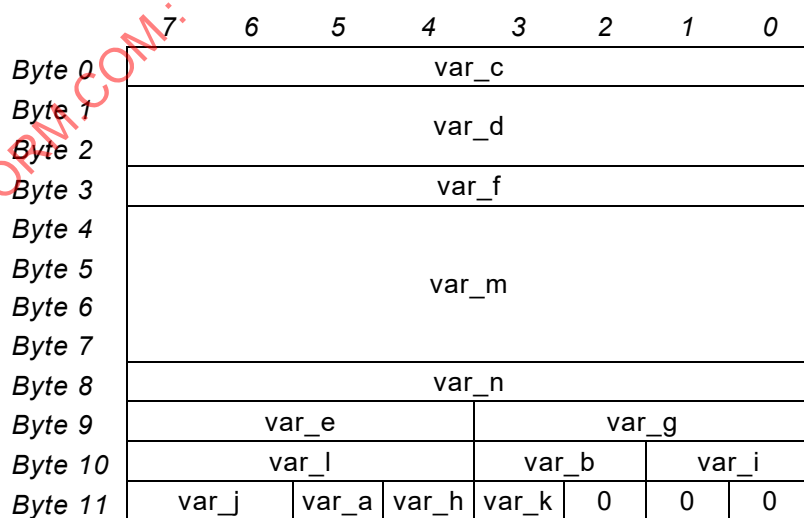
- Group variables by types following the order below:
 - Variables of 1 byte length or bigger (multiple of 1 byte)
 - Variables of 4 bits length.
 - Variables of 2 bits length.
 - Variables of 1 bit length.
- Within each group of types, alphabetical order shall be applied.
- All information travels following Big Endian fashion.

EXAMPLE Figure B.2 and Figure B.3 show the application of this ordering criterion.



IEC

Figure B.2 – Example of ordering criteria



IEC

Figure B.3 – Example of values grouping

EXAMPLE (continued): As shown in Figure B.3, this way of ordering variables will allow grouping their values minimizing the length of the field Values.

Supposing the following parameter “Values” arrives to a subscriber (in hexadecimal format where the less significant bit is at the right and the most significant at the left):

1A 2B CF 56 8C 14 4E 86 98 5F F5 98

The way of obtain the values of each variable (according with Figure B.3) is depicted in Table B.1.

Table B.1 – Example of values decoding

Variable	Bytes	Mask (AND)	Result (binary)
var_c	0	None	0001 1010
var_d	1 + 2	None	0010 1011 1100 1111
var_f	3	None	0101 0110
var_m	4 + 5 + 6 + 7	None	1000 1100 0001 0100 0100 1110 1000 0110
var_n	8	None	1001 1000
var_e	9	0xF0	0101
var_g	9	0x0F	1111
var_l	10	0xF0	1111
var_b	10	0x0C	01
var_i	10	0x03	01
var_j	11	0xC0	10
var_a	11	0x20	0
var_h	11	0x10	1
var_k	11	0x80	1

IECNORM.COM : Click to view the full PDF of IEC 61375-2-6:2018

Bibliography

IEC 62888-1, *Railway applications – Energy measurement on board trains – Part 1: General*

IEC 62888-2, *Railway applications – Energy measurement on board trains – Part 2: Energy measuring*

IEC 62888-3, *Railway applications – Energy measurement on board trains – Part 3: Data handling*

IEC 62888-4, *Railway applications – Energy measurement on board trains – Part 4: Communication*

ISO/IEC 7498 (all parts), *Information Technology – Open Systems Interconnection – Basic Reference Model*

EN 50463-1, *Railway applications – Energy measurement on board trains – Part 1: General*

EN 50463-2, *Railway applications – Energy measurement on board trains – Part 2: Energy measuring*

EN 50463-3, *Railway applications – Energy measurement on board trains – Part 3: Data handling*

EN 50463-4, *Railway applications – Energy measurement on board trains – Part 4: Communication*

DIN VDE V 0831-104, *Electric signalling systems for railways – Part 104: IT Security Guideline based on IEC 62443*

UIC 556, *Information transmission in the train (train-bus)*

UIC 559, *Diagnostic data transmission from railway vehicles*

Java Authentication and Authorization Service (JAAS) Reference Guide

<https://docs.oracle.com/javase/8/docs/technotes/guides/security/jaas/JAASRefGuide.html>

IECNORM.COM : Click to view the full PDF of IEC 61375-2-6:2018

SOMMAIRE

AVANT-PROPOS	125
INTRODUCTION.....	127
1 Domaine d'application	128
2 Références normatives	128
3 Termes, définitions, symboles, termes abrégés et conventions	129
3.1 Termes et définitions	129
3.2 Symboles et termes abrégés	136
3.3 Conventions de diagramme d'état	139
4 Architecture de système de communication train-sol.....	139
4.1 Généralités	139
4.2 Exigences	139
4.3 Architecture de réseau de communication mobile.....	141
4.3.1 Généralités	141
4.3.2 Interface de réseau embarqué	141
4.4 Structure de décomposition de système	142
4.4.1 Généralités	142
4.4.2 Structure de décomposition de système au niveau système train-sol	143
4.4.3 Structure de décomposition de système au niveau sous-système de MCG	143
4.4.4 Structure de décomposition de système au niveau sous-système de GCG	143
4.5 Structure de décomposition fonctionnelle	144
4.6 Passerelle de communication mobile	145
4.6.1 Architecture	145
4.6.2 Passerelle de communication mobile	147
4.7 Redondance de communication mobile	149
4.7.1 Généralités	149
4.7.2 Redondance à efficacité totale.....	150
4.7.3 Redondance à efficacité partielle	150
4.8 Modifications de la composition d'un train	150
4.9 Sécurité	151
4.9.1 Zones de sécurité	151
4.9.2 Mesures de sécurité	153
4.9.3 Modèle pour authentification, autorisation et comptabilité	154
4.9.4 Classification du réseau et des MCG	156
5 Référentiel de communication.....	158
5.1 Généralités	158
5.2 Architecture de service de courtage via MCG.....	159
5.3 Concept d'adressage	160
5.3.1 Cas d'utilisation	160
5.3.2 Identification de rame et de train	160
5.3.3 Frontières du réseau T2G	160
5.3.4 Réseau minimal de base T2G	160
5.3.5 Adressage T2G.....	161
5.3.6 URI HTTP.....	163
5.4 Classes de données pour la communication T2G	164
5.4.1 Généralités	164

5.4.2	Etablissement du canal de communication.....	165
5.4.3	Données de messagerie	165
5.4.4	Données de processus	165
5.4.5	Données de flux.....	166
5.4.6	Données du mode «au mieux».....	167
5.5	Protocole de communication	167
5.5.1	Généralités	167
5.5.2	HTTP(S)	167
5.5.3	MQTT (facultatif)	169
5.6	Services de communication.....	170
5.6.1	Généralités	170
5.6.2	Service de communication Données de messagerie	170
5.6.3	Service de transfert de fichiers	174
6	Services et interfaces (MCG).....	198
6.1	Vue d'ensemble	198
6.1.1	Architecture des services système MCG	198
6.1.2	Interfaces des services système MCG / GCG	199
6.1.3	Relation de communication MCG / GCG	200
6.2	Délivrance des services	200
6.3	Description des services du système MCG / GCG	201
6.3.1	Services de communication	201
6.3.2	Service Localisation du train (facultatif)	204
6.3.3	Service Informations sur le train	210
6.3.4	Service Sélecteur de réseau de MCG	215
6.3.5	Service Télémétrie de train (facultatif)	216
6.3.6	Service Réveil du train de MCG (facultatif)	228
7	Services et interfaces (GCG).....	230
7.1	Vue d'ensemble de la GCG	230
7.2	Adressage des GCG	232
7.2.1	Interface MCG sans fil	232
7.2.2	Interface GCG au sol	232
7.3	Mise en œuvre de GCG	233
7.3.1	Généralités (informatives).....	233
7.3.2	Disponibilité d'une GCG.....	233
7.3.3	Capacité de traitement d'une GCG	233
7.3.4	Sécurité d'une GCG	233
7.4	Accès aux services d'une GCG	234
7.4.1	Protocole d'accès aux services d'une GCG	234
7.4.2	Base de données flotte d'une GCG	234
7.4.3	Services entre MCG et GCG	234
7.4.4	Service de transfert de fichiers	235
7.4.5	Interface sol d'une GCG	235
7.4.6	Services entre «Home GCG» et «Foreign GCG»	236
7.4.7	Services publics d'une GCG	236
Annexe A (normative)	Présentation d'un message	237
A.1	Généralités	237
A.2	Règles de transmission	237
A.3	Message général	237
Annexe B (normative)	Codage et classement des données téléométriques	238

B.1	Généralités	238
B.2	Codage des données utiles MQTT	238
B.3	Regroupement de variables et critère de classement	239
	Bibliographie.....	242
Figure 1	– Système de communication embarqué de train (exemple)	141
Figure 2	– Système de communication au sol (exemple)	142
Figure 3	– Option 1: communication dispositif terminal embarqué-sol via MCG	146
Figure 4	– Option 2: communication dispositif terminal embarqué-sol via une interface dédiée	147
Figure 5	– Schéma fonctionnel du modèle abstrait de MCG	148
Figure 6	– MCG configurée comme une ALG	149
Figure 7	– Exemple d'architecture de communication train-sol redondante.....	149
Figure 8	– Zones de sécurité (simplifiées).....	152
Figure 9	– Modèle pour authentification, autorisation et comptabilité	155
Figure 10	– MCG connectant des systèmes de transmission ouverts et fermés	158
Figure 11	– Architecture de service de courtage via MCG	159
Figure 12	– Configuration minimale du réseau train-sol.....	160
Figure 13	– Train composé de quatre véhicules	161
Figure 14	– Piles de communication.....	168
Figure 15	– Modèle de communication Données de messagerie basé sur HTTP(S).....	168
Figure 16	– Demande/événement HTTP(S).....	169
Figure 17	– Réponse HTTP(S).....	169
Figure 18	– Echange de données de messagerie (exemple)	171
Figure 19	– Structure de télégramme Données de messagerie.....	172
Figure 20	– Exemple de téléchargement de fichiers en liaison montante.....	176
Figure 21	– Cas d'erreur: aucun message ComID 203 reçu.....	182
Figure 22	– Cas d'erreur: aucun message ComID 206 reçu, aucun fichier téléchargé en liaison montante côté sol	183
Figure 23	– Cas d'erreur: aucun message ComID 206 reçu, fichier téléchargé en liaison montante côté sol	184
Figure 24	– Cas d'erreur: aucun message ComID 207 reçu.....	185
Figure 25	– Exemple de téléchargement de fichiers en liaison descendante	186
Figure 26	– Cas d'erreur: aucun message ComID 209 reçu.....	192
Figure 27	– Cas d'erreur: aucun message ComID 211 reçu.....	193
Figure 28	– Cas d'erreur: aucun message ComID 210 reçu.....	194
Figure 29	– Architecture des services	198
Figure 30	– Interfaces des services	200
Figure 31	– Procédure d'établissement de la liaison radio à partir de la MCG	202
Figure 32	– Procédure d'établissement de la liaison radio à partir de la GCG	202
Figure 33	– Procédure de mise à jour du serveur DNS au sol	203
Figure 34	– Exemple d'architecture pour la localisation du train	205
Figure 35	– Exemple de procédure de notification de la localisation actuelle d'un train	206
Figure 36	– Exemple d'architecture de notification des informations sur le train	210

Figure 37 – Exemple de procédure de notification des informations sur le train.....	211
Figure 38 – Illustration du sélecteur de réseau.....	215
Figure 39 – Architecture de fourniture de données télémétriques	217
Figure 40 – Procédure de notification de la localisation actuelle d'un train	218
Figure 41 – Exemple de procédure de réveil du train	229
Figure 42 – Interfaces train-sol	231
Figure B.1 – Format des données utiles de notification MQTT	238
Figure B.2 – Exemple de critères de classement.....	240
Figure B.3 – Exemple de regroupement de valeurs	240
Tableau 1 – Exigences applicables à la communication train-sol.....	140
Tableau 2 – Décomposition de système train-sol	143
Tableau 3 – Décomposition de sous-système de MCG.....	143
Tableau 4 – Décomposition de sous-système de GCG	144
Tableau 5 – Exemple de la décomposition fonctionnelle de la MCG	144
Tableau 6 – Exemple de la décomposition fonctionnelle de la GCG	145
Tableau 7 – Dispositif – Etat de mise en œuvre du TIS	151
Tableau 8 – Composition – Etat de mise en œuvre du TIS	151
Tableau 9 – Mesures de sécurité	153
Tableau 10 – Catégories de MCG	157
Tableau 11 – Exigences de sécurité.....	157
Tableau 12 – Zone DNS mondiale d'URI TCN	163
Tableau 13 – Paramètres de service recommandés pour les données de messagerie.....	165
Tableau 14 – Paramètres de service recommandés pour les données de processus	166
Tableau 15 – Paramètres de service recommandés pour les données de flux	166
Tableau 16 – Paramètres de service recommandés pour les données du mode «au mieux».....	167
Tableau 17 – Modèle de demande/réponse de paramètres HTTP(S).....	169
Tableau 18 – En-tête Données de messagerie (MD-header) général.....	172
Tableau 19 – Corps Données de messagerie (MD-body) général	173
Tableau 20 – Somme de contrôle Données de messagerie (MD-checksum).....	173
Tableau 21 – Types de messages.....	174
Tableau 22 – Représentation de message	174
Tableau 23 – Terminologie du transfert de fichiers.....	175
Tableau 24 – ComID 202: valeurs d'en-tête du télégramme de données de messagerie.....	177
Tableau 25 – ComID 202: valeurs du corps du télégramme de données de messagerie.....	177
Tableau 26 – ComID 202: corps de données de messagerie – objet mdPayload	178
Tableau 27 – ComID 203: valeurs d'en-tête du télégramme de données de messagerie.....	178
Tableau 28 – ComID 203: valeurs du corps du télégramme de données de messagerie.....	179
Tableau 29 – ComID 203: corps de données de messagerie – objet mdPayload	179
Tableau 30 – ComID 206: valeurs d'en-tête du télégramme de données de messagerie.....	179
Tableau 31 – ComID 206: valeurs du corps du télégramme de données de messagerie.....	180
Tableau 32 – ComID 206: corps de données de messagerie – objet mdPayload	180

Tableau 33 – ComID 207: valeurs d'en-tête du télégramme de données de messagerie.....	181
Tableau 34 – ComID 207: valeurs du corps du télégramme de données de messagerie.....	181
Tableau 35 – ComID 207: corps de données de messagerie – objet mdPayload	181
Tableau 36 – ComID 208: valeurs d'en-tête du télégramme de données de messagerie.....	187
Tableau 37 – ComID 208: valeurs du corps du télégramme de données de messagerie.....	187
Tableau 38 – ComID 208: corps de données de messagerie – objet mdPayload	188
Tableau 39 – ComID 209: valeurs d'en-tête du télégramme de données de messagerie.....	189
Tableau 40 – ComID 209: valeurs du corps du télégramme de données de messagerie.....	189
Tableau 41 – ComID 209: corps de données de messagerie – objet mdPayload	189
Tableau 42 – ComID 210: valeurs d'en-tête du télégramme de données de messagerie.....	190
Tableau 43 – ComID 210: valeurs du corps du télégramme de données de messagerie.....	190
Tableau 44 – ComID 210: corps de données de messagerie – objet mdPayload	190
Tableau 45 – ComID 211: valeurs d'en-tête du télégramme de données de messagerie.....	190
Tableau 46 – ComID 211: valeurs du corps du télégramme de données de messagerie.....	191
Tableau 47 – ComID 211: corps de données de messagerie – objet mdPayload	191
Tableau 48 – Principales composantes d'un URI dITarget.....	195
Tableau 49 – Principales composantes de l'élément host.....	195
Tableau 50 – Valeurs valides de l'étiquette «device»	196
Tableau 51 – Valeurs valides de l'étiquette «vehicle»	196
Tableau 52 – Valeurs valides de l'étiquette «consist»	197
Tableau 53 – Valeurs valides de l'étiquette «closed train»	197
Tableau 54 – Valeurs valides de l'étiquette «train»	197
Tableau 55 – Exemples de valeurs dITarget.....	198
Tableau 56 – ComID 240: message de capacité	203
Tableau 57 – ComID 240: valeurs du corps du télégramme d'événement de données de messagerie	204
Tableau 58 – ComID 240: corps de l'événement de données de messagerie – objet mdPayload.....	204
Tableau 59 – ComID 230: valeurs d'en-tête du télégramme de demande de données de messagerie	207
Tableau 60 – ComID 230: valeurs du corps du télégramme de demande de données de messagerie	207
Tableau 61 – ComID 230: corps de la demande de données de messagerie – objet mdPayload.....	207
Tableau 62 – ComID 230: valeurs d'en-tête du télégramme de réponse de données de messagerie	208
Tableau 63 – ComID 230: valeurs du corps du télégramme de réponse de données de messagerie	208
Tableau 64 – ComID 230/232: corps de la réponse/notification de données de messagerie – objet mdPayload	209
Tableau 65 – Exemple de latitude/longitude avec proposition de notation à virgule fixe	209
Tableau 66 – ComID 232: valeurs d'en-tête du télégramme de données de messagerie.....	210
Tableau 67 – ComID 232: valeurs du corps du télégramme de données de messagerie.....	210
Tableau 68 – ComID 234: valeurs d'en-tête du télégramme de demande de données de messagerie	212

Tableau 69 – ComID 234: valeurs du corps du télégramme de demande de données de messagerie	212
Tableau 70 – ComID 234: corps de la demande de données de messagerie – objet mdPayload	212
Tableau 71 – ComID 234: valeurs d'en-tête du télégramme de réponse de données de messagerie	213
Tableau 72 – ComID 234: valeurs du corps du télégramme de réponse de données de messagerie	213
Tableau 73 – ComID 234: corps de la réponse de données de messagerie – objet mdPayload	213
Tableau 74 – ComID 236: valeurs d'en-tête du télégramme de données de messagerie	214
Tableau 75 – ComID 236: valeurs du corps du télégramme de données de messagerie	214
Tableau 76 – ComID 240: valeurs d'en-tête du télégramme de demande de données de messagerie	219
Tableau 77 – ComID 240: valeurs du corps du télégramme de demande de données de messagerie	219
Tableau 78 – ComID 240: valeurs d'en-tête du télégramme de réponse de données de messagerie	220
Tableau 79 – ComID 240: valeurs du corps du télégramme de réponse de données de messagerie	220
Tableau 80 – ComID 240: corps de la réponse de données de messagerie – objet mdPayload	221
Tableau 81 – ComID 242: valeurs d'en-tête du télégramme de demande de données de messagerie	222
Tableau 82 – ComID 242: valeurs du corps du télégramme de demande de données de messagerie	222
Tableau 83 – ComID 242: corps de la demande de données de messagerie – objet mdPayload	222
Tableau 84 – ComID 242: valeurs d'en-tête du télégramme de réponse de données de messagerie	223
Tableau 85 – ComID 242: valeurs du corps du télégramme de réponse de données de messagerie	223
Tableau 86 – ComID 242: corps de la réponse de données de messagerie – objet mdPayload	224
Tableau 87 – ComID 243: valeurs d'en-tête du télégramme de demande de données de messagerie	225
Tableau 88 – ComID 243: valeurs du corps du télégramme de demande de données de messagerie	225
Tableau 89 – ComID 243: corps de la demande de données de messagerie – objet mdPayload	225
Tableau 90 – ComID 244: valeurs d'en-tête du télégramme de demande de données de messagerie	226
Tableau 91 – ComID 244: valeurs du corps du télégramme de demande de données de messagerie	226
Tableau 92 – ComID 244: corps de la demande de données de messagerie – objet mdPayload	226
Tableau 93 – ComID 244: valeurs d'en-tête du télégramme de réponse de données de messagerie	226
Tableau 94 – ComID 244: valeurs du corps du télégramme de réponse de données de messagerie	227

Tableau 95 – ComID 244: corps de la réponse de données de messagerie – objet mdPayload	227
Tableau 96 – ComID 245: valeurs d'en-tête du télégramme de demande de données de messagerie	227
Tableau 97 – ComID 245: valeurs du corps du télégramme de demande de données de messagerie	228
Tableau 98 – ComID 245: corps de la demande de données de messagerie – objet mdPayload	228
Tableau 99 – ComID 238: en-tête de l'événement MD twsWakeUp	229
Tableau 100 – ComID 238: corps de l'événement MD twsWakeUp	229
Tableau 101 – ComID 238: corps de l'événement de données de messagerie MD twsWakeUp – objet mdPayload	230
Tableau B.1 – Exemple de décodage de valeurs	241

IECNORM.COM : Click to view the full PDF of IEC 61375-2-6:2018

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**MATÉRIEL ÉLECTRONIQUE FERROVIAIRE –
RÉSEAU EMBARQUÉ DE TRAIN (TCN) –****Partie 2-6: Communication train-sol****AVANT-PROPOS**

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les Références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 61375-2-6 a été établie par le comité d'études 9 de l'IEC: Matériels et systèmes électriques ferroviaires.

Le texte de cette norme internationale est issu des documents suivants:

FDIS	Rapport de vote
9/2374/FDIS	9/2402/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme internationale.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 61375, publiées sous le titre général *Matériel électronique ferroviaire – Réseau embarqué de train (TCN)*, peut être consultée sur le site Web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site Web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "*colour inside*" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

IECNORM.COM : Click to view the full PDF of IEC 61375-2-6:2018

INTRODUCTION

Etant donné que la série de normes sur le réseau embarqué de train inclut l'IEC 61375-2-3: *Matériel électronique ferroviaire – Réseau embarqué de train (TCN) – Partie 2-3: Profil de communication TCN*, des références à ce document sont données lorsqu'il y a lieu.

Le présent document suit le modèle ISO-OSI.

Le présent document ne couvre pas la spécification des technologies et protocoles radio pertinents pour la communication radio train-sol.

Lors de l'élaboration du présent document, les principaux cas d'utilisation suivants, auxquels la communication train-sol s'applique, ont été pris en considération:

- a) Application de mise en service
 - 1) Application opérationnelle.
 - 2) Application de données de mission.
 - 3) Application d'assistance du conducteur.
 - 4) Application de compteur d'énergie.
- b) Application de maintenance
 - 1) Application de données de configuration.
 - 2) Surveillance d'état de train (par exemple, télémétrie).
 - 3) Application de données de diagnostic.
 - 4) Application d'enregistreur d'événement.
- c) Application multimédia
 - 1) Application d'information des voyageurs.
 - 2) Application de divertissement des voyageurs.
 - 3) Application de billetterie électronique.
 - 4) Système de télévision en circuit fermé (CCTV) et de vidéosurveillance.

MATÉRIEL ÉLECTRONIQUE FERROVIAIRE – RÉSEAU EMBARQUÉ DE TRAIN (TCN) –

Partie 2-6: Communication train-sol

1 Domaine d'application

La présente partie de l'IEC 61375 couvre la spécification pour la communication entre les sous-systèmes embarqués et les sous-systèmes au sol.

Le système, les interfaces et les protocoles de communication sont spécifiés comme une fonction de communication mobile, utilisant toute technologie radio disponible.

Le présent document spécifie des exigences pour:

- a) sélectionner le réseau radio sur la base des paramètres de Qualité de Service (QoS) requis par l'application;
- b) permettre aux applications du système de contrôle et de gestion de train (TCMS) et/ou du sous-système multimédia et télématique embarqué (OMTS), installées à bord du train et communiquant sur le réseau de communication embarqué, d'avoir un accès à distance aux applications s'exécutant au sol;
- c) permettre aux applications s'exécutant au sol d'avoir un accès à distance aux applications TCMS et/ou OMTS embarquées.

Le présent document spécifie d'autres exigences qui permettent aux applications s'exécutant à bord et aux applications s'exécutant au sol de se connecter les unes aux autres en appliquant le mécanisme d'adressage virtuel/fonctionnel spécifié par l'IEC 61375-2-3 et en échangeant des ensembles de données d'application produits ou exploités par les fonctions embarquées mises en œuvre dans les dispositifs reliés au réseau TCN.

En outre, le présent document couvre les exigences de sécurité afin de n'accorder l'accès qu'à des applications authentifiées et autorisées et de permettre un cryptage des données échangées.

