

BS EN 13757-1:2014



BSI Standards Publication

Communication systems for meters

Part 1: Data exchange

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This British Standard is the UK implementation of EN 13757-1:2014. It supersedes BS EN 13757-1:2002 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee PEL/894, Remote Meter Reading.

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.

© The British Standards Institution 2014.
Published by BSI Standards Limited 2014

ISBN 978 0 580 78122 3

ICS 33.200; 35.100.70

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 30 November 2014.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English Version

Communication systems for meters - Part 1: Data exchange

Systèmes de communication et de télérelevé de compteurs
- Partie 1 : Echange de données

Kommunikationssysteme für Zähler - Teil 1:
Datenaustausch

This European Standard was approved by CEN on 30 August 2014.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents	Page
Foreword.....	9
Introduction	10
1 Scope	11
2 Normative references	11
3 Terms and definitions	13
4 General description and security.....	15
4.1 Basic vocabulary	15
4.2 Layered protocols.....	15
4.2.1 General.....	15
4.2.2 7 Layer Protocol.....	15
4.2.3 IP Protocol	16
4.2.4 3 Layer Protocol.....	17
4.3 Security	18
4.3.1 General.....	18
4.3.2 Security Requirement Analysis/ Threat Analysis.....	19
4.3.3 Key Management	19
4.3.4 COSEM Upper Layer Security	20
4.3.5 Lower Layer Security	21
5 Network Architecture	22
5.1 M/441 Mandate	22
5.2 General.....	23
5.3 Basic architecture.....	23
5.4 Metering Architecture.....	24
5.5 One unique access point at any time: a tree structure.....	26
5.6 Self-configurable network.....	26
5.7 Hand Held Unit for local access	26
5.8 Network layers	26
5.9 Multiple access	26
6 Application Layers for Metering.....	27
6.1 General.....	27
6.2 COSEM Application Layer for Metering	27
6.3 Companion Specification.....	27
6.4 COSEM Basic Principles.....	28
6.5 Management of a COSEM Device.....	29
6.6 Lower layers	29
7 Data Exchange	30
7.1 General.....	30
7.2 Data exchange using direct local connection	30
7.2.1 General.....	30
7.2.2 Security.....	31
7.2.3 Physical layer.....	31
7.2.4 Link Layer	31
7.3 Data exchange using wired local area network (LAN)	31
7.3.1 General.....	31
7.3.2 Twisted pair, baseband signalling	32
7.3.3 Twisted pair, baseband limited systems	32
7.3.4 Twisted pair, carrier signalling.....	32
7.4 Data exchange using wide area network (WAN)	32

7.4.1	General	32
7.4.2	PSTN based connection	32
7.4.3	IP connection	36
7.5	Data exchange using M-Bus radio communication	37
7.5.1	General	37
7.5.2	Basic M- Bus radio networks	38
7.5.3	Routed M-Bus radio networks	38
7.6	Data Exchange using HDLC for some innovative communications technologies and local interfaces	38
7.6.1	General	38
7.6.2	Security.....	38
7.6.3	Physical layer.....	38
7.6.4	Link Layer.....	39
8	Upper Layer Protocols	39
8.1	Introduction.....	39
8.2	Transport sub-layer	39
8.2.1	Introduction.....	39
8.2.2	EN 62056-46 related Transport sub-layer.....	40
8.2.3	EN 62056-47 related Transport sub-layer.....	40
8.2.4	Transport sub-layer	40
8.3	Application sub-layer	42
8.3.1	Introduction.....	42
8.3.2	Application layer structure	42
8.3.3	Service specification.....	42
8.3.4	Protocol specification	43
9	Cross-application data handling.....	43
9.1	General	43
9.2	Data tunnelling.....	43
9.2.1	General	43
9.2.2	M-Bus Application Layer transferred by DLMS.....	44
9.3	Data translation	48
10	Extensions to COSEM.....	49
10.1	Introduction.....	49
10.2	Dedicated Interface classes	49
10.3	Specific object types — Error reporting object.....	56
10.3.1	Introduction.....	56
10.3.2	General error object	57
10.3.3	Media specific error object.....	58
10.3.4	Manufacturer specific error object	58
11	Object Identification System (OBIS).....	58
11.1	Object Identification System (Variable naming rules)	58
11.1.1	Introduction.....	58
11.1.2	Structure.....	58
11.1.3	Manufacturer, utility, consortia and country specific codes	59
11.1.4	Common value groups.....	60
11.2	Abstract Objects (A = 0).....	63
11.2.1	Abstract objects, general service entries	63
11.2.2	Error registers, alarm registers and alarm filters – Abstract	68
11.2.3	List objects – Abstract.....	68
11.2.4	Register table objects – Abstract	69
11.2.5	Data profile objects – Abstract	69
11.3	Media specific value groups.....	69
11.3.1	General	69
11.3.2	Value groups specific to Heat Cost Allocators	69
11.3.3	Value groups specific to Heat or Cooling Meters	73

11.3.4	Value groups specific to Gas Meters	79
11.3.5	Value groups specific to Water Meters (A = 8 and A = 9)	108
11.4	Other media (Value group A = F)	111
11.4.1	General	111
11.4.2	Value group C codes – Other media	112
11.4.3	Value group D codes – Other media	112
11.4.4	Value group E codes – Other media	112
11.4.5	Value group F codes – Other media	112
11.5	Code presentation	112
11.5.1	Reduced ID codes (e.g. for EN 62056-21)	112
11.5.2	Display	113
11.5.3	Special handling of value group F	113
Annex A	(normative) Basic class meters	115
A.1	General	115
A.2	Basic requirements for Heat Cost Allocators	115
A.3	Basic requirements for Heat/ Cooling meters	116
A.4	Basic requirements for Gas meters	116
A.5	Basic requirements for Cold/ Hot water meters	117
Annex B	(informative) DLMS Glossary	118
B.1	Introduction	118
B.2	Activation mask	118
B.3	Activity calendar	118
B.4	Association LN	118
B.5	Association SN	118
B.6	Automatic capturing	118
B.7	Billing Period in COSEM	118
B.8	Capture	119
B.9	Channel	119
B.10	Clock	119
B.11	Current and last average value objects	120
B.12	Date and time	120
B.13	Daylight saving	120
B.14	Demand Register	120
B.15	Device ID	122
B.16	Error values	122
B.17	High level security	123
B.18	Interface modelling	123
B.19	I/O Control Signals	123
B.20	Interoperability	123
B.21	Logical device	123
B.22	Logical name referencing	124
B.23	Low level security	124
B.24	Manufacturer defined ID-s	124
B.25	Manufacturer specific abstract objects	124
B.26	Manufacturer specific class id	124
B.27	Manufacturer specific data and parameters	124
B.28	Manufacturer specific OBIS codes	125
B.29	Maximum and minimum value objects	125
B.30	Measurement of different media	125
B.31	Measurement method and tariffs	125
B.32	Measurement values series	125
B.33	Missing measurement values	125
B.34	Node	125
B.35	Password	126
B.36	Physical device	126
B.37	Power failure handling	126

