BS EN 50463-4:2012

BSI Standards Publication

Railway applications — Energy measurement on board trains -

Part 4: Communication

raising standards worldwide™

National foreword

This British Standard is the UK implementation of EN 50463-4:2012. Together with BS EN 50463-1:2012, BS EN 50463-2:2012, BS EN 50463-3:2012 and BS EN 50463-5:2012 it supersedes BS EN 50463:2007, which is withdrawn.

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

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

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

ISBN 978 0 580 69932 0

ICS 45.060.10

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 January 2013.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50463-4

December 2012

ICS 45.060.10

Supersedes EN 50463:2007 (partially)

English version

Railway applications - Energy measurement on board trains - Part 4: Communication

Applications ferroviaires - Mesure d'énergie à bord des trains - Partie 4: Communications

Bahnanwendungen - Energiemessung auf Bahnfahrzeugen - Teil 4: Kommunikation

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 50463-4:2012 E

Contents

Figures

Tables

Foreword

This document (EN 50463-4:2012) has been prepared by CLC/TC9X "Electrical and electronic applications for railways".

The following dates are proposed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2013-10-15
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2015-10-15

This document (EN 50463-4:2012), together with parts 1, 2, 3 and 5, supersedes EN 50463:2007.

EN 50463-4:2012 includes the following significant technical changes with respect to EN 50463:2007:

— the series is based on and supersedes EN 50463:2007;

— the scope is extended, new requirements are introduced and conformity assessment arrangements are added.

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

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

For relationship with EU Directive 2008/57/EC amended by Commission Directive 2011/18/EU, see informative Annex ZZ, which is an integral part of this document.

This document is Part 4 of the EN 50463 series which consists of the following parts, under the title *Railway applications - Energy measurement on board trains*:

Part 1, General;

Part 2, Energy measuring;

Part 3, Data handling;

Part 4, Communication;

Part 5, Conformity assessment.

This series of European Standards follows the functional guidelines description in Annex A “Principles of conformity assessment” of EN ISO/IEC 17000 tailored to the Energy Measurement System (EMS).

The requirements for Energy Measurement Systems in the relevant Technical Specifications for Interoperability are supported by this series of European Standards.

Introduction

The Energy Measurement System provides measurement and data suitable for billing and may also be used for energy management, e.g. energy saving.

This series of European Standards uses the functional approach to describe the Energy Measurement System. These functions are implemented in one or more physical devices. The user of this series of standards is free to choose the physical implementation arrangements.

Structure and main contents of the EN 50463 series

This series of European Standards is divided into five parts. The titles and brief descriptions of each part are given below:

EN 50463-1 – General

The scope of EN 50463-1 is the Energy Measurement System (EMS).

EN 50463-1 provides system level requirements for the complete EMS and common requirements for all devices implementing one or more functions of the EMS.

EN 50463-2 – Energy measuring

The scope of EN 50463-2 is the Energy Measurement Function (EMF).

The EMF provides measurement of the consumed and regenerated active energy of a railway traction unit. If the traction unit is designed for use on a.c. traction supply systems the EMF also provides measurement of reactive energy. The EMF provides the measured quantities via an interface to the Data Handling System.

The EMF consists of the three functions: Voltage Measurement Function, Current Measurement Function and Energy Calculation Function. For each of these functions, accuracy classes are specified and associated reference conditions are defined. EN 50463-2 also defines all specific requirements for all functions of the EMF.

The Voltage Measurement Function measures the voltage of the Contact Line system and the Current Measurement Function measures the current taken from and returned to the Contact Line system. These functions provide signal inputs to the Energy Calculation Function.

The Energy Calculation Function inputs the signals from the Current and Voltage Measurement Functions and calculates a set of values representing the consumed and regenerated energies. These values are transferred to the Data Handling System and are used in the creation of Compiled Energy Billing Data.

The standard has been developed taking into account that in some applications the EMF may be subjected to legal metrological control. All relevant metrological aspects are covered in EN 50463-2.

EN 50463-2 also defines the conformity assessment of the EMF.

EN 50463-3 – Data handling

The scope of EN 50463-3 is the Data Handling System (DHS).

The on board DHS receives, produces and stores data, ready for transmission to any authorised receiver of data on board or on ground. The main goal of the DHS is to produce Compiled Energy Billing Data and transfer it to an on ground Data Collection Service (DCS). The DHS can support other functionality on board or on ground with data, as long as this does not conflict with the main goal.

EN 50463-3 also defines the conformity assessment of the DHS.

EN 50463-4 – Communication

The scope of EN 50463-4 is the communication services.

This part of the EN 50463 gives requirements and guidance regarding the data communication between the functions implemented within EMS as well as between such functions and other on board units where data are exchanged using a communications protocol stack over a dedicated physical interface or a shared network.

It includes the on board to ground communication service and covers the requirements necessary to support data transfer between DHS and DCS.

EN 50463-4 also defines the conformity assessment of the communications services.

EN 50463-5 – Conformity assessment

The scope of EN 50463-5 is the conformity assessment procedures for the EMS.

EN 50463-5 also covers re-verification procedures and conformity assessment in the event of the replacement of a device of the EMS.

EMS functional structure and dataflow

Figure 1 illustrates the functional structure of the EMS, the main sub-functions and the structure of the dataflow and is informative only. Only the main interfaces required by this standard are displayed by arrows.

Since the communication function is distributed throughout the EMS, it has been omitted for clarity. Not all interfaces are shown.

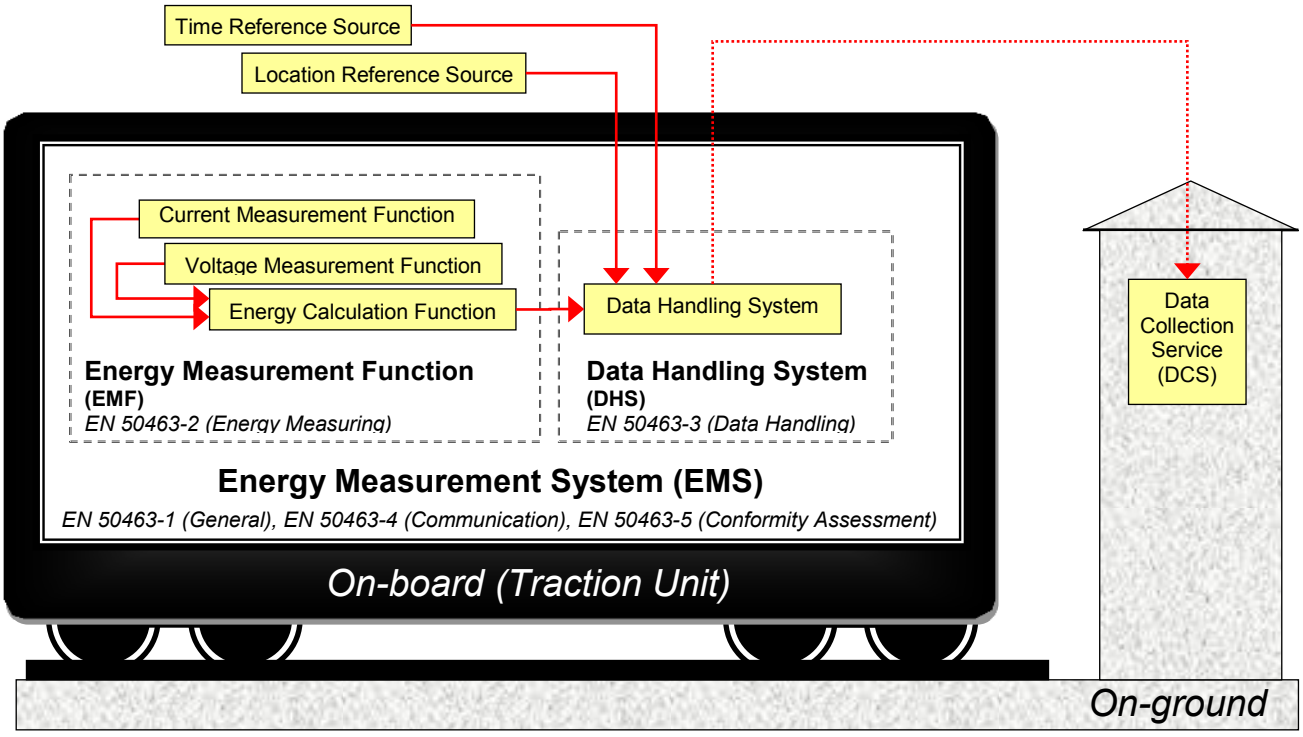


Figure 1 – EMS functional structure and dataflow diagram

1 Scope

This European Standard applies to the on board and on board to ground communication services, i.e. it covers the data communication using digital interfaces:

a) between functions implemented within the EMS;

b) between EMS function and other on board subsystems;

c) between EMS and ground communication services.

The on board data communication services of the EMS are covering the data exchange between functions of the EMS and the data exchange between EMS and other on board units, where data is exchanged using a communications protocol stack over a dedicated physical interface or a shared communication network.

The on board to ground communication services are covering the wireless data communication between the DHS and the on ground server.

Furthermore, this document includes conformity assessment requirements.

2 Normative references

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

EN 50463-1:2012, *Railway applications — Energy measurement on board trains — Part 1: General*

EN 50463-2:2012, *Railway applications — Energy measurement on board trains — Part 2: Energy measuring*

EN 50463-3:2012, *Railway applications — Energy measurement on board trains — Part 3: Data handling*

EN 50463-5, *Railway applications — Energy measurement on board trains — Part 5: Conformity assessment*

EN 60870-5 (all parts), *Telecontrol equipment and systems — Part 5: Transmission protocols (IEC 60870-5 series)*

EN 61158-2, *Industrial communication networks — Fieldbus specifications — Part 2: Physical layer specification and service definition (IEC 61158-2)*

IEC 61375 (all parts), *Electronic railway equipment — Train communication network (TCN)*

ISO 11898-1:2003, *Road vehicles — Controller area network (CAN) — Part 1: Data link layer and physical signalling*

ISO 11898-2:2003, *Road vehicles — Controller area network (CAN) — Part 2: High-speed medium access unit*

ISO/IEC 8482, *Information technology — Telecommunications and information exchange between systems — Twisted pair multipoint interconnections*

ISO/IEC 8825 (all parts), *Information technology — ASN.1 encoding rules*

ISO/IEC 8802-3:2000, *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 method and physical layer specifications*

ISO/IEC 9646-1:1994, *Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 1: General concepts* [1)]

ITU-T Recommendation V.24, *List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)*

RFC 1035, *Domain names: implementation and specification*

RFC 1123, *Requirements for Internet Hosts – Application and Support*

RFC 1535, *A Security Problem and Proposed Correction With Widely Deployed DNS Software*

RFC 2181, *Clarifications to the DNS specification*

TIA/EIA-422-B, May 1994, *Electrical Characteristics of Balanced Voltage Digital Interface Circuits*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 50463-1:2012 and the following apply.