Les communications de données relatives à la sécurité entre des applications embarquées et des applications au sol ne relèvent pas du domaine d'application du présent document de même que le service de connectivité Internet destiné aux voyageurs.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61375-1:2012, *Matériel électronique ferroviaire – Réseau embarqué de train (TCN) – Partie 1: Architecture générale*

IEC 61375-2-3:2015, *Matériel électronique ferroviaire – Réseau embarqué de train (TCN) – Partie 2-3: Profil de communication TCN* (disponible en anglais seulement)

IEC 61375-3-4, *Matériel électronique ferroviaire – Réseau embarqué de train (TCN) – Partie 3-4: Réseau Ethernet de rame (ECN)*

IEC 62280, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Communication de sécurité dans le système de transmission*

IEC 62443 (toutes les parties), *Réseaux de communication industriels – Sécurité des systèmes d'automatisation et de commande industrielles*

IEC 62443-3-3, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels* (disponible en anglais seulement)

IEC 62580-1, *Matériel électronique ferroviaire – Sous-systèmes ferroviaires multimédias et télématiques embarqués – Partie 1: Architecture générale*

ISO/IEC 20922:2016, *Technologies de l'information – Transport par télémessure des messages en file d'attente (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 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 Termes, définitions, symboles, termes abrégés et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>
- ISO Online browsing platform: disponible à l'adresse <http://www.iso.org/obp>

3.1.1

Authentification Autorisation Comptabilité

cadre de contrôle d'accès, d'application de politique et d'audit pour des systèmes informatiques

3.1.2

service authentification autorisation comptabilité

architecture de sécurité pour des systèmes distribués, qui permet de contrôler l'accès des utilisateurs aux services en fonction de l'utilisateur et du service en question, ainsi que la quantité de ressource consommée

3.1.3

couche application

couche supérieure du modèle OSI en interface directe avec l'application

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

3.1.4

processus d'application

élément d'un système ouvert réel qui effectue le traitement de l'information pour une application particulière

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

3.1.5

taux d'erreur résiduel

taux des erreurs sur les bits dans un flux de données, dû principalement au bruit (erreurs sur les bits aléatoires), mais également dû à des défauts de mémoire dans les dispositifs d'archivage des données (erreurs sur les bits systématiques)

3.1.6

pont

appareil qui stocke et retransmet les trames d'un bus à l'autre en fonction de leurs adresses de couche liaison

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

3.1.7

diffusion

transmission quasi simultanée des mêmes informations vers plusieurs destinataires

Note 1 à l'article: La diffusion dans le TCN n'est pas considérée comme fiable, c'est-à-dire que certains destinataires peuvent recevoir les informations et d'autres pas.

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

3.1.8

bus

système de transfert de données entre plusieurs participants, qui sont des unités fonctionnelles de traitement de données, par l'intermédiaire d'une voie de transmission commune, les participants n'étant pas impliqués dans le transfert des données entre d'autres participants

Note 1 à l'article: La définition logique et fonctionnelle d'un bus s'applique indépendamment de la configuration topologique et de la mise en œuvre physique du bus. Un bus peut avoir une configuration linéaire ou en anneau.

Note 2 à l'article: Dans certains cas, les droits de transmission sont distribués par un autre participant, par exemple, par un administrateur de bus.

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

3.1.9

rame non modifiable

train composé d'une rame ou d'un ensemble de rames, dont la composition ne change pas en exploitation normale

EXEMPLE Métro, train suburbain ou rame à grande vitesse.

Note 1 à l'article: Les rames sont accouplées en atelier afin de constituer une rame non modifiable pour exploitation.

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

3.1.10

dispositif de communication

dispositif relié au réseau de rame ou au réseau central de train avec la capacité de transporter, émettre ou recevoir des données

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

3.1.11

canal de communication

connexion logique sur un support multiplexé, tel qu'un canal radio, ou état conceptuel dans lequel une MCG a annoncé sa présence à la GCG de manière à permettre à cette dernière d'interagir avec la MCG

3.1.12

liaison radio

liaison sans fil qui relie un dispositif à un réseau pour permettre à ce dernier d'établir une communication avec d'autres dispositifs par le biais de ce réseau

3.1.13

composition

nombre et caractéristiques des rames composant un train

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

3.1.14

configuration réseau

définition de la topologie d'un réseau, des dispositifs qui lui sont connectés, de leurs capacités et du trafic qu'ils génèrent. Par extension, l'opération consistant à charger dans les dispositifs les informations de configuration de façon préalable à leur passage en mode opérationnel

3.1.15

rame

véhicule unique ou groupe de véhicules qui ne sont pas séparés en exploitation normale

Note 1 à l'article: Une rame peut contenir aucun, un seul ou plusieurs réseaux de rame.

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

3.1.16

réseau de rame

bus connectant des équipements dans une rame (le MVB, par exemple) et qui se conforme ou s'adapte aux protocoles en temps réel TCN

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

3.1.17

dispositif terminal

entité reliée à un réseau de rame ou à un ensemble de réseaux de rame préparé pour des raisons de redondance

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

3.1.18

référentiel

ensemble de services et protocoles servant à soutenir la communication train-sol

3.1.19

fonction

processus d'application qui échange des messages avec un autre processus d'application

3.1.20

passerelle <dans un réseau embarqué de train>

connexion de différents bus au niveau de la couche application requérant une analyse des données dépendant de l'application ainsi qu'une conversion de protocole

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

3.1.21

adresse de groupe

adresse d'un groupe de multidiffusion auquel appartient un appareil

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

3.1.22

hôte

toute unité adressable reliée au réseau: dispositifs terminaux, dispositifs réseau, etc.

3.1.23

inauguration

opération entreprise en cas de modification de la composition, qui donne à tous les nœuds du réseau central de train leur adresse, leur orientation et les informations concernant tous les nœuds nommés présents sur le même réseau central

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

3.1.24

intégrité

état dans lequel l'information est complète et non altérée

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

3.1.25

parcours de train

parcours ferroviaire programmé

3.1.26

train sur parcours

composition se déplaçant sur un parcours de train programmé

3.1.27

réseau local

portion d'un réseau caractérisée par un mode d'accès et par un espace d'adressage communs

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

3.1.28**contrôle d'accès au support**

sous-couche de la couche liaison qui contrôle l'accès au support (arbitrage, transfert de maîtrise, interrogation)

3.1.29**support**

support physique de propagation du signal

Note 1 à l'article: Câbles électriques, fibres optiques, etc.

3.1.30**message <dans les systèmes de transmission>**

information qui est transmise en un ou plusieurs paquets par un émetteur à un ou plusieurs récepteurs

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

3.1.31**multidiffusion**

transmission du même message à un groupe de destinataires identifiés par leur adresse de groupe.

Note 1 à l'article: Le terme «distribution» est utilisé même si le groupe comprend tous les destinataires.

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

3.1.32**réseau**

ensemble de différents systèmes possibles de communication qui échangent de l'information selon un moyen communément accepté

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

3.1.33**adresse réseau**

adresse qui identifie un dispositif de communication sur une couche de réseau

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

3.1.34**dispositif réseau**

composants utilisés pour la constitution de réseaux de rame et de réseaux de trains

Note 1 à l'article: Il peut s'agir de composants passifs tels que des câbles ou des connecteurs, de composants actifs non gérés tels que des répéteurs, des convertisseurs de supports ou des commutateurs (non gérés), ou de composants actifs gérés tels que des passerelles, des routeurs et des commutateurs (gérés).

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

3.1.35**couche réseau**

couche du modèle OSI assurant le routage entre les différents bus

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

3.1.36

gestion de réseau

opérations nécessaires à la configuration, la surveillance, le diagnostic et la maintenance à distance du réseau

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

3.1.37

nœud <dans un réseau embarqué de train>

appareil placé sur le réseau central de train, pouvant servir de passerelle entre le réseau central de train et le réseau de rame

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

3.1.38

octet

byte

ensemble ordonné de huit éléments binaires ou éléments de signal binaires, traité comme un tout

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

3.1.39

train à composition variable

train composé d'une rame ou d'un ensemble de rames, dont la composition peut changer en exploitation normale

EXEMPLE Les trains internationaux UIC (Union Internationale des Chemins de fer, association internationale des opérateurs de chemins de fer) tractés par une locomotive.

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

3.1.40

compagnie de chemin de fer

entreprise ou organisme dont l'activité consiste à exploiter des trains

3.1.41

paquet

ensemble de données numériques constituant un message ou une partie de message et d'éléments numériques de service comprenant une adresse, organisés selon une disposition déterminée par le procédé de transmission et acheminés comme un tout

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

3.1.42

routeur

unité fonctionnelle qui établit un chemin à travers un ou plusieurs réseaux d'ordinateurs et achemine les paquets vers leur destination

Note 1 à l'article: Dans les réseaux d'ordinateurs conformes à l'OSI, un routeur fonctionne à la couche réseau.

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

3.1.43

de sécurité

porte la responsabilité de la sécurité

Note 1 à l'article: Une fonction, un composant, un produit, un système ou une procédure est dit(e) de sécurité si au moins l'une de ses propriétés est utilisée dans l'argument de sécurité du système dans lequel il ou elle est

appliqué(e). Ces propriétés peuvent être fonctionnelles ou non fonctionnelles par nature. Les exigences attribuées à la fonction peuvent être des exigences d'intégrité systématiques ou aléatoires.

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

3.1.44

service <dans un réseau embarqué de train>

capacités et moyens d'un sous-système (une couche de communication, par exemple) offerts à un utilisateur

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

3.1.45

service <dans le secteur ferroviaire>

service correspondant à un transport de marchandises (fret) ou de voyageurs

3.1.46

travail

séquences de transactions

Note 1 à l'article: L'exactitude du travail peut être établie en déterminant l'exactitude de chaque transaction qu'il exécute, ainsi que l'exactitude des interactions entre les transactions.

3.1.47

transaction

séquences d'interactions entre des composants d'un système

3.1.48

commutateur <dans un réseau embarqué de train>

pont MAC tel que défini dans l'IEEE 802.1D

Note 1 à l'article: MAC signifie «Contrôle d'Accès au Support» (de l'anglais Medium Access Control), sous-couche au sein de la couche liaison décidant quel dispositif est autorisé à émettre vers le bus.

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

3.1.49

topologie

interconnexion de câbles et nombre de dispositifs éventuels dans un réseau donné

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

3.1.50

train

composition d'une rame ou d'un ensemble de rames, pouvant être exploitée(s) comme une unité autonome, par exemple contenant des commandes et au moins une cabine de conduite

Note 1 à l'article: Les trains peuvent être catégorisés en trains à composition variable (voir 3.1.39) et rames non modifiables (voir 3.1.9).

3.1.51

réseau embarqué de train

réseau de communication de données permettant de connecter des équipements électroniques programmables embarqués sur des véhicules ferroviaires

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

3.1.52

réseau central de train

bus connectant les rames d'un train, en particulier le bus de train filaire, et qui est conforme aux protocoles TCN

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

3.1.53

couche transport

couche du modèle OSI responsable du contrôle de flux de bout en bout et de la reprise sur erreur

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

3.1.54

transfert vertical

fait référence à un nœud de réseau modifiant le type de connectivité qu'il utilise pour accéder à une infrastructure de prise en charge, généralement pour prendre en charge une mobilité de nœud

3.2 Symboles et termes abrégés

AAA (Authentication Authorization Accounting)	Authentification, autorisation, comptabilité
ALG (Application Layer Gateway)	Passerelle de couche application
ARP (Address Resolution Protocol)	Protocole de résolution d'adresses
ASCII (American Standard Code for Information Interchange)	Code normalisé américain pour l'échange d'informations
BER (Bit Error Rate)	Taux d'erreur résiduel
CCTV (Closed Circuit Television)	Télévision en circuit fermé
ComID (Communication Identifier)	Identificateur de communication
CRC	Contrôle par Redondance Cyclique, vérification de l'intégrité des données par division en polynômes
DDNS (Dynamic Domain Name Server)	Serveur de noms de domaine dynamique
DHCP (Dynamic Host Configuration Protocol)	Protocole DHCP
DIN (Deutsches Institut für Normung)	Organisme national de normalisation allemand
DNS (Domain Name Server)	Serveur de noms de domaine
DoS (Denial of Service)	Déni de service
ECM (Entity in Charge of Maintenance)	Entité en charge de la maintenance
ECN (Ethernet Consist Network)	Réseau de rame Ethernet
ED (End Device)	Dispositif terminal
EDGE (Enhanced Data Rates for GSM Evolution)	Taux de données améliorées pour extension au GSM
ERA (European Railways Agency)	Agence européenne des chemins de fer, rebaptisée en 2017 Agence de l'Union européenne pour les chemins de fer, qui la remplace et lui succède
EMS (Energy Metering System)	Système de mesure d'énergie
ETB (Ethernet Train Backbone)	Réseau central de train Ethernet
ETSI (European Telecommunications Standards Institute)	Institut européen de normalisation des télécommunications

EVN (European Vehicle Number)	Numéro de véhicule européen
FBS (Function Breakdown Structure)	Structure de décomposition fonctionnelle
FCS (Frame Check Sequence)	Code de détection d'erreurs
FQDN (Full Qualified Domain Name)	Nom de domaine totalement qualifié
FTP (File Transfer Protocol)	Protocole de transfert de fichiers
G2T (Ground to Train)	Sol-train
GCG (Ground Communication Gateway)	Passerelle de communication au sol
GNSS (Global Navigation Satellite System)	Système mondial de navigation par satellite
GSM (Global System for Mobile Communications)	Système mondial de téléphonie mobile
GSM-R (Global System for Mobile Communications – Railway)	Système mondial de téléphonie mobile pour applications ferroviaires
GPRS (General Packet Radio Service)	Service général de données radio en mode paquets
HSCSD (High Speed Circuit Switched Data)	Données commutées sur circuit à haute vitesse
HSPA (High Speed Packet Access)	Accès par paquets à haute vitesse
HTTP (HyperText Transfer Protocol)	Protocole de transfert hypertexte
HTTPS (HyperText Transfer Protocol Secure)	Protocole de transfert hypertexte sécurisé
ICMP (Internet Control Message Protocol)	Protocole de message de contrôle Internet
ID	Identifiant
IDS (Intrusion Detection System)	Système de détection d'intrusion
IEEE (Institute of Electrical and Electronics Engineers)	Institut des ingénieurs électriciens et électroniciens, New York
IETF (Internet Engineering Task Force)	Groupe de travail qui participe à l'ingénierie et à l'évolution des technologies de l'Internet
IP (Internet Protocol)	Protocole Internet
JSON (Java Script Object Notation)	Notation d'objet JavaScript
LTE (Long Term Evolution)	Evolution sur le long terme
MAC (Medium Access Control)	Contrôle d'accès au support, sous-couche au sein de la Couche Liaison décidant quel équipement est autorisé à émettre vers le bus
MAR (Mobile Access Router)	Routeur d'accès mobile
MCG (Mobile Communication Gateway)	Passerelle de communication mobile
MD (Message Data)	Données de messagerie
MQTT (Message Queuing Telemetry Transport)	Transport par télémessagerie des messages en file d'attente
MVB (Multifunction Vehicle Bus)	Bus de véhicule multifonctions
n.a.	Non applicable
NSS (Network Selection Service)	Service de sélection de réseau
OMTS (Onboard Multimedia and Telematic Services)	Services multimédias et télématiques embarqués
OSI (Open Systems Interconnection)	Interconnexion de systèmes ouverts [SOURCE: IEC 60050-716:1995, 716-01-20]
OTIF (Intergovernmental Organisation for	Organisation intergouvernementale pour les

International Carriage by Rail)	transports internationaux ferroviaires
PAM (Pluggable Authentication Module)	Module d'authentification enfichable
PCG (Partner Communication Gateway)	Passerelle de communication avec un partenaire
PNAT (Port Network Address Translation)	Traduction d'adresse réseau de port
QoS (Quality of Service)	Qualité de service
RFC (Request for Comments)	Appel à commentaires (document RFC), Norme Internet publiée par le groupe Internet Engineering Task Force (IETF)
RTP (Real-Time Transport Protocol)	Protocole de transport en temps réel
RTCP (RealTime Control Protocol)	Protocole de contrôle en temps réel
RU (Railway Undertaking)	Compagnie de chemin de fer
SBS (System Breakdown Structure)	Structure de décomposition de système
SCP (Secure Copy)	Copie sécurisée
SDT (Safe Data Transmission)	Transmission de données sécurisées
SFTP (SSH File Transfer Protocol)	Protocole de transfert de fichiers SSH
SSH (Secure Shell)	Protocole SSH
T2G (Train to Ground)	Train-sol
TBN (Train Backbone Node)	Nœud de réseau central de train, nom général donné à un nœud qui est connecté au réseau central de train indépendamment de la technologie utilisée.
TCMS (Train Control and Monitoring System)	Système de contrôle et de gestion de train
TCN (Train Communication Network)	Réseau embarqué de train, ensemble de véhicules et de réseaux centraux de trains communiquant entre eux
TCP (Transmission Control Protocol)	Protocole de contrôle de transmission
TIS (Train Information Service)	Service Informations sur le train
TLOS (Train Location Service)	Service Localisation du train
TLS (Transport Layer Security)	Protocole de sécurité de la couche transport
TRDP (Train Real Time Data Protocol)	Protocole temps réel de données de train
TTDB (Train Topology DataBase)	Base de données topologiques de train
TWS (Train Wake-up Service)	Service Réveil du train
TTS (Train Telemetry Service)	Service Télémétrie de train
UDP (User Datagram Protocol)	Protocole de datagramme d'utilisateur
UMTS (Universal Mobile Telecommunications System)	Système universel de télécommunications mobiles
UIC (Union Internationale des Chemins de fer)	Association internationale des opérateurs de chemins de fer
UID (Unique Identifier)	Identifiant unique
URI (Uniform Resource Identifier)	Identifiant uniforme de ressource
UML (Unified Modeling Language)	Langage de modélisation unifié
VPN (Virtual Private Network)	Réseau privé virtuel
XML (eXtensible Markup Language)	Langage XML
WiFi (Wireless Fidelity)	Technologie sans fil
WLAN (Wireless Local Area Network)	Réseau local sans fil

WTB (Wire Train Bus)

Bus de train filaire

3.3 Conventions de diagramme d'état

Les diagrammes d'état sont définis suivant la notation des machines d'état UML.

4 Architecture de système de communication train-sol

4.1 Généralités

Le présent document couvre la communication train-sol des données connexes qui sont produites et/ou consommées par les utilisateurs. La liste suivante répertorie des exemples d'utilisateurs:

- a) compagnie de chemin de fer;
- b) gestionnaire d'infrastructure;
- c) opérateur de centre de contrôle de flotte;
- d) gestionnaire du trafic;
- e) ECM (entité en charge de la maintenance);
- f) propriétaire de la flotte;
- g) constructeur de trains;
- h) fournisseur de sous-systèmes de train;
- i) tierces parties autorisées (par exemple, fournisseurs de contenus multimédias, utilisateur de données sur l'énergie).

relatifs au transfert des données connexes.

NOTE Certains utilisateurs de la liste ci-dessus peuvent appartenir à la même organisation.

4.2 Exigences

Les exigences applicables à la communication train-sol sont spécifiées dans le Tableau 1.

Pour faciliter la compréhension de ces exigences, un exemple d'architecture train-sol est illustré sur la Figure 1 et la Figure 2.

Tableau 1 – Exigences applicables à la communication train-sol

N° d'exigence	Exigence	Informations supplémentaires
1	Le système de communication train-sol interopérable doit répondre à tous les besoins utilisateur associés à des applications non relatives à la sécurité.	La communication relative à la sécurité n'est pas couverte par le domaine d'application du présent document.
2	Le système de communication doit inclure une partie de communication embarquée (MCG) et une partie au sol (GCG).	MCG = passerelle de communication mobile GCG = passerelle de communication au sol
3	Le système de communication train-sol doit utiliser toute liaison IP (support) sans fil disponible.	La liaison IP sans fil connecte la MCG et la GCG. La commutation et la sélection de liaisons sans fil devant être utilisées dépendent de l'application. Une liaison radio privée peut aussi être utilisée, par exemple GSM-R.
4	La MCG doit être connectée à Internet directement ou par le biais d'une GCG.	Seuls les utilisateurs autorisés peuvent atteindre le train au moyen d'une connexion Internet.
5	Il doit être possible d'avoir plusieurs MCG dans la même rame.	Plusieurs MCG peuvent être utilisées soit pour la gestion de la redondance, soit pour l'équilibrage de la charge.
6	Afin d'assurer la redondance de la fonction de communication train-sol, le système doit permettre l'utilisation d'une MCG installée dans une autre rame du même train.	
7	Il doit être possible d'avoir plusieurs GCG au sol desservant le même train. La GCG par défaut doit être unique, comme le requiert le processus d'enregistrement. Il est permis d'avoir une GCG unique pour chaque flotte.	
8	La MCG doit pouvoir agir comme une passerelle d'application ou comme un routeur. Le routeur peut faire partie de la MCG. Les adresses IP embarquées doivent concorder avec des adresses IP au sol si la MCG est un routeur.	
9	Les modifications de la composition des trains résultant de l'accouplement et du désaccouplement de rames doivent être gérées.	
10	Une rame doit être identifiée par un nom symbolique unique.	Par exemple EVN + n où n est l'identification de la MCG au sein de la rame. EVN peut devenir OTIF au plan international.
11	Une rame doit s'annoncer à la GCG. Le DDNS doit faire correspondre le nom symbolique de la rame à l'adresse IP (voir exigence 6).	
12	Une application peut demander un travail. Un travail peut être initié à la fois par des applications embarquées et par des applications au sol.	
13	Un travail peut aboutir à un certain nombre de transactions.	
14	Une transaction doit être initiée soit par la MCG, soit par la GCG. Une transaction doit être initiée soit par des applications embarquées, soit par des applications au sol.	

N° d'exigence	Exigence	Informations supplémentaires
15	Il doit exister différents modes de connectivité: 1: communication strictement limitée entre la MCG et une seule GCG 2: communication dans le cadre de laquelle la MCG peut se connecter à plusieurs GCG	Dans le mode 1, la MCG et la GCG ont une liaison privée avec des adresses IP privées. Toute application au sol ne doit pouvoir atteindre la MCG que par le biais de sa GCG spécifique. Dans le mode 2, la MCG a une adresse IP dynamique publique qui peut être utilisée par plusieurs GCG.
16	Les dispositifs terminaux au sol sont atteignables par un nom symbolique/une adresse IP unique et sont adressables par un nom symbolique/une adresse IP unique.	
17	Les MCG embarquées doivent pouvoir être atteintes depuis le sol par le nom symbolique/l'adresse IP unique et sont adressables par un nom symbolique/une adresse IP unique. Cette adresse peut être définie de manière statique ou assignée de manière dynamique, par exemple par un serveur DHCP au sol.	Voir également exigence 10
18	L'infrastructure de réseau au sol assure la mobilité de l'adresse IP de la MCG.	
19	L'infrastructure de réseau au sol tient compte des mesures de sécurité nécessaires au sol pour la protection contre les cyberattaques.	
20	L'infrastructure de réseau au sol fournit un serveur DNS pour transformer les adresses URI de TCN en adresses IP.	
21	La MCG doit refuser toute demande d'établissement d'un canal de communication émanant de la GCG.	La communication au niveau de l'application peut être initiée soit par des applications embarquées, soit par des applications au sol.

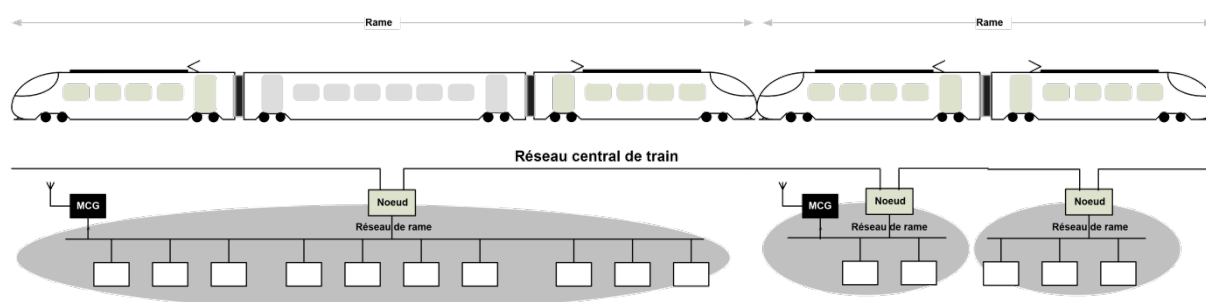
4.3 Architecture de réseau de communication mobile

4.3.1 Généralités

L'infrastructure de communication globale peut être divisée en réseau de communication embarqué de train et système de communication non embarqué (au sol).

Le réseau de communication embarqué de train est défini dans l'IEC 61375-1 comme une structure hiérarchique avec un réseau central de train pour la communication dans tout le train et des réseaux de rame subordonnés pour une communication intrarame (voir Figure 1).