B.38	Power failure monitoring	126
B.39	Preferred readout-values	127
B.40	Profile objects	127
B.41	Profile for billing periods	127
B.42	Profile generic interface class	127
B.43	Register interface class	127
B.44	Reset, IC Demand register	127
B.45	Reset, IC Extended register	128
B.46	Reset, IC Profile generic	128
B.47	Reset, IC Register	128
B.48	Reset, indication of source	128
B.49	Scaler	128
B.50	Scaler-unit	128
B.51	Schedule	128
B.52	Script	128
B.53	Script table interface class	129
B.54	Season	129
B.55	Selective access	129
B.56	Set date	129
B.57	Short name referencing	129
B.58	Special days table interface class	129
B.59	Standard readout definitions	129
B.60	Tariff	129
B.61	Tariffication	129
B.62	Threshold	130
B.63	Time integral value objects	130
B.64	Time setting, in relation with IC Schedule	130
B.64.1	General	130
B.64.2	Time setting forward	130
B.64.3	Time setting backward	130
B.64.4	Time synchronization	131
B.64.5	Daylight Saving	131
B.65	Time stamps (in relation with IC PSTN Auto dial)	131
B.66	Time stamp (in relation with billing periods)	131
B.67	Time synchronization	131
B.68	Unique identifier	131
B.69	Unit	131
B.70	Utility tables	134
Annex C	(informative) Gas Volume Conversion	135
C.1	Introduction	135
C.2	Foreword to abstract data model of gas volume converter	135
C.3	Abstract data model of gas volume converter — Common objects in gas conversion and energy calculation	136
C.4	Principle of measurement for volume conversion and energy calculation	137
C.5	Data flow in volume conversion and energy calculation	139
Annex D	(normative) Country specific identifiers	140
Bibliography		142

Tables

Table 1	— Typical Client Access Levels	21
Table 2	— M-Bus Port Setup Object	44
Table 3	— Description of Class ID “Data”	45
Table 4	— Tunnelling, Value group E	46

Table 5 — M-Bus slave port setup	49
Table 6 — M-Bus client.....	51
Table 7 — Wireless Mode Q channel	55
Table 8 — M-Bus master port setup	56
Table 9 — OBIS code structure and use of value groups	59
Table 10 — Reserved OBIS codes	60
Table 11 — Value group A	61
Table 12 — Value group B	61
Table 13 — Value group C codes where A = 0 (abstract objects).....	62
Table 14 — Abstract objects, general service entries	64
Table 15 — Codes for error registers, alarm registers and alarm filters – Abstract.....	68
Table 16 — OBIS codes for list objects – Abstract	68
Table 17 — OBIS codes for register table objects – Abstract.....	69
Table 18 — OBIS codes for data profile objects – Abstract	69
Table 19 — Value group C codes where A = 4 (HCA objects).....	70
Table 20 — Value group D codes where A = 4, C < > 0, 96 .. 99 (HCA objects).....	71
Table 21 — OBIS codes for general and service entry objects – HCA.....	71
Table 22 — OBIS codes for error register objects – HCA.....	72
Table 23 — OBIS codes for data profile objects – HCA.....	73
Table 24 — OBIS codes for HCA related objects (examples)	73
Table 25 — Value group C codes where A = 5 or A = 6 (Heat/cooling objects)	74
Table 26 — Value group D codes where A = 5 or A = 6 and C < > 0, 96...99 (Heat/cooling objects)	75
Table 27 — OBIS codes for general and service entry objects – Heat/cooling.....	76
Table 28 — OBIS codes for error register objects – Heat/ cooling.....	78
Table 29 — OBIS codes for data profile objects – Heat/ cooling.....	78
Table 30 — OBIS codes for heat/ cooling related objects (examples)	79
Table 31 — Value group C codes where A = 7 – Gas	81
Table 32 — Value group D codes for Gas – Indexes and index differences (A = 7, C = 1...8, 11...16, 21...26, 31...36, 61...66)	84
Table 33 — Value group D codes – Gas – Flow rate: A = 7, C = 43	88
Table 34 — Value group D codes – Gas – Process values (A = 7, C = 41, 42, 44...49)	90
Table 35 — Value group D codes – Gas – Correction, conversion and compressibility values (A = 7, C = 51...55).....	93
Table 36 — Value group D codes – Gas – Natural gas analysis values (A = 7, C = 70).....	93
Table 37 — Value group E codes – Gas – Indexes and index differences – Tariff rates for A = 7, C = 1...8, 11...16, 21...26, 31...36, 61...66, D = 0...3, 6...98.....	95
Table 38 — Value group E codes – Gas – Correction, conversion and compressibility values – Averages: A = 7, C = 51...55, D = 0, 2, 3, 10, 11	95
Table 39 — Value group E codes – Gas – Calculation methods A = 7, C = 51...55, D = 12	97

Table 40 — Value group E codes – Gas – Natural gas analysis values – Averages: A = 7, C = 70, D = 8...20, 60...84	98
Table 41 — OBIS codes for general and service entry objects – Gas	99
Table 42 — OBIS codes for error register objects – Gas	106
Table 43 — OBIS codes for list objects - Gas.....	107
Table 44 — OBIS codes for data profile objects – Gas	108
Table 45 — Value group C codes where A = 8 or A = 9 (Water volume objects)	109
Table 46 — Value group D codes where A = 8 or A = 9, C < > 0, 96...99 (Water volume objects).....	109
Table 47 — OBIS codes for general and service entry objects – Water	110
Table 48 — OBIS codes for error register objects – Water	111
Table 49 — OBIS codes for data profile objects – Water	111
Table 50 — OBIS codes for water related objects (examples).....	111
Table 51 — Value group C codes – Other media.....	112
Table 52 — Example of display code replacement – Value group C.....	113
Table 53 — Value group F – Billing periods	114
Table A.1 — Basic requirements for Heat Cost Allocators	115
Table A.2 — Basic requirements for Heat/ Cooling meters	116
Table A.3 — Basic requirements for Gas meters	116
Table A.4 — Basic requirements for Cold/ Hot water meters	117
Table B.1 — Enumerated values for physical units	132
Table C.1 — OBIS-Value group A = 7, B = X, E = 0, F = FF	136
Table D.1 — Value group D codes — Country specific identifiers C = 94	140

Figures

Figure 1 — The OSI 7-layer model	16
Figure 2 — Connection method independent Application Layers	17
Figure 3 — IEC 3-layer model.....	17
Figure 4 — Link and Physical layers in the 3 layer model	18
Figure 5 — Network Architecture — The architecture diagram in CEN/CLC/ETSI TR 50572	22
Figure 6 — System and physical architecture.....	24
Figure 7 — Basic Metering architecture.....	25
Figure 8 — Scope of Companion Specifications	27
Figure 9 — Companion Specification in relation to lower layers (3 layer model)	28
Figure 10 — An interface class and its instances.....	29
Figure 11 — Full protocol stack.....	30
Figure 12 — Typical PSTN configuration.....	33
Figure 13 — The location of the Physical Layer.....	34
Figure 14 — COSEM over IP	36
Figure 15 — EN 60870-5-2-related Transport PDU format.....	40

Figure 16 — CI field format	41
Figure 17 — The structure of the COSEM Application Layers	42
Figure 18 — Transporting DLMS/COSEM APDU's via M-Bus	44
Figure 19 — Reduced ID code presentation	113
Figure B.1 — The generalized time concept	119
Figure B.2 — The attributes when measuring sliding demand.....	120
Figure B.3 — Attributes when measuring current_average_value if number of periods is 1.....	121
Figure B.4 — The attributes if number of periods is 3.....	122
Figure B.5 — The COSEM server model.....	126
Figure C.1 — Energy Conversion Calculation flow chart.....	139

Foreword

This document (EN 13757-1:2014) has been prepared by Technical Committee CEN/TC 294 “Communication systems for meters and remote reading of meters”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by April 2015, and conflicting national standards shall be withdrawn at the latest by April 2015.