NOTE When possible, the following definitions have been taken from the relevant chapters of the International Electrotechnical Vocabulary (IEV), IEC 60050. In such cases, the appropriate IEV reference is given. Certain new definitions or modifications of IEV definitions have been added in this standard in order to facilitate understanding. Expression of the performance of electrical and electronic measuring equipment has been taken from EN 60359.

3.1.1
Board to Ground Interface
BGI
interface used for the communication between the train and the ground

3.1.2
consist
single vehicle or group of vehicles that are not separated during normal operation; train set and rake of coaches are synonyms

Note 1 to entry: A consist may contain one or more traction units.

3.1.3
consist network
CN
communication network interconnecting communication devices in one consist

Note 1 to entry: It is possible that more than one CN is installed in the same consist.

3.1.4
Consist Network Interface
CNI
interface to an on board consist network used by the EMS and by other on board devices interfacing with the EMS

---

1) Also available as ITU-T Recommendation X.290 (04/95), *OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications – General concepts*

3.1.5
Coordinated Universal Time
UTC
time scale which forms the basis of a coordinated radio dissemination of standard frequencies and time signals; it corresponds exactly in rate with international atomic time, but differs from it by an integral number of seconds

Note 1 to entry: Coordinated universal time is established by the International Bureau of Weights and Measures (BIPM) and the International Earth Rotation Services (IERS).

Note 2 to entry: The UTC scales is adjusted by the insertion or deletion of seconds, so called positive or negative leap seconds, to ensure approximate agreement with UT1.

[SOURCE: ITU-R Recommendation TF.686, modified]

3.1.6
DHS to Service Interface
DSI
interface between the DHS and a maintenance/administration tool

3.1.7
DHS to MCF Interface
DMI
interface between the DHS and the MCF; it may be dedicated or shared on CNI

3.1.8
EMF to DHS Interface
EMDI
interface between the EMF and the DHS

3.1.9
EMF to Service Interface
ESI
interface between the EMF and a maintenance/administration tool

3.1.10
energy delta value
energy consumed and/or regenerated during a time period

Note 1 to entry: See Figure 2 for example.

3.1.11
energy index value
total accumulated energy consumption and/or energy regeneration at the end of a time period

Note 1 to entry: See Figure 2 for example.

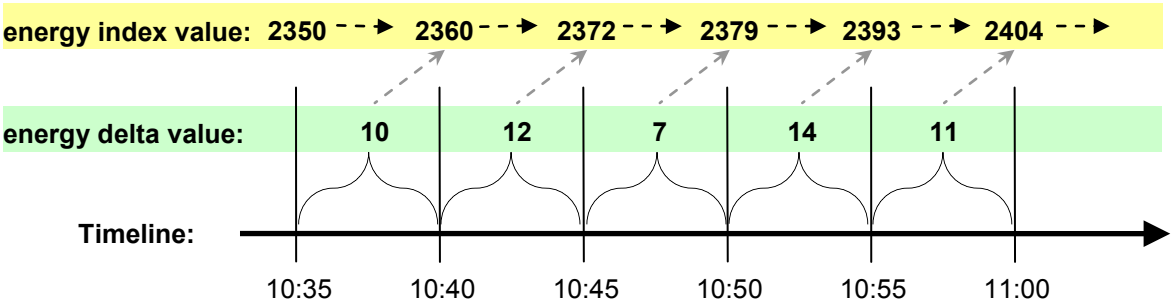


Figure 2 – Example of energy index value

3.1.12
flag
code indicating information relevant to the functioning of the EMS

Note 1 to entry: Examples include data quality, operational status, etc.

3.1.13
Fully Qualified Domain Name
FQDN
domain name which specifies its exact location in the tree hierarchy of the Domain Name System (DNS); it specifies all domain levels, starting from the host name up to the top-level domain

3.1.14
Ground Station
GS
any station on ground which is able to communicate with the EMS

Note 1 to entry: A GS may host different services such as DCS or any EMS management service.

3.1.15
integrity
security measures addressing the detection of a corrupted payload

3.1.16
Internet Engineering Task Force
IETF
organised activity of the Internet Society in charge of producing technical documents relevant to the design, use and management of the Internet

3.1.17
Implementation Under Assessment
IUA
implementation of one or more protocols specified in this part of EN 50463 in an adjacent user/provider relationship being a part of the EMS that is submitted to the conformity assessment

3.1.18
location data
data describing the geographical position of the traction unit

3.1.19
Location Function to DHS Interface
LFDI
interface linking the location function to the DHS

Note 1 to entry: The location function can be interfaced with the DHS via a CNI.

3.1.20
Mobile Communication Function
MCF
function performing the EMS to on ground communication

Note 1 to entry: It includes the sub-function(s) for the wireless link between the train and ground and the sub-functions that execute the communication protocols up to the application interface.

3.1.21
Mobile Communication Gateway
MCG
device that implements the MCF

Note 1 to entry: It may be embedded into the DHS, shared on CNI or connected as a dedicated device by means of the DMI.

3.1.22
non-voluntary change
accidental or unintentional change

Note 1 to entry: Accidental change is caused by unpredictable physical influences, and unintentional change is the effect caused by user functions and residual defects of the software even though the best efforts in development techniques have been applied.

3.1.23
payload
part of the message containing the useful data produced by the source application and used by the destination application

3.1.24
Protocol Analyser
PA
instrument which is used to record and analyse the frames produced by the IUA during the protocol testing

3.1.25
Protocol Frame Generator
PFG
instrument which is used to inject the testing frames into the interface of the IUA

3.1.26
Protocol Implementation Conformity Statement
PICS
document containing the information of the claim of conformity of the IUA in respect of the specification

3.1.27
protective interface
interface which permits intended data to be exchanged, and prevents unintended data being exchanged

3.1.28
Protocol Implementation Extra Information for Testing
PIXIT
document used when testing the user defined aspects of the protocol for the IUA

3.1.29
sensor
device performing the VMF and/or CMF

Note 1 to entry: Sensor is used as a general term and encompasses a wide variety of technology / devices for measurement purposes e.g. inductive transformers, hall-effect devices, capacitive and resistive dividers, and resistive shunts etc.

Note 2 to entry: One sensor can perform multiple functions.

3.1.30
software
executable code, databases, registers and any parameter that affect the software execution

3.1.31
test authority
organisation responsible for conformity testing

3.1.32
test bench
arrangement of test equipment for testing an IUA

Note 1 to entry: Test equipment may include oscilloscopes, signal generators and other instruments.

3.1.33
TGZ
file format and the name of a program used to handle such files

Note 1 to entry: The format was created in the early days of Unix and standardized by POSIX.1-1988 and later POSIX.1-2001.

3.1.34
Time Reference Period
TRP
period of time for which CEBD is produced

3.1.35
Train Control and Monitoring System
TCMS
set of interrelated objects providing on board control and monitoring of the train

3.1.36
UNIX time
EPOCH
number of seconds elapsed since midnight on the 1st of January 1970 according to the Coordinated Universal Time (UTC); coded as a signed integer data type of 32 bits

3.1.37
UTC source to DHS interface
TFDI
dedicated interface of the UTC Source to the DHS

Note 1 to entry: The UTC source can be interfaced with the DHS via a CNI.

3.1.38
verdict
statement of “pass”, “fail”, or “inconclusive”, as specified in an abstract test case, concerning conformity of an IUA with respect to the test case when it is executed

3.1.39
VMF/CMF to ECF Interface
VEI
interface between a VMF/CMF and an ECF

Note 1 to entry: It may be a combined interface for VMF and CMF or two separated interfaces.

3.1.40
voluntary change
intentional change consisting in a modification of software elements and/or modification, loading or swapping of the memory

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

All the abbreviations are listed in alphabetical order.

The definition of some of the abbreviations can be found in EN 50463-1:2012, Clause 3.

BGI Board to Ground Interface

CEBD Compiled Energy Billing Data

CMF Current Measurement Function

CNI Consist Network Interface

CPID	Consumption Point ID
CRC	Cyclic Redundancy Check
DCS	Data Collection System
DHS	Data Handling System
DMI	DHS interface to Mobile Communication Function
DSI	Data Handling System to service interface
ECF	Energy Calculation Function
EMDI	EMF to DHS interface
EMF	Energy Measurement Function
EMS	Energy Measurement System
EPOCH	UNIX Time
ESI	Energy Measuring Function to service interface
EVN	European Vehicle Number
FQDN	Fully Qualified Domain Name
GS	Ground Station
IETF	Internet Engineering Task Force
IUA	Implementation Under Assessment
LFDI	Location Function to DHS interface
MCF	Mobile Communication Function
MCG	Mobile Communication Gateway
NMEA	National Marine Electronics Association
PA	Protocol Analyser
PFG	Protocol Frame Generator
PICS	Protocol Implementation Conformity Statement
PIXIT	Protocol Implementation Extra Information for Testing
RAMS	Reliability, Availability, Maintainability and Safety
SNTP	Simple Network Time Protocol
TCMS	Train Control and Monitoring System
TFDI	UTC Source to DHS interface
TRP	Time Reference Period
UTC	Coordinated Universal Time
VEI	VMF/CMF to ECF interface
VMF	Voltage Measurement Function

4 Requirements

4.1 General

The requirements in EN 50463-1:2012, Clause 4, apply to any device containing one or more implementation of the Communication Services where applicable. EN 50463-4 defines additional requirements specific to the Communication Services.

4.2 On board communication subsystem

4.2.1 General

Figure 3 describes the functional structure of the communication between two functions and/or sub-functions. Embedded communication is implemented using a virtual channel and exposed communication is implemented using physical channel. Whether the communication between functions/sub-functions is performed by a virtual or a physical link, is an implementation choice.