4.3.2 Interface de réseau embarqué

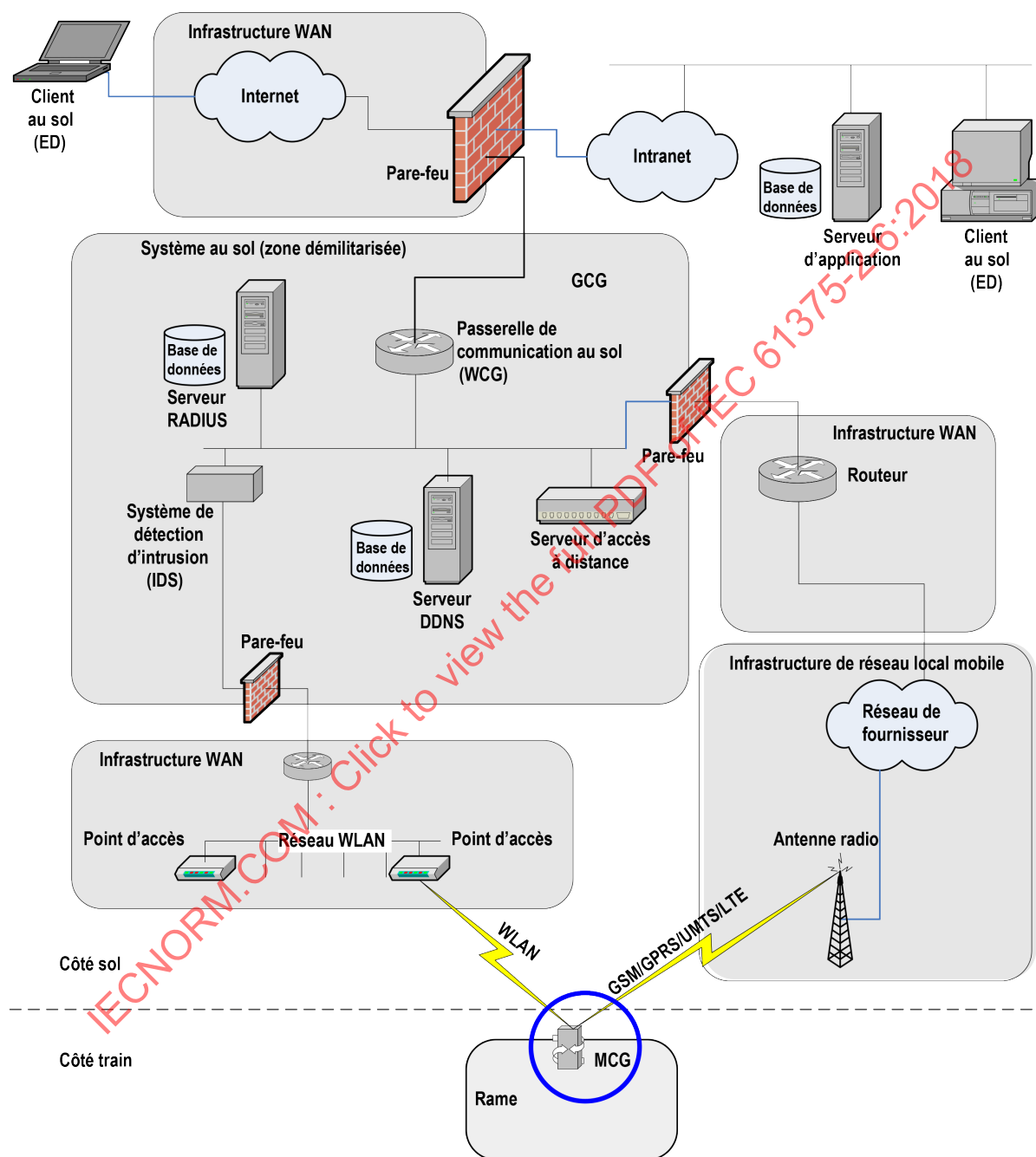


IEC

Figure 1 – Système de communication embarqué de train (exemple)

La MCG connecte le réseau de communication embarqué au système de communication au sol. Un exemple d'architecture est présenté à la Figure 2.

Pour la spécification de la communication train-sol, l'architecture du système de communication au sol est sans importance dans la mesure où les exigences du 4.2 sont satisfaites.



IEC

Figure 2 – Système de communication au sol (exemple)

4.4 Structure de décomposition de système

4.4.1 Généralités

Conformément aux exigences essentielles spécifiées dans le Tableau 1, la structure de décomposition de système et la structure de décomposition fonctionnelle sont spécifiées par les paragraphes suivants.

La structure de décomposition de système est limitée au premier niveau de communication train-sol.

Le deuxième niveau est scindé entre:

- a) le niveau sous-système embarqué;
- b) le niveau sous-système au sol.

4.4.2 Structure de décomposition de système au niveau système train-sol

Le Tableau 2 répertorie les éléments pertinents pour la structure de décomposition de système (SBS) au premier niveau.

Tableau 2 – Décomposition de système train-sol

N°	Système	Description
1	MCG	La passerelle de communication mobile est spécifiée par le présent document et est prévue comme un sous-système côté train fournissant des services train-sol sur les dispositifs terminaux embarqués ou comme une fonction de communication intégrée dans le dispositif terminal embarqué.
2	Liaison sans fil	Cela inclut les supports intranet et Internet qui ne sont pas couverts par les exigences spécifiées par le présent document.
3	GCG	La passerelle de communication au sol est spécifiée par le présent document en ce qui concerne ses services et ses interfaces.

4.4.3 Structure de décomposition de système au niveau sous-système de MCG

Le Tableau 3 répertorie les éléments de la MCG qui sont pertinents pour la structure de décomposition de système au deuxième niveau.

Tableau 3 – Décomposition de sous-système de MCG

N°	Sous-système	Description
1	Technologie radio	Différents supports selon les technologies radio disponibles sont possibles (par exemple, GPRS, UMTS, LTE, WiFi).
2	Interface de liaison radio	Tout type spécifié par l'UIT, l'ETSI ou l'IEEE.
3	Interface de réseau de rame/train	Interface ECN/ETB.
4	Passerelle/routeur de communication	La MCG se comporte comme un routeur ou comme une passerelle d'application respectant les exigences en matière d'accès sécurisé et/ou le mode du train qui est l'état actif du train (par exemple, exploitation, maintenance, mise en service).
5	Profils de communication/d'application	Les exigences applicables à cet élément sont spécifiées en tenant compte de l'IEC 61375-2-3 et de l'IEC 62580-1.

4.4.4 Structure de décomposition de système au niveau sous-système de GCG

Le Tableau 4 répertorie les éléments de la GCG qui sont pertinents pour la structure de décomposition de système au deuxième niveau.

Tableau 4 – Décomposition de sous-système de GCG

N°	Sous-système	Description
1	Profils de communication/d'application	
2	Enregistrement de rame/composition	
3	Gestion d'identité	

4.5 Structure de décomposition fonctionnelle

La structure de décomposition fonctionnelle (FBS) n'est spécifiée que sur les sous-systèmes de MCG et de GCG.

Aucune structure de décomposition fonctionnelle de la liaison sans fil n'est spécifiée; en fait, la spécification d'un tel élément n'est pas couverte par le présent document, mais il est supposé que la liaison sans fil est fournie par un réseau sans fil privé ou public spécifié par l'UIT, l'ETSI ou l'IEEE, etc.

Le Tableau 5 donne un exemple des sous-fonctions qui sont pertinentes pour la FBS de la MCG.

Tableau 5 – Exemple de la décomposition fonctionnelle de la MCG

N°	Fonction	Description
1	Processeur frontal de liaison radio	Interface de gestion du support radio physique
2	Fonction d'annonce	Il s'agit de la fonction embarquée impliquée dans le processus d'enregistrement dans l'infrastructure au sol
3	Fonction de contrôle AAA	Fonction d'authentification, d'autorisation et de comptabilité des applications
4	Pare-feu et fonction NAT	Protection du réseau contre un accès non autorisé
5	Fonction Sélecteur de réseau	Sélection d'un réseau radio approprié
6	Fonction Gestionnaire de session	Gestion du contexte d'application pendant un travail
7	Fonction Gestion des données de messagerie	Gestion de la classe de données «Données de messagerie»
8	Fonction Gestion des données en masse	Gestion de la classe de données «Données en masse»
9	Fonction Gestion des données de flux	Gestion de la classe de données «Données de flux»

Le Tableau 6 donne un exemple des sous-fonctions qui sont pertinentes pour la FBS de la GCG.

Tableau 6 – Exemple de la décomposition fonctionnelle de la GCG

N°	Fonction	Description
1	Processeur frontal de liaison radio	
2	Interface Internet avec pare-feu	
3	AAA (authentification, autorisation, comptabilité)	
4	DDNS (serveur de noms de domaine dynamique)	
5	Cryptage et décryptage de données	Cette fonctionnalité peut sinon être fournie au niveau application
6	IDS (système de détection d'intrusion)	

4.6 Passerelle de communication mobile

4.6.1 Architecture

4.6.1.1 Généralités

Tout dispositif embarqué, supportant une fonction, qui doit communiquer avec une fonction hébergée par un système au sol, doit utiliser l'une des deux options architecturales possibles:

Option 1: unité de communication partagée devant être utilisée par un(e) ou plusieurs dispositifs/fonctions embarqué(e)s.

Option 2: unité de communication dédiée devant être utilisée par un(e) seul(e) dispositif/fonction spécifique.

4.6.1.2 Option 1: unité de communication partagée

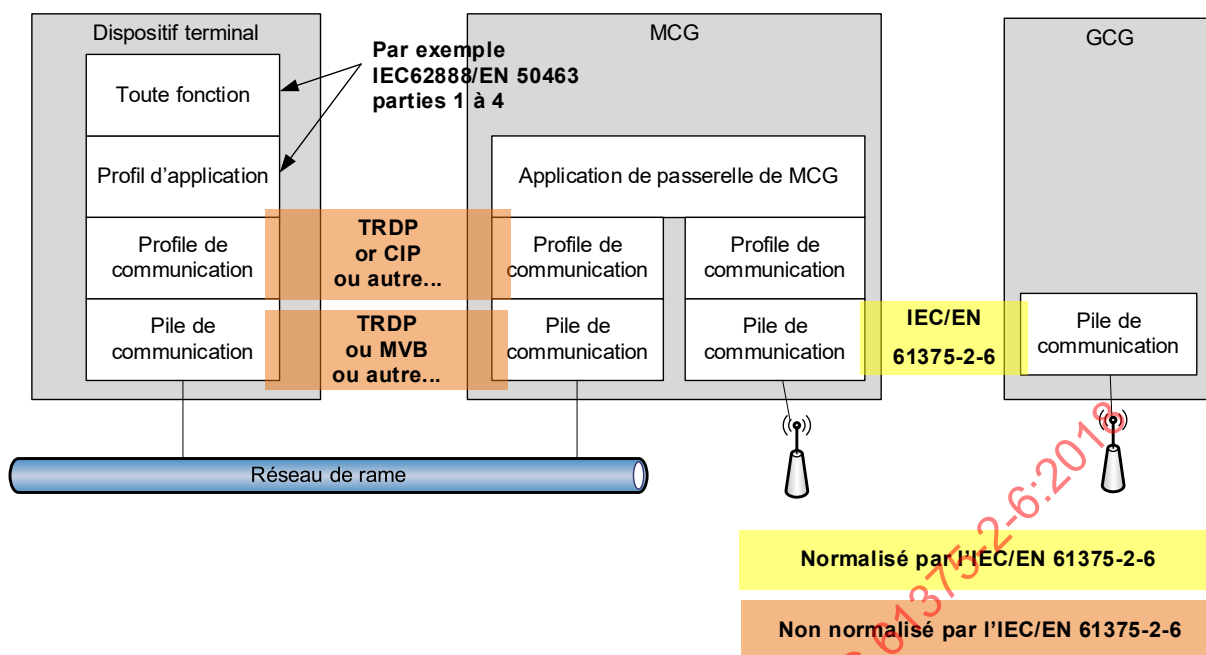
Lorsque cette option est retenue, la fonction supportée par le dispositif embarqué communique, en utilisant une interface de dispositif terminal sur le réseau de rame, avec la MCG qui offre des services de communication train-sol comme un routeur ou une passerelle.

La Figure 3 présente l'architecture en couches du dispositif terminal embarqué et de la MCG communiquant sur le réseau de rame. La Figure 3 présente les références aux parties de la série relative au TCN qui spécifient les exigences applicables à chaque couche.

Une fonction désigne toute fonction TCMS ou OMTS qui est supportée par le dispositif terminal. Un seul dispositif terminal peut supporter plusieurs fonctions; dans un souci de clarté, l'architecture en couches sur la Figure 3 ne présente qu'une seule fonction.

La fonctionnalité de passerelle doit être utilisée lorsque le dispositif embarqué souhaite établir une connexion pendant que le train est à l'état opérationnel normal et/ou automatique. Dans ce cas, le système au sol ne peut pas avoir un accès direct au dispositif terminal embarqué; l'application de passerelle de MCG fournit le niveau de sécurité requis au moyen de services d'authentification, d'autorisation et de cryptage.

La fonctionnalité de routeur peut être utilisée pour un train à l'état de mise en service ou de maintenance ou lorsque les exigences de communication d'application le requièrent (par exemple CCTV) et que des méthodes de sécurité appropriées sont déployées. Dans ce cas, un accès direct du système au sol au dispositif embarqué est accepté.



IEC

Figure 3 – Option 1: communication dispositif terminal embarqué-sol via MCG

4.6.1.3 Option 2: unité de communication dédiée

Lorsque cette option est retenue, la fonction supportée par le dispositif embarqué communique, en utilisant une interface sans fil intégrée, avec la fonction supportée par le système au sol.

L'architecture en couches du dispositif terminal est présentée sur la Figure 4.

Une fonction désigne toute fonction TCMS ou OMTS qui est supportée par le dispositif terminal. Un seul dispositif terminal peut supporter plusieurs fonctions; dans un souci de clarté, l'architecture en couches sur la Figure 4 ne présente qu'une seule fonction.

La pile sans fil doit fournir des services de communication avec le niveau de sécurité pertinent en fonction de l'état du train, en garantissant qu'aucun accès direct au dispositif embarqué n'est accepté sur le système au sol lorsque le train est en mode opérationnel ou automatique. L'accès doit être fourni par des services de communication qui garantissent le niveau de sécurité requis par authentification, autorisation et cryptage.

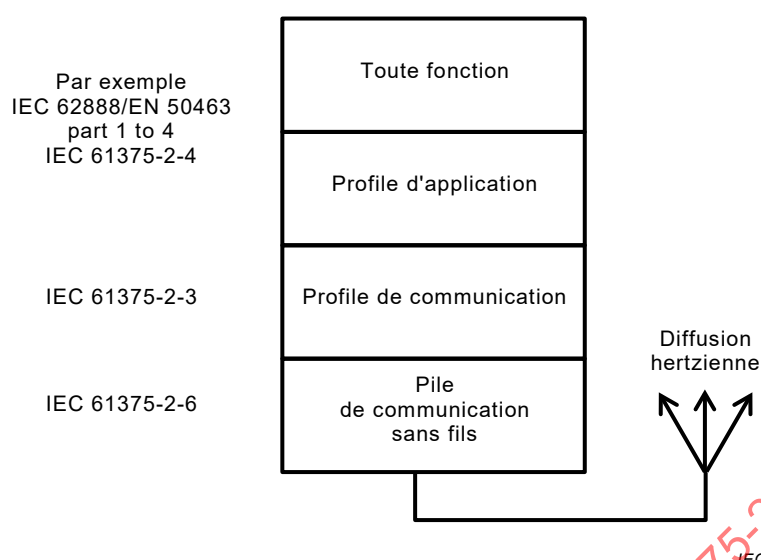


Figure 4 – Option 2: communication dispositif terminal embarqué-sol via une interface dédiée

4.6.2 Passerelle de communication mobile

Un modèle abstrait d'une MCG est présenté sur la Figure 5. Le cœur de la MCG est un routeur d'accès mobile qui interconnecte des réseaux embarqués avec des réseaux au sol. Le modèle abstrait peut être mis en œuvre à l'aide de plusieurs architectures physiques (par exemple, une unité de traitement distincte accompagnée d'un routeur distinct ou un dispositif MCG entièrement intégré) à condition que les services et interfaces indispensables de la MCG soient assurés.

Vis-à-vis du sol, la MCG doit fournir une ou plusieurs interfaces radio, chacune étant associée à une technologie radio spécifique et chacune se connectant au réseau au sol.

Des exemples de technologies radio sont:

- GSM (et ses extensions HSCSD, GPRS, EDGE);
- UMTS (et ses extensions comme HSPA);
- LTE;
- WLAN, tel que spécifié dans l'IEEE 802.11.

NOTE 1 D'autres technologies appropriées peuvent être ajoutées dès qu'elles seront disponibles.

NOTE 2 Les différentes technologies mobiles peuvent être mises en œuvre dans un routeur d'accès mobile intégré à la MCG. Le routeur d'accès mobile peut se présenter sous la forme d'une unité autonome.

Les exigences pour traiter la sélection d'interfaces radio pour une communication de données sont spécifiées en 4.9.

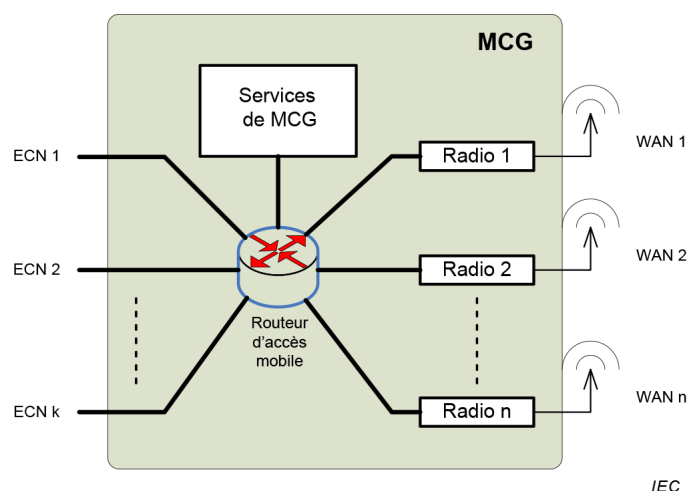


Figure 5 – Schéma fonctionnel du modèle abstrait de MCG

Vis-à-vis du réseau embarqué, la MCG doit fournir au moins une interface permettant la connexion au réseau embarqué, par exemple un ECN. En cas de multiples réseaux de rame dans une rame, la MCG peut prendre en charge plusieurs interfaces, une interface pour chaque réseau de rame.

NOTE 3 Une mise en œuvre minimale d'une MCG fournit une seule interface embarquée et une seule interface radio, par exemple un WLAN.

Outre le routeur d'accès mobile, la MCG prend en charge des services de MCG, exécutés sur une plateforme de services qui est connectée au routeur d'accès mobile. Ces services sont utilisés pour établir et prendre en charge la communication train-sol et sont également importants pour des aspects de sécurité. Les services fournis par la plateforme de services de MCG sont définis en 4.9.

Pour prendre en charge la sécurité, la MCG fournit un pare-feu entre:

- les interfaces radio (pour contrôler le flux de données entre différentes porteuses radio);
- les interfaces radio et les interfaces embarquées (pour contrôler le flux de données entre le train et le sol);
- les interfaces embarquées (pour contrôler le flux de données entre des réseaux de rame embarqués qui relèvent de différentes zones de sécurité).

Les détails sur le pare-feu et les autres mesures de sécurité sont définis en 4.9.

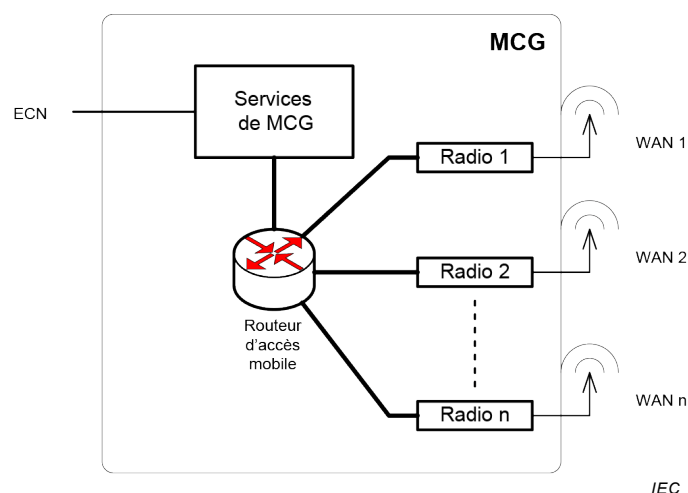


Figure 6 – MCG configurée comme une ALG

La Figure 6 présente un modèle abstrait de la façon dont la MCG peut agir comme une ALG. La fonctionnalité de passerelle est gérée dans le périmètre des services de MCG, ces derniers agissant comme un intermédiaire entre l'ECN et le côté sol.

4.7 Redondance de communication mobile

4.7.1 Généralités

La Figure 7 décrit un exemple d'une architecture train-sol permettant de fournir une redondance de communication mobile:

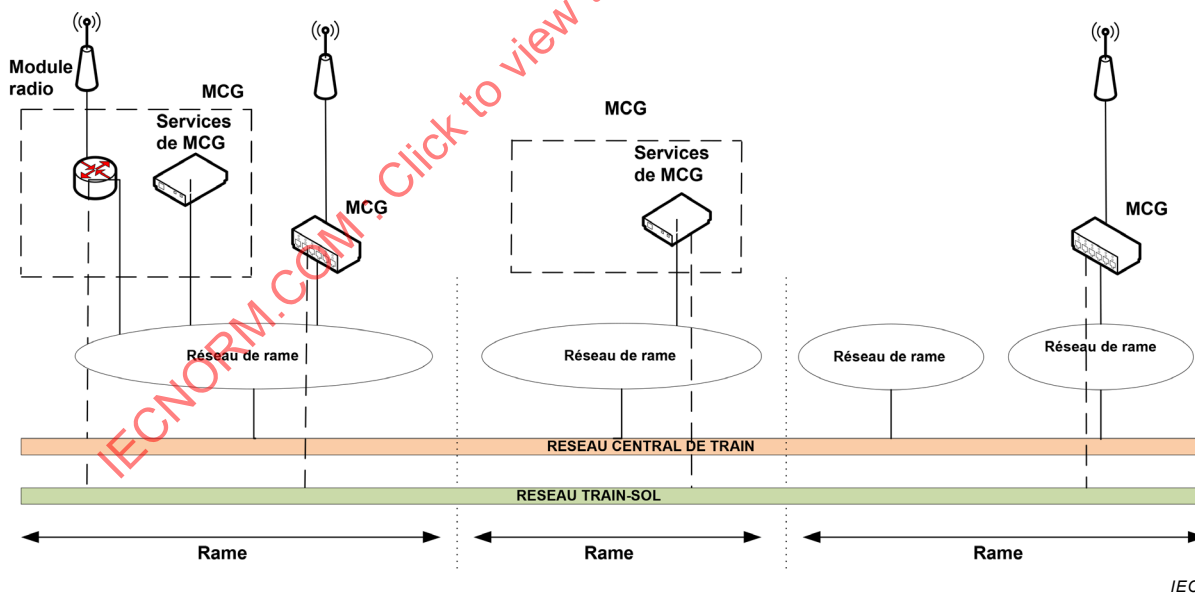


Figure 7 – Exemple d'architecture de communication train-sol redondante

Les caractéristiques suivantes de cet exemple peuvent être identifiées:

- Une rame peut comporter un ou plusieurs réseaux de rame.
- Un réseau de rame peut comporter zéro ou plusieurs MCG. De manière à pouvoir utiliser une communication train-sol, il est nécessaire qu'il y ait au moins une MCG par train.
- Une MCG peut être connectée aux réseaux suivants dans le train:
 - à un réseau de rame;

- à un réseau distinct (appelé ici «réseau train-sol») qui est distinct du réseau TCMS (par exemple: cela pourrait être un réseau OMTS).
- Une MCG contient en interne des composants tels que décrits en 4.6, par exemple:
 - des services de MCG;
 - un routeur d'accès mobile (MAR, de l'anglais Mobile Access Router);
 - une connexion à un module radio.

Les exigences de redondance pour la communication train-sol dépendent des besoins des applications à prendre en charge. Deux approches peuvent être utilisées à cet égard:

- redondance à efficacité totale, voir 4.7.2;
- redondance à efficacité partielle, voir 4.7.3.

4.7.2 Redondance à efficacité totale

La redondance fonctionnelle totale est obtenue par duplication de la MCG.

Deux architectures sont recommandées pour la redondance à efficacité totale:

a) Réserve passive

Cette architecture fournit deux MCG identiques. L'une est active et l'autre est désactivée. Lorsque la MCG active tombe en panne, une intervention manuelle est nécessaire de manière à désactiver l'unité défaillante et à activer l'unité redondante. Il est à noter qu'une telle opération peut exiger des conditions maîtrisées pour être effectuée, par exemple un train stoppé en gare.

b) Réserve semi-active

Cette architecture fournit deux MCG identiques. L'une est active et l'autre est désactivée et surveille la communication sur le réseau de rame sans offrir de service aux dispositifs terminaux. Lorsque la MCG active tombe en panne, une unité de sélection détecte la défaillance, désactive la MCG défaillante et active l'unité redondante. Il convient que cet événement soit détecté par l'application qui est en charge de rétablir la liaison de communication avec le système au sol.

4.7.3 Redondance à efficacité partielle

Cette architecture fournit deux MCG identiques localisées dans deux rames/véhicules différent(e)s du même train. Les deux MCG sont actives. Les applications embarquées utilisent les services de la MCG qui est rattachée au même réseau de rame.

Lorsqu'une MCG tombe en panne, l'application utilisant cette MCG souscrit des services sur la deuxième MCG, qu'il atteint via le réseau central de train.

4.8 Modifications de la composition d'un train

Les modifications de la composition d'un train sont supervisées par le service Informations sur le train (TIS, de l'anglais Train Information Service). Le TIS fournit une interface permettant d'informer la GCG des informations actuelles sur le train et des modifications de ces informations. Le TIS peut utiliser la base de données topologiques de train (TTDB) qui est une bibliothèque de données pour toutes les informations relatives à la composition réelle du train et à l'état réel de l'ETB.

Il est nécessaire qu'il y ait au moins un TIS actif par train. Les exigences de redondance pour le TIS dépendent des besoins des applications à prendre en charge.