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

This document supersedes EN 13757-1:2002.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

This document has been revised in order to reflect the 7 – layer OSI model, significant updates in Security practices, and updates to the OBIS model to reflect the state of the art.

EN 13757 comprises the following parts:

- *Part 1: Data exchange* [the present document];
- *Part 2: Physical and link layer*;
- *Part 3: Dedicated application layer*;
- *Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands)*;
- *Part 5: Wireless relaying*;
- *Part 6: Local Bus*.

This document is referred to in the CEN/CLC/ETSI TR 50572:2011, *Functional Reference Architecture for Communications in Smart Metering Systems*, as a standard for communications between elements in the Smart Metering Architecture. The M/441 Mandate, which led to the CEN/CLC/ETSI TR 50572, is driving significant development of standards in smart metering.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

There are a number of other activities taking place in the smart metering and smart grid environment. The reader's attention is drawn to M/490, the mandate for standardization for smart grid, available from http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf, and C(2012) 1342, "Guidelines for conducting a cost-benefit analysis of Smart Grid projects", available from http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/20120427_smartgrids_guideline.pdf.

This document describes the data exchange and communications for meters and remote reading of meters in a generic way. It is Part 1 of EN 13757.

The main use of EN 13757-1 is to provide an overview of the protocols at the different levels and to provide a specification for the DLMS/COSEM application Layer for meters.

Additional parts to the series of standard EN 13757 are:

- *Part 2: Physical and link layer;*
- *Part 3: Dedicated application layer;*
- *Part 4: Wireless meter readout (radio meter reading for operation in SRD bands);*
- *Part 5: Wireless relaying;*
- *Part 6: Local Bus.*

The world of metering is going through a period of rapid change, and it is anticipated that this and other parts of the standard will require amendment in a short period of time.

NOTE 1 This document makes reference to EN 62056 standards repeatedly. An exercise is taking place to reissue and renumber these standards, and it is anticipated that CEN-listed versions of these standards will be confirmed shortly. References to older versions of these standards will be comprehensively updated as part of the response to comments to this draft.

NOTE 2 Some of the ISO/IEC documents listed under Clause 2 may be available only from ISO or IEC directly. If the document you require is not available from your national standards organization, it is recommended that you contact ISO or IEC to establish the status of the document and its availability. ISO can be contacted via www.iso.org.

NOTE 3 Clause 3 contains the terms and definitions special to remote reading of meters. Annex B is used to explain terms related to the object oriented model used in COSEM, detailed in EN 62056-6-2 and OBIS, detailed in EN 62056-6-1.

1 Scope

This European Standard specifies data exchange and communications for meters and remote reading of meters in a generic way.

This European Standard establishes a protocol specification for the Application Layer for meters and establishes several protocols for meter communications which may be applied depending on the application being fulfilled.

NOTE Electricity meters are not covered by this standard, as the standardization of remote readout of electricity meters is a task for CENELEC.

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 834, *Heat cost allocators for the determination of the consumption of room heating radiators — Appliances with electrical energy supply*

EN 1434-1, *Heat meters — Part 1: General requirements*

EN 1434-2, *Heat meters — Part 2: Constructional requirements*

EN 1434-3, *Heat Meters — Part 3: Data exchange and interfaces*

EN 13757-2:2004, *Communication systems for and remote reading of meters — Part 2: Physical and link layer*

EN 13757-3:2013, *Communication systems for and remote reading of meters — Part 3: Dedicated application layer*

EN 13757-4:2013, *Communication systems for meters and remote reading of meters — Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands)*

EN 13757-5:2008, *Communication systems for meters and remote reading of meters — Part 5: Wireless relaying*

EN 13757-6, *Communication systems for meters and remote reading of meters — Part 6: Local Bus*

CEN/CLC/ETSI TR 50572, *Functional Reference Architecture for Communications in Smart Metering Systems*

EN 60870-5-2, *Telecontrol equipment and systems — Part 5: Transmission protocols — Section 2: Link transmission procedures (IEC 60870-5-2)*

EN 61334-4-1, *Distribution automation using distribution line carrier systems — Part 4: Data communication protocols — Section 1: Reference model of the communication system (IEC 61334-4-1)*

EN 61334-4-41, *Distribution automation using distribution line carrier systems — Part 4: Data communication protocols — Section 41: Application protocols — Distribution line message specification (IEC 61334-4-41)*

EN 62056-3-1, *Electricity metering data exchange — The DLMS/COSEM suite — Part 3-1: Use of local area networks on twisted pair with carrier signalling (IEC 62056-3-1)*

EN 62056-5-3, *Electricity metering data exchange — The DLMS/COSEM suite — Part 5-3: DLMS/COSEM application layer (IEC 62056-5-3)*

EN 62056-6-1:2013¹⁾, *Electricity metering data exchange — The DLMS/COSEM suite — Part 6-1: Object Identification System (OBIS) (IEC 62056-6-1:2013)*

EN 62056-6-2:2013¹⁾, *Electricity metering data exchange — The DLMS/COSEM suite — Part 6-2: COSEM interface classes (IEC 62056-6-2:2013)*

EN 62056-21:2002¹⁾, *Electricity metering — Data exchange for meter reading, tariff and load control — Part 21: Direct local data exchange (IEC 62056-21:2002)*

EN 62056-42¹⁾, *Electricity metering - Data exchange for meter reading, tariff and load control — Part 42: Physical layer services and procedures for connection-oriented asynchronous data exchange (IEC 62056-42)*

EN 62056-46:2002¹⁾, *Electricity metering — Data exchange for meter reading, tariff and load control — Part 46: Data link layer using HDLC protocol (IEC 62056-46:2002)*

EN 62056-47¹⁾, *Electricity metering — Data exchange for meter reading, tariff and load control — Part 47: COSEM transport layers for IPv4 networks (IEC 62056-47)*

ISO 1155, *Information processing — Use of longitudinal parity to detect errors in information messages*

ISO 1177, *Information processing — Character structure for start/stop and synchronous character oriented transmission*

ISO 1745, *Information processing — Basic mode control procedures for data communication systems*

ISO 7498-2, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

ISO 9506-1, *Industrial automation systems — Manufacturing Message Specification — Part 1: Service definition*

ISO/IEC 646, *Information technology — ISO 7-bit coded character set for information interchange*

ISO/IEC 7498-1, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

ISO/IEC 8802-2, *Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 2: Logical link control*

ISO/IEC 13239, *Information technology — Telecommunications and information exchange between systems — High-level data link control (HDLC) procedures*

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 15953, *Information technology — Open Systems Interconnection — Service definition for the Application Service Object Association Control Service Element*

ISO/IEC 15954, *Information technology — Open Systems Interconnection — Connection-mode protocol for the Application Service Object Association Control Service Element*

ISO/IEC 27033 (all parts), *Information technology — Security techniques — Network security*

IETF RFC 791, *Internet Protocol — Darpa Internet Program — Protocol Specification [IPv4 Network Layer]*

1) The EN 62056 series of standards are in the process of revision/renumbering.