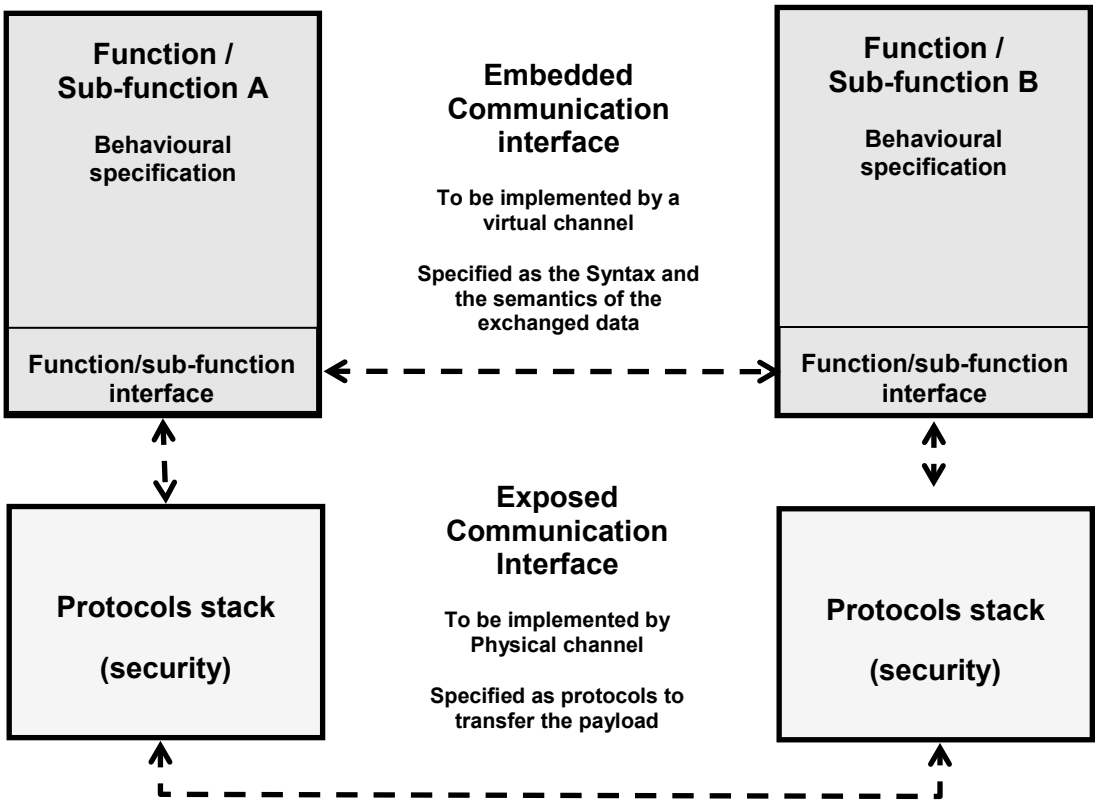
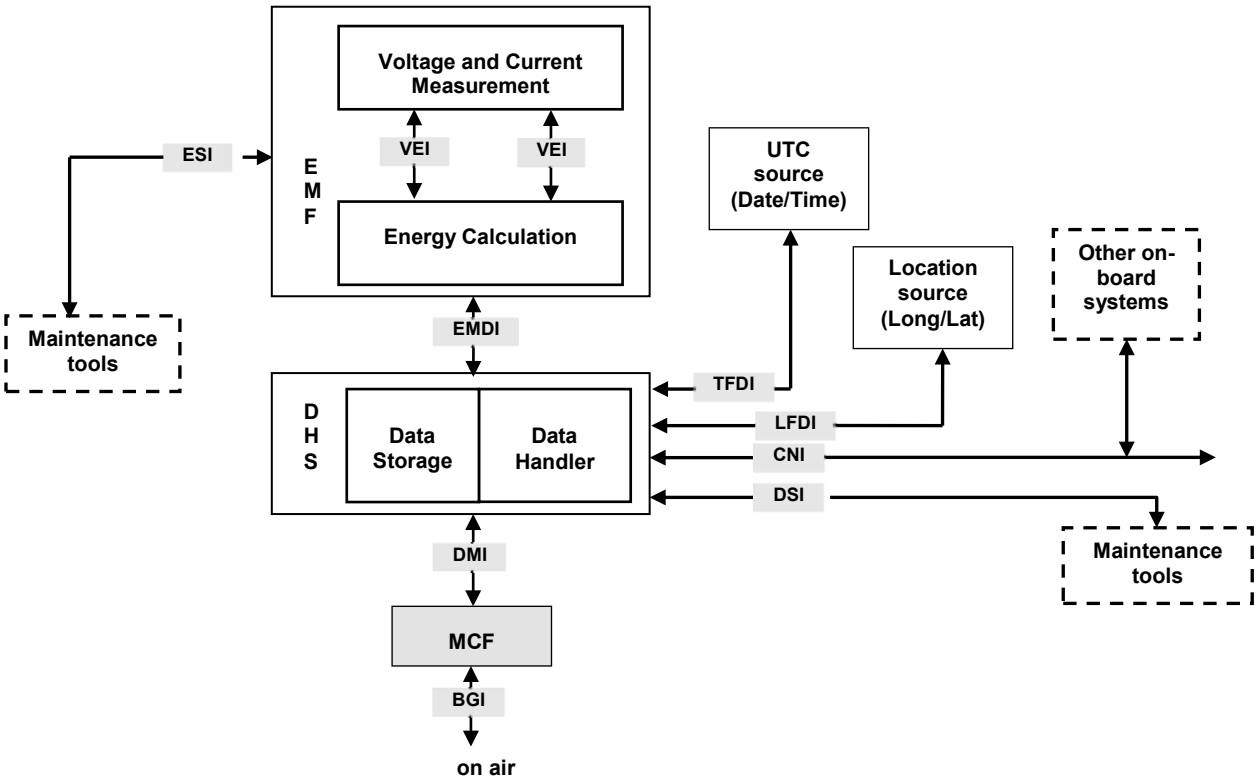


Figure 3 – Communication interface between function/sub-function

The on board communication subsystem covers the specification of the communication protocol stack, the communication security sub-function and the communication profile for digital interfaces where it is implemented using an exposed communication interface over a physical channel. Figure 4 illustrates some of the possible interfaces, noting that some of them may be combined or may be alternative.

Data transfer using an embedded communication interface, implemented using a virtual channel, is specified elsewhere in the relevant part of this series of standards.

Figure 4 shows the EMS functions which communicate through interfaces. The BGI interface is specified in 4.3.



Key

BGI	Board to Ground interface
CNI	Consist Network interface between DHS and other on board subsystems
DMI	interface between DHS and MCF
EMDI	interface between EMF and DHS
ESI	interface between EMF and the maintenance tools
DSI	interface between DHS and the maintenance tools
LFDI	interface between the DHS and location device
TFDI	interface between the DHS and UTC source
VEI	interface between VMF and/or CMF and ECF

Figure 4 – EMS block diagram and interfaces

ESI and DSI are exposed interfaces which are intended to be used for:

1) maintenance;

2) EMF and/or DHS administration;

3) testing.

More than one interface, dedicated to this purpose, may exist according to the structure of the EMS implementation, e.g. if the EMF and DHS are implemented in two separate devices, it is possible to implement one interface attached to EMF and one attached to DHS.

The interface LFDI is required if the data are exchanged between DHS and a dedicated location function. Alternatively, the location function may be interfaced with the DHS via the CNI.

The interface TFDI is required if the data are exchanged between DHS and a dedicated UTC source device. Alternatively, the UTC source may be interfaced with the DHS via the CNI.

The interface DMI is required if the data are exchanged between DHS and a dedicated Mobile Communication Function. Alternatively, the Mobile Communication Function may be interfaced with the DHS via the CNI.

The interface CNI is required if the data are exchanged between DHS and external TCMS subsystems or non-embedded EMS function, e.g. TCMS subsystems attached to the consist network or location device linked to DHS via the shared consist network.

4.2.2 Communication protocols stack

The communication protocol stack executed by each on board physical interface shall be one of those listed in Table 1. A different protocol stack can be used for each interface.

If the protocol chosen from Table 1 is 'user defined', the IUA Supplier shall give the evidence that the capabilities and performance characteristics are comparable with the ones provided by the protocols listed in Table 1 and specified in the referenced standards. The capabilities and the performance parameters shall be reported in the relevant PIXIT that shall be compiled by the IUA Supplier when the IUA is submitted to the Conformity Assessment.

Table 1 – List of permitted protocol stacks

Protocol stack	Physical layer Reference standard	Link layer Reference standard	Upper layer Reference standard
RS232	ITU-T Recommendation V.24	user defined.	user defined
RS485	ISO/IEC 8482	EN 60870-5 (all parts)	Application specific using the following services: S1 (send/no reply) S2 (send/confirm) S3 (request/respond)
RS422	TIA/EIA-422-B, May 1994	EN 60870-5 (all parts)	Application specific using the following services: S1 (send/no reply) S2 (send/confirm) S3 (request/respond)
CANopen	ISO 11898-2:2003	ISO 11898-1:2003	EN 61375-3-3
ETHERNET	ISO/IEC 8802-3:2000	EN 61375-3-4	EN 61375-3-4
MVB	EN 61375-3-1	EN 61375-3-1	EN 61375-3-1
FIP	EN 61158-2	EN 61158-2	EN 61158-2
user defined	user defined	user defined	user defined
NOTE 1 The USB is not listed because it is not specified by a standardisation body recognised by CENELEC. Nevertheless, it may be possible to use it as user defined solution.			
NOTE 2 The RS232 is listed but should be used with care because it is not sufficiently robust for the demanding electromagnetic environment found typically on board of trains.			

Irrespective of the chosen protocol and in order to execute the conformity Design Review and the Conformity Test procedure, the IUA Supplier shall provide the PICS relevant to this protocols stack and the mapping to the specifications stated in the clauses relevant to the design review and to the Conformity module test procedure.

4.2.3 Communication security

4.2.3.1 General

4.2.3 specifies the requirements for achieving the proper level of communication security of the interface. The communication security shall assure the integrity and authenticity of the exchanged payload data.

Referring to integrity, it shall be assured that the risk of accepting exchanged information containing unintentional or accidental changes and/or intentional changes is reduced to an acceptable level.

Referring to authenticity, it shall be assured that the risk of accepting exchanged data transmitted by a wrong source function/sub-function and received by the wrong consumer function/sub-function is reduced to an acceptable level.

In order to reach an acceptable level, two cases are considered:

1) data transfer is protected by physical means;

2) data transfer is protected by software means.

The protection by physical means is specified in EN 50463-1:2012, 4.3.5.1 and 4.3.5.2.

4.2.3.2 Security implemented by software

4.2.3.2.1 General

If the physical means cannot assure an adequate security level, the security shall be assured by a dedicated software layer that shall be added to the communication protocol stack of the relevant interface.

The protection by software shall respect the general requirements specified in EN 50463-1:2012, 4.3.4.2, 4.3.4.3, 4.3.4.4, 4.3.4.5 and 4.3.5.3.

The software security layer shall provide:

a) the data integrity at application level;

b) the authenticity to ensure data transfer over the interface only occurs between the correct devices. This is optional if the requirement a) adequately covers the detection of data changes (caused by intentional and unintentional actions).

NOTE Bounding is one method for ensuring authenticity.

When the secrecy of data is required by the purchaser and agreed with the supplier, the software security layer may provide encryption of the transferred data.

4.2.3.2.2 Data integrity

The integrity of the data shall be assured by an error detecting code applied at application level on the payload data.

The type of error detecting code and its length shall be chosen considering the payload length in order to assure at a reasonable level that any change in the payload data is detected.

NOTE CRC is one method for communication error detecting.

4.2.3.2.3 Bounding procedure and data encryption

This clause is informative.

The bounding procedure is applied in order to generate a secret key that is transferred under controlled condition between the two units that communicate throughout the interface. The key is generated by the master unit and transferred in a controlled environment to the slave unit. This key is used to encrypt the payload by the transmitting unit and to decrypt the payload extracted from the received frame by the receiving unit.

This procedure is executed attaching the maintenance tool (e.g. a PC) to the maintenance interface of the master unit and activating the procedure after a successful authentication based on User ID and password owned only by the authorised personnel.