L'état de mise en œuvre du TIS au niveau du dispositif ou de la composition est synthétisé dans le Tableau 7 et dans le Tableau 8:

Tableau 7 – Dispositif – Etat de mise en œuvre du TIS

Dispositif	Mise en œuvre
Dispositif terminal	Facultatif
MCG	Obligatoire

Tableau 8 – Composition – Etat de mise en œuvre du TIS

Composition	Mise en œuvre
rame	Facultatif
Train	Obligatoire

Dans un «train réel totalement fonctionnel», au moins un dispositif exécutant une instance du TIS doit être disponible à bord. La redondance du TIS peut être gérée au niveau du train.

La TTDB est spécifiée dans l'IEC 61375-2-3. Un autre exemple de base de données topologiques de train est le répertoire d'adresses et d'attributs de nœuds (NADI, de l'anglais Node Address and Attribute Directory) conformément à la fiche UIC 556.

Le TIS permet à la GCG de récupérer des informations sur la composition réelle du train.

Le TIS fournit également, par l'intermédiaire de la MCG, un service de notification concernant les modifications de la composition du train.

Le 6.3.3 décrit en détail les exigences du TIS.

4.9 Sécurité

4.9.1 Zones de sécurité

L'architecture de sécurité d'un système de communication train-sol peut être modélisée selon le concept de «zones» et de «conduits» tels que définis dans l'IEC 62443. Une zone est définie comme un regroupement d'actifs logiques ou physiques qui partagent des exigences de sécurité communes. Si l'équipement dans la zone a un niveau de sécurité non supérieur ou égal au niveau exigé, des mesures de sécurité complémentaires doivent être prises. Chaque zone peut être définie plus précisément par un document de définition de zone qui spécifie les exigences de sécurité d'une zone.

Il est essentiel que la communication entre zones n'ait lieu que par le biais de conduits définis. Les conduits mettent en œuvre les mesures de sécurité qui sont nécessaires pour contrôler l'accès à la zone, empêcher les attaques par déni de service (DoS), éviter le transfert de programmes malveillants et protéger l'intégrité du trafic du réseau et, si besoin, la confidentialité. Généralement, les mesures de sécurité mises en œuvre dans les conduits visent à limiter la différence entre les capacités en termes de niveau de sécurité d'une zone et ses exigences de sécurité.

Un niveau de sécurité (SL) doit être assigné à chaque zone et à chaque rame. Le niveau de sécurité doit être déterminé à partir d'une analyse de sécurité et suivant les recommandations et les profils ferroviaires spécifiques donnés dans l'IEC 62443-3-3, tels que ceux donnés par exemple dans la DIN VDE V 0831-104.

Un modèle de zone simplifié de l'architecture train-sol est présenté sur la Figure 8.

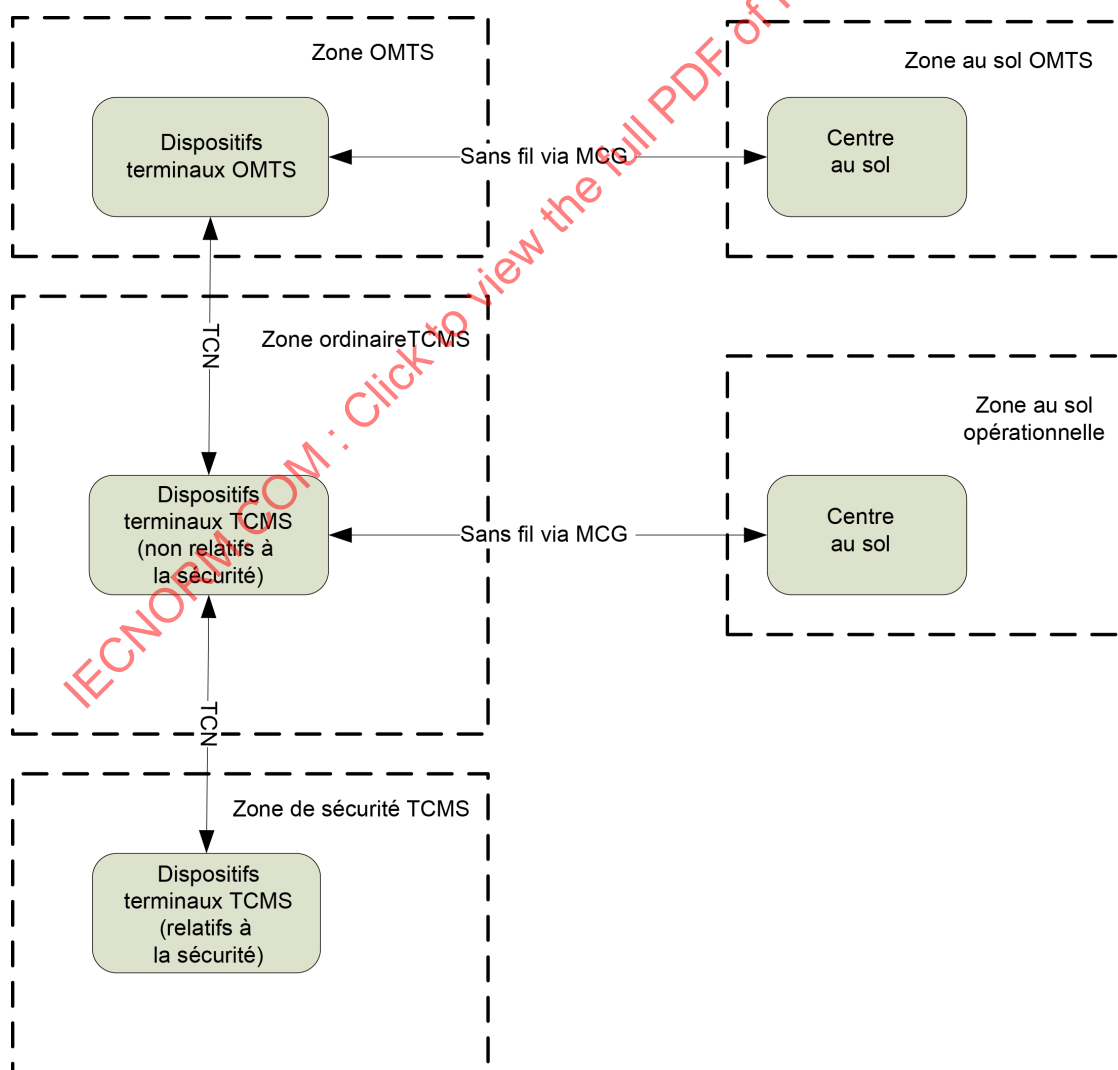
Les zones suivantes sont identifiées à bord des trains:

- La zone de sécurité TCMS, chargée de gérer les données critiques du point de vue de la sécurité et de l'exploitation (par exemple freins, portes). La zone de sécurité est généralement intégrée dans le réseau embarqué opérationnel tel que défini dans l'IEC 61375-2-3.
- La zone ordinaire TCMS, chargée de gérer les données non relatives à la sécurité (par exemple, diagnostics, système de chauffage, ventilation et climatisation). La zone ordinaire est généralement intégrée dans le réseau embarqué opérationnel tel que défini dans l'IEC 61375-2-3.
- La zone OMTS, chargée de gérer les données orientées services multimédias et télématiques. La zone OMTS est généralement intégrée dans le réseau embarqué multimédia tel que défini dans l'IEC 61375-2-3.

Les mesures homologues pour le côté sol pourraient être par exemple:

- une zone de centre opérationnel, chargée de gérer les données de contrôle d'exploitation;
- la zone de centre OMTS, chargée de gérer les données orientées services multimédias et télématiques.

Dans la plupart des cas, il y aura plus de zones au sol, par exemple des zones pour les centres, mais aussi une zone pour le réseau Internet ouvert. Les zones au sol ne relèvent pas du domaine d'application du présent document.



IEC

Figure 8 – Zones de sécurité (simplifiées)

NOTE Il n'existe aucun conduit entre la zone de sécurité TCMS et le sol, ce qui signifie qu'il ne peut y avoir aucun échange de données relatives à la zone de sécurité entre le train et le sol.

L'IEC 61375-2-3 requiert que la zone de sécurité TCMS appartienne à un système fermé tel que défini dans l'IEC 62280. Du fait que la zone de sécurité TCMS et la zone ordinaire TCMS partagent normalement le même réseau de rame, la MCG connectant la zone ordinaire TCMS à la zone au sol opérationnelle doit être conçue de manière à ce que les conditions de système fermé ne soient pas violées.

4.9.2 Mesures de sécurité

Les mesures de sécurité qui sont applicables aux conduits connectant un train avec le sol sont répertoriées dans le Tableau 9.

Tableau 9 – Mesures de sécurité

Mesure de sécurité	Prise en charge par	Description
Pare-feu	MCG	Un pare-feu entre deux réseaux permet de filtrer les paquets IP selon leur contenu, par exemple: • Adresse IP source • Adresse IP destinataire • Numéro de port UDP/TCP source • Numéro de port UDP/TCP destinataire • Identifiant ComID TRDP La MCG commence par s'authentifier avant de fournir un mécanisme de filtrage des paquets d'adresses IP en fonction du contenu, ce qui signifie qu'elle prend en charge le suivi de connexion, par exemple des sessions TCP et UDP. Avec un suivi de connexion, elle peut par exemple empêcher l'ouverture d'une session à partir d'un réseau non fiable.
PNAT	MCG	Traduction en adresses de port et de réseau. Cette caractéristique évite que les adresses IP et numéros de ports de dispositifs ED réels dans un réseau de confiance ne soient vus dans un réseau non fiable. Cette caractéristique est souvent prise en charge par des mises en œuvre de pare-feu.
Authentification et autorisation	MCG GCG	Un dispositif au sol (par exemple, une GCG) tentant de se connecter à la MCG doit tout d'abord s'authentifier avant de se voir accorder l'accès à des services de MCG. La procédure d'authentification dépend de la technologie radio utilisée (par exemple, SIM, IEEE 802.1X). L'authentification doit être appliquée soit par l'application (par exemple, par le protocole TLS 1.2 avec authentification mutuelle), soit au niveau du réseau (par exemple, en utilisant un protocole IPSEC/IKEv2 ou SSL-VPN avec authentification mutuelle).
Cryptage	MCG GCG ED	Il convient de crypter les données échangées et de protéger leur intégrité en utilisant des normes établies comme TLS 1.2 ou HTTPS.
VPN	ED	Un VPN entre ED de confiance inclut une authentification ainsi qu'un cryptage des données transférées. L'établissement d'un VPN entre un ED au sol et la MCG sera dans la plupart des cas suffisant pour une communication train-sol.

Mesure de sécurité	Prise en charge par	Description
ALG	MCG	Une ALG entre deux réseaux quelconques permet un contrôle total des données échangées. Depuis chaque réseau, une ALG est vue comme un ED, de sorte que l'ALG endosse le rôle de serveur proxy pour chaque fonction qu'elle exécute sur un ED «caché». La MCG agit comme une ALG pour les services de communication de données de messagerie et de transfert de fichiers.
Etablissement d'un registre d'événements de sécurité	MCG GCG	Les événements relatifs à la sécurité sont consignés dans un registre. Il convient que les événements relatifs à la sécurité incluent: - les tentatives d'authentification (validées et non validées) les modifications d'authentifiants - l'activation/la désactivation/la reconfiguration de pare-feu - les événements de pare-feu (par exemple, accès à des adresses IP ou à des ports sur liste noire) - le trafic entrant non prévu - les événements de DHCP (par exemple, identifiant d'hôte inconnu) - les événements liés à l'heure système (par exemple, mise à jour)
Mises à jour de sécurité	MCG GCG ED	La surveillance des vulnérabilités de sécurité (SVM) et les mises à jour de sécurité sont essentielles pour garantir la sécurité à long terme des composants. Il doit être également possible de mettre à jour les composants en appliquant des correctifs de sécurité en temps opportun (en local ou diffusion hertzienne). Les composants doivent vérifier l'intégrité et l'authenticité des mises à jour logicielles par une évaluation des signatures cryptographiques.

4.9.3 Modèle pour authentification, autorisation et comptabilité

Le modèle identifie les composants uniques qui sont essentiels dans une interaction de système générale:

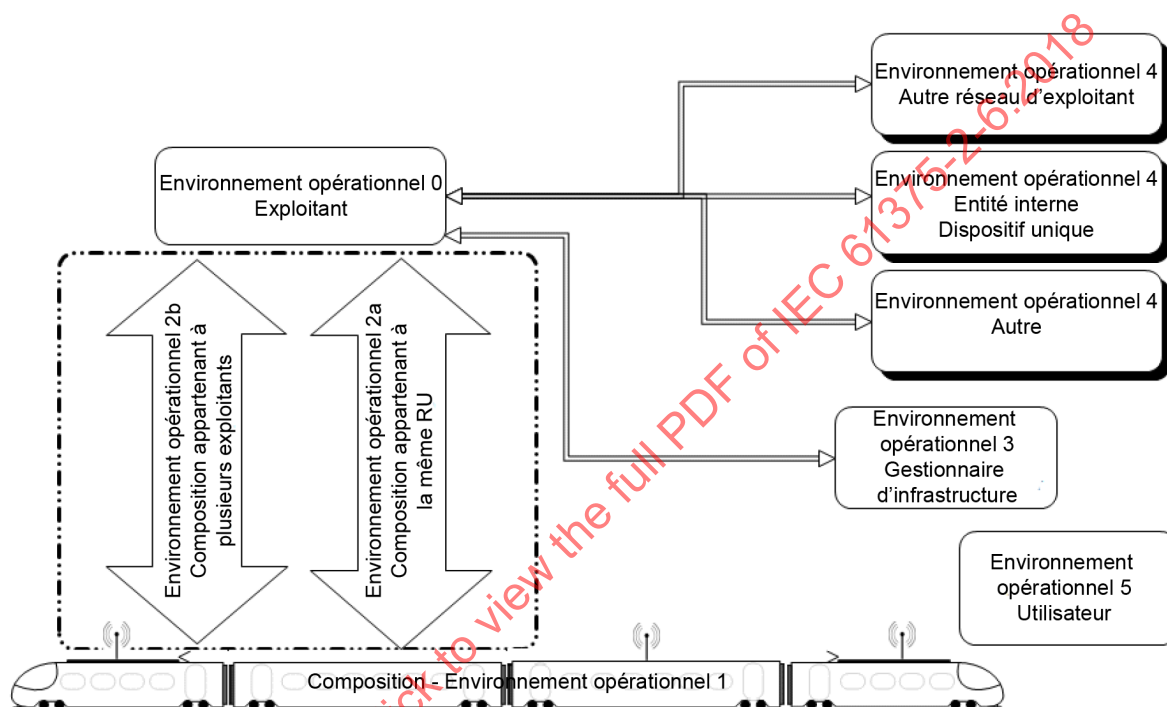
- la composition se déplaçant sur la voie;
- l'infrastructure de l'exploitant, constituée de ses différents composants uniques;
- l'infrastructure au sol, sauf pour le système de signalisation;
- l'utilisateur qui intervient sur la composition ou au dépôt (conducteur, agent de maintenance, agent de mise en service, etc.);
- les services actifs à bord et au sol.

Le modèle considère les différents canaux de communication qui sont supposés être utilisés dans un scénario de communication type (par exemple, communication sans fil ou filaire).

Un identifiant (de 1 à 5) est associé à chaque liaison de communication qui peut être considérée comme un «environnement opérationnel», voir Figure 9. Chaque environnement opérationnel sert à son tour de base pour l'identification de cas d'utilisation de communication et peut être résumé à ce qui suit:

- Environnement opérationnel 0 – Communication à l'intérieur d'un seul réseau central d'exploitant utilisant des pratiques TI standard
- Environnement opérationnel 1 – Liaison de communication à l'intérieur du train – canal sans fil ou filaire

- Environnement opérationnel 2 – Liaison de communication composition-exploitant – canal sans fil
- Environnement opérationnel 2a – L'infrastructure composition-exploitant appartient au même exploitant
- Environnement opérationnel 2b – L'infrastructure composition-exploitant appartient à plusieurs exploitants
- Environnement opérationnel 3 – Liaison de communication au sol – canal sans fil ou filaire
- Environnement opérationnel 4 – Liaison de communication entre exploitants – canal filaire
- Environnement opérationnel 5 – Liaison de communication d'utilisateur – canal sans fil



IEC

Figure 9 – Modèle pour authentification, autorisation et comptabilité

En considérant le système intégré global, il est nécessaire que chaque composant du système soit authentifié et autorisé pour faire partie du réseau. De manière à contrôler la constitution du système intégré et des composants admis, il est important de reconnaître et d'authentifier les nœuds uniques (par exemple, composition ou dispositif), les éléments uniques, mais aussi les applications fournies afin de gérer et d'évaluer ce qui pourrait se trouver dans le système. Dans tous les cas, le modèle adopté pour le système est également destiné à accorder l'extensibilité de la solution de sécurité et notamment du modèle authentifié. Etant donné que des nœuds, applications et utilisateurs pourraient être répartis, il est nécessaire d'adopter et d'utiliser une solution d'authentification qui peut prendre en charge une approche de répartition avec un maximum de flexibilité.

L'accès aux ressources internes de la composition se fait par le biais de la MCG.

Les trains à composition variable, le large éventail de profils de mission et les connexions en zone frontalière posent certaines questions concernant l'accès aux informations disponibles à bord du train. Un exemple de cette problématique est donné ci-dessous pour les données de maintenance:

- Une RU doit avoir accès à tous les équipements qu'elle a achetés, mais pas aux équipements qu'elle n'a pas achetés.

- Les fabricants d'équipements doivent avoir accès aux équipements qu'ils ont vendus, si la RU le permet.
- Un fabricant d'équipements ne doit pas avoir accès aux données d'autres fabricants, sauf s'il a obtenu les droits d'accès associés.

Les procédures de dépannage doivent être partagées entre les différentes entités, mais les données de fiabilité sont certainement des informations à caractère «privé».

Le modèle fourni doit octroyer différents niveaux de droits d'accès selon l'utilisateur et selon les données conservées ou fonctions/applications disponibles. Pour cette raison, il est nécessaire d'associer à chaque utilisateur un ensemble d'informations relatives aux rôles qu'il peut endosser, aux ressources ou fonctionnalités auxquelles il peut avoir accès et au niveau d'opérations qu'il peut effectuer sur l'accès requis (par exemple, lecture, exécution, etc.). Il convient également que les données soient classées et mises à jour de telle sorte que le système soit en permanence en mesure d'indiquer qui détient le droit d'accès à ces données.

En outre, il est possible d'établir une méthode de signature ad hoc et/ou cryptographique pouvant être invoquée sur demande d'un utilisateur ou d'une application qui peut réellement protéger les données transmises de toute modification externe ou d'une simple lecture.

Les dispositifs et exigences d'adressage fonctionnel sont détaillés à l'Article 8.

La fonction AAA gère localement pour chaque utilisateur les différents profils d'accès définis par la politique générale de la RU. La méthode AAA fondée sur des jetons permet de valider une identité d'utilisateur lorsque la composition n'est pas connectée au réseau de la RU.

4.9.4 Classification du réseau et des MCG

4.9.4.1 Catégories

L'IEC 62280 définit trois catégories de systèmes de transmission. La catégorie 1 est définie comme un système de transmission fermé, alors que les catégories 2 et 3 sont des systèmes de transmission ouverts.

Il est à noter que l'IEC 61375-3-4 et l'IEC 61375-2-3 ne définissent aucune mesure de sécurité particulière (par exemple, authentification ED et cryptage des données à utiliser dans le réseau embarqué opérationnel). Le réseau embarqué opérationnel, s'il est utilisé pour la transmission de données relatives à la sécurité, est considéré comme un système de transmission fermé de catégorie 1 selon l'IEC 62280.

Le réseau multimédia embarqué peut être, en fonction des services et mesures de sécurité qu'il offre, un système de transmission de catégorie 2 ou 3, c'est-à-dire un système ouvert.

Selon le rôle de la MCG, par exemple si elle connecte le réseau opérationnel embarqué ou le réseau multimédia embarqué avec le sol, il doit être garanti que les catégories associées seront conservées.

D'après la définition des catégories de systèmes de transmission, la MCG peut être classée de la même manière selon les catégories répertoriées dans le Tableau 10.

Tableau 10 – Catégories de MCG

MCG de catégorie 1	MCG qui connecte un système de transmission fermé à un système de transmission ouvert (Exemple: connectant un réseau opérationnel ou un réseau opérationnel/multimédia combiné avec le sol)
MCG de catégorie 2	MCG qui connecte un système de transmission ouvert de catégorie 2 à un système de transmission ouvert de catégorie 2/3 (Exemple: connectant un réseau multimédia avec le sol)
MCG de catégorie 3	MCG qui interconnecte des systèmes de transmission de catégorie 3 (Exemple: routeurs Internet)

Les paragraphes suivants définissent des mesures de sécurité pour une MCG de catégorie 1.

Les MCG de catégories 2 et 3 ne relèvent pas du domaine d'application du présent document.

4.9.4.2 MCG en tant que barrière de système fermé (MCG de catégorie 1)

Les caractéristiques d'un système de transmission fermé (système de transmission de catégorie 1) (voir Tableau 10) sont définies de la manière suivante:

- Le nombre d'équipements individuels pouvant être connectés (qu'ils soient associés à la sécurité ou non) au système de transmission est connu et fixe.
- Les caractéristiques physiques du système de transmission (par exemple, support de transmission, environnement conforme à l'hypothèse de conception, etc.) sont fixées et restent inchangées pendant la durée de vie du système.
- Le risque d'accès non autorisé est jugé négligeable.

Les exigences de sécurité de la MCG, telles que dérivées des caractéristiques répertoriées, sont indiquées dans le Tableau 11.

Tableau 11 – Exigences de sécurité

N° d'exigence	Exigence
S1	La MCG doit être le point final de la liaison de communication entre le train et le sol.
S2	La MCG doit également marquer la limite des réseaux de rame du train, par exemple MVB et Ethernet (ECN).
S3	La MCG doit fournir une fonction de pare-feu qui protège le réseau opérationnel embarqué.
S4	Une fois la connexion au canal établie (selon l'exigence 21), la MCG ne doit autoriser l'établissement d'une connexion depuis le sol qu'à des ports bien définis (par exemple, port 80).
S5	En mode de fonctionnement normal, il ne doit pas être possible d'accéder par protocole SSH à la MCG depuis le sol. L'accès par protocole SSH peut être bloqué par le pare-feu.
S6	La MCG ne doit pouvoir communiquer qu'avec un ensemble connu de dispositifs au sol authentifiés et enregistrés.
S7	La MCG ne doit pas envoyer de messages relatifs à la sécurité à une installation au sol.
S8	La MCG doit être capable de recevoir les mises à jour/correctifs de sécurité.
S9	La MCG doit vérifier l'intégrité et l'authenticité des mises à jour logicielles par une évaluation des signatures cryptographiques.

NOTE Au sein du réseau opérationnel, les MCG sont considérées comme des dispositifs terminaux. Depuis le sol, les MCG sont les seuls points de visibilité pour le réseau opérationnel embarqué.

4.9.4.3 MCG connectant à la fois catégorie 1 et catégorie 2/3

Une MCG peut être utilisée pour connecter à la fois des systèmes de transmission de catégorie 1 et des systèmes de transmission de catégorie 2/3 comme cela est illustré dans l'exemple de la Figure 10.

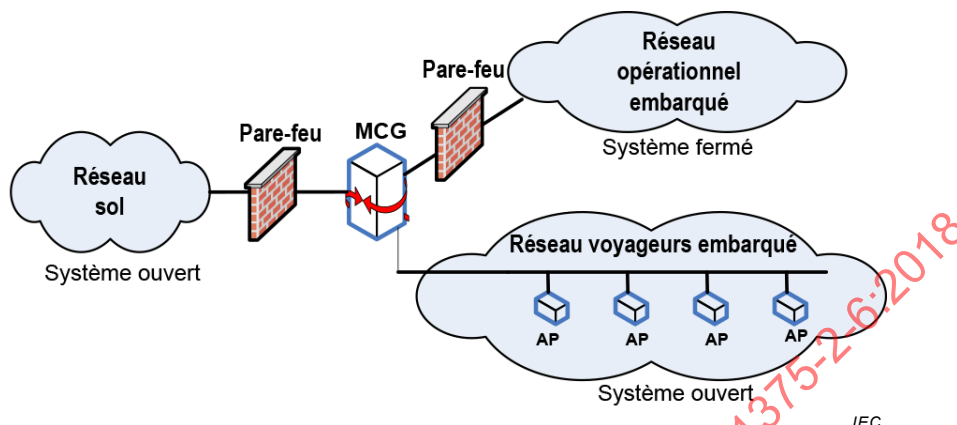


Figure 10 – MCG connectant des systèmes de transmission ouverts et fermés

Dans ce cas, la MCG doit agir comme une MCG de catégorie 1 envers le système fermé.

Cela signifie aussi en particulier qu'il ne doit y avoir aucune possibilité de changer la configuration de la MCG à partir de l'un des systèmes ouverts.

EXEMPLE Le pare-feu dans la MCG est configuré pour bloquer la totalité du trafic direct entre les systèmes ouverts et le système fermé (tout se terminant dans la plateforme de services de MCG), mais est plus ouvert pour le trafic entre les systèmes ouverts.