IETF RFC 793, *Transmission Control Protocol — Darpa Internet Program — Protocol Specification*

IETF RFC 768, *User Datagram Protocol*

IETF RFC 2460, *Internet Protocol, Version 6 (IPv6) — Specification*

IETF RFC 4301, *Security Architecture for the Internet Protocol [IPsec]*

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol — Version 1.2*

3 Terms and definitions

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

3.1

authorized party

utility, energy retailer, network operator, meter operator or data collection company authorized to access the information stored in the meter that is accessible to them according to the application association they can use

3.2

base conditions

fixed conditions used to express the volume of gas independently of the measurement conditions (e.g. temperature of 273,15 K and absolute pressure of 1,013 25 bar or temperature of 288,15 K and absolute pressure of 1,013 25 bar)

3.3

billing period

period over which a consumer bill is calculated

Note 1 to entry: See also B.7.

3.4

calendar

mechanism to program changes to active registers for Time-of-Use Tariffs

Note 1 to entry: See Activity Calendar B.3.

3.5

concentrator

intelligent station in a hierarchical communications network where incoming data (generated by multiple meters) is processed as appropriate and then repackaged, relayed, retransmitted, discarded, responded to, consolidated, prioritized and / or increased to multiple messages

3.6

disturbances

influence quantity having a value within the limits specified, but outside the specified rated operating conditions of the measurement instrument

3.7

gas-volume conversion device

device that computes, integrates and indicates the volume increments measured by a gas meter as if it were operating at base conditions, using as inputs the volume at measurement conditions as measured by the gas meter, and other characteristics such as gas temperature and gas pressure

Note 1 to entry: The conversion device can also include the error curve of the gas meter and associated measuring transformers.

Note 2 to entry: The deviation from the ideal gas law can be compensated by the compressibility factor.

3.8
hand held terminal
portable device for reading and programming metering equipment at the customer's premises or at the access point

3.9
index
for gas and water metering, current reading of the total volume (mass) passed through the meter

3.10
index difference
for gas and water metering, difference between the index at the end of a measurement or billing period and the index at the start of the same measurement or billing period

Note 1 to entry: Index difference over a certain measurement or billing period is also known as consumption. For consumption, thresholds may be defined.

3.11
IPsec
end-to-end security scheme operating in the Internet Layer

Note 1 to entry: It works on IPv4 and IPv6 Networks.

Note 2 to entry: It is described in IETF RFC 4301.

3.12
measurement conditions
conditions of the gas whose volume is measured, at the point of measurement (e.g. the temperature and the pressure of the gas)

3.13
scaler
exponent (to the base of 10) of the multiplication factor

Note 1 to entry: If the value is not numerical, then the scaler will be set to 0.

Note 2 to entry: See also B.49.

3.14
specified measuring range
set of values of measurements (the pressure for the pressure transducer or temperature for the temperature transducer) for which the error of the conversion device is intended to lie within the limits specified in the standard

Note 1 to entry: The upper and lower limits of the specified measuring range are called maximum value and minimum value respectively.

3.15
specified field of measurement of a conversion device
set of values at measurement conditions for which the error of the conversion device is within specified limits

Note 1 to entry: A conversion device has a measuring range for every quantity that it processes.

Note 2 to entry: The specified field of measurement applies to the characteristic quantities of the gas that are used to determine the conversion factor.

3.16
unit
enumeration defining the physical unit

Note 1 to entry: See also B.69.

4 General description and security

4.1 Basic vocabulary

All communications involve two sets of equipment represented by the terms **Caller** system and **Called** system. The **Caller** is the system that decides to initiate a communication with a remote system known as the **Called** party; these denominations remain valid throughout the duration of the communication.

A communication is broken down into a certain number of transactions. Each transaction is represented by a transmission from the **Transmitter** to the **Receiver**. During the sequence of transactions, the **Caller** and **Called** systems take turns to act as **Transmitter** and **Receiver**.

The terms **Client** and **Server** have the same meanings as in the DLMS model EN 61334-4-41. The **Server** is the system (meter) that acts as a receiver for service requests. The **Client** is the system (usually a data collecting system) that uses the Server for a specific purpose by means of one or more service requests.

The situation involving a **Caller Client** and a **Called Server** is undoubtedly the most frequent case, but a communication based on a **Caller Server** and a **Called Client** is also possible, in particular to report the occurrence of an urgent alarm and may offer savings in terms of data volumes in mass metering applications.

While the terms **Caller** and **Called** may imply a session, sessionless communications using, for example UDP over IP are also a valid approach to communications for smart meters depending on the type of network.

4.2 Layered protocols

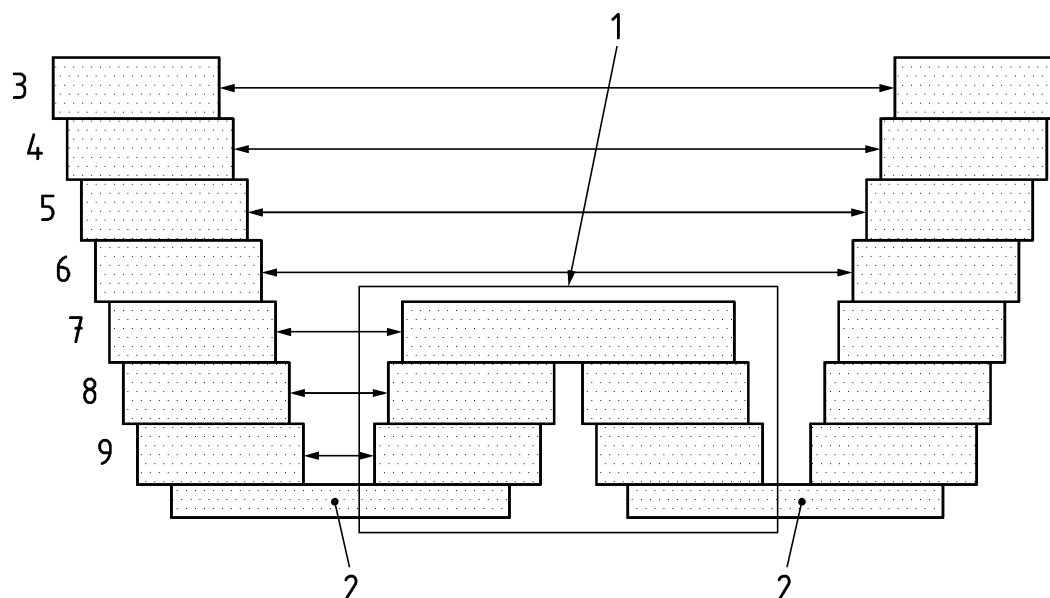
4.2.1 General

The purpose of this subclause is to explain, in a summarized way, the layered approaches and to explain the development since the initial issue of this standard.

In order to perform automatic reading of meters, this standard assumes a protocol stack approach. A protocol stack is divided into layers in order to reduce the complexity of the communicating system. Each layer provides services to the layer above on the basis of the layer below.

4.2.2 7 Layer Protocol

The architecture of data communication in this standard is modelled using the ISO – OSI 7- layer reference model ISO/IEC 7498-1. The model is shown in Figure 1.



Key

1	relay entity	6	transport
2	physical media	7	network
3	application	8	data link
4	presentation	9	physical
5	session		

Figure 1 — The OSI 7-layer model

All layers have a corresponding layer at the other end of the communications link. The three upper layers are application related. The three lower layers are communications related. The Transport Layer creates the link between them. There may be multiple instances of the three lower layers if a relay is inserted between the communicating partners.