As soon as the bounding procedure is started, the following events occur.

a) The master unit generates a key and stores it in a dedicated memory cell that cannot be accessed in the future except by the software that has to decrypt the payload.

b) The key is transmitted to the slave unit that stores it in a dedicated memory cell that cannot be accessed in the future except by the software that has to encrypt the payload.

c) The encryption and decryption of a known payload is transmitted from the master unit to the slave unit and vice-versa to check that the two are correctly bounded.

d) The procedure is closed.

4.2.4 VMF/CMF to ECF Interface (VEI)

If this interface is digital, it shall be implemented according to EN 50463-2:2012, 4.3 and 4.4, and the requirements listed in this document under 4.2.2 and 4.2.3.

An example of implementation is given in informative Annex B.

NOTE VEI may be implemented as a shared interface like CNI provided that the performance, safety and security level is adequate and comparable with the level of a direct and exclusive serial interface.

4.2.5 EMF to DHS interface (EMDI)

This shall be a protective interface.

This interface shall be implemented according to one of the following options:

a) a direct and exclusive serial interface between EMF and DHS;

b) a shared interface like CNI provided that the security level is adequate and comparable with the level of a direct and exclusive serial interface.

The interface shall transfer at least the data in accordance with EN 50463-2 and EN 50463-3.

4.2.6 Maintenance/testing interfaces (DSI and ESI)

This shall be a protective interface.

This is a serial interface to be used by the tools dedicated to the EMS maintenance and testing.

If the EMF and DHS functions are implemented in a single device, at least one interface shall be provided for the maintenance and testing purposes.

If the EMF and DHS functions are implemented in two separate devices, one of the two cases shall apply:

Case 1: there is only one maintenance/testing interface that shall be controlled by the main processing unit of the DHS. In this case, a software module, called the agent, is in charge of routing the information relevant to the maintenance/testing of EMF through the EMDI interface invoking a software module, called the manager, which is in charge of executing the maintenance/testing tasks in the EMF.

Case 2: there are two interfaces dedicated to maintenance/testing, one attached to the device implementing the DHS function and one attached to the device implementing the EMF function.

NOTE The above statements give maintenance/testing interfaces requirements when the implementation of an EMS is done with multiple devices.

The access shall be controlled according to the requirements specified in EN 50463-1:2012, 4.3.2.1.3 and 4.3.2.2.

4.2.7 DHS to location function

Two interfaces are possible:

a) the LFDI interface;

b) the CNI interface that connects the DHS to the location function by means of the consist network digital interface.

If the case a) applies, the interface shall be a direct and exclusive serial interface to the location function.

If the case b) applies, requirements are given in 4.2.9.

The interface shall transfer location information in accordance with EN 50463-3:2012, 4.4.

If this interface is able to provide UTC information compliant to the specification given in EN 50463-3:2012, 4.2, it can be used as UTC source interface.

4.2.8 DHS to UTC source

Two interfaces are possible:

a) the TFDI interface;

b) the CNI interface that connects the DHS to the UTC source by means of the consist network digital interface.

If case a) applies, the interface shall be a direct and exclusive interface between a UTC source and the DHS. No other on board subsystem shall be attached to this time function by any means or interface.

If the case b) applies, requirements are given in 4.2.9.

The information from UTC source is used to synchronise the internal DHS clock. This interface may be a serial interface that is transmitting date and time or a serial interface plus a pulse per second line.

The communication shall assure that the synchronisation error, due to the communication itself, is less than 500 ms.

If the UTC source does not provide a UTC date and time updated according to the leap second adjustment, it shall provide the information of the offset of its own date and time to the UTC date and time with leap second adjustment.

4.2.9 DHS to Consist Network digital interface (CNI)

The CNI interface can connect the DHS to other on board devices and/or to EMF as specified in 4.2.5.

The data exchanged over this interface are:

a) CEBD and CEBD related data;

b) non-CEBD related data.

This shall be a protective interface if the exchanged data is listed in point a). The protection shall be assured by a security software layer that is put between the communication stack and the application software that consume and/or produce CEBD and CEBD related data. This applies respectively to DHS and to the on board devices that communicate with DHS by means of the consist network.

The exchange of CEBD related data via a CNI can be expected to occur, if the DHS uses data from devices located elsewhere in the consist to provide time data and location data.

The preferred types of CNI interfaces and relevant communication protocol stacks are specified in IEC 61375.

4.3 On board to ground communication subsystem

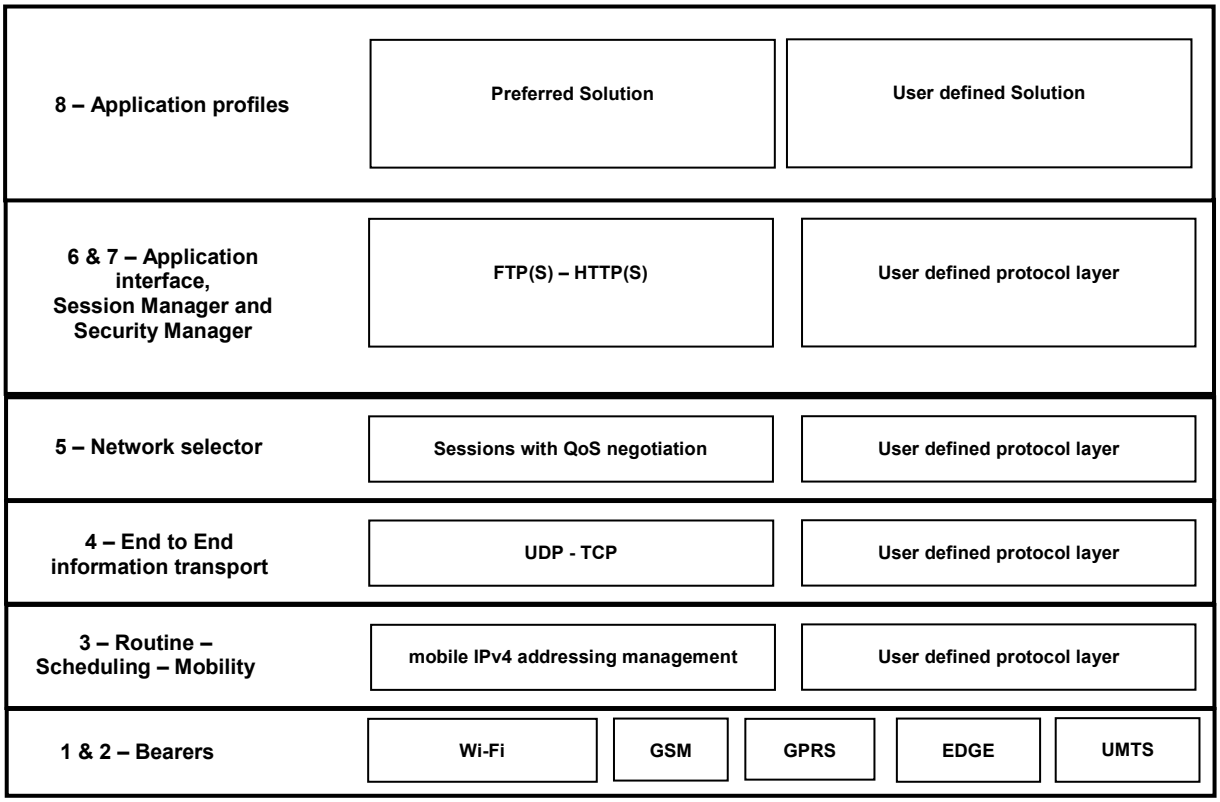
This clause sets out the specification of the on board to ground communication subsystem. The basic requirements are set in EN 50463-1 and EN 50463-3.

Two options shall apply:

1) the preferred solution that is specified in Annex A;

2) the user defined solution that is specified by the agreement between the parties (e.g. purchaser and supplier).

Figure 5 describes the structure of the communication stack, the identification of the stack layers is shown on the left, the preferred solution stack is shown in the middle and the user defined solution stack is shown on the right, except for the layers “1 and 2 bearers” that are applicable to both solutions.



NOTE 1 GSM bearer covers GSM or GSM-R and GPRS covers GPRS or GPRS-R.

NOTE 2 IPv4 is indicated in the layer 3 being the recommended addressing, nevertheless IPv6 may be used.

NOTE 3 Wi-Fi indicates the bearers specified in IEEE 802.11-2007.

Figure 5 – On board to ground communication stack

The layers 1 and 2 list different bearers that can be applicable to the preferred solution and to the user defined solution. More than one bearer can be implemented in the MCG. It shall be noted that, for clarity, not all possible bearers are listed in Figure 5. Any bearer, even those not listed, may be used as far as it is specified by a standardisation body.

4.4 Access security

Access to the EMS data and data structures shall be under access control according to EN 50463-1:2012, 4.3.2.1.1 and 4.3.2.2.

5 Conformity assessment

5.1 General

Any communication service executed by the EMS shall be assessed according to the methods specified in Clause 5.

The conformity assessment methods specified in Clause 5 cover the requirements specified in Clause 4 and in EN 50463-1:2012, 4.3.2, 4.3.3 and 4.3.4.

The conformity testing requirements in Clause 5 applies only to parts of the EMS (on board communication and on board to ground communication services).

The Clause 5 is developed with reference to the conformity testing approach specified in ISO/IEC 9646-1.

When submitting the user defined solution to the conformity assessment, the IUA supplier shall provide the specification of the user defined communication stack from layer 3 to 8.

5.1.1 Applicability

The conformity assessment methods specified in Clause 5 shall be performed and concluded for any device carrying any communication service covered by Clause 4.

5.1.2 Methodology

The conformity assessment shall be executed by the following methods to be applied to the communication services following the list order:

a) communication services design review;

b) communication services type test;

c) communication services routine test;

All conformity assessment activities at EMS level are contained in EN 50463-5.

NOTE The communication services include the physical layer that is implemented in hardware by a physical device.

5.2 PICS and PIXIT

5.2.1 General

The PICS relevant to Clause 4 of this document are listed herein after and are used by 5.3 and 5.4.

The supplier shall determine what extra IUA specific information is necessary for protocol testing. The IAU supplier shall complete a PIXIT pro-forma with the necessary information, and make it available.

5.2.2 PICS

To evaluate the conformity of a particular architecture, it is necessary to have a statement of the capabilities and options that have been implemented, and any features which have been omitted, so that the architecture can be checked for conformity against relevant requirements, and against those requirements only. Such a statement is called a Protocol Implementation Conformity Statement (PICS). The structure and instructions for completion of the PICS are given in the informative Annex C.

5.2.3 PIXIT

In order to test a protocol implementation, the test authority will require information relating to the IUA and its testing environment in addition to that provided by the PICS. This "Protocol Implementation eXtra Information for Testing" (PIXIT) will be provided by the supplier submitting the implementation for testing, as a result of consultation with the test authority.