5 Référentiel de communication

5.1 Généralités

Le référentiel de communication train-sol définit les fonctions de base et les concepts de base qui sont nécessaires pour établir et maintenir la communication sécurisée et fiable entre les dispositifs embarqués et les dispositifs (par exemple, ordinateurs, serveurs) au sol.

Cela traite notamment des aspects suivants dans le contexte de l'architecture de réseau de communication mobile, voir également 4.3:

- MCG en tant qu'architecture de service de courtage, voir 5.2.
- Adressage, voir 5.3.
- Classes de données, voir 5.4.
- Protocoles de communication, voir 5.5.
- Services de communication, voir 5.6.

Etant donné que la MCG est le dispositif embarqué qui gère la partie embarquée de la communication train-sol, tous ces aspects seront associés à la MCG et au système de communication embarqué sous-jacent. Le système de communication au sol étant assez hétérogène et dépendant principalement de l'infrastructure des exploitants ferroviaires et des fournisseurs de réseau cellulaire, ces systèmes ne sont donc considérés que de manière abstraite.

5.2 Architecture de service de courtage via MCG

La Figure 11 présente une vue d'ensemble des services que la MCG fournit pour les applications embarquées.

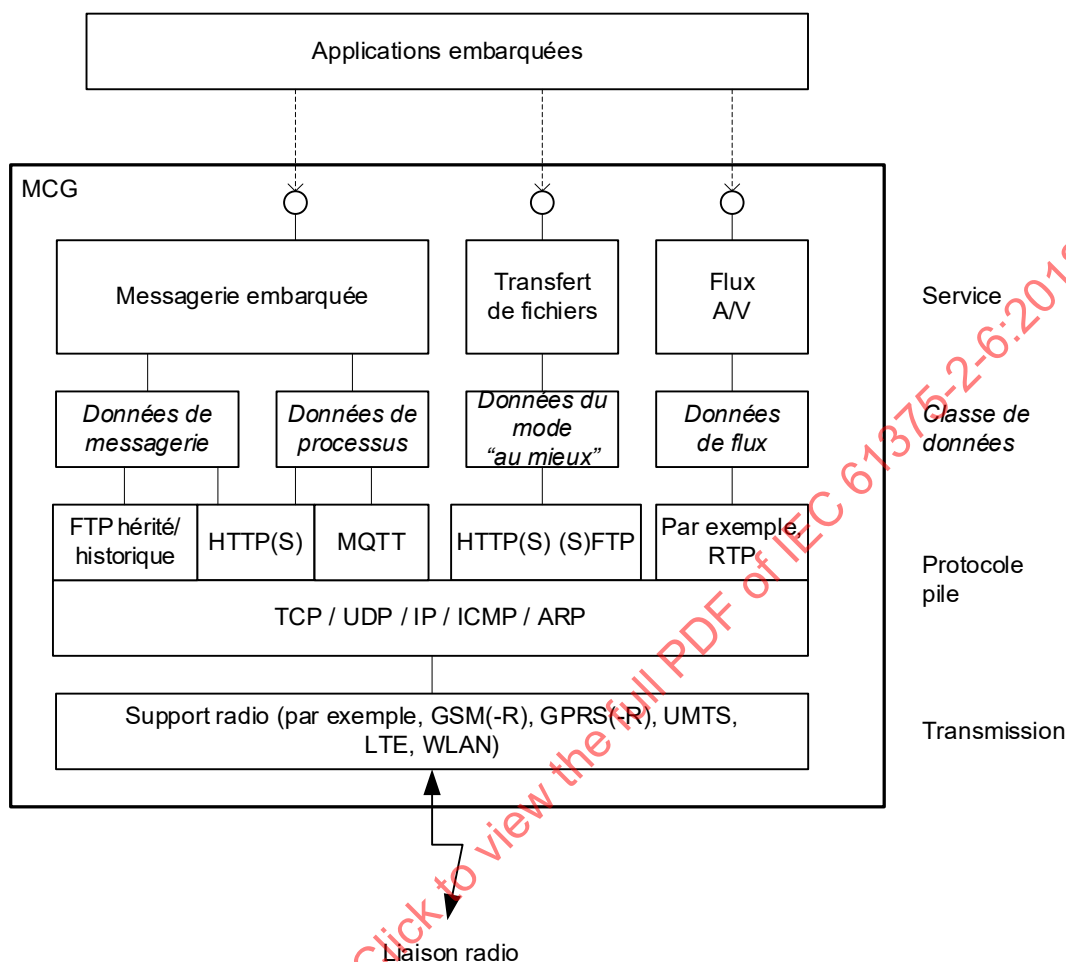


Figure 11 – Architecture de service de courtage via MCG

En fonction des exigences fonctionnelles, les applications embarquées peuvent utiliser un ou plusieurs des services de communication suivants:

- service de messagerie embarqué pour un échange d'informations cyclique ou basé sur un événement (par exemple, événements de diagnostic ou télémétrie);
- service de transfert de fichiers pour des fichiers de données complets (par exemple, données de facturation d'énergie);
- service de diffusion en flux (streaming) audio/vidéo (par exemple vidéo ou voix).

Les classes de données utilisées dépendent des exigences fonctionnelles de l'application.

Les protocoles utilisés sont basés sur des protocoles Internet standard (par exemple, IP, TCP, UDP, FTP, HTTP, DHCP, DDNS).

Les supports radio utilisés (par exemple, GSM, UMTS ou autres) ne sont pas couverts par le domaine d'application du présent document.

5.3 Concept d'adressage

5.3.1 Cas d'utilisation

Pour l'adressage d'une composition de train, les cas d'utilisation suivants doivent être pris en charge:

- accès à une rame spécifique indépendamment de l'endroit où se trouve la rame;
EXEMPLE Demande d'informations d'état auprès d'une rame ayant l'ID «50 80 89 – 43 501 – 2».
- accès à un parcours de train spécifique, indépendamment des rames et de la composition des trains. Cela signifie que le train est déclaré prêt pour le service programmé et lié à un unique ID de parcours de train.

EXEMPLE Téléchargement d'informations sur les horaires dans le train avec l'ID de parcours de train ES9558.

5.3.2 Identification de rame et de train

Chaque rame est supposée disposer de son propre identifiant unique, lequel, dans la plupart des cas, est dérivé de son ID de rame.

Cet identifiant unique correspond au paramètre '*cstId*' défini dans l'IEC 61375-2-3. Ces identifiants sont par exemple alloués par ERA ou OTIF.

Une composition de train, formée en connectant des rames pour un parcours de train, doit être identifiable par un identifiant de parcours de train unique.

Il n'est pas nécessaire que cet identifiant de parcours de train unique corresponde au paramètre '*trnId*' défini dans l'IEC 61375-2-3.

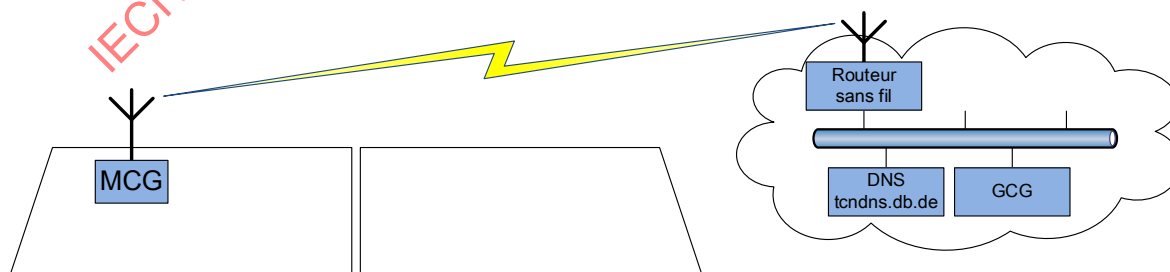
5.3.3 Frontières du réseau T2G

Le réseau entre le train (ou, mieux, la rame) et le sol est principalement constitué par la MCG agissant en tant que dispositif terminal du train et par la GCG agissant en tant que dispositif terminal du réseau sol.

NOTE L'échange d'informations structurelles sur le réseau induit des risques de sécurité.

5.3.4 Réseau minimal de base T2G

Les entités concernées sont présentées à la Figure 12, qui fournit une représentation simplifiée à un système minimal absolu.



IEC

Figure 12 – Configuration minimale du réseau train-sol

Le routeur sans fil est considéré transparent et supposé complet sur le plan technique. De même, la mobilité IP est gérée au sein de ce dispositif, lequel peut prendre la forme de n'importe quel type d'infrastructure WLAN allant jusqu'au fournisseur LTE.

Axiome du point de terminaison:

La MCG constitue essentiellement le point de terminaison vu du réseau attaché à la GCG et inversement, tel que spécifié en 5.3.3.

Cette distinction répond essentiellement à un besoin de sécurité et structure également l'organisation du réseau train-sol.

L'application de l'axiome du point de terminaison implique un autre axiome:

Aucun des réseaux n'échange d'autres informations concernant le DNS.

La combinaison de ces deux axiomes réduit considérablement la diversité des dénominations qui serait imposée par l'IEC 61375-2-3.

Autrement dit, des URI du type

`mcg.anyVeh.UIC94910101123.anyClTr.anyTrn.tcndns.db.de`

ne peuvent exister en raison de leur ambiguïté (liée aux parties `any*` de l'adresse) et le protocole TCP utilisé comme couche de transport HTTP ne prend pas en charge la diffusion/multidiffusion.

5.3.5 Adressage T2G

5.3.5.1 Adressage de rame

L'ambiguïté potentielle présentée en 5.3.4 est atténuée en privilégiant des noms d'hôte qui prennent en charge l'adressage du type URL HTTP.

La simplification suit le dernier raisonnement:

- Le seul dispositif vu du sol est une MCG, autrement dit le paramètre `mcg` n'est pas nécessaire.
- Un adressage de rame utilisant un ID de rame n'a besoin ni du paramètre `anyClTr` ni du paramètre `anyTrn`.
- L'adressage d'une voiture dédiée au moyen d'un URI pointe toujours vers la même MCG.

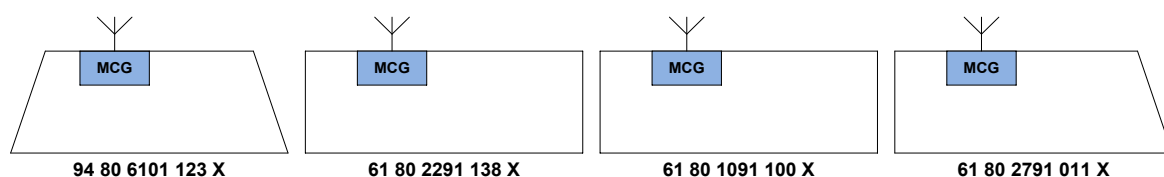
L'application conduit obligatoirement à passer à un identifiant d'hôte au format suivant:

<ID de rame>.tcndns.<domaine opérateur>

Par exemple, `UIC94806101123.tcndns.db.de`

5.3.5.2 Adressage de parcours de train

La fonction souhaitée pour l'adressage d'un parcours de train («train» au sens de l'IEC 61375-2-3) nécessite de mapper l'ID de parcours de train au véhicule de tête du train.



IEC

Figure 13 – Train composé de quatre véhicules

La Figure 13 présente une composition de train type.

Le mode d'adressage d'un train (ici EC41), en tant qu'alias du véhicule de tête, se présenterait sous forme concise, voir 5.3.5.3:

EC41.tcndns.db.de

Le modèle d'identifiant d'hôte requis est donc:

<ID parcours>.tcndns.<domaine opérateur>

NOTE Bien que la relation <train: rames> demeure importante, elle n'est pas résolue lors de la construction des identifiants d'hôtes suivants:

EC41.UIC94806101123.tcndns.db.de

EC41.UIC61802291138.tcndns.db.de

EC41.UIC61801091100.tcndns.db.de

EC41.UIC61802791011.tcndns.db.de

étant donné que les informations intrinsèques concernant le véhicule de tête (rame) n'existent pas dans ce modèle.

5.3.5.3 Inauguration du train, changement de direction

Il est nécessaire que les MCG évaluent l'événement d'inauguration du train (lequel est également déclenché par un changement de direction) afin de maintenir la cohérence des entrées DNS dans le cadre d'un adressage basé sur les adresses IP de parcours de train.

Chaque MCG d'un train a besoin de déterminer si elle doit ou non se trouver dans la rame de tête pour assurer la maintenance des entrées DNS basées sur l'adresse IP de parcours de train.

Les entrées DNS d'adressage de parcours de train pointent toujours vers la MCG principale. La disparition d'une entrée dans un DNS opérateur ne peut être couverte dans ce cas de figure.

L'attribution au train d'un ID de parcours de train, telle que décrite à la Figure 13, donne les résultats suivants:

a) Locomotive en tête:

EC41.tcndns.db.de et UIC94806101123.tcndns.db.de étant identiques en ce qui concerne l'adresse IP

b) Voiture pilote en tête:

EC41.tcndns.db.de et UIC61802791011.tcndns.db.de étant identiques en ce qui concerne l'adresse IP

La relation entre l'ID de parcours de train, les rames du train et le véhicule de tête peut être gérée par le mécanisme décrit en 4.8 et en 6.3.3.

5.3.5.4 ID de parcours de train en tant qu'élément de configuration variable

L'ID individuel de parcours de train constitue un élément de configuration pour chaque train (au sens de l'IEC 61375-2-3), lequel peut évoluer au fil du temps pour des questions d'exploitation de la RU.

Les MCG au sein du train ont besoin d'accéder à ces informations, qui à leur tour doivent être échangées à travers l'ensemble du train.

La mise en œuvre de ce mécanisme ne relève pas du domaine d'application de l'IEC 61375-2-6.

5.3.5.5 Unicité des ID de parcours de train dans le DNS

Les ID de rame sont uniques par nature; en revanche, l'ID de parcours de train n'est pas unique à proprement parler entre les différentes RU.

Les ID de parcours de train utilisés dans le *tcndns* doivent être uniques.

5.3.5.6 Extension du schéma URI TCN à un périmètre de DNS mondial

5.3.5.6.1 Zone DNS mondiale d'URI TCN

Pour intégrer un URI TCN dans un DNS mondial, un suffixe doit être ajouté à l'URI TCN. Ce suffixe doit commencer par un «tcndns» de zone DNS mondiale propre à l'URI TCN et se terminer par le nom de sous-domaine des exploitants ou des prestataires de maintenance conformément au Tableau 12.

Tableau 12 – Zone DNS mondiale d'URI TCN

Nom de zone DNS	Suffixe de zone DNS	Définition
tcndns	tcndns.railway.org	Cette zone DNS est utilisée pour intégrer tous les noms d'hôtes DNS TCN dans le DNS mondial. Le nom de sous-domaine «railway.org» doit être remplacé par le véritable nom de sous-domaine des exploitants ou des prestataires de maintenance. EXEMPLE 'tcndns.sncf.fr'

5.3.5.6.2 Résolution de noms dans un DNS T2G

Les règles suivantes doivent être appliquées pour la résolution de noms dans un DNS TCN:

- La zone DNS réservée par l'exploitant ferroviaire pour un DNS TCN, par exemple *tcndns.railway.org*, doit être déléguée au serveur de noms DNS TCN de la GCG.
- En raison de la nature dynamique et de la disponibilité des connexions entre la GCG et les MCG, les enregistrements des ressources (RR) DNS du domaine DNS *tcndns* doivent être configurés avec des valeurs permettant d'éviter une mise en antémémoire dans des serveurs DNS intermédiaires et de soumettre des demandes à des serveurs DNS TCN ou DNS faisant autorité.

5.3.6 URI HTTP

5.3.6.1 Modèle d'URI HTTP

Une communication train-sol telle que définie ici utilise HTTP(S) comme protocole de communication. Pour l'adressage de ressources, HTTP utilise un schéma «http-URI» comme défini dans les documents RFC 3986 et RFC 2616.

L'URI HTTP doit être conforme au modèle suivant (en utilisant le modèle d'identifiant hôte en 5.3.5.1 et en 5.3.5.2):

http-URI := "http://<autorité>/<chemin>"

autorité: est l'identifiant de l'hôte, correspondant au nom DNS TCN (voir 5.3.5.1 et 5.3.5.2)

chemin: identifie une ressource dans le périmètre du schéma de l'URI et de l'autorité de nommage.

EXEMPLE Un URI HTTP complet pourrait ressembler à:

`http://UIC94806101123.tcndns.db.de/mcgservice`

5.3.6.2 URI HTTP côté MCG (facultatif)

En fonction du mode d'adressage choisi (ID de rame ou ID de parcours de train), il est nécessaire que les identifiants d'hôtes respectent les règles définies en 5.3.5.1 et 5.3.5.2. Il convient d'aligner le chemin d'accès aux services de communication (décrits en 5.6.3 et 6) afin de faciliter l'interopérabilité.

Cette dernière est assurée à l'aide du chemin `mcgservice`.

Les URI HTTP obtenus prennent donc, par exemple, les formes suivantes:

`http://UIC94806101123.tcndns.db.de/mcgservice`

`http://EC41.tcndns.db.de/mcgservice`

5.3.6.3 URI HTTP côté GCG (facultatif)

L'URI HTTP de la GCG peut être considérée comme un élément de configuration, bien qu'il serait extrêmement utile que l'identifiant d'hôte de la GCG soit également enregistré dans le *tcndns* nommé selon le modèle

`gcg.tcndns.<domaine opérateur>`

possède un espace de nommage uniforme.

NOTE L'utilisation d'adresses IP ordinaires exerce plusieurs contraintes sur l'architecture du réseau sans fil.

De la même manière qu'indiquée en 5.3.6.2, le chemin défini sur `gcgservice` donne un exemple d'URI HTTP:

`http://gcg.tcndns.db.de/gcgservice`

5.4 Classes de données pour la communication T2G

5.4.1 Généralités

L'IEC 61375-1 définit quatre classes de données, chacune résultant de son riche passé dans l'histoire des communications avec des technologies associées, des solutions types et de l'état d'esprit général des développeurs d'applications.

Ces classes de données sont:

- a) Données de processus
- b) Données de messagerie
- c) Données de flux
- d) Données du mode «au mieux»

La MCG utilisée pour la communication train-sol par les dispositifs terminaux embarqués doit prendre en charge les données de messagerie, les données de flux et les données du mode «au mieux» telles que décrites au 7.5.3 de l'IEC 61375-1:2012. En fonction de la classe de données, des protocoles de communication appropriés sont utilisés.

Dans le cas où une communication de «Données de processus» entre le train et le sol est nécessaire, le modèle de communication d'événement cyclique défini pour les données de

messaging peut être utilisé à cette fin. Il est cependant possible d'utiliser le protocole de transport MQTT en lieu et place du protocole HTTP (voir Figure 12) pour tirer parti de ses avantages (voir 5.5.3).

5.4.2 Etablissement du canal de communication

Le principe essentiel est que la MCG établit le canal de communication indépendamment des classes de données à utiliser.

La MCG refuse toute demande d'établissement d'un canal de communication émanant des dispositifs côté sol (par exemple, de la GCG).

5.4.3 Données de messagerie

Lorsque la MCG prend en charge les données de messagerie, les paramètres de service recommandés dépendent des exigences de l'application et des propriétés de la technologie radio disponible (voir Tableau 13).

Tableau 13 – Paramètres de service recommandés pour les données de messagerie

Paramètre de service	Description
Taille du paquet de données	Volume des données à transmettre dans un paquet de données: ≤ 65507 octets NOTE Il convient que le paquet corresponde à un paquet UDP ayant une taille maximale de 65 507 octets (65535 – 8 octets d'en-tête UDP – 20 octets d'en-tête IP). Dans la pratique, cette taille est souvent encore plus limitée, par exemple en raison d'options dans l'en-tête IP et de contraintes liées aux piles de protocoles utilisées.
Débit de paquets de données	Nombre de paquets de données transmis par seconde. Multiplié par la taille du paquet de données * 8, équivaut au débit binaire (net). $\leq (\text{bande passante radio} / \text{taille du paquet de données}) * 20 \%$ (avec une bande passante radio nette disponible en octets par seconde).
Latence	Temps de transmission du paquet de données entre l'émetteur des données et le destinataire des données. ≤ 1 s NOTE La latence dépend de l'application.
Gigue	Ecart dans la durée de transmission pour des transmissions consécutives de paquets de données. ≤ 1 s NOTE La gigue dépend de l'application.
Intégrité des données	Paquet de données d'application reçu par le destinataire. taux d'erreur résiduel (BER) $\leq 10^{-6}$
	Probabilité de détection des défaillances suivantes: a) altération des données; b) erreur de séquençement (répétition intempestive, séquence erronée); c) erreur de livraison hors délai; d) erreur d'authentification (émetteur et destinataire erronés). Probabilité P_{DU} d'occurrence de défaillances non détectées dangereuses 10^{-5} par heure

5.4.4 Données de processus

Lorsque la MCG prend en charge les données de processus, les paramètres de service recommandés dépendent des exigences de l'application et des propriétés de la technologie radio disponible (voir Tableau 14).

Tableau 14 – Paramètres de service recommandés pour les données de processus

Paramètre de service	Description
Taille du paquet de données	Volume des données à transmettre dans un paquet de données: ≤ 1436 octets NOTE Il convient que le paquet tienne dans un seul paquet UDP non segmenté.
Débit de paquets de données	Nombre de paquets de données transmis par seconde. Multiplié par la taille du paquet de données * 8, équivaut au débit binaire (net). $\leq (\text{bande passante radio} / \text{taille du paquet de données}) * 20 \%$
Latence	Temps de transmission du paquet de données entre l'émetteur des données et le destinataire des données. ≤ 32 ms NOTE Latence du point de vue de l'application. Bien évidemment, le réseau peut introduire des latences supplémentaires de plus grande amplitude.
Gigue	Ecart dans la durée de transmission pour des transmissions consécutives de paquets de données. ≤ 32 ms
Intégrité des données	Paquet de données d'application reçu par le destinataire. taux d'erreur résiduel (BER) $\leq 10^{-6}$

5.4.5 Données de flux

Lorsque la MCG prend en charge les données de flux entre le train et le sol, les paramètres de service recommandés dépendent des exigences de l'application et des propriétés de la technologie radio disponible (voir Tableau 15).

Tableau 15 – Paramètres de service recommandés pour les données de flux

Paramètre de service	Description
Taille du paquet de données	Volume des données à transmettre dans un paquet de données: dépend du protocole de flux
Débit binaire	Nombre de données transmises par seconde. $\leq \text{bande passante radio} * 50 \%$ (par exemple, vidéo sur WLAN) ≤ 64 kbit/s (pour données audio) (avec une bande passante radio nette disponible en octets par seconde)
Latence	Temps de transmission du paquet de données entre l'émetteur des données et le destinataire des données. $\leq 0,100$ s NOTE La latence dépend de l'application.
Gigue	Ecart dans la durée de transmission pour des transmissions consécutives de paquets de données. $\leq 0,030$ s (pour les flux audio) NOTE La gigue dépend de l'application.
Intégrité des données	Paquet de données d'application reçu par le destinataire. taux d'erreur résiduel (BER) $\leq 10^{-6}$

5.4.6 Données du mode «au mieux»

Lorsque la MCG prend en charge les données du mode «au mieux» entre le train et le sol, les paramètres de service recommandés dépendent des exigences de l'application et des propriétés de la technologie radio disponible (voir Tableau 16).

Tableau 16 – Paramètres de service recommandés pour les données du mode «au mieux»

Paramètre de service	Description
Débit binaire	Nombre de paquets de données transmis par seconde. Multiplié par la taille du paquet de données * 8, équivaut au débit binaire (net). $\leq$ bande passante radio * 20 % (avec une bande passante radio nette disponible en octets par seconde).
Latence	Temps de transmission du paquet de données entre l'émetteur des données et le destinataire des données. $\leq$ 5 s NOTE La latence dépend de l'application.
Gigue	Ecart dans la durée de transmission pour des transmissions consécutives de paquets de données. $\leq$ 5 s NOTE La gigue dépend de l'application.
Intégrité des données	Paquet de données d'application reçu par le destinataire. taux d'erreur résiduel (BER) $\leq$ 10^{-6}

5.5 Protocole de communication

5.5.1 Généralités

La communication train-sol utilise les protocoles suivants:

- HTTP, pour les données de processus, les données de messagerie et le transfert de fichiers
- HTTPS, pour les données de processus, les données de messagerie et le transfert de fichiers sécurisé

Ces protocoles sont décrits dans les paragraphes suivants.

En option, les protocoles suivants peuvent être pris en charge:

- FTP, à titre d'alternative pour le transfert de fichiers
- SFTP, à titre d'alternative pour le transfert de fichiers sécurisé
- RTP, pour les flux audio et vidéo en direct
- MQTT, pour les connexions à des sites distants qui requièrent un «faible encombrement du code» ou qui disposent d'une faible bande passante réseau

5.5.2 HTTP(S)

5.5.2.1 Généralités

HTTP(S) doit être utilisé comme protocole de communication train-sol pour les données de messagerie et pour le transfert de fichiers. L'empilage de communication principal est présenté sur la Figure 14.