It shall be kept in mind that this is a model and not an implementation guide, i.e. not all implementations follow this model. An example of this is the Internet series of standards. They follow the model for the four lower layers, but do not specify the application related part as independent layers. Layers not necessary and thus not implemented in a specific protocol may be handled as null layers.

4.2.3 IP Protocol

IPv4, and its successor IPv6 are becoming widely used protocols for transport of all kinds of data, including metering data. Its principal advantages are that it can be used to carry a wide variety of applications over a wide range of communications media.

Application Layer	Common, method independent layer	
	TCP/UDP IP Wrapper	
Transport	UDP	TCP
Network	IP	
Data Link	Any	Any
Physical	Any	Any

Figure 2 — Connection method independent Application Layers

The architecture shown in Figure 2 allows for multiple different communications media, while at the same time keeping a common connection method independent Application Layer. This is important as different connection methods are suited for different operating environments. The use of common layers lowers the overall cost and complexity of a remote readout metering system.

Users of the TCP/IP or UDP/IP protocol shall follow the standard EN 62056-47.

4.2.4 3 Layer Protocol

A very common model for simple meter readout, without any relays is a collapsed three layer model as depicted in Figure 3.

This is the IEC 3-layer model EN 61334-4-1, which is derived from OSI 7-layer model documented in ISO/IEC 7498-1.

The three layers of the IEC model are shown on the figure below:

Layer 7	Application
Layer 2	Data link
Layer 1	Physical

Figure 3 — IEC 3-layer model

NOTE The layer numbers refers to the numbering in the ISO-OSI 7-layer model.

This model ensures that the original concept of a model where the Application Layer is independent of communication transport method used, is maintained.

This division makes it possible to achieve an Application Layer that is independent of the communication connection method used, and the possibility of using the same communication method transport mechanism for different Application Layers. An example of this is shown in Figure 4. The Physical Layer and in some cases the Data Link Layer are closely related and highly dependent on the Layers 1 and 2 depend on the connection method used (Optical interface, Power Line Carrier-Low Voltage (PLC - LV), Public Switched Telephone Network (PSTN), VHF/UHF radio, Twisted Pair cable (TP)). This standard requires Application Layers that are independent of the connection method used.

Application Layer	Common, method independent layer				
Link Layer	EN 62056–46		EN 13757–3		... ?
Physical Layer	EN 62056–21	EN 62056–42	EN 13757–2/ EN 13757–6	EN 13757–4/ EN 13757–5	... ?
Connection Method	Optical (Local) Port	PSTN	Wired M-Bus (twisted pair baseband)	Wireless M-Bus	Future methods (to be defined)

Figure 4 — Link and Physical layers in the 3 layer model

4.3 Security

4.3.1 General

The data transferred between meters and head end systems may, in many cases, be regarded as the private data of the energy user, and therefore is subject to EU and national rules for the protection of said data. If communications to the meter can influence demand, then the meter may form part of critical national infrastructure. If data transferred from the head end to the meter can control the meter, then the integrity of the data may be a safety issue as well.

A mandate for standardization for security, M/487, is in place, and this is driving further standardization efforts in this area. A copy of the mandate can be obtained at ftp://ftp.cencenelec.eu/CENELEC/EuropeanMandates/M_487.pdf.

Security, therefore, is a much higher priority than in the earlier version of this standard.

There are four key security aspects required for smart metering:

- Ensuring that only those who should have access to information are granted access;
- Ensuring that information is not changed accidentally or deliberately;
- Ensuring that the source of the information cannot be falsified;
- Ensuring that the source of information cannot be denied.

Item a) is normally named Privacy. This can be achieved by limiting the physical access, or by using cryptographic methods. Both methods shall be considered depending on the application and communications methods being used. It should be noted that data encrypted cannot be retrieved again if the 'key' is lost. The normal method for ensuring privacy is by encrypting information. With the cryptographic methods available this is very safe and reasonably easy to perform. The real issue is not the encryption and decryption, but the handling and distribution of the encryption/decryption key(s) – see 4.3.3.

Item b) is normally named Integrity. Integrity in communication is normally achieved by generating a compressed signature over the message, referred to as a message digest. If the message digest cannot be recalculated on the data received, then it is possible that the data may be damaged. A method that is falling out of favour is Cyclic Redundancy Check. CRC has been in use for a long time to generate message digests. The strength of CRC is that is very simple to implement efficiently in hardware and that it is reasonably good at detecting random / accidental errors. The weakness is that it is unable to detect deliberate changes to the information. Protection against deliberate changes to information can be achieved by using cryptographic methods in the generation of the message digest. A message digest is calculated using a secure hashing method or a key based method. The result of this is a 'signature' or Message Authentication Code added to the end of the message. The MAC is recalculated when data are received. The strength of the MAC is that it is impossible to modify the message in such a way that the MAC is correct unless the 'key' is known.

Item c) is named Authentication. Authentication ensures that the source of the message is the one stated. It can be combined with Integrity. Authentication is not encryption but uses cryptographic methods. It is not possible to distinguish between sources of information if they use the same key, and therefore keys need to be dedicated to both ends of the data flow. Authentication will often ensure the integrity of the data as well.

Item d) is an extension to item c) and named Non-repudiation. This requires that unique keys are used, and that the sender and receives are using a cryptographic method with asymmetric keys. This ensures that the receiver cannot generate a message that appears as if it came from the sender. This is often achieved using a public key system.

4.3.2 Security Requirement Analysis/ Threat Analysis

There are a number of items that need to be considered with respect to security. It is clear that a simple AMR system that grabs meter index values infrequently is likely to require significantly lower levels of security than more sophisticated meter management systems, especially where the network is used to control devices in the home, or the meter is used for prepayment. Selection of key management and encryption strategies is driven by the threat analysis. Such a threat analysis shall as well take man-in-the middle and replay attacks into account.

An assessment of the risks and alternatives shall be carried out using a recognized method; for example ISO/IEC 27033 (all parts) or ISO/IEC 15408 (all parts).

The financial world has had a focus on cost efficient data security for many years, and processes, procedures and methods used there should be taken into account.

4.3.3 Key Management

4.3.3.1 General

Correct key management is essential to meet the security requirements of the smart metering system. Correct handling of secure information like encryption keys is not straightforward. The keys require a high level of protection. The principle of "need to know" shall be applied. In some situations there may be a need for dual control, i.e. that one person alone cannot handle the whole key. Part of the threat analysis should address the following concepts:

- 1) how many entities need access to the keys in order to be able to encrypt and decrypt data passed from/to the meter;
- 2) how often keys will need changing;
- 3) how often some of the entities will change;
- 4) how key information is going to be distributed.

A meter is expected to have a lifetime in the order of 10 years. Therefore it is expected that keys will need to be changed several times within that time span. Given the prohibitive cost of site visits it is necessary that there is a method to distribute key information through the network in a secure manner.

The general concept is that there should at least be three levels of keys:

- a) there is a master key used for distribution of a key encryption key, KEK;
- b) there is a key-encryption-key, KEK, used for the distribution or generation of the normal key;
- c) there are 'normal' keys for encryption and signing the data.

Depending on the level of security required, there may be a need for at least two keys, one for encrypting the data and one for generating the message digest (secure hash), and these shall be different keys. Different

clients for the meter data should necessitate different sets of keys. It should also be considered that meters with tariff functions, prepayment, and/or valves will need to be confident in the instructions being received them may need further keys to ensure non-repudiation of these instructions.

Where a meter is supplied with a master key, care shall be taken to ensure that the key cannot be derived from other data (for example serial number), and suitable methods shall be used to store and distribute such master keys.