The PIXIT may contain the following information:

a) information needed by the test authority in order to be able to run the appropriate test suite on the specific system (e.g. information related to the test method to be used to run the test cases, addressing information);

b) information already mentioned in the PICS and which needs to be made precise (e.g. a timer value range which is declared as a parameter in the PICS should be specified in the PIXIT);

c) information to help determine which capabilities stated in the PICS as being supported are testable and which are not testable;

d) other administrative matters (e.g. the IUA identifier, reference to the related PICS).

The PIXIT shall not conflict with the appropriate PICS.

The supplier should ensure that the entities responsible for the abstract test suite, the test implementation, and test authority all contribute to the development of the PIXIT pro-forma.

5.3 Design review

The Design Review shall assess that the protective interfaces have the adequate means to assure that the voluntary changes of the software are granted only to the authorised and authenticated entity, the non-voluntary changes of the software are not possible or at least are detected and reported.

NOTE One aim of the design review is to verify that the requirements of EN 50463-4 are implemented by the design of the IUA in order to ensure that a pass verdict, obtained as result of the execution of the Conformity Testing, has a high level of confidence to be maintained in all the real working conditions.

5.4 Type test procedure

5.4.1 General

The following procedure shall be applied in order to assess the conformity to the specification of the IUA that implements the Communication Services of the EMS.

NOTE Protocols implemented by previously approved software are not to be tested.

5.4.2 Testing the communication

The communication test shall be executed respecting the specification given in ISO/IEC 9646-1 with the aim of checking the conformity of the IUA to the requirements specified by this document and the PICS and PIXIT provided to the test authority by the IUA supplier.

5.4.3 Testing the on board interfaces

5.4.3.1 General

Each interfaces covered by this document shall be tested according to the following approach which is applicable to type testing and routine testing.

5.4.3.2 Test bench

The test bench shown in Figure 6 shall be used:

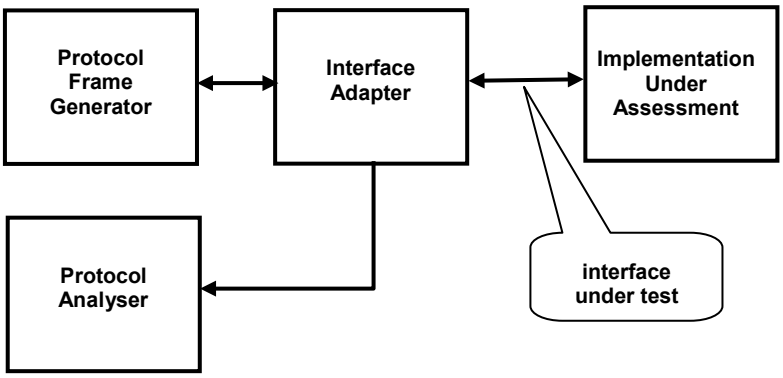


Figure 6 – Test bench for on board interface

The Protocol Frame Generator is a programming and testing station capable of injecting into the IUA interface non-corrupted frames and corrupted frames in order to test the interface itself for all capabilities.

The Interface Adapter is a passive device that connects the Protocol Frame Generator interface to the IUA interface and to the PA interface eventually adapting the voltage level of the signals.

The Protocol Analyser is a testing unit that is able to monitor and record the frame traffic present on the interface under test and to compare such record with the expected traffic and traffic parameters, e.g. time-outs and frame spacing.

5.4.3.3 Abstract test suites

With reference to 4.2 and the PICS and PIXIT provided for the IUA, the abstract test suite shall be performed in order to execute:

a) basic interconnection tests, which provide *prima facie* (at a first examination) evidence that an IUA conforms to the specification clauses in this part of EN 50463;

b) capability tests, which check that the observable capabilities of the IUA are in accordance with the static conformance requirements and the capabilities stated in the PICS;

c) behaviour tests, which endeavour to provide testing which is as comprehensive as possible over the full range of dynamic conformance requirements within the capabilities of the IUA.

No conformity resolution tests are required.

With reference to Figure 3, all the interfaces between EMS sub-functions, e.g. EMDI, shall be tested by two different sessions:

1) **First Session:** the sub-function A is performed by the IUA and the sub-function B is performed by the Protocol Frame Generator. The traffic produced during the test is recorded by the Protocol Analyser and compared with the expected traffic according to the tested requirements.

2) **Second Session:** the sub-function B is performed by the IUA and the sub-function A is performed by the Protocol Frame Generator. The traffic produced during the test is recorded by the Protocol Analyser and compared with the expected traffic according to the tested requirements.

With reference to Figure 3, all the physical interfaces between an EMS function/sub-function and any external device shall be tested by just one session where the EMS function/sub-function is performed by the IUA and the external device is performed by the Protocol Frame Generator.

If the protocols running on the EMS interface are conforming to norms that specify Conformity testing, the EMS interface shall be also submitted to such Conformity testing, e.g. a CNI conforming to IEC 61375.

The a) and b) tests are performed by the IUA supplier, the test procedure and the test report shall be provided. A positive verdict of the a) and b) tests is a prerequisite to execute the c) tests.

5.4.4 Testing the on board to ground interface

5.4.4.1 General

The on board to ground interface implemented according to the specification of this document, (whether preferred solution or user defined solution) shall be tested on air, i.e. at the level of the wireless transfer, according to the following approach.

5.4.4.2 Test benches

The following test benches shall be used.

The test bench 1, see Figure 7, is used to execute the basic capability tests and the interconnection tests.

The test bench 2, see Figure 8, is used to execute the basic capability tests and the behaviour tests, particularly the addressing capability are tested.

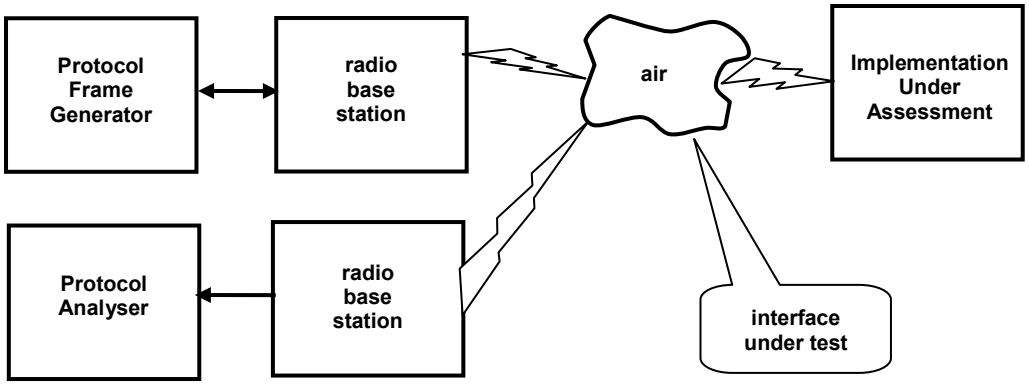


Figure 7 – On board to ground test bench 1

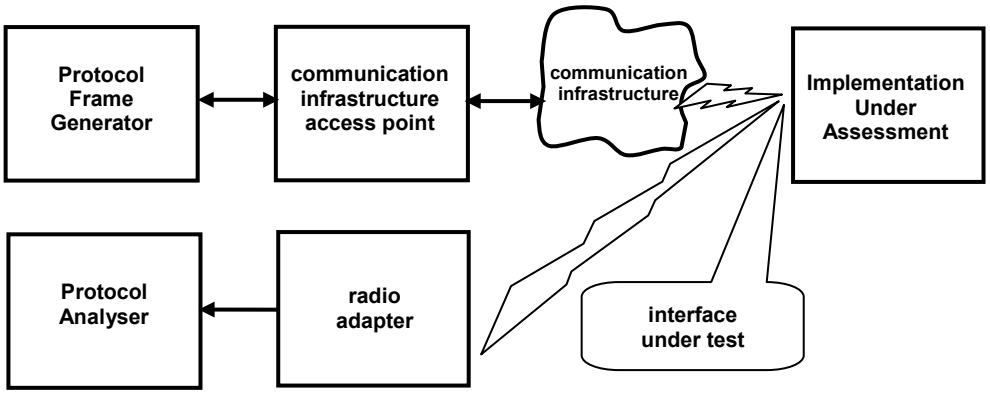


Figure 8 – On board to ground test bench 2

5.4.4.3 Abstract test suites

With reference to 4.3 and to the provided PICS and PIXIT completed and supplied by the IUA supplier, the Abstract Test Suites shall be performed in order to execute:

a) basic interconnection tests, which provide *prima facie* (at a first examination) evidence that an IUA conforms to the specification clauses in EN 50463-4;

b) capability tests, which check that the observable capabilities of the IUA are in accordance with the static conformance requirements and the capabilities stated in the PICS;

c) behaviour tests, which endeavour to provide testing which is as comprehensive as possible over the full range of dynamic conformance requirements within the capabilities of the IUA.

No conformity resolution tests are required.

The a) and b) tests are performed by the IUA supplier, the test procedure and the test report shall be provided. A positive verdict of the a) and b) tests is a prerequisite to execute the c) tests.

Annex A
(normative)

On board to ground communication preferred solution

A.1 Communication services

This annex specifies one of two options as set out in 4.3.

A.1.1 General

A train, as a cluster of devices connected by a network, is "a mobile object" that is performing some services like passenger information, train identification, fleet management and energy measuring for billing and saving purposes. The train is connected to the Ground Station with a set of wireless connections and is capable of switching between them “on the fly” according to the requirement of bandwidth requested by the “service”.

Figure A.1 shows the key components for the communication scenario. The following clauses cover the interaction between the network’s elements existing between the Ground Station and the on board MCG. The behaviour of the MCG depends on the EMS architecture:

- in case of shared MCG, it acts as a proxy, representing the train functional structure to the ground network;
- in case of dedicated MCG, it acts as an IP sub domain allowing each function/service to be reached through its functional address.

Considering the existing network structures and services of the railway operators, key points are the interoperability of the system and the communication protocols of the applications.