HTTP(S) est le protocole de communication de niveau d'application de base, utilisant la pile de protocoles TCP/IP pour un transfert et une couche réseau. HTTP(S) est ensuite utilisé pour prendre en charge les services de communication de couche application suivants:

- Données de messagerie (telles que définies dans le présent document)
- Transfert de fichiers (tel que défini dans le présent document)
- Autres (non définis dans le présent document)

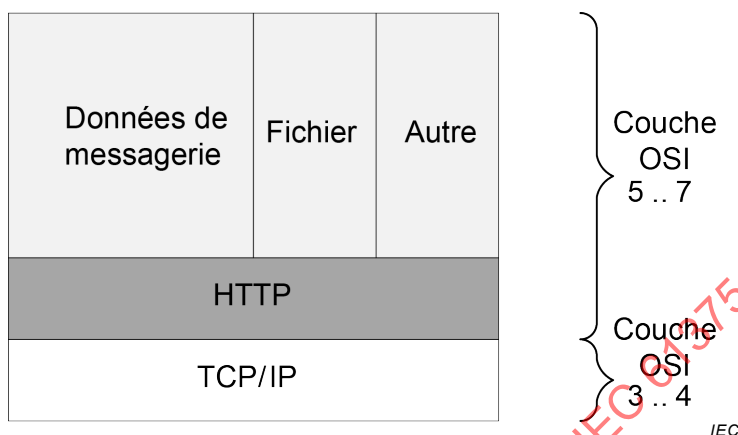


Figure 14 – Piles de communication

5.5.2.2 Paramètres de protocole de base

Pour un transfert de données utilisant HTTP, les exigences suivantes doivent être satisfaites conformément au document RFC 2616:

- La version de protocole doit être HTTP1.1
- Méthodes prises en charge: POST
- Propriétés d'en-tête prises en charge:
 - «Host» (hôte)
 - «Content-Type» (type de contenu)
 - «Content-Length» (longueur du contenu)

Version sécurisée de HTTP telle que définie dans le document RFC 2818. HTTPS doit être utilisé à la place de HTTP si les exigences de sécurité le requièrent.

5.5.2.3 Modèle d'échange HTTP(S)

Le modèle de communication de base «Données de messagerie» basé sur HTTP(S) facilite le modèle de demande/réponse normalisé présenté à la Figure 15.

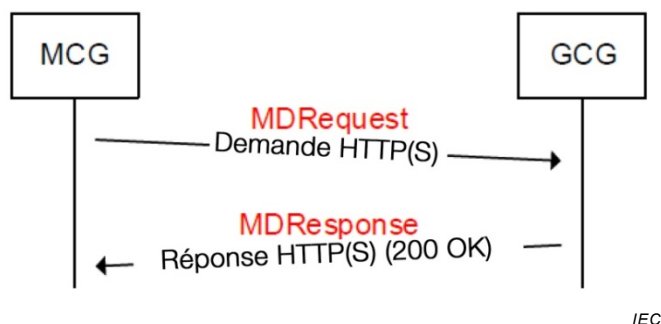


Figure 15 – Modèle de communication Données de messagerie basé sur HTTP(S)

La Figure 16 et la Figure 17 présentent les informations d'en-tête HTTP(S) pertinentes qui sont à utiliser par la communication train-sol de «Données de messagerie».

```
POST /[authority/path] HTTP/1.1
User-Agent:      [voir RFC 2616, 14.43 pour définition]
Host:            [voir RFC 2616, 14.23 pour définition]
Content-type:    [packetType]
Content-length:  [longueur du packetBody en nombre décimal d'octets]

[packetBody]
```

IEC

Figure 16 – Demande/événement HTTP(S)

```
HTTP/1.1 [code d'état] [expression d'état]
Content-type: [packetType]
Content-length: [longueur du packetBody en nombre décimal d'octets]

[packetBody]
```

IEC

Figure 17 – Réponse HTTP(S)

Les champs d'en-tête HTTP(S) pour le modèle de demande/réponse HTTP(S) sont donnés dans le Tableau 17.

Tableau 17 – Modèle de demande/réponse de paramètres HTTP(S)

En-tête de la demande HTTP(S) (méthode POST)	
authority (autorité)	Voir 5.3.6
path (chemin)	Voir 5.3.6
packetType (type de paquet)	Les valeurs suivantes du paramètre «Content-Type» doivent au moins être prises en charge: • «text/xml» • «text/html» • «application/octet-stream» • «application/json» (RFC 4627)
packetBody (corps de paquet)	Données utiles
Réponse HTTP(S)	
status code (code d'état)	voir RFC 2616, 6.1.1
status phrase (expression d'état)	voir RFC 2616, 6.1.1
packetBody (corps de paquet)	Données utiles

Outre le modèle MDRequest/MDResponse, il est possible d'envoyer de manière sporadique ou cyclique un message MDEvent qui utilise le même format que celui présenté dans le Tableau 17, mais où la réponse HTTP inclut uniquement un code d'état et une expression d'état. Ce message ne comporte aucun paramètre packetBody.

5.5.3 MQTT (facultatif)

La MCG peut prendre en charge le protocole allégé de transport par télémesure des messages en file d'attente (MQTT, de l'anglais Message Queue Telemetry Transport) conformément à l'ISO/IEC 20922:2016, qui présente certains avantages par rapport au protocole HTTP(S):

- taille d'en-tête minimale qui réduit la surcharge de données;
- utilisation de la même connexion TCP pour toutes les données échangées, ce qui augmente le débit des données et réduit la latence;
- paradigme de publication/abonnement pour des relations de communication «un à plusieurs»;
- prise en charge native de la QoS pour la catégorisation des messages;
- mesure des «battements de cœur» (signaux «heartbeat») des connexions TCP clientes pour la supervision des communications;
- aucun port d'écoute sur les dispositifs terminaux, ce qui renforce la sécurité;
- traitement efficace des données grâce à un protocole de données binaires compact.

5.6 Services de communication

5.6.1 Généralités

Le présent paragraphe définit les services de communication nécessaires pour le transfert de données entre un ED embarqué et un ED au sol. Les services de communication sont définis pour les types de données suivants:

- a) Données de messagerie
 - transfert du train au sol
 - transfert du sol au train
- b) Données de processus
 - transfert du train au sol
- c) Transfert de fichiers
 - transfert du train au sol
 - transfert du sol au train
- d) Flux (audio/vidéo)
 - transfert du train au sol
 - transfert du sol au train

Les services de communication font une distinction entre le contrôle du transfert de données et le transfert de données à proprement dit. Le contrôle du transfert de données est basé sur des télégrammes «Données de messagerie», qui sont échangés entre les parties prenantes impliquées. Le transfert de données à proprement dit est principalement fondé sur des protocoles dédiés, comme HTTP(S) pour le transfert de fichiers et RTP/RTCP pour les données en flux.

5.6.2 Service de communication Données de messagerie

5.6.2.1 Généralités

Le service de communication «Données de messagerie» est l'un des services de communication basés sur HTTP, comme défini en 5.5. Le présent paragraphe décrit les cas d'utilisation pris en charge et définit les télégrammes «Données de messagerie» associés.

5.6.2.2 Echange de données de messagerie

Le service d'échange de données de messagerie est utilisé pour échanger une seule fois des données de messagerie sur demande.

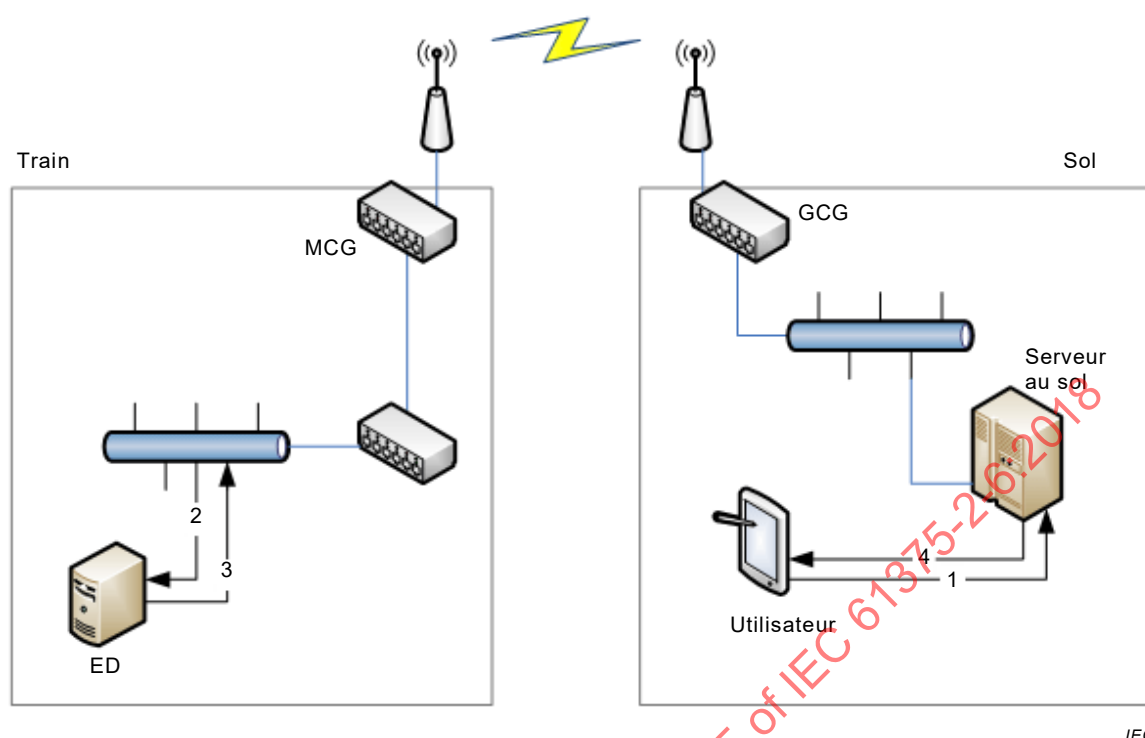


Figure 18 – Echange de données de messagerie (exemple)

Le transfert de données de messagerie du train au sol initié suite à un abonnement aux données de messagerie requiert les étapes suivantes comme cela est décrit dans l'exemple de la Figure 18. L'utilisateur utilise une application pour envoyer une demande de données de messagerie au train. Cette application peut par exemple être hébergée par le serveur au sol ou par un autre dispositif réseau qui peut se connecter à la GCG.

- La demande de données (1) est transmise à l'ED (2) qui fournit les informations.
- L'ED prépare une réponse qui contient les informations requises et envoie les informations au sol (3).
- Les informations sont ensuite transmises à l'utilisateur à l'origine de la demande (4).

5.6.2.3 Définitions des télégrammes

5.6.2.3.1 Généralités

Un télégramme «Données de messagerie» (MD, de l'anglais Message Data) est constitué d'un en-tête de message général et d'un corps de message propre au service. Les paramètres de l'en-tête de message et les paramètres des corps de message associés aux services de communication définis ici sont spécifiés dans le présent paragraphe. Pour la transmission de données, le message complet sera représenté dans le format de transmission défini et placé dans les données utiles d'un paquet HTTP(S) (voir Figure 19).

Le format de transmission du message doit être JSON comme défini dans le document RFC 7159. Une définition du format de transmission du message est donnée à l'Annexe A.

Même si le format de transmission du corps de message est JSON, la structure du corps permet d'intégrer des informations dans d'autres formats (voir Annexe A). Les formats recommandés sont:

- JSON (comme pour message)
- XML
- données binaires codées en base64

NOTE La norme IEC 62888/EN 50463 définit des messages au format XML. Dans les architectures où le système de mesure d'énergie (EMS de l'anglais Energy Metering System) est connecté à l'ECN embarqué et utilise la MCG pour une communication au sol (connexion réseau de rame EMS basée sur la série IEC 61375), le message complet de l'IEC 62888/EN 50463 peut être placé dans le corps de message puis transféré entre la MCG et GCG.

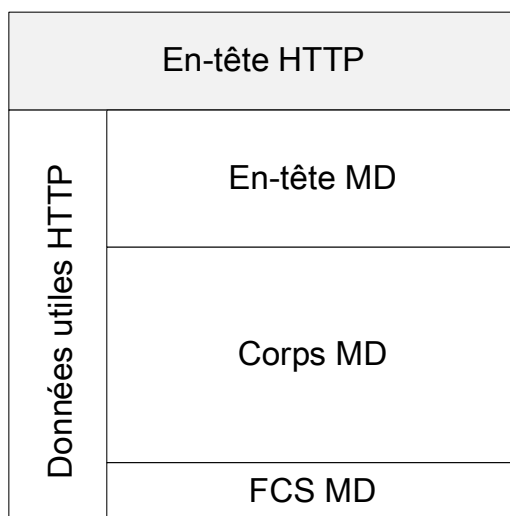


Figure 19 – Structure de télégramme Données de messagerie

5.6.2.3.2 Format de télégramme Données de messagerie général

5.6.2.3.2.1 Généralités

Les paramètres de l'en-tête «Données de messagerie» doivent être conformes au Tableau 18.

Tableau 18 – En-tête Données de messagerie (MD-header) général

Paramètre	Description	Type de données	Plage de valeurs	Valeur
MDHeader	En-tête de message	JSON		
protocolVersion	Version de protocole de la trame MD (paire de chiffres indiquant le numéro de version). La version de protocole est annotée sur deux octets, le mappage étant considéré de la manière suivante: 0x10: version de protocole 1.0 valeur: 16 0x1A: version de protocole 1.10 valeur: 26 0xB5: version de protocole 11.5 valeur: 181	valeur numérique	uint8	16
msgType	Type de message	valeur numérique	uint16	configurée voir Tableau 21
source	Spécification de l'ID de rame ou de parcours de train	chaîne	char[32]	envoyée par la MCG ou lorsque le message initial est émis par la GCG: configuration dans la GCG
comID	Identifiant pour le corps de message (dépend de l'application)	valeur numérique	uint16	configurée
msgTimestamp	Horodatage indiquant quand le message a été envoyé	valeur numérique	uint64	calculée format d'horodatage unix

Paramètre	Description	Type de données	Plage de valeurs	Valeur
MDHeader	En-tête de message	JSON		
msgTimeValidity	Indique la durée de validité en millisecondes (par exemple, durée de vie prévue) du contenu envoyé dans le corps de message.	valeur numérique	uint32	configurée 0: n.a. 1..'FFFFFFFF'H

Les éléments de données contenus dans le corps du message de la trame «Données de messagerie» doivent être conformes au Tableau 19.

Tableau 19 – Corps Données de messagerie (MD-body) général

Elément de données	Description	Type de données	Plage de valeurs	Valeur
mdPayloadType	Décrit quel type de contenu est intégré dans les données utiles de corps de données de messagerie.	chaîne	char[16]	configurée voir Tableau 22
mdPayload	Contient un contenu propre à l'application (par exemple, trame TRDP, trame EMS-XML, flux d'octets)	objet	objet	calculée

La somme de contrôle de la trame «Données de messagerie» doit être conforme au Tableau 20.

Tableau 20 – Somme de contrôle Données de messagerie (MD-checksum)

Elément de données	Description	Type de données	Plage de valeurs	Valeur
mdFCS	Somme de contrôle calculée sur les paramètres MDHeader et MDBody. Voir 5.6.2.3.2.2	chaîne hexadécimale	char[8]	0..'FFFFFFFF'H Calculée sur les balises complètes MDHeader et MDBody conformément à l'IEC 61375-2-3:2015, Article A.3. Valeur de base: 0x0.

Le télégramme «Données de messagerie» étant défini comme un télégramme basé sur ASCII, il est nécessaire d'encapsuler le contenu de manière à n'inclure dans les données aucun caractère de contrôle, qui indiquerait à tort la fin de l'objet de données.

La méthode d'encapsulation préférée (par exemple, codage en base64) relève du périmètre de l'application.

Les types de messages définis pour les trames «Données de messagerie» doivent être conformes au Tableau 21.

Tableau 21 – Types de messages

Valeur	Description
1	MDEvent-sporadic
2	MDEvent-cyclic
3	MDRequest
4	MDResponse

La représentation de message définie pour les trames «Données de messagerie» doit être conforme au Tableau 22.

Tableau 22 – Représentation de message

Valeur	Description
«JSON»	Contenu représenté en format JSON (voir Annexe A)
«XML»	Contenu représenté en format XML (par exemple, pour un EMS)
«Octet»	Contenu représenté sous la forme de flux d'octets
«Base64»	Contenu représenté sous la forme d'un flux d'octets codés en base64
...	Autres

5.6.2.3.2.2 Calcul de mdFcs

La FCS de la trame «Données de messagerie» doit être calculée de la manière suivante:

- Le contenu de données de messagerie JSON suivant doit être utilisé pour le calcul de mdFCS:

```
"MDHeader":
{
    // all frame-header elements
},
"MDBody":
{
    // all frame-body elements
}
```

La somme de contrôle doit être calculée sur les balises complètes MDHeader et MDBody du message JSON, incluant la balise, un signe deux points, une accolade ouvrante, tous les éléments du corps de trame à transmettre (la somme de contrôle est calculée sur le tampon de texte JSON réel) et l'accolade fermante comme dernier élément.

- Puisque l'élément mdFcs n'est pas un élément de MDHeader ou de MDBody, il n'est pas nécessaire de définir une valeur par défaut obligatoire.
- Pour le calcul de l'élément mdFCS, le CRC32 conforme à l'IEEE 802.3 doit être utilisé.
- La valeur de départ pour le calcul CRC32 doit être: **0**.

5.6.3 Service de transfert de fichiers

5.6.3.1 Généralités

En matière de transfert de fichiers, les termes suivants doivent s'appliquer conformément au Tableau 23.

Tableau 23 – Terminologie du transfert de fichiers

Terme	Description
Téléchargement en liaison descendante	Un fichier est transféré du sol vers le train
Téléchargement en liaison montante	Un fichier est transféré du train vers le sol

Le service de transfert de fichiers procure le moyen de transférer des fichiers du train au sol et vice versa. Pour des raisons de sécurité, les transferts de fichiers directs de point de terminaison à point de terminaison ne sont pas autorisés entre les dispositifs terminaux à bord du train et au sol.

Les fichiers sont transférés au moyen d'un stockage intermédiaire, autrement dit les fichiers doivent être temporairement placés à un emplacement de stockage prédéfini à partir duquel ils pourront être téléchargés en liaison montante ou descendante.

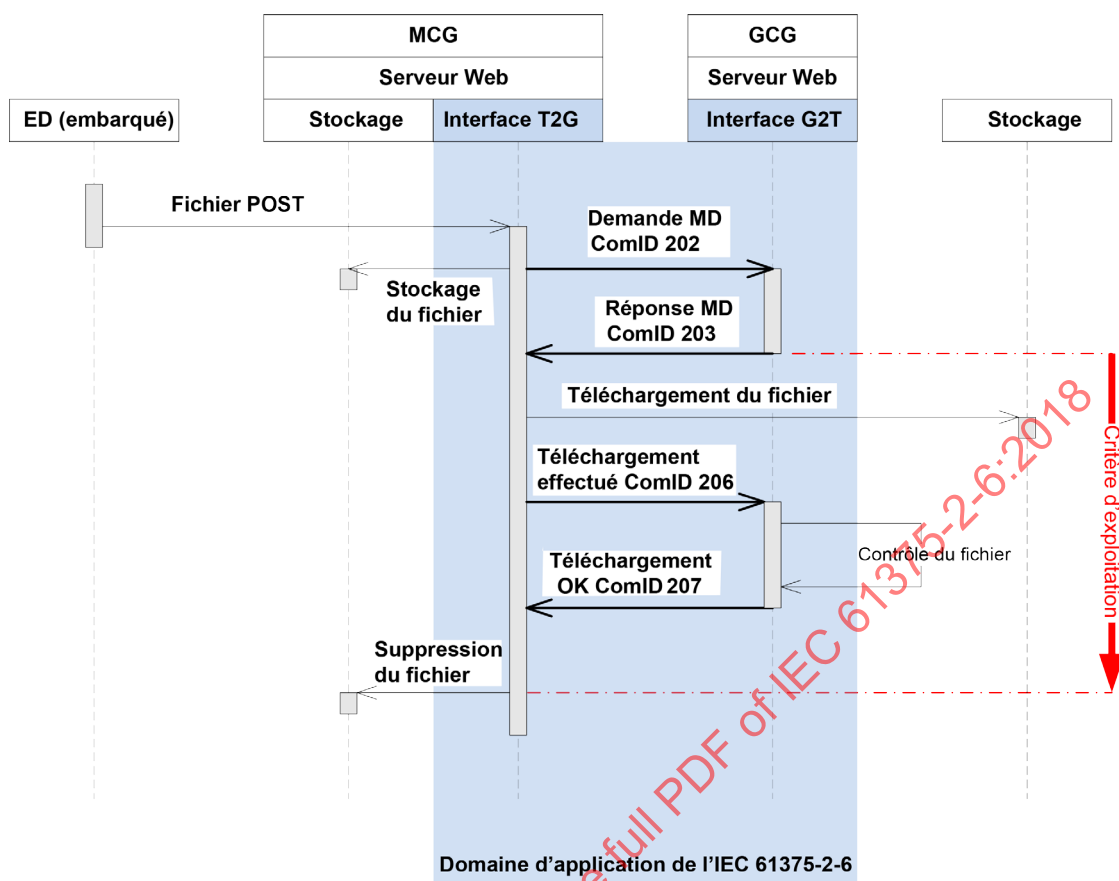
NOTE La définition et la spécification exactes d'un emplacement de stockage acceptable ne relèvent pas du domaine d'application du présent document.

La récupération des fichiers au cours des processus de téléchargement en liaison montante ou descendante est toujours assurée par la MCG. Le téléchargement d'un fichier en liaison montante ou descendante est donc associé à des concepts asymétriques.

5.6.3.2 Téléchargement de fichiers en liaison montante

5.6.3.2.1 Généralités

La Figure 20 décrit un exemple de téléchargement d'un fichier en liaison montante entre un dispositif terminal embarqué et le sol. Le périmètre du modèle de téléchargement de fichiers en liaison montante tel qu'il est spécifié dans le présent document est mis en évidence par un fond bleu pastel.



IEC

Figure 20 – Exemple de téléchargement de fichiers en liaison montante

Un dispositif terminal embarqué peut télécharger un fichier en liaison montante vers le sol en seulement quelques étapes, comme indiqué ci-dessous:

- Le dispositif terminal commence par transférer le fichier à la MCG, par exemple en utilisant une interface de service Web exposée par la MCG aux seuls dispositifs à bord du train.
- Une fois le fichier correctement transféré à la MCG, la MCG demande automatiquement à la GCG l'autorisation de transférer le fichier côté sol. La MCG envoie un message de demande (ComID 202) à l'interface de service Web exposée par la GCG.
- La GCG répond à la demande de transfert de fichiers émise par la MCG, en indiquant si l'exécution de ce transfert de fichier est autorisée ou non. La GCG envoie un message de réponse (ComID 203) à l'interface de service Web exposée par la MCG, en indiquant à la MCG un emplacement de stockage à utiliser pour le stockage du fichier côté sol.
- La MCG télécharge le fichier en liaison montante à l'emplacement de stockage spécifié.
- Une fois le téléchargement en liaison montante terminé, la MCG informe la GCG que le transfert de fichier est terminé. La MCG envoie un message d'information (ComID 206) à l'interface de service Web exposée par la GCG.
- La GCG utilise un mécanisme de vérification de l'intégrité du fichier transféré afin de déterminer si l'intégrité du fichier transféré peut être confirmée ou non côté sol.
- Une fois l'intégrité du fichier vérifiée côté sol, la GCG envoie un message de réponse à l'interface de service Web exposée par la MCG. La GCG envoie un message de réponse (ComID 207) à l'interface de service Web exposée par la MCG pour confirmer la bonne réception du fichier.
- Après avoir reçu confirmation par la GCG de la bonne réception du fichier, la MCG peut supprimer le fichier de son stockage interne.

NOTE La MCG peut déterminer quel support radio utiliser pour le téléchargement d'un fichier en liaison montante. Voir 6.3.4 pour plus d'informations.

5.6.3.2.2 Définition d'un message

5.6.3.2.2.1 Demande d'autorisation de téléchargement en liaison montante (ComID 202)

Le message ComID 202 est un télégramme de données de messagerie envoyé par la MCG à la GCG. La MCG utilise ce message pour demander l'autorisation de télécharger un fichier en liaison montante côté sol.

Le télégramme de demande MD ComID 202 doit être envoyé avec les paramètres d'en-tête suivants conformément au Tableau 24. Pour obtenir des informations générales sur les paramètres d'en-tête des données de messagerie, se référer au Tableau 18.

Tableau 24 – ComID 202: valeurs d'en-tête du télégramme de données de messagerie

Paramètre	Valeur
msgType	3 (demande MD)
msgTimeValidity	0 (aucun délai d'expiration)
comID	202

Le télégramme de demande MD ComID 202 doit être envoyé avec les paramètres de corps suivants conformément au Tableau 25. Pour obtenir des informations générales sur les paramètres de corps des données de messagerie, se référer au Tableau 19.

Tableau 25 – ComID 202: valeurs du corps du télégramme de données de messagerie

Paramètre	Valeur
mdPayloadType	«JSON»
mdPayload	voir Tableau 26

Le télégramme de demande MD ComID 202 doit être envoyé avec l'objet de données utiles suivant conformément au Tableau 26.