When keys are being supplied or updated, consideration should be given to using the three pass protocol exchange method.

4.3.3.2 Symmetrical or Asymmetrical Encryption

The classical concept is the use of a secret key, used for encryption as well as decryption, and hence is known as symmetrical.

Asymmetric encryption dates back to around 1970. It uses two keys, a public and a private key. Messages encrypted with a private key can only be decrypted with the public key and vice versa. Public/private key are easier to handle as the public part can be distributed as plain text but they are much larger than symmetrical keys take much more computing power to use. Public/private keys are traditionally used for the distribution of secret keys and the generation of certificates with secret keys being used for the data transactions.

A strategy often used is a hybrid approach, where a secret symmetrical key is created and shared using asymmetrical encryption. This minimizes the risk of decryption of data, as long as the key is replaced in less time than the expected time to use an attack to identify the key. This is because the data that could be accessed is limited, and the key will have changed before simulated data can be effectively inserted into the network. In practice, the use of this approach will depend on a reliable threat analysis and monitoring, to ensure that keys are changed promptly. Asymmetrical encryption does not by itself provide authentication. Authentication is provided by letting trusted third party sign the public key / information from the sender. The receiver can then verify the authenticity of the sender by verifying the signature.

NOTE EN 62056-5-3 and EN 62056-6-2 supports symmetric key algorithms. Work continues to amend these standards to support public key algorithms.

4.3.4 COSEM Upper Layer Security

COSEM has a system of clients with access to data in the meter governed by application associations. The public client and management client shall be implemented. This requires that users create application associations when initiating a session with the meter. When this session is established, the Meter will limit data and configuration options to that permitted by configuration of the meter. The exception is the management client, which generally has complete access to all aspects of the meter. Establishment of this session can be done in an insecure way or a number of secure ways. Typical client associations are listed in Table 1.

Table 1 — Typical Client Access Levels

Name	Description
Public Client	This client is usually configured to provide very little access, except to prove that communications to the meter exist.
Data Collection Client	Allows reading of ID's, Alarm, Date/Time, Load Profile, TOU's, MD's, Blocks, Cumulative Registers, measurement parameters
Extended Data Collection Client	Correction of time and Date, Resetting of MD's
Management Client	Allows Programming of Displays, setting of measurement, setting of 'secret' for Data Collection and Extended Data Collection Clients
Manufacturer Client	Allows specialized access for manufacturing operations

Application associations can be associated with the properties and methods of OBIS objects directly, either as a configurable object accessed via the management client or manufacturer client or defined in a companion specification.

When an application association has been created using an appropriate level of security for the application, the client messages can be expected to be encrypted and/or signed depending on the level of privacy and authentication that are required.

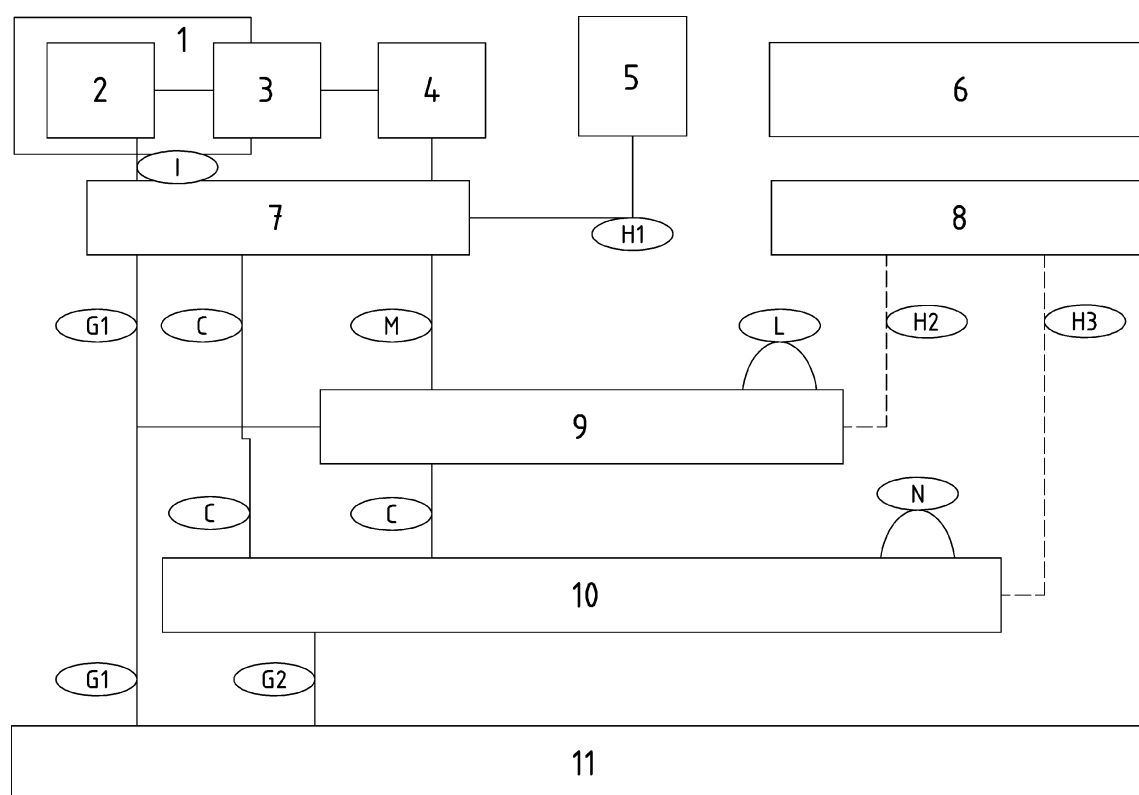
Both encryption and signature can be achieved by use of keys shared between the meter and the client.

4.3.5 Lower Layer Security

Lower layer security can be applied in addition to the upper layer security discussed above. The types of lower layer security that can be used depend on the lower layers being employed, and therefore these are discussed further within the relevant subclauses of Clause 7, Data Exchange. ISO 7498-2 recommends that encryption is performed end-to-end and not at the Data Link Layer.

5 Network Architecture

5.1 M/441 Mandate



Key

1	items required by MID	7	meter communication functions
2	metrology	8	HA communication functions
3	display	9	Local Network Access Point (LNAP)
4	additional functions	10	Neighbourhood Network Access Point (NNAP)
5	simple external consumer display	11	AMI Head End System
6	home automation functions		

Figure 5 — Network Architecture — The architecture diagram in CEN/CLC/ETSI TR 50572

This standard (in whole or part) is referred to in CEN/CLC/ETSI TR 50572 as a relevant standard for the interfaces noted as M, C, G1, and G2 in Figure 5.

The actual network architecture is dependent on the operating environment, meter functionality and the connection method used. It varies between basic readout networks to full Local Area Networks. The latter has turned applicable due to the low cost and high performance of such network components.

It is generally assumed that the communications interface is an integral part of the meter within this standard, but this may not be the case in the physical world. The communications interface may there be an add-on device to the meter.

5.2 General

This clause presents a simplified architecture for communicating with meters, concerning only the basic metering LAN.

This architecture should permit the quick introduction and installation of communicating meters, as well as the ability to extend the system afterwards. Therefore, some rules are given.

The principles of the metering network architecture are as follows:

- There shall be a single access point to the metering network.
- The single access point shall support multiple authorized parties accessing the metering network. It may be possible for the access point to support multiple concurrent accesses to one or multiple meters.
- The network should have a logical tree structure.
- The system shall be reasonably secure.
- The network should allow the use of a Hand Held Unit.