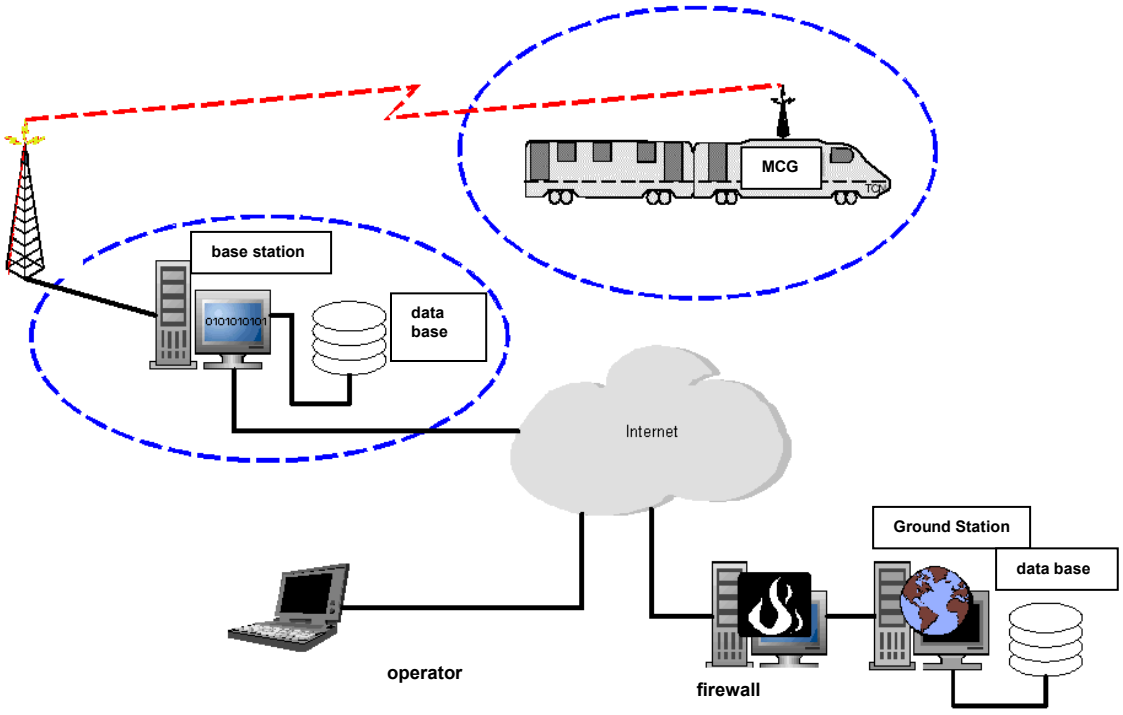


Figure A.1 – Communication components

A.1.2 General requirements

A.1.2.1 General

The on board mobile communication subsystem shall meet the following general requirements:

a) stable connection from the application point of view irrespectively of changes of the mobile communication networks and providers when the train is moving through different areas (countries and regions);

NOTE Stable connection is referred to the application interface and does not mean a permanent physical connection.

b) hand-over according to Quality of Service parameters in case that more than one bearer is available in the MCG. Provided by the network selector protocol;

c) hand-over of network provider according to roaming availability. Provided by the network selector protocol;

d) communication security (authentication, authorisation and, if required, encryption).

Some trains could have a communications unit dedicated to the DHS, and a general purpose communications unit which is also available to the DHS. Where the DHS can use both units, the application interface between DHS and communications units shall be based on middleware which ensures the requirements listed in a) to d) are fulfilled.

A.1.2.2 Addressing requirements

The on board mobile communication subsystem shall fulfil the following particular requirements:

- management of the IPv4 and/or IPv6 addresses;
- mapping between physical addressing and logical addressing;
- addresses and functions discovery.

NOTE IPv6 is not so widely supported at this time.

The addressing of the EMS and ground server shall be based on a FQDN as specified by the following IETF documents: RFC 1035, RFC 1123, RFC 1535 and RFC 2181.

A.1.2.3 EMS addressing

The address of the EMS shall be unique and allow the identification of more than one EMS installed on the same vehicle or consist.

The FQDN is derived from the Consumption Point ID and has the following format:

CPID.owner.ns

where:

- CPID is composed by 13 characters having the format EVNn:
  - EVN is the European Vehicle Number. It is the unique identifier of the vehicle/consist on which one or more EMS are installed and is composed of 12 characters;
  - n is the number identifying the EMS installed in the consist;
- owner is a set of character identifying the vehicle owner;
- ns are two characters identifying the member state of the owner of the vehicle/consist.

The above specified domains shall be used to produce the FQDN to be recorded in the DNS and stored in the GS data base that contains the list of the EMS that are allowed to transfer data to that GS.

NOTE The EMS can carry fictitious CPID until the EMS is commissioned into commercial use.

A.1.2.4 GS Addressing

The address of the GS shall be unique and the corresponding FQDN has the following format:

GSF.owner.ns

where:

- GSF is the function identifier composed by the three characters;
- owner is the GS owner identification that may be any sequence of six characters;
- ns are two characters identifying the member state of the owner of the GS.

NOTE Examples of the GSF function are Data Collecting Server and Fleet Management Server.

A.1.2.5 Communication stack requirements

Figure 5 shows the layering of the quasi-OSI model that has minor differences from the OSI model and includes the communication stack (layer 1 to 5), the communication profile (layers 6 and 7) and the application profile (layer 8).

The preferred solution shall use the stack shown in the middle of Figure 5.

A.1.2.6 Communication hierarchy

The communication between the on board subsystem and the ground subsystem is based on a client-server hierarchy where:

- the on board subsystem is the client;
- the ground subsystem is the server.

The connection is initiated and established by the client.

The data transfer between EMS and the DCS shall use client initiated spontaneous transfer, which also ensures the requirements specified in EN 50463-3:2012, 4.9.3, are respected.

In addition, the data transfer may also use transfer which is initiated when the DHS receives a request from the server.

The EMS is identified by a logical address defined as FQDN and a dynamic IP address.

The DCS is identified by a logical address defined as FQDN and a fixed IP address.

In case of the spontaneous transfer approach, the EMS calls the DCS and establishes a communication session that is used for transferring data from EMS to DCS. The session is closed as soon as the DCS sends an application acknowledge that confirms to the EMS that the files were correctly received and correctly checked for integrity and authenticity.

If the transfer is initiated by request from the server, the EMS calls the GS and establishes a communication session to invite the GS to request for the relevant services. This session is opened at least once every 24 h and is closed:

- by time-out if GS is not answering (the time-out duration shall be agreed between the EMS and GS owners);
- when the requested service is completed.

If the transfer is not successful, EMS shall retry periodically until the requested service is completed.

The supplier and purchaser should consider the frequency of the communication session opening, taking into consideration the further use of the data on ground.

A.1.3 Communication services specification

The services listed in Table A.1 shall be implemented according to the capability of the EMS.

All the services are invoked remotely using the on board to ground interface and may be locally invoked using the service interface(s).

The communication services are used by the application services specified in A.1.4.

Table A.1 – Preferred solution communication services

Service	Short description
Initd	Super-demon for communication network management used to: • configure and monitor the network communication ports; • launch the communication services; • managing the FTP and Telnet services.
Telnetd	Telnet service to be used for remote maintenance of the EMS.
Httpd	Web Server that provides WEB pages for the management of the following services: • EMS functional parameters management; • EMS hardware and software configuration; • application software updating.
ECFd	Service for real time reading of converted voltage and current values respectively coming from the VMF and the CMF
Ppp-client	PPP service for the serial service interface, e.g. ESI and DSI
Ftp server and Ftp client	FTP services used for: • uploading and downloading of the configuration files; • board to ground transfer of CEBD; • uploading and downloading of any non CEBD related data files.
NOTE The **ECFd** service is useful for diagnostic and testing purposes when the output interfaces of digital sensor are not exposed.	

A.1.4 Application services specification

The application services listed in Table A.2 shall be implemented according to the capability of the EMS.

All the services are invoked remotely from the on board to ground interface and may be locally invoked using the service interface(s).

All the services listed in Table A.2 shall be invoked under access control.

Table A.2 – Preferred solution application services

Service	Classification	Short description
ECF supervision service	mandatory	This service can be activated and suspended. Once activated the service transmits the energy data spontaneously until it is suspended. The transferred data are identified by the EMS unique identifier, the measuring channel and a time stamping. The following values may be requested: 1. CEBD data; 2. user defined values e.g. energy, voltage and current. This service, when activated, provides quality measurement notification transmitting a string in case that a diagnostic event is detected by the run time self test which verifies the capability of the ECF to produce measurement values that are within the specifications of EN 50463-2. NOTE Do not confuse this service to be used for supervision purposes with the service that transmit the CEBD files for DCS use.
EMS Functional Configuration and CEBD downloading service	mandatory	The following functionalities shall be provided by this service: 1. VMF configuration (Read-Write-Change); 2. CMF configuration (Read-Write-Change); 3. TRP and other time parameters configuration (Read-Write-Change); 4. EMS configuration status request; 5. EMS configuration file request; 6. CEBD file spontaneous transmission activation/suspension; 7. non-CEBD related spontaneous transmission activation/suspension.
Web Service	mandatory	Web Service which provides WEB pages for the management of the following functionalities: 1. new software release loading; 2. EMS hardware configuration (e.g. board composition, option installed/not installed, interfaces activated/not activated); 3. EMS software configuration (e.g. software modules composition, option installed/not installed, IP addressing, message filtering); 4. CEBD file transmission on demand (request to transfer a CEBD file including records from a starting date to an end date); 5. calibration mode; 6. CEBD memory data dumping; 7. real time visualisation of the main functional EMS parameters and EMS produced data.
SNTP	optional	EMS internal clock synchronisation to UTC by means of the Simple Network Time Protocol.
Location	optional	EMS transfer of the NMEA string received from the GPS unit

A.2 EMS data transfer

A.2.1 CEBD transmission record format

The data relevant to each Time Reference Period are retrieved from the memory and used to prepare the records to be transferred as a CEBD file up to 128 records of 128 byte each. The file shall have a header file according to A.2.3.

NOTE 1 The choice of file of 128 records is a trade-off between file length and transmission duration, this allows to transmit data relevant to about 10 h recording.

Transmission in more than one session per day will reduce the risk of failure due to non-availability of communication.

CEBD data shall not be manipulated, only casting operation are performed, e.g. the end time of the measurement time reference period that is coded as YYYYMMDDHHMMSS according to the EN 50463-3 is casted as EPOCH according to UNIX time format.

NOTE 2 The EPOCH format is chosen because it is used widely in Unix-like and many other operating systems and file formats. Furthermore it is used in EN 61375 and it is consequently available in vehicles equipped with the CN specified by such standard. Casting operations are permitted in order to take advantage of the use of object-oriented programming.

According to EN 50463-2:2012, Annex B, in some cases, the EMS may need to transmit data using more than one channel (e.g. where an EMS handles multiple traction supply systems and stored values for each system separately).

In such cases, channels shall be paired as Channel A and Channel B.

The relevant data shall be used to compile the corresponding record. When the EMS requires an odd number of channels, the record with the unused channel (Channel B), shall have the unused fields populated to indicate that they are void fields using the coding described at the end of this clause.

The record includes some further optional fields that may be filled with ancillary data.

The record format was chosen following the principle of being unspanned and rigid in the channel data field in order to be easily used even when data relevant to some fields are not implemented.

After preparing the record in the transmission buffer and including the application CRC as the last record field and prior to the file transmission, the CEBD in the record shall be verified against the CEBD stored into the DHS memory.