Tableau 26 – ComID 202: corps de données de messagerie – objet mdPayload

Elément de données	Description	Type de données	Plage de valeurs	Valeur
objet	Données utiles du paramètre de corps de données de messagerie «mdPayload»	JSON		
fileTransferUID	Identifiant unique. Défini par la MCG, utilisé par la MCG et la GCG pour identifier un fichier téléchargé en liaison montante.	valeur numérique	uint32	calculée
filename	Nom du fichier à transférer à la GCG. Utilisé ultérieurement par la GCG pour permettre l'accès au fichier téléchargé.	chaîne	char[256]	prédéfinie
fileType	Indique le type de fichier qui est téléchargé en liaison montante.	valeur numérique	uint8	0 = n.a. 1 = ASCII 2 = binaire 3 = audio 4 = vidéo 5-255 pas utilisée
fileServiceFunction	Indique le service source.	valeur numérique	uint8	0 = pas dans la liste 1 = EMS 2 = CCTV autres valeurs réservées
fileSize	Indique la taille du fichier à télécharger, en octets. Déterminée par la MCG.	valeur numérique	uint64	prédéfinie

5.6.3.2.2.2 Réponse à une demande de téléchargement en liaison montante (ComID 203)

Le message ComID 203 est un télégramme de données de messagerie envoyé par la GCG à la MCG. La GCG utilise ce télégramme en réponse à une demande de téléchargement d'un fichier en liaison montante côté sol.

Le télégramme de réponse MD ComID 203 doit être envoyé avec les paramètres d'en-tête suivants conformément au Tableau 27. Pour obtenir des informations générales sur les paramètres d'en-tête des données de messagerie, se référer au Tableau 18.

Tableau 27 – ComID 203: valeurs d'en-tête du télégramme de données de messagerie

Paramètre	Valeur
msgType	4 (réponse de données de messagerie à la demande MD reçue)
msgTimeValidity	0 (aucun délai d'expiration)
comID	203

Le télégramme de réponse MD ComID 203 doit être envoyé avec les paramètres de corps suivants conformément au Tableau 28. Pour obtenir des informations générales sur les paramètres de corps des données de messagerie, se référer au Tableau 19.

Tableau 28 – ComID 203: valeurs du corps du télégramme de données de messagerie

Paramètre	Valeur
mdPayloadType	«JSON»
mdPayload	voir Tableau 29

Le télégramme de réponse MD ComID 203 doit être envoyé avec l'objet de données utiles suivant conformément au Tableau 29.

Tableau 29 – ComID 203: corps de données de messagerie – objet mdPayload

Élément de données	Description	Type de données	Plage de valeurs	Valeur
objet	Données utiles du paramètre de corps de données de messagerie «mdPayload»	JSON		
fileTransferUID	Identifiant unique. Utilisé par la MCG et la GCG pour identifier un fichier téléchargé en liaison montante.	valeur numérique	uint32	prédéfinie (reprise du message ComID 202)
storageURL	URL indiquant un emplacement de stockage à utiliser par la MCG pour le téléchargement d'un fichier en liaison montante.	chaîne	char[512]	prédéfinie

5.6.3.2.2.3 Réussite du téléchargement en liaison montante (ComID 206)

Le message ComID 206 est un télégramme de données de messagerie envoyé par la MCG à la GCG. La MCG utilise ce message pour faire suite à un précédent échange de messages ComID 202 et ComID 203. La MCG indique à la GCG qu'elle a correctement téléchargé le fichier en liaison montante à l'emplacement de stockage indiqué.

Pour plus d'informations sur les paramètres d'en-tête de données de messagerie (MD header), se référer au Tableau 18. Pour plus d'informations sur le corps de données de messagerie (MD body), se référer au Tableau 19.

Le télégramme de demande MD ComID 206 doit être envoyé avec les paramètres d'en-tête suivants conformément au Tableau 30. Pour obtenir des informations générales sur les paramètres d'en-tête des données de messagerie, se référer au Tableau 18.

Tableau 30 – ComID 206: valeurs d'en-tête du télégramme de données de messagerie

Paramètre	Valeur
msgType	3 (demande MD)
msgTimeValidity	0 (aucun délai d'expiration)
comID	206

Le télégramme de demande MD ComID 206 doit être envoyé avec les paramètres de corps suivants conformément au Tableau 31. Pour obtenir des informations générales sur les paramètres de corps des données de messagerie, se référer au Tableau 19.

Tableau 31 – ComID 206: valeurs du corps du télégramme de données de messagerie

Paramètre	Valeur
mdPayloadType	«JSON»
mdPayload	voir Tableau 32

Le télégramme de demande MD ComID 206 doit être envoyé avec l'objet de données utiles suivant conformément au Tableau 32.

Tableau 32 – ComID 206: corps de données de messagerie – objet mdPayload

Elément de données	Description	Type de données	Plage de valeurs	Valeur
objet	Données utiles du paramètre de corps de données de messagerie «mdPayload»	JSON		
fileTransferUID	Identifiant unique. Utilisé par la MCG et la GCG pour identifier un fichier téléchargé en liaison montante.	valeur numérique	uint32	prédéfinie (reprise du message ComID 202)
storageURL	URL indiquant l'emplacement de stockage dans lequel la MCG a téléchargé un fichier en liaison montante.	chaîne	char[512]	prédéfinie
fileUploadResult	Indique les résultats du téléchargement de fichier en liaison montante du point de vue de la MCG.	valeur numérique	uint8	0 = n.a 1 = téléchargement OK 2 = téléchargement interrompu 3 = démarrage impossible du téléchargement 4–254 pas utilisée actuellement 255 = erreur
fileChecksum	Somme de contrôle MD5 permettant de vérifier côté sol que le téléchargement de fichier en liaison montante a été envoyé avec succès. Le mécanisme de somme de contrôle utilisé relève du périmètre de l'application.	chaîne	char[256]	calculée

5.6.3.2.2.4 Vérification de l'intégrité du téléchargement en liaison montante (ComID 207)

Le message ComID 207 est un télégramme de données de messagerie envoyé par la GCG à la MCG. La GCG utilise ce message en réponse à un message ComID 206 reçu d'une MCG.

La GCG indique à la MCG que la vérification de l'intégrité du fichier téléchargé en liaison montante côté sol a bien été effectuée.

Le télégramme de réponse MD ComID 207 doit être envoyé avec les paramètres d'en-tête suivants conformément au Tableau 33. Pour obtenir des informations générales sur les paramètres d'en-tête des données de messagerie, se référer au Tableau 18.

Tableau 33 – ComID 207: valeurs d'en-tête du télégramme de données de messagerie

Paramètre	Valeur
msgType	4 (réponse de données de messagerie à la demande MD reçue)
msgTimeValidity	0 (aucun délai d'expiration)
comID	207

Le télégramme de réponse MD ComID 207 doit être envoyé avec les paramètres de corps suivants conformément au Tableau 34. Pour obtenir des informations générales sur les paramètres de corps des données de messagerie, se référer au Tableau 19.

Tableau 34 – ComID 207: valeurs du corps du télégramme de données de messagerie

Paramètre	Valeur
mdPayloadType	«JSON»
mdPayload	voir Tableau 35

Le télégramme de réponse MD ComID 207 doit être envoyé avec l'objet de données utiles suivant conformément au Tableau 35.

Tableau 35 – ComID 207: corps de données de messagerie – objet mdPayload

Élément de données	Description	Type de données	Plage de valeurs	Valeur
objet	Données utiles du paramètre de corps de données de messagerie «mdPayload»	JSON		
fileTransferUID	Identifiant unique. Utilisé par la MCG et la GCG pour identifier un fichier téléchargé en liaison montante.	valeur numérique	uint32	prédéfinie (reprise du message ComID 202)

5.6.3.2.2.5 Traitement des erreurs

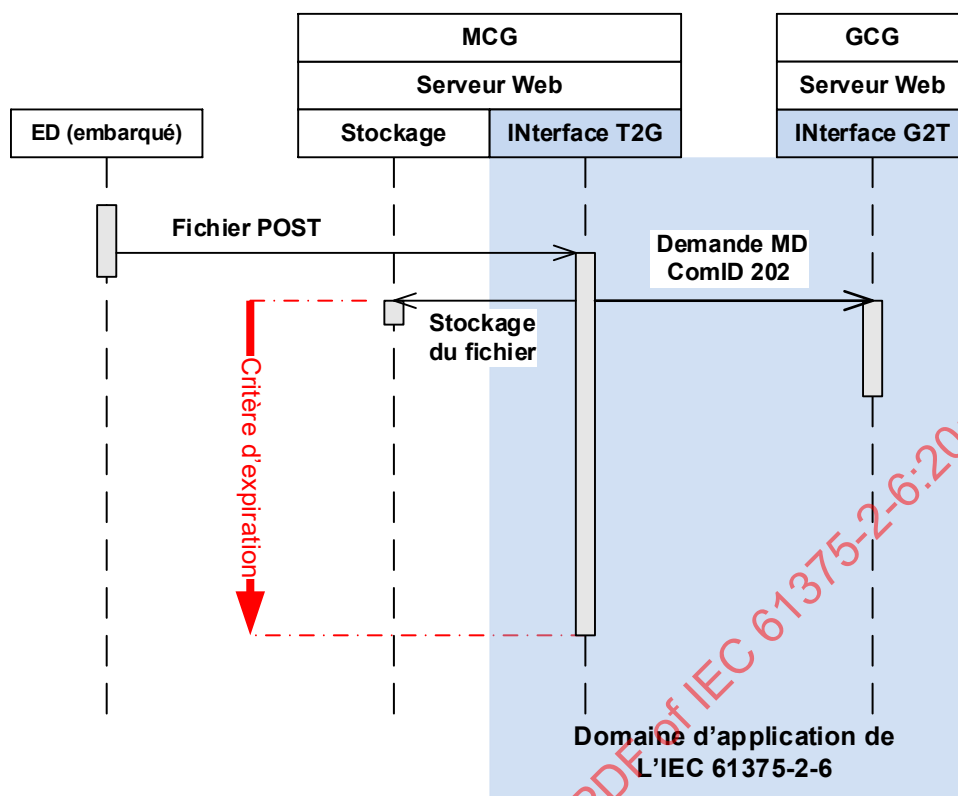
5.6.3.2.2.5.1 Généralités

Le présent paragraphe répertorie les cas d'erreur qui peuvent se produire lors de l'utilisation du service de transfert de fichiers. Chaque cas d'erreur et le problème associé sont décrits dans un paragraphe distinct.

NOTE Les cas d'erreur qui ne relèvent pas du domaine d'application du présent document ne sont pas décrits dans le présent paragraphe.

5.6.3.2.2.5.2 Cas d'erreur: aucun message ComID 203 reçu

La Figure 21 présente un cas où la MCG ne reçoit aucun message ComID 203.



IEC

Figure 21 – Cas d'erreur: aucun message ComID 203 reçu

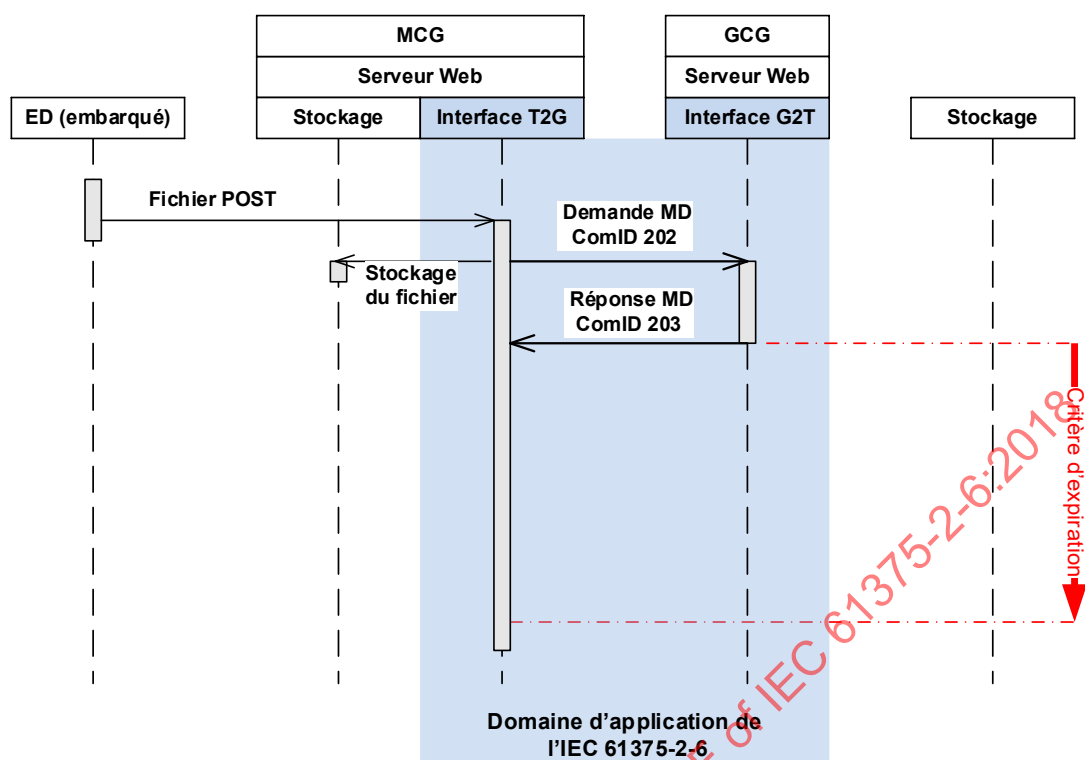
Le message ComID 202 est envoyé par la MCG à la GCG. La MCG utilise ce message pour demander l'autorisation de télécharger un fichier en liaison montante côté sol. La MCG ne reçoit pas de message ComID 203 en réponse à sa demande.

Description du problème: La MCG doit détecter les cas où la GCG ne répond pas à une demande ComID 202 de téléchargement de fichier en liaison montante.

Mesure corrective: Aucune demande de téléchargement en liaison montante ne doit perdurer dans un état indéfini, autrement dit la demande doit être renouvelée ou la demande de téléchargement en liaison montante doit être interrompue.

5.6.3.2.2.5.3 Cas d'erreur: aucun message ComID 206 reçu, aucun fichier téléchargé en liaison montante côté sol

La Figure 22 décrit un cas où la GCG ne reçoit aucun message ComID 206 et aucun fichier n'est téléchargé en liaison montante côté sol.



IEC

Figure 22 – Cas d'erreur: aucun message ComID 206 reçu, aucun fichier téléchargé en liaison montante côté sol

Le message ComID 206 est envoyé par la MCG à la GCG. La MCG utilise ce message pour faire suite à un précédent échange de messages ComID 202 et ComID 203, indiquant à la GCG la réussite d'un téléchargement.

Description du problème: La MCG n'a pas téléchargé le fichier à l'emplacement de stockage indiqué et n'envoie pas le message ComID 206.

Mesure corrective: La GCG doit détecter les cas où aucun téléchargement de fichier ou confirmation n'a lieu après qu'elle ait accepté la demande de transfert d'un fichier. La MCG doit s'assurer que la demande de téléchargement en liaison montante ne demeure pas dans un état indéfini, autrement dit la demande doit être renouvelée ou la demande de téléchargement en liaison montante doit être interrompue.

5.6.3.2.2.5.4 Cas d'erreur: aucun message ComID 206 reçu, fichier téléchargé en liaison montante côté sol

La Figure 23 décrit un cas où la GCG ne reçoit aucun message ComID 206, alors que le fichier a bien été téléchargé en liaison montante côté sol.

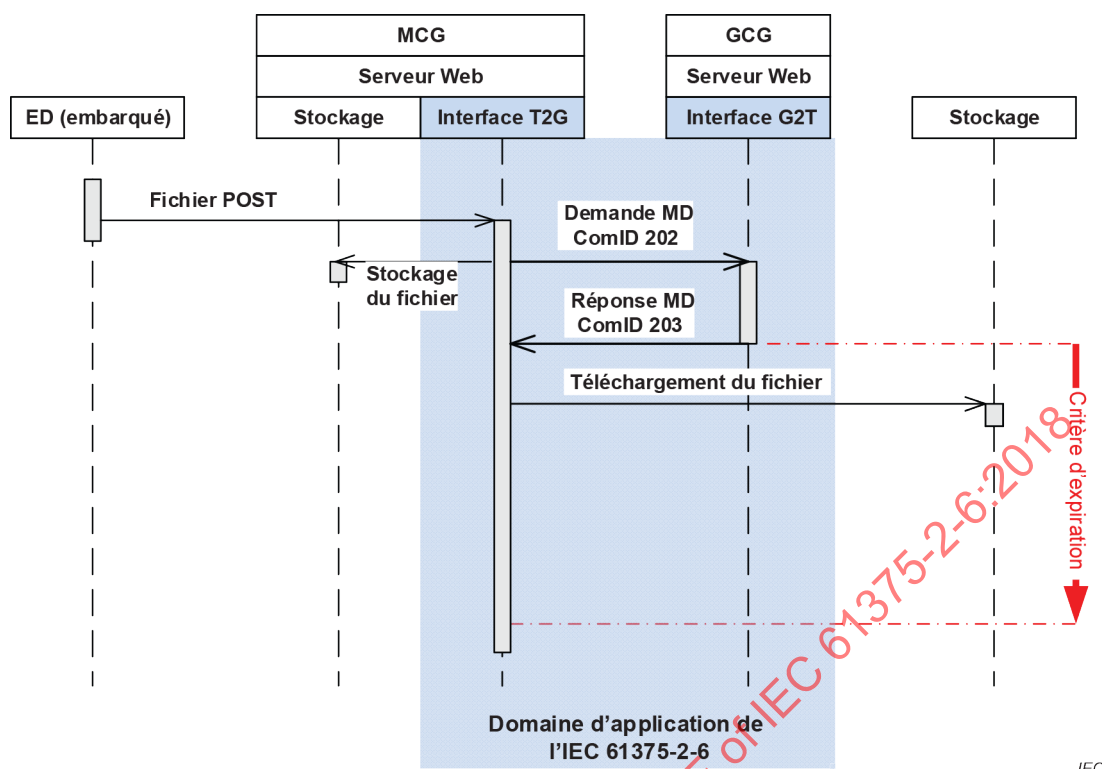


Figure 23 – Cas d'erreur: aucun message ComID 206 reçu, fichier téléchargé en liaison montante côté sol

Le message ComID 206 est envoyé par la MCG à la GCG. La MCG utilise ce message pour faire suite à un précédent échange de messages ComID 202 et ComID 203, indiquant à la GCG la réussite d'un téléchargement.

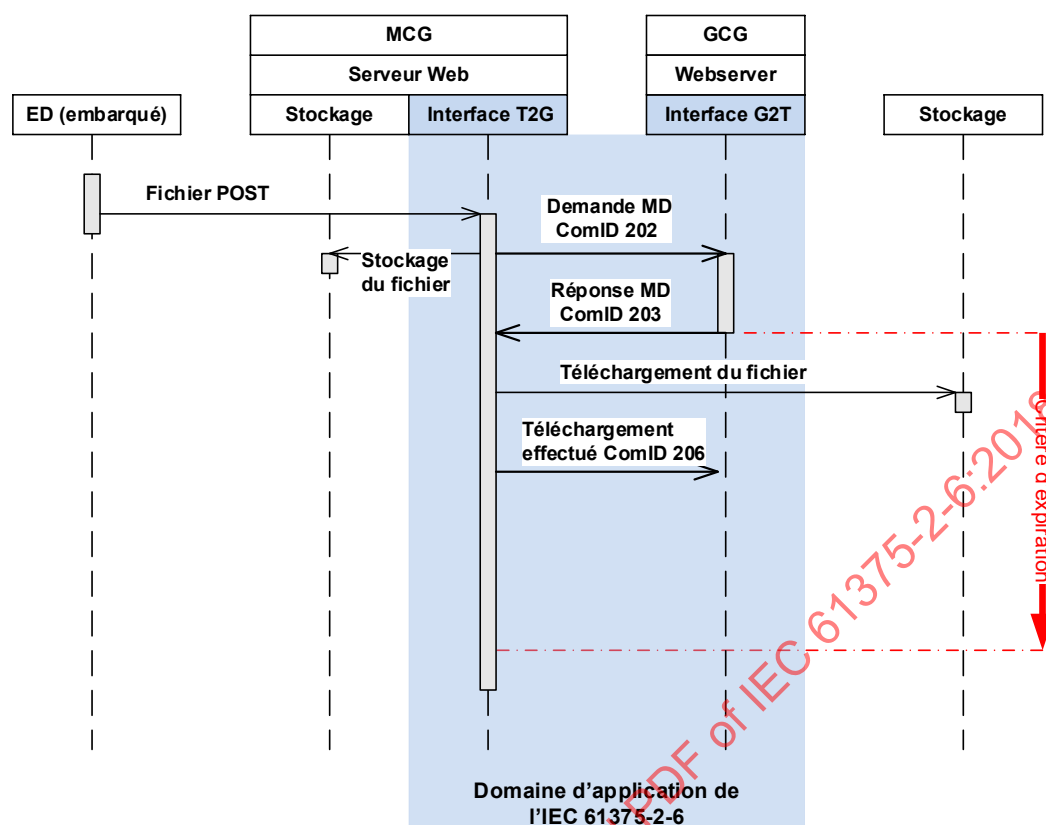
Description du problème: La MCG a téléchargé le fichier à l'emplacement de stockage indiqué, mais la GCG n'a pas reçu le message ComID 206. L'emplacement de stockage dans lequel est téléchargé le fichier peut ne pas être un emplacement interne à la GCG, ce qui signifie que la GCG ne peut pas indiquer que le fichier a bien été téléchargé.

Mesure corrective: La GCG doit détecter les cas où aucun téléchargement de fichier ou confirmation n'a lieu après qu'elle ait accepté la demande de transfert d'un fichier. La GCG peut être en mesure de déterminer si le fichier a été téléchargé en utilisant les informations envoyées dans le message ComID 202, mais cet aspect ne relève pas du domaine d'application du présent document.

La MCG doit s'assurer que la demande de téléchargement en liaison montante ne demeure pas dans un état indéfini, autrement dit la demande doit être renouvelée ou la demande de téléchargement en liaison montante doit être interrompue. La GCG doit s'assurer qu'aucun fichier ne perdure à l'emplacement de stockage indiqué par la GCG.

5.6.3.2.2.5.5 Cas d'erreur: aucun message ComID 207 reçu

La Figure 24 présente un cas où la MCG ne reçoit aucun message ComID 207.



IEC

Figure 24 – Cas d'erreur: aucun message ComID 207 reçu

Le message ComID 207 est envoyé par la GCG à la MCG. La GCG utilise ce message en réponse à un message ComID 206 reçu d'une MCG pour lui indiquer que la vérification de l'intégrité du fichier téléchargé en liaison montante a bien été effectuée.

Description du problème: La MCG a téléchargé le fichier à l'emplacement de stockage indiqué et a informé la GCG de la réussite du téléchargement. La GCG n'a pas répondu au message ComID 206.

Mesure corrective: La MCG doit détecter les cas où aucune confirmation de la vérification de l'intégrité côté sol n'est reçue après le téléchargement d'un fichier en liaison montante et indication de la réussite du téléchargement. La GCG doit s'assurer que l'intégrité du fichier téléchargé en liaison montante a été confirmée côté sol et que le fichier est correctement téléchargé côté sol.

5.6.3.3 Téléchargement de fichiers en liaison descendante

5.6.3.3.1 Généralités

La Figure 25 décrit un exemple de téléchargement d'un fichier en liaison descendante entre un dispositif terminal au sol et le train. Le périmètre du modèle de téléchargement de fichiers en liaison descendante tel qu'il est spécifié dans le présent paragraphe est mis en évidence par un fond bleu pastel.