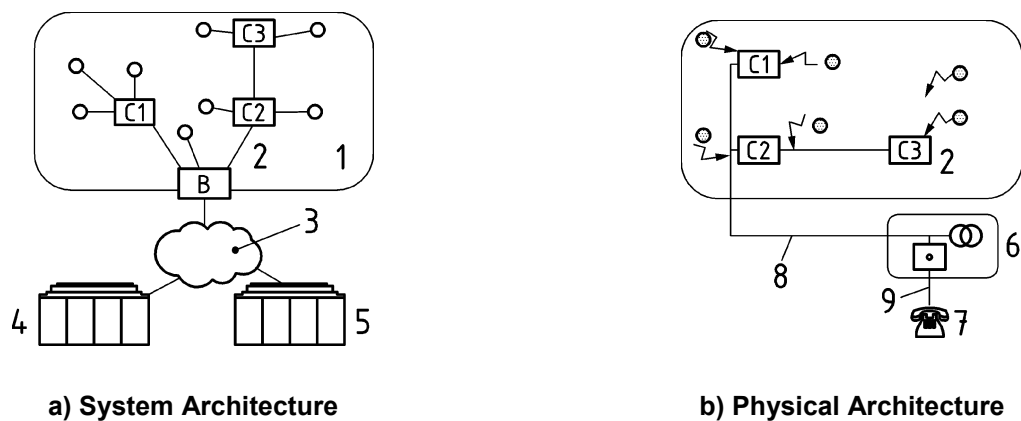
This architecture shall facilitate the fast installation and operation of meters and their associated communications onto a metering LAN. The potential for extending the architecture is a prime requirement.

The implementation of a physical architecture is determined by the media used.

This document focuses on the system architecture, in order to accommodate a wide range of types of physical media.

5.3 Basic architecture

Figure 6 shows a typical basic architecture based on a tree topology and the corresponding physical architecture.



Key

1	meter LAN	6	MV/LV Station
2	access point	7	MODEM
3	WAN	8	PLC
4	authorized party 1 Central Station	9	PSTN or IP connection
5	authorized party 2 Central Station		
	TC 294 compliant meter		radio meter

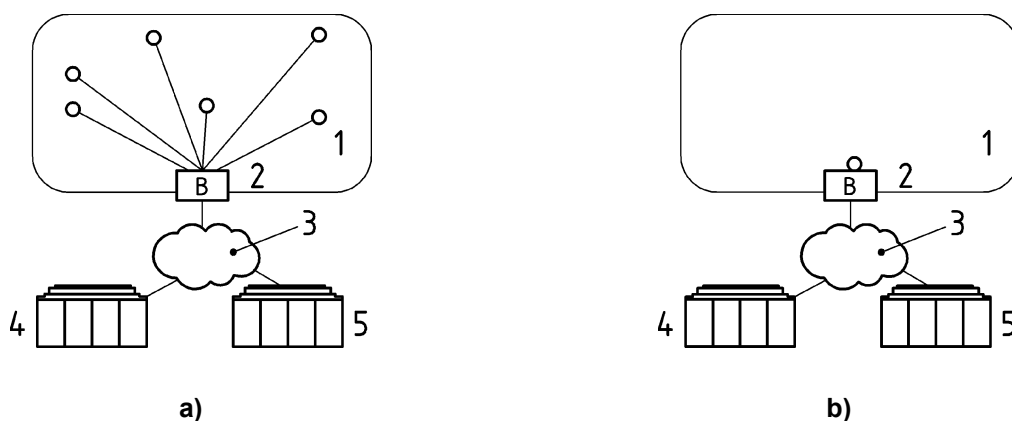
Figure 6 — System and physical architecture

C1, C2 and C3 are optional nodes (data concentrators) of the system that may be used to help access meters.

The access point B is the unique way to remotely access the system. Several authorized parties may access the system using access point B, providing they have access to the WAN connection.

5.4 Metering Architecture

The metering architecture may be analysed in terms of the systems architecture and physical architecture, as shown in Figure 6. The system architecture represents the key elements of the metering network, showing data flow, and providing the connectivity from the meter to the authorized party central station via a wide area network. The physical architecture represents the practical implementation of the system. In the example given in Figure 7, the meters are connected via radio to the concentrator, followed by the low voltage line to the MV/LV substation and finally via the telephone line to the central station. Although the figure shows that three different transmission media are used in this connection it may be more economical to use a single media throughout the system. The actual setup to use will have to be selected as part of the system design.



Key

1	meter LAN
2	access point
3	WAN
4	authorized party 1 Central Station
5	authorized party 2 Central Station
○	TC 294 compliant meter

1	meter LAN
2	access point
3	WAN
4	authorized party 1 Central Station
5	authorized party 2 Central Station

Figure 7 — Basic Metering architecture

A system architecture with a single master station and a number of meters connected to a physical bus as Figure 7 a) is an example of a basic network where the concentrators have been integrated into the access point.

A system with a single meter connected via the WAN to the integrated collection system as Figure 7 b) is an example of a system where the whole LAN has been integrated into the access point and combined with the meter.

The structure shall conform to the following rules:

- the architecture is a tree structure;
- there is only one access point per LAN;
- the unique access point (B) may have zero or more meters connected;
- the access point (B) may have zero or more 'concentrators' connected;
- a 'concentrator' may have zero or more meters attached;
- a 'concentrator' may have zero or more 'concentrators' attached;
- The logical meter may not communicate with another meter, but it may be appropriate to combine the concentrator with the meter in a single device;

- ‘concentrators’ have no external access point apart from zero or more data collection computers that may use the access point of (B).

NOTE Exact mapping of concentrators and access points to the architecture in 5.1 may depend on the implementation being carried out.

5.5 One unique access point at any time: a tree structure

An economic and easy to manage system may be achieved by having only one unique access point. A system with one unique access point is feasible with a tree structure. The actual physical structure depends on the actual physical layer used. Besides the line or star topology a loop or a ring would also be acceptable.

5.6 Self-configurable network

The proposed hierarchical architecture allows a level of self-configuration of a meter in a network. Self-configuration is managed, because each device needs to indicate to only one unique device that it is present and unassigned. This configuration is usually the responsibility of the Management Application in the meter.

The concentrator shall be resistant to unauthorized meters joining the network.

5.7 Hand Held Unit for local access

The requirement to be able to interrogate a device on the LAN using a Hand Held Unit (HHU) makes a temporary modification to the connectivity in order to maintain the network topology. The device may disconnect itself from its master, conducts the dialogue with the HHU as required and then reconnect to the system.

If a HHU is connected to a concentrator, the equipment itself and all the equipment under it may be made temporarily unavailable for the remote system (for the local operation duration), and be controlled by the HHU.

The Hand Held unit interfaces shall be treated as any other interfaces in the network with respect to their security requirements.

5.8 Network layers

There is no network layer required in a meter in a basic architecture. The meter will need some network layer functionality, as soon as it is possible to connect the meter to different destinations. This may be a part of more elaborate meters.

If one or more independent concentrators are in the Meter LAN, the protocol stack interconnecting the concentrators requires a network layer.

The collapsed models shown in Figure 7 b), does not require a network layer.

The consequential cost of a network layer is offset by the benefits of a concentrator. (e.g. to improve physical distance).

If a network uses IP, then the IP network layer is necessary.