Table A.3 – Record format

Data Type	Data Attribute	Data Id	Short Description
WORD	Mandatory	label	Label to identify the starting of the record
DWORD	Mandatory	key	Binary value to identify the record number
DWORD	Mandatory	tm	Number of seconds from EPOCH corresponding to the end of the TRP
DWORD	Mandatory	Lat	Latitude at the end of the TRP (degrees dot decimals)
DWORD	Mandatory	Lon	Longitude at the end of the TRP (degrees dot decimals)
DWORD	Mandatory	EmA	Channel A Consumed Active Energy delta value (KWh dot decimal)
DWORD	Mandatory	EmnA	Channel A Regenerated Active Energy delta value (KWh dot decimal)
DWORD	Mandatory	ErA	Channel A Consumed Reactive Energy delta value (kvarh dot decimal)
DWORD	Mandatory	ErnA	Channel A Regenerated Reactive Energy delta value (kvarh dot decimal)
DWORD	Mandatory	flagsA	Channel A CEBD flags: Energy data, Location data, time data (spare bits available)
DWORD	Optional	EtA	Channel A Consumed Active Energy index value (KWh dot decimal)
DWORD	Optional	EtnA	Channel A Regenerated Active Energy index value (KWh dot decimal)
DWORD	Optional	EtrA	Channel A Consumed Reactive Energy index value (kvarh dot decimal)
DWORD	Optional	EtrnA	Channel A Regenerated Reactive Energy index value (kvarh dot decimal)
WORD	User defined	VminA	Voltage minimum of channel A in the TRP (Volt)
WORD	User defined	IvminA	Current value at the voltage minimum of channel A in the TRP (Ampere)
DWORD	User defined	LatA	Latitude relevant to the voltage minimum of channel A in the TRP (degrees dot decimals)
DWORD	User defined	LonA	Longitude relevant to the voltage minimum of channel A in the TRP (degrees dot decimals)
WORD	User defined	TvminA	Number of seconds from the Channel A Vmin time to the TRP end
WORD	User defined	VavA	Channel A Voltage average value in the TRP (Volt)
DWORD	Optional	EmB	Channel B Consumed Active Energy delta value (KWh dot decimal)
DWORD	Optional	EmnB	Channel B Regenerated Active Energy delta value (kvarh dot decimal)
DWORD	Optional	ErB	Channel B Consumed Reactive Energy delta value (kvarh dot decimal)
DWORD	Optional	ErnB	Channel B Regenerated Reactive Energy delta value (kvarh dot decimal)
DWORD	Optional	EtB	Channel B Consumed Active Energy index value (KWh dot decimal)
DWORD	Optional	EtnB	Channel B Regenerated Active Energy index value (KWh dot decimal)
DWORD	Optional	EtrB	Channel B Consumed Reactive Energy index value (kvarh dot decimal)
DWORD	User defined	EtrnB	Channel B Regenerated Reactive Energy index value (kvarh dot decimal)
WORD	User defined	VminB	Voltage minimum of channel B in the TRP (Volt)
WORD	User defined	IvminB	Current value at the voltage minimum of channel B in the TRP (Ampere)
WORD	User defined	TvminB	Number of seconds from the Channel B Vmin time to the TRP end
WORD	User defined	VavB	Channel B Voltage average value in the TRP (Volt)
DWORD	Optional	flagsB	Channel B CEBD flags: Energy data, Location data, time data (spare bits available)
DWORD	Optional	LatB	Latitude relevant to the voltage minimum of channel B in the TRP (degrees dot decimals)
DWORD	Optional	LonB	Longitude relevant to the voltage minimum of channel B in the TRP (degrees dot decimals)
DWORD	User defined	spare	Void fields to complete the record
WORD	Mandatory	CRC16	Application CRC16
NOTE 1 Word (WORD = 16 bits) and Double Word (DWORD = 32 bits) are organised as little-endian, increasing numeric significance with increasing memory addresses.			
NOTE 2 The number of ECF channels depends on the EMF configuration (as specified in EN 50463-2:2012, Annex B).			
NOTE 3 The preferred location formats listed in EN 50463 series are used.			

For the user defined fields, Data Id and Short Description are given as examples.

Irrespectively to the coding of data fields, the all ones binary value is reserved in order to indicate that the field is void. Consequently, the fields which are not used according to the hardware and software configuration shall be filled with all ones.

NOTE 1 This does not limit the coding capability of each field considering that the word value "111111111111111" and the double word value "11111111111111111111111111111111" are meaningless or out of scale for the chosen coding.

NOTE 2 The CEBD flags field is divided into 16 sub-fields of two bits each. Each sub-field is allocated a CEBD flag coded as a balance code according to the ASN.1 notation specified in ISO/IEC 8825. As an example, the energy data flag "measured" is coded as 01 if valid and 10 if not valid.

A.2.2 CRC calculation and verification

The Cyclical Redundancy Checking (CRC) field is two bytes, containing a 16–bit binary value.

The CRC value is calculated by the source, which appends the CRC to the message.

The destination also calculates a CRC during reception of the record, and compares this value with the actual value it received in the CRC field. If these two values are not equal, an error results.

The CRC is started by first pre-loading a 16–bit register to all 1's. Then a process begins of applying successive 8–bit bytes of the message to the current contents of the register. Any start, stop or parity bits associated with the local data transfer of characters shall be omitted in the record format of Table A.3 and shall also be neglected for the generation of CRC

During generation of the CRC, the exclusive OR between each 8–bit character and the 16–bit register contents is calculated.

Then the result is shifted in the direction of the least significant bit (LSB), with a zero filled into the most significant bit (MSB) position. The LSB is extracted and examined. If the LSB was a 1, the exclusive OR between the 16–bit register and a pre-set, fixed value is calculated. If the LSB was a 0, no exclusive OR takes place.

This process is repeated until eight shifts have been performed. After the last (eighth) shift, the exclusive OR between the next 8–bit character and the register's current value is calculated, and the process repeats for eight more shifts as described above.

The final content of the 16–bit register, after all the characters of the message have been applied, is the CRC value.

A procedure for generating a CRC is:

1) Load a 16–bit register with FFFF hex (all 1's). Call this the CRC register.
2) Exclusive OR the first 8–bit byte of the message with the low–order byte of the 16–bit CRC register, putting the result in the CRC register.
3) Shift the CRC register one bit to the right (toward the LSB), zero–filling the MSB. Extract and examine the LSB.
4) (If the LSB was 0): Repeat Step 3 (another shift).
5) (If the LSB was 1): Exclusive OR the CRC register with the polynomial value 0xA001 (1010 0000 0000 0001).
6) Repeat Steps 3 and 4 until 8 shifts have been performed. When this is done, a complete 8–bit byte will have been processed.
7) Repeat Steps 2 through 5 for the next 8–bit byte of the message. Continue doing this until all bytes have been processed.
8) The final content of the CRC register is the CRC value.
9) When the CRC is placed into the message, its upper and lower bytes shall be swapped.

10) When the 16–bit CRC (two 8–bit bytes) is transmitted in the message, the low-order byte will be transmitted first, followed by the high-order byte.

A.2.3 CEBD file structure

The CEBD recorded into the memory are transmitted spontaneously to ground according to the requirements in A.1.2.6 or are transmitted on demand. The file includes all the records relevant to the specified time interval expressed as time of the first TRP and time of the last TRP.

The records are retrieved from memory and compiled as XML file.

NOTE 1 The CRC are used to assure that the XML file has no corrupted records but the CRC are not included in the XML file. The integrity is assured by the immediate coding of the XML file using the TGZ compressor which applies its own integrity check.

The file shall have a header that includes:

1) CPID;
2) TRP duration;
3) date and time of the first record;
4) date and time of the last record;
5) identification of ECF channels pair and related traction system types;
6) date and time of compilation;
7) latitude and longitude of the location of compilation.

NOTE 2 The specification at line 7) is optional and provides an information that may be used for maintenance purposes.

Referring to line 5 in the list above, the traction supply system types handled by each channel shall be coded as the following:

a) 01 = 25 kV a.c.;
b) 02 = 15 kV a.c.;
c) 03 = 3 kV d.c.;
d) 04 = 1,5 kV d.c.;
e) 05 = 600 V d.c. / 750 V d.c.

EXAMPLE In case of a 25 kV a.c. and 3 kV d.c. traction system, EMS has two channels that will handle the two traction voltages and the code is 0102 or 0201 respectively if the channel A is 25 kV a.c. or 3 kV d.c.

The XML file is compressed in a TGZ archive.

NOTE 3 Typically 80 Kbytes result in about 4 Kbytes.

The TGZ archive is encrypted by means of the DES algorithm using the 64 bits key stored in the EMS by the Administrator and given under controlled procedure to the DCS Administrator.

The obtained file shall be transmitted using a client protocol of the following types: FTP, FTPS, HTTP or HTTPS.