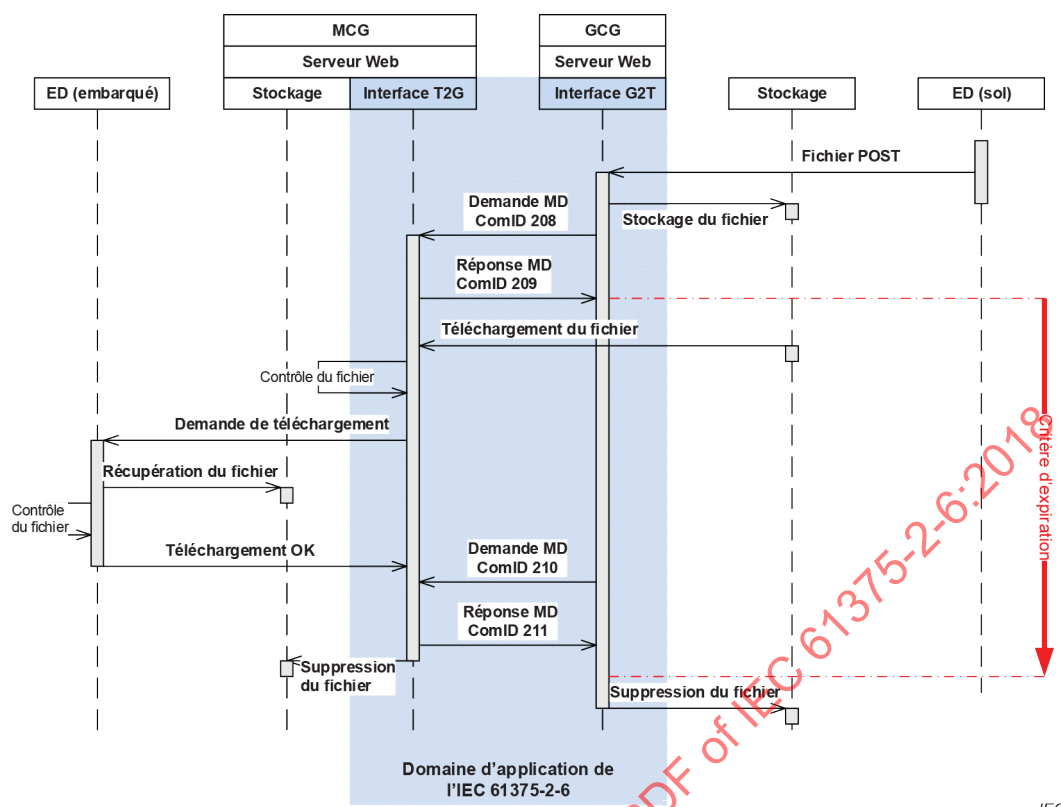


Figure 25 – Exemple de téléchargement de fichiers en liaison descendante

Un dispositif terminal au sol peut télécharger un fichier en liaison descendante vers le train en suivant les étapes logiques décrites ci-dessous:

- Le dispositif terminal commence par transférer le fichier à la GCG, par exemple en utilisant une interface de service Web exposée par la GCG aux seuls dispositifs au sol.
- Une fois le fichier correctement transféré à la GCG, la GCG demande automatiquement à la MCG de récupérer le fichier. Pour cela, la GCG envoie un message de demande (ComID 208) à une interface de service Web exposée par la MCG; ce message inclut l'emplacement de stockage à partir duquel la MCG peut récupérer le fichier, voir une **formule** de téléchargement en liaison descendante (voir 5.6.3.3.5).
- La MCG répond à la demande de récupération du fichier émanant de la GCG et envoie un message de réponse (ComID 209) indiquant si elle téléchargera ou non le fichier.
- Après avoir indiqué que le fichier sera bien téléchargé, la MCG récupère le fichier dans l'emplacement de stockage.
- La GCG vérifie de manière cyclique (le temps de cycle utilisé étant un élément de configuration) l'état du téléchargement en liaison descendante en contactant la MCG. La GCG envoie à la MCG un message de demande (ComID 210), auquel la MCG répond par un message de réponse (ComID 211) indiquant l'état actuel du téléchargement.
- Une fois le téléchargement terminé, la MCG utilise un mécanisme de vérification de l'intégrité du fichier qui a été transféré au train.
- Une fois l'intégrité du fichier vérifiée, la MCG informe la GCG de la réussite du transfert de fichier à la MCG lors de la réception du prochain message ComID 210 (voir étape e).
- Si une formule de téléchargement est incluse dans la demande envoyée par la GCG, la MCG utilise maintenant cette formule pour informer un ou plusieurs dispositifs terminaux de la disponibilité du fichier téléchargé.
- La MCG envoie un message de demande de téléchargement en liaison descendante à chaque dispositif terminal cible potentiel.

- j) Un dispositif terminal prêt à recevoir des fichiers télécharge le fichier indiqué en liaison descendante depuis la MCG, par exemple en utilisant une interface de service Web exposée uniquement au train par la MCG.
- k) Une fois le téléchargement terminé, le dispositif terminal utilise un mécanisme de vérification de l'intégrité du fichier qui a été transféré au train afin de déterminer si l'intégrité du fichier peut être confirmée.
- l) Une fois l'intégrité du fichier dûment vérifiée, le dispositif terminal envoie un message de réponse à l'interface de service Web exposée par la MCG pour confirmer le bon téléchargement du fichier.
- m) Lorsque la MCG reçoit le prochain message ComID 210 (voir étape e), elle indique à la GCG que le fichier a bien été reçu et distribué. Après quoi, la MCG et la GCG peuvent supprimer le fichier de leurs emplacements de stockage respectifs.

5.6.3.3.2 Définition d'un message

5.6.3.3.2.1 Demande de téléchargement d'un fichier en liaison descendante (ComID 208)

Le message ComID 208 est un télégramme de données de messagerie envoyé par la GCG à la MCG. La GCG utilise ce message pour demander le téléchargement d'un fichier en liaison descendante vers le train; il contient toutes les informations pour permettre le téléchargement d'un fichier vers la MCG.

Le télégramme de demande MD ComID 208 doit être envoyé avec les paramètres d'en-tête suivants conformément au Tableau 36. Pour obtenir des informations générales sur les paramètres d'en-tête des données de messagerie, se référer au Tableau 18.

Tableau 36 – ComID 208: valeurs d'en-tête du télégramme de données de messagerie

Paramètre	Valeur
msgType	3 (demande MD)
msgTimeValidity	0 (aucun délai d'expiration)
comID	208

Le télégramme de demande MD ComID 208 doit être envoyé avec les paramètres de corps suivants conformément au Tableau 37. Pour obtenir des informations générales sur les paramètres de corps des données de messagerie, se référer au Tableau 19.

Tableau 37 – ComID 208: valeurs du corps du télégramme de données de messagerie

Paramètre	Valeur
mdPayloadType	«JSON»
mdPayload	voir Tableau 38

Le télégramme de demande MD ComID 208 doit être envoyé avec l'objet de données utiles suivant conformément au Tableau 38.

Tableau 38 – ComID 208: corps de données de messagerie – objet mdPayload

Élément de données	Description	Type de données	Plage de valeurs	Valeur
objet	Données utiles du paramètre de corps de données de messagerie «mdPayload»	JSON		
fileTransferUID	Identifiant unique. Défini par la GCG, utilisé par la MCG et la GCG pour identifier un fichier téléchargé en liaison descendante.	valeur numérique	uint32	calculée
filename	Nom du fichier à transférer à la MCG puis à un dispositif terminal cible.	chaîne	char[256]	prédéfinie
fileType	Indique le type de fichier qui est téléchargé en liaison descendante.	valeur numérique	uint8	0 = n.a. 1 = ASCII 2 = binaire 3 = audio 4 = vidéo 5-255 pas utilisée
fileSize	Indique la taille du fichier en octets	valeur numérique	uint64	prédéfinie
fileChecksum	Somme de contrôle permettant de vérifier que le fichier a été correctement téléchargé en liaison descendante. Le mécanisme de somme de contrôle utilisé relève du périmètre de l'application.	chaîne	char[256]	calculée
storageURL	URL indiquant l'emplacement à partir duquel la MCG peut télécharger le fichier en liaison descendante.	chaîne	char[512]	prédéfinie
dITarget	Indique le ou les dispositifs terminaux concernés par le téléchargement en liaison descendante. Pour plus d'informations, voir 5.6.3.3.6.	chaîne	char[128]	prédéfinie
recipe	Indique un traitement du fichier téléchargé spécifique à l'application. Peut être traité par la MCG; sinon, doit être ignoré. Pour plus d'informations, voir 5.6.3.3.5.	chaîne	char[512]	prédéfinie

5.6.3.3.2.2 Réponse à une demande de téléchargement en liaison descendante (ComID 209)

Le message ComID 209 est un télégramme de données de messagerie envoyé par la MCG à la GCG. La MCG utilise ce message pour répondre à une demande de téléchargement en liaison descendante envoyée par la GCG. La MCG indique si elle exécutera la demande de téléchargement d'un fichier en liaison descendante vers le train.

Le télégramme de réponse MD ComID 209 doit être envoyé avec les paramètres d'en-tête suivants conformément au Tableau 39. Pour obtenir des informations générales sur les paramètres d'en-tête des données de messagerie, se référer au Tableau 18.

Tableau 39 – ComID 209: valeurs d'en-tête du télégramme de données de messagerie

Paramètre	Valeur
msgType	4 (réponse de données de messagerie à la demande MD reçue)
msgTimeValidity	0 (aucun délai d'expiration)
comID	209

Le télégramme de réponse MD ComID 209 doit être envoyé avec les paramètres de corps suivants conformément au Tableau 40. Pour obtenir des informations générales sur les paramètres de corps des données de messagerie, se référer au Tableau 19.

Tableau 40 – ComID 209: valeurs du corps du télégramme de données de messagerie

Paramètre	Valeur
mdPayloadType	«JSON»
mdPayload	voir Tableau 38

Le télégramme de réponse MD ComID 209 doit être envoyé avec l'objet de données utiles suivant conformément au Tableau 41.

Tableau 41 – ComID 209: corps de données de messagerie – objet mdPayload

Élément de données	Description	Type de données	Plage de valeurs	Valeur
objet	Données utiles du paramètre de corps de données de messagerie «mdPayload»	JSON		
fileTransferUID	Identifiant unique. Utilisé par la MCG et la GCG pour identifier et référencer un fichier téléchargé en liaison descendante.	valeur numérique	uint32	prédéfinie (reprise du message ComID 208)
reqResponse	Réponse de la MCG indiquant si la demande sera exécutée ou non.	valeur numérique	uint8	0 = n.a. 1 = le fichier sera téléchargé 2 = impossible de télécharger le fichier 3..255 = à définir
fileCheckResult	Indique le résultat de la vérification de l'intégrité du fichier téléchargé en liaison descendante.	valeur numérique	booléen	calculée (true, false)

5.6.3.3.2.3 Demande d'état actuel du téléchargement en liaison descendante (ComID 210)

Le message ComID 210 est un télégramme de données de messagerie envoyé par la GCG à la MCG. La GCG utilise ce message pour obtenir des informations sur l'état actuel du téléchargement d'un fichier en liaison descendante vers le train. Ce message peut être envoyé de manière cyclique par la GCG, le temps de cycle étant un élément de configuration.

Le télégramme de demande MD ComID 210 doit être envoyé avec les paramètres d'en-tête suivants conformément au Tableau 42. Pour obtenir des informations générales sur les paramètres d'en-tête des données de messagerie, se référer au Tableau 18.

Tableau 42 – ComID 210: valeurs d'en-tête du télégramme de données de messagerie

Paramètre	Valeur
msgType	3 (demande MD)
msgTimeValidity	0 (aucun délai d'expiration)
comID	210

Le télégramme de demande MD ComID 210 doit être envoyé avec les paramètres de corps suivants conformément au Tableau 43. Pour obtenir des informations générales sur les paramètres de corps des données de messagerie, se référer au Tableau 19.

Tableau 43 – ComID 210: valeurs du corps du télégramme de données de messagerie

Paramètre	Valeur
mdPayloadType	«JSON»
mdPayload	voir Tableau 41

Le télégramme de demande MD ComID 210 doit être envoyé avec l'objet de données utiles suivant conformément au Tableau 44.

Tableau 44 – ComID 210: corps de données de messagerie – objet mdPayload

Élément de données	Description	Type de données	Plage de valeurs	Valeur
objet	Données utiles du paramètre de corps de données de messagerie «mdPayload»	JSON		
fileTransferUID	Identifiant unique. Utilisé par la MCG et la GCG pour identifier et référencer un fichier téléchargé en liaison descendante.	valeur numérique	uint32	prédéfinie (reprise du message ComID 208)

5.6.3.3.3 Réponse à la demande d'état actuel du téléchargement en liaison descendante (ComID 211)

Le message ComID 211 est un télégramme de données de messagerie envoyé par la MCG à la GCG. La MCG utilise ce message en réponse à la GCG pour lui indiquer l'état actuel de la demande de téléchargement d'un fichier en liaison descendante.

Le télégramme de réponse MD ComID 211 doit être envoyé avec les paramètres d'en-tête suivants conformément au Tableau 45. Pour obtenir des informations générales sur les paramètres d'en-tête des données de messagerie, se référer au Tableau 18.

Tableau 45 – ComID 211: valeurs d'en-tête du télégramme de données de messagerie

Paramètre	Valeur
msgType	4 (réponse de données de messagerie à la demande MD reçue)
msgTimeValidity	0 (aucun délai d'expiration)
comID	211

Le télégramme de réponse MD ComID 211 doit être envoyé avec les paramètres de corps suivants conformément au Tableau 46. Pour obtenir des informations générales sur les paramètres de corps des données de messagerie, se référer au Tableau 19.

Tableau 46 – ComID 211: valeurs du corps du télégramme de données de messagerie

Paramètre	Valeur
mdPayloadType	«JSON»
mdPayload	voir Tableau 44

Le télégramme de réponse MD ComID 211 doit être envoyé avec l'objet de données utiles suivant conformément au Tableau 47.

Tableau 47 – ComID 211: corps de données de messagerie – objet mdPayload

Élément de données	Description	Type de données	Plage de valeurs	Valeur
objet	Données utiles du paramètre de corps de données de messagerie «mdPayload»	JSON		
fileTransferUID	Identifiant unique. Utilisé par la MCG et la GCG pour identifier et référencer un fichier téléchargé en liaison descendante.	valeur numérique	uint32	prédéfinie (reprise du message ComID 208)
statFileTransfer	Indique l'état actuel du transfert de fichier à la MCG, tel que le voit la MCG.	valeur numérique	uint8	0 = n.a. 1 = téléchargement vers la MCG non démarré 2 = téléchargement vers la MCG démarré 3 = téléchargement vers la MCG terminé
statFileIntegrity	Indique l'état actuel de la vérification de l'intégrité du fichier effectuée par la MCG.	valeur numérique	uint8	0 = n.a. 1 = vérification de l'intégrité par la MCG non effectuée 2 = vérification de l'intégrité par la MCG exécutée avec succès 3 = échec de la vérification de l'intégrité par la MCG
statFileDistribution	Indique l'état actuel de la distribution du fichier au(x) dispositif(s) terminal(aux) cible(s).	valeur numérique	uint8	0 = n.a. 1 = transfert de fichier au dispositif terminal non démarré 2 = transfert de fichier au dispositif terminal démarré 3 = transfert de fichier au dispositif terminal terminé 4 = téléchargement au dispositif terminal OK

5.6.3.3.4 Traitement des erreurs

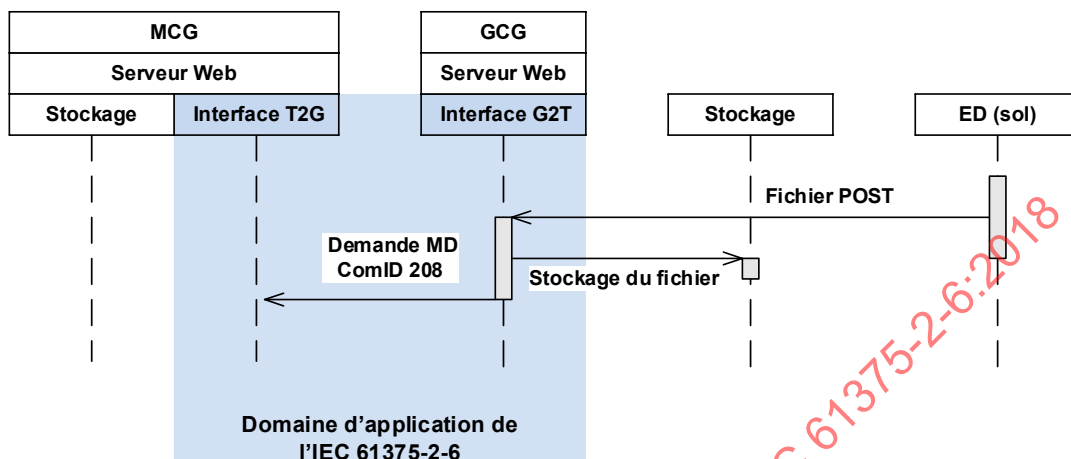
5.6.3.3.4.1 Généralités

Le présent paragraphe répertorie les cas d'erreur qui peuvent se produire lors de l'utilisation du service de transfert de fichiers. Chaque cas d'erreur et le problème associé sont décrits dans un paragraphe distinct.

NOTE Les cas d'erreur qui ne relèvent pas du domaine d'application du présent document ne sont pas décrits dans le présent paragraphe.

5.6.3.3.4.2 Cas d'erreur: aucun message ComID 209 reçu

La Figure 26 présente un cas où la MCG ne reçoit aucun message ComID 209.



IEC

Figure 26 – Cas d'erreur: aucun message ComID 209 reçu

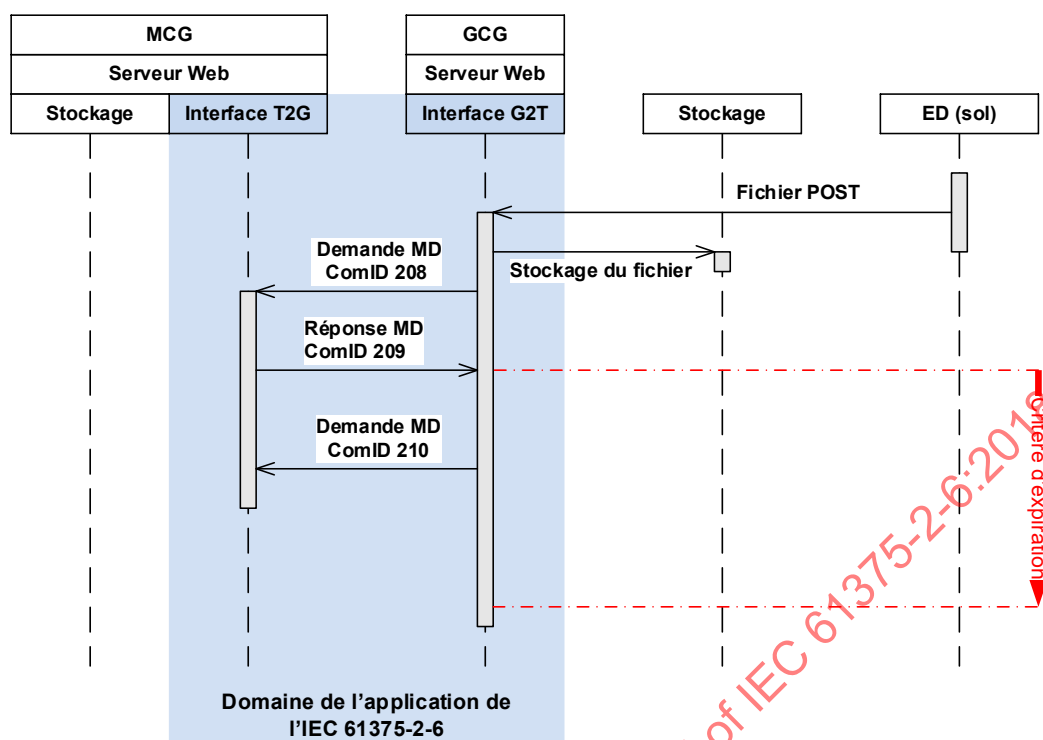
Le message ComID 208 est envoyé par la GCG à la MCG. La GCG utilise ce message pour demander à une MCG de télécharger un fichier en liaison descendante vers le train. La GCG ne reçoit pas de message ComID 209 en réponse à sa demande.

Description du problème: La GCG doit détecter les cas où la MCG n'a pas répondu au message ComID 208 envoyé. L'hypothèse à retenir est que la MCG ne peut pas télécharger le fichier.

Mesure corrective: Aucune demande de téléchargement en liaison descendante ne doit perdurer dans un état indéfini, autrement dit la demande doit être renouvelée ou la demande de téléchargement en liaison descendante doit être interrompue. En outre, il reste encore à télécharger en liaison montante ou à supprimer le fichier déjà placé sous le contrôle de la GCG.

5.6.3.3.4.3 Cas d'erreur: aucun message ComID 211 reçu

La Figure 27 présente un cas où la GCG ne reçoit aucun message ComID 211.



IEC

Figure 27 – Cas d'erreur: aucun message ComID 211 reçu

A la suite d'un précédent échange de messages ComID 208 et ComID 209, la GCG envoie un message ComID 210 à la MCG. La GCG utilise ce message pour vérifier l'état actuel du téléchargement d'un fichier en liaison descendante. La GCG ne reçoit pas de réponse de la MCG à un message ComID 211.

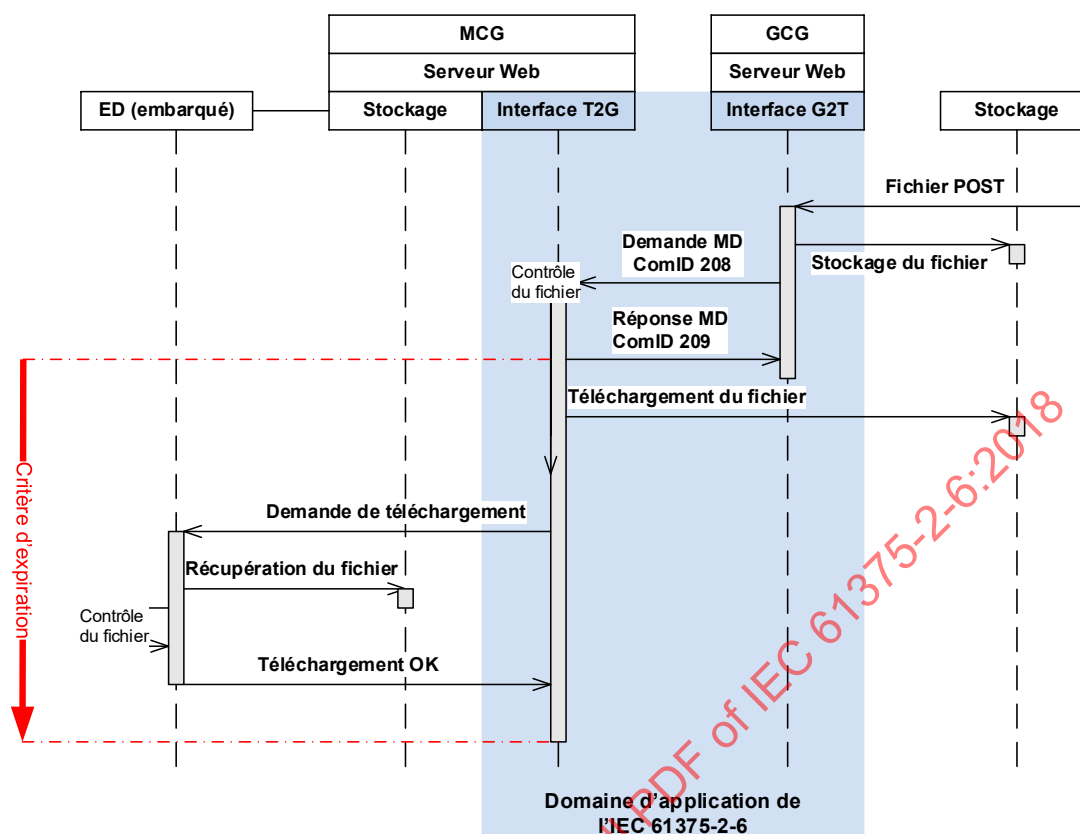
Description du problème: La MCG n'envoie pas le message ComID 211.

Mesure corrective: La GCG doit détecter les cas où la MCG ne répond pas aux demandes d'information sur l'état actuel du téléchargement en liaison descendante, alors que la MCG a bien indiqué qu'elle téléchargerait le fichier.

La GCG doit s'assurer que la demande de téléchargement en liaison descendante ne demeure pas dans un état indéfini, autrement dit la demande doit être renouvelée ou la demande de téléchargement en liaison descendante doit être interrompue.

5.6.3.3.4.4 Cas d'erreur: aucun message ComID 210 reçu

La Figure 28 décrit un cas où la MCG ne reçoit pas de message ComID 210 de la GCG.



IEC

Figure 28 – Cas d'erreur: aucun message ComID 210 reçu

Le message ComID 210 est envoyé par la GCG à la MCG. La GCG utilise ce message pour faire suite à un précédent échange de messages ComID 208 et ComID 209 afin de déterminer si le téléchargement du fichier en liaison descendante vers la MCG, puis vers le ou les dispositifs terminaux cibles a bien été effectué.

A la suite d'un précédent échange de messages ComID 208 et ComID 209, la MCG télécharge le fichier en liaison descendante vers le train. Elle vérifie l'intégrité du fichier, et informe le ou les dispositifs terminaux cibles de la disponibilité du fichier.

Même si le téléchargement s'est correctement terminé, elle ne reçoit aucune demande de la GCG concernant l'état du téléchargement en liaison descendante et la MCG ne peut donc pas lui indiquer la bonne exécution de la demande de téléchargement en liaison descendante.

Description du problème: La MCG ne reçoit pas le message ComID 210. Puisque le fichier peut être correctement téléchargé par la MCG, ce problème ne peut être détecté qu'après que le fichier ait été correctement distribué au(x) dispositif(s) terminal(aux) cible(s).

Mesure corrective: La MCG peut détecter les cas où aucun message ComID 210 n'a été reçu après le téléchargement d'un fichier en liaison descendante vers le(s) dispositif(s) terminal(aux) cible(s). Du point de vue de la MCG, aucune action n'est à effectuer afin d'informer la GCG et le fichier peut donc être supprimé de l'emplacement de stockage de la MCG.

5.6.3.3.5 Formule de téléchargement en liaison descendante

Dans le message ComID 208 (voir 5.6.3.3.2.1), le champ «recipe» peut être utilisé pour inclure une chaîne spécifique à l'application.