A.2.4 Transferred data file XML schema

According to the record structure that is specified in A.2.1, the CEBD transferred data file is structured as specified in the following XML schema.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
   <xs:element name="dataroot">
    <xs:complexType>
      <xs:sequence>
        <xs:element minOccurs="0" maxOccurs="unbounded" name="record">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="label" type="xs:string" />
              <xs:element name="key" type="xs:string" />
              <xs:element name="Epoch" type="xs:string" />
              <xs:element name="LAT" type="xs:string" />
              <xs:element name="LON" type="xs:string" />
              <xs:element name="EM-A" type="xs:string" />
              <xs:element name="EMN-A" type="xs:string" />
              <xs:element name="ER-A" type="xs:string" />
              <xs:element name="ERN-A" type="xs:string" />
              <xs:element name="FLAGS-A" type="xs:string" />
              <xs:element name="ET-A" type="xs:string" />
              <xs:element name="ETN-A" type="xs:string" />
              <xs:element name="ETR-A" type="xs:string" />
              <xs:element name="ETRN-A" type="xs:string" />
              <xs:element name="VMIN-A" type="xs:string" />
              <xs:element name="IVMIN-A" type="xs:string" />
              <xs:element name="LAT-A" type="xs:string" />
              <xs:element name="LON-A" type="xs:string" />
              <xs:element name="TVMIN-A" type="xs:string" />
              <xs:element name="VAV-A" type="xs:string" />
              <xs:element name="EM-B" type="xs:string" />
              <xs:element name="EMN-B" type="xs:string" />
              <xs:element name="ER-B" type="xs:string" />
              <xs:element name="ERN-B" type="xs:string" />
              <xs:element name="ET-B" type="xs:string" />
              <xs:element name="ETN-B" type="xs:string" />
              <xs:element name="ETR-B" type="xs:string" />
              <xs:element name="ETRN-B" type="xs:string" />
              <xs:element name="VMIN-B" type="xs:string" />
              <xs:element name="IVMIN-B" type="xs:string" />
              <xs:element name="TVMIN-B" type="xs:string" />
              <xs:element name="VAV-B" type="xs:string" />
              <xs:element name="FLAGS-B" type="xs:string" />
              <xs:element name="LAT-B" type="xs:string" />
              <xs:element name="LON-B" type="xs:string" />
              <xs:element name="SPARE" type="xs:string" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute name="SN" type="xs:string" use="required" />
      <xs:attribute name="LOCO" type="xs:string" use="required" />
    </xs:complexType>
  </xs:element>
</xs:schema>
```

A.3 Access security

The access security is specified in 4.4 and a proposal is given in Annex D.

Annex B
(informative)

VEI–VMF/CMF to ECF interface implementation example

B.1 General

This informative annex aims to present an implementation example for the application data exchanged through the VMF/CMF to the ECF interface (VEI). This interface transfers digital values that are obtained by conversion and processing of the analogue input values applied to the VMF/CMF inputs. The format of these digital values and the format of the payload to be transferred are described by the following informative clauses. The security is assured by a procedure that bounds the VMF/CMF (the slave unit) to the ECF (the master unit). All digital values obtained by conversion of the voltage and current applied to the input of the VMF/CMF unit use format specified in ISO/IEC 8825.

B.2 Payload format

The Payload format is the format of the useful data that are contained inside the frame that is periodically transmitted by the sensor unit to the handling unit and that contains the data values to be used to calculate the electric energy taken from or returned (during regenerative braking) to the contact line by the traction unit. Furthermore, the payload contains the ancillary information necessary to assure the integrity and the authenticity.

The format of payload may be as depicted in Figure B.1.

Header	CkCnt	DC Voltage	DC Current	AppCRC

Header	CkCnt	AC Voltage	AC Current	AppCRC

Figure B.1 – Payload format

Header: 8 bits that represent the Sensor unit identification.

CkCnt: 8 bits representing the Check variable and the sequence counter. The format of this word is the following:

CTN3	CTN2	CTN1	CTN0	CK22	CK21	CK12	CK11

CNT3-CNT0: it is a 4-digit free running counter to be used by the Data Handling unit to check that the frames are received in correct sequence.

CK22-CK21: it is a two bits check variable that is related to the AC or DC Voltage value and indicates the validity according to this table: 00 = Not valid, 01 = AC valid, 10 = DC valid, 11 = error.

CK12-CK11: it is a two bits check variable that is related to the AC or DC Current value and indicates the validity according to this table: 00 = Not valid, 01 = AC valid, 10 = DC valid, 11 = error.

DC Voltage: 16 bits encoded as UNSIGNED16. It represents the converted values of the DC contact line voltage. The validity of this value is defined by the relevant Check Variable.

DC Current: 16 bits encoded as INTEGER16. It represents the converted values of the DC contact line absorbed or returned current. The validity of this value is defined by the relevant Check Variable.

AC Voltage: 16 bits encoded as INTEGER16. It represents the converted values of the AC contact line voltage. The validity of this value is defined by the relevant Check Variable.

AC Current: 16 bits encoded as INTEGER16. It represents the converted values of the AC contact line absorbed or returned current. The validity of this value is defined by the relevant Check Variable.

AppCRC: it is a CRC8 that is calculated on the complete payload. It is used to check integrity at application level.

B.3 Encryption

The payload prior to be transmitted may be encrypted to enhance security, the decryption key given to the VMF/CMF by the ECF unit during the Bounding Procedure or is embedded in the ECF software during the commissioning.

Annex C
(informative)

PICS structure and instruction

C.1 Structure

PICS pro-forma is a set of tables containing questions, to be answered by an implementer, and limitations on the possible answers.

It contains two types of questions:

- questions to be answered by either "YES" or "NO", related to whether a clause (ranging from a macroscopic functional unit to a microscopic one) has been implemented or not. The allowed answers, which reflect the base specification, are documented in the PICS as requirement; the answers constitute the support;
- questions on numerical values implemented (for timers, for sizes of messages, for frequencies, etc.). The legitimate range of variation of this value, which reflects the base specification, is given in the relevant part of EN 50463. The answers constitute the supported values.

C.2 Instructions for completing the PICS pro-forma

C.2.1 PICS table structure

PICS are organised in tables. Columns in the tables are

- **Ref.**: It is a number to be used as line reference,
- **Subclause**: This column lists the sub-clause of EN 50463-4 that is supported,
- **Capability**: This column lists the supported capability,
- **Requirement**: This column lists the supported requirement relevant to the listed clause,
- **Implementation:** Brief note useful to understand how the requirement is implemented,
- **Param. values**: If applicable, this column report Parameter values relevant to the implementation.

Table C.1 is an example of the PICS table structure.

Table C.1 – PICS table format

Ref.	Subclause	Capability	Requirement	Implementation	Param. values

C.2.2 Abbreviations used in PICS

The following abbreviations are used in this PICS pro-forma:

m mandatory;

n/a not applicable;

o optional;

c conditional;

d default;

Y yes;

N no.

C.2.3 Ref. column

This column is used for reference purposes inside the PICS in order to identify each line of the table.

C.2.4 Subclause column

This column gives the mapping between EN 50463-4 sub-clause and the corresponding entry in the PICS.

C.2.5 Capability column

This column lists the supported capability with reference to the relevant sub-clause.

The capability is supported if the Implementation Under Assessment is able to:

- generate the corresponding service parameters (either automatically or because the end user explicitly requires that capability);
- interpret, handle and when required make available to the end user the corresponding service parameter(s).

C.2.6 Requirement column

This column indicates the level of support required for conformity to EN 50463-4.

The values are as follows:

m mandatory support is required;

o optional support is permitted for conformity to EN 50463-4. If implemented it should conform to the specifications and restrictions contained in the relevant clause. These restrictions may affect the optional classification of other items;

c the item is conditional, the support of this item is subject to a predicate which is referenced in the note column;

n/a the item is not applicable.

If options are not supported the corresponding items should be considered as not applicable.

C.2.7 Implementation column

This column is completed by the supplier or implementer of the IUA. The pro-forma has been designed so that the only entries required in its own column are:

Y yes, the item has been implemented;

N no, the item has not been implemented;

– the item is not applicable.

In the PICS pro-forma tables, every leading item marked 'm' should be supported by the IUA.

Sub-items marked 'm' should be supported if the corresponding leading feature is supported by the IUA.

C.2.8 Parameter values column

C.2.8.1 Allowed min.

This column is already filled and indicates the minimum value for a parameter.

C.2.8.2 Default value

This column indicates the default value for a parameter. When EN 50463-4 defines the default for the parameter, such a value is used as the entry in this column. When the standard recommends a range, the mean value is used.

C.2.8.3 Allowed max.

This column is already filled and indicates the maximum value for a parameter.

C.2.8.4 Implemented value

This column is completed by the supplier or implementer. The pro-forma has been designed so that the entry required is the implemented value. In case of multiple values, the default value is chosen.

C.3 PICS pro-forma examples

C.3.1 Identification of PICS

Table C.2 is completed in order to identify the pro-forma.

Table C.2 – PICS identification table

Ref. No.	Question	Response
1	Date of statement	
2	PICS serial number	

C.3.2 Identification of the implementation under assessment

Table C.3 is completed in to identify the implementation under assessment.

Table C.3 – IUA identification table

Ref. No.	Question	Requirement	Response
1	Implementation name	m	
2	Version number	m	
3	Special configuration	o	
4	Power supply voltage	m	
5	Power supply current	m	
6	Other information	o	

NOTE 1 Implementation name refers to the identifier of the IUA as indicated by the supplier. The specific conformity test is applied to the entity identified by the implementation name.

NOTE 2 This is the version number of the IUA. When a version number is defined for an IUA, no subsystem that composes it can progress without a change of this figure (the architecture is frozen and constitutes a configuration).

NOTE 3 Indicated if PIXIT pro-forma are provided for this IUA.

NOTE 4 Indicated the applicable power supply voltage. Power supply voltage is chosen amongst the values specified in EN 50155.

NOTE 5 Indicated the applicable maximum power supply current. Power supply current is chosen amongst the values specified in EN 50155.

NOTE 6 Other information the supplier considers relevant for IUA identification.

C.3.3 Identification of the IUA supplier

Table C.4 is completed to identify the IUA supplier.

Table C.4 – IUA supplier identification table

Ref. No.	Question	Requirement	Response
1	Organisation name	m	
2	Contact name(s)	m	
3	Address:	m	
4	Telephone number	m	
5	Fax number	m	
6	e-mail address	m	
7	Other information	m	

C.3.4 Identification of the standards

Table C.5 is completed to identify the Standards applied to the IUA for the conformity test.

Table C.5 – Applicable standards identification table

Ref. No.	Question	Response
1	Specification document title	
2	Specification document IEC/CLC/CEN reference number	
3	Specification document date of publication	
4	Specification document version number	
5	Conformity document title	
6	Conformity document number	
7	Conformity document date of publication	
8	Conformity document version number	

C.3.5 Global statement of conformity

Table C.6 is filled by the IUA supplier in the “Implementation” column.

Table C.6 – Global statement table

Ref. No.	Question	Requirement	Implementation
1	Are all mandatory capabilities implemented?	m	[ ]
NOTE Answering "No" to this section indicates non-conformity to the protocol specification. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming.			

C.3.6 Level of conformity

Table C.7 is completed by the IUA supplier in order to identify the IUA level of conformity.

Only the clauses and sub-clauses that are implemented are listed irrespectively if they are mandatory or optional.

Table C.7 shows five lines but obviously, the number of lines is determined by the implemented clauses and sub-clauses.

Table C.7 – Level of conformity

Ref. No.	EN 50463-4 subclause	Capability	Implementation
1			[ ]
2			[ ]
3			[ ]
4			[ ]
5			[ ]

Annex D
(informative)

Access security

The following text offers a proposal for the managements of the access rights.

The password and the granted access permissions (e.g. to the application services) should be mapped in a Password/Permission Table that should be stored in a non-volatile memory of the EMS. The access to this table should be granted only to the Administrator.

When the EMS is produced, the Password/Permission Table should be programmed in order that:

1) Manager password grants access to all information;
2) Administrator password grants the access to the functional parameters, calibration parameters and all the other information granted to the lower levels;
3) User password grants the access to the data and software essential to metrological performance and creation of CEBD, furthermore grants access to functional parameters not affecting this data;
4) download password grants the read only access to data essential to metrological performance and creation of CEBD and to CEBD.

The retrieving and visualisation of real time data should be available without any access control.

Annex ZZ
(informative)

Coverage of Essential Requirements of EU Directives

This European Standard has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and within its scope the standard covers all relevant essential requirements as given in Annex III of the EU Directive 2008/57/EC.

Compliance with this standard provides one means of conformity with the specified essential requirements of the Directive(s) concerned.

WARNING: Other requirements and other EU Directives may be applicable to the products falling within the scope of this standard.

Bibliography

EN 50155:2007, *Railway applications — Electronic equipment used on rolling stock*

IEC 60050 (all parts), *International Electrotechnical Vocabulary*

EN 60359:2002, *Electrical and electronic measurement equipment — Expression of performance (IEC 60359:2001)*

EN 61373, *Railway applications — Rolling stock equipment — Shock and vibration tests (IEC 61373)*

ITU-R Recommendation TF.686, *Glossary and definitions of time and frequency terms*

IEEE 802.11-2007, *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*

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

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

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similary for PASs, please notify BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about British Standards is available on the BSI website at **www.bsi-group.com/standards**

Copyright

BSI

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™