5.9 Multiple access

The access point to the network is unique, but different communication channels may connect from the upper side. Several access networks are allowed, but not simultaneously, depending on the capabilities of the access point.

Network traffic priority will be handled by the access point.

6 Application Layers for Metering

6.1 General

There are at the present at least two Application Layers applicable to metering. This standard discusses the M-Bus based Application Layer and the DLMS COSEM Application Layer. The DLMS COSEM Application Layer is specified in EN 62056-5-3. It provides services to access COSEM interface object attributes and methods, modelling the functions of the meter. The COSEM interface classes are specified in EN 62056-6-2. The OBIS Object Identification System is specified in EN 62056-6-1 for abstract objects and electricity metering objects, and in this standard for other metering technologies. The M-Bus based Application Layer is specified in EN 13757-3. The M-Bus Application Layer has a simpler functionality and requires thus less electrical and processing power when implemented. This standard does not preclude alternative application layers as they are developed. Alternative Application layers are applicable only if they will co-exist with the existing M-Bus and DLMS COSEM application layers.

6.2 COSEM Application Layer for Metering

DLMS/COSEM is an application layer (AL) protocol specified in EN 62056-5-3. It covers the Application, Session and Presentation layer functionalities of the OSI model.

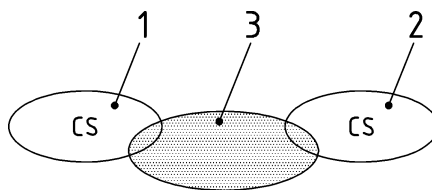
The DLMS COSEM AL provides services for establishing Application Associations (AAS) based on ISO/IEC 15953 and ISO/IEC 15954, the standards specifying the Association Control Service Element (ACSE) services and connection-oriented protocols.

It also provides services for accessing attributes and methods of COSEM interface objects that model the functions on the server. These services are provided by the xDLMS Application Service Element. xDLMS is an upper compatible extension of the DLMS standard specified in EN 61334-4-41. It can be considered as a companion specification to EN 61334-4-41.

The xDLMS ASE also provides cryptographic protection of the APDUs, the application layer level messages. To transport long messages, a block transfer mechanism is also available.

6.3 Companion Specification

A **Companion Specification (CS)** is an extension to a generic standard. It may contain extension to the existing standard, as well as operating rules within the scope of the existing standard, as shown in Figure 8.



Key

- 1 operating rules inside scope of the existing standard
- 2 extensions not compatible with the existing standard
- 3 messaging system kernel

Figure 8 — Scope of Companion Specifications

DLMS is a powerful messaging system, derived from MMS, ISO 9506-1 (Manufacturing Messaging System). In order to fully adapt DLMS to the metering application, the COSEM Application Layer is based on an extended version of DLMS. These extensions are made such that there is no conflict with the current version of DLMS. This can be viewed as a **Companion Specification** (CS). The CS can be seen as a set of additional rules to DLMS, which are semantically and syntactically compatible with the DLMS kernel.

Extensions can be found in EN 62056-5-3 (COSEM Application Layer).

A **Companion Specification** may go beyond pure data communication. It specifies the functionality of an application, as seen through the communication system as shown in Figure 9. In the current context, this is the functionality, of the meter or meters, defined in terms of the objects contained within them (e.g. Index, ID, meter type, manufacturer, date and time, rate and even communication entities such as a phone number). This standard bases its generic functional application requirements on the EN 62056-6-2, "Companion Specification for Energy Metering", approach.

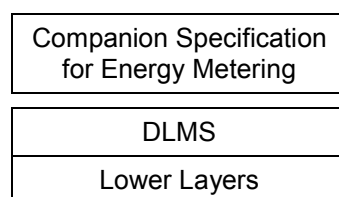


Figure 9 — Companion Specification in relation to lower layers (3 layer model)

6.4 COSEM Basic Principles

This Clause 4 describes the basic principles on which the COSEM interface classes (ICs) are built. It also gives a short overview on how interface objects – instantiations of the ICs – are used for communication purposes. Data collection systems and metering equipment from different vendors, following these specifications, can exchange data in an interoperable way.

For specification purposes, this standard uses the technique of object modelling.

An object is a collection of attributes and methods. Attributes represent the characteristics of an object. The value of an attribute may affect the behaviour of an object. The first attribute of any object is the "logical_name". It is one part of the identification of the object. An object may offer a number of methods to either examine or modify the values of the attributes.

Objects that share common characteristics are generalized as an IC, identified with a class_id. Within a specific IC, the common characteristics (attributes and methods) are described once for all objects. Instantiations of ICs are called COSEM interface objects.

Manufacturers may add proprietary methods and attributes to any object. Figure 10 illustrates these terms by means of an example:

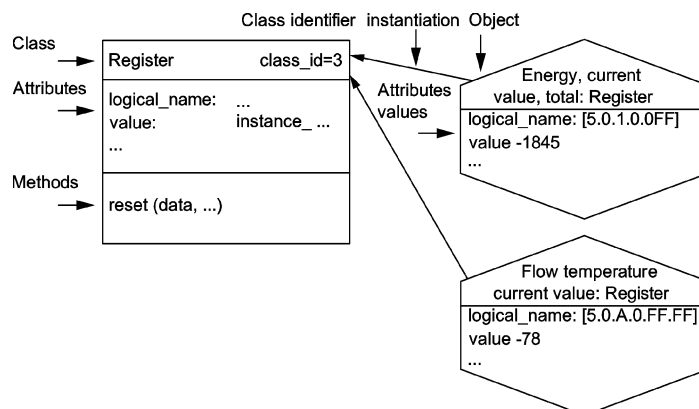


Figure 10 — An interface class and its instances

The IC “Register” is formed by combining the features necessary to model the behaviour of a generic register (containing measured or static information) as seen from the client (data collection system, hand-held terminal). The contents of the register are identified by the attribute “logical_name”. The logical_name contains an OBIS identifier. The actual (dynamic) content of the register is carried by its “value” attribute.

Defining a specific meter means defining several specific objects. In the example of Figure 10, the meter contains two registers; i.e. two specific instances of the IC “Register” are instantiated. Through the instantiation, one COSEM object becomes a “total, positive, active energy register” whereas the other becomes a “total, positive, reactive energy register”.

NOTE The COSEM interface objects (instances of COSEM ICs) represent the behaviour of the meter as seen always initiated from the outside. Internally initiated changes of the attributes – for example updating the value of a register – are not described in this model.

6.5 Management of a COSEM Device

One physical unit may contain or represent multiple metering units or logical devices. Such a physical unit will have one physical communications interface but multiple metering applications. This calls for a management application inside the unit that performs communications management. This is handled by COSEM as well.

The COSEM Logical Device is a set of COSEM objects. Each Physical Device shall contain a Management Logical Device. The mandatory contents of each Logical Device are:

- COSEM Logical Device Name;
- Current Association (LN or SN) object.

The Management Logical Device shall support an Application Association with lowest security level to a Public Client. The Management Logical Device shall support at least one further Application Association with security appropriate to the network structure and risk.

The addressing of the COSEM Logical Devices shall be provided by the addressing scheme of the lower layers of the protocols used.

6.6 Lower layers

The Lower layers shall include the Physical Layer and the Link Layer. If the seven layer OSI Model is used, the lower layers shall include network and transport layers. If the IP Model is used, the lower layers are managed by the IP system. The need for multiple communications methods causes the need for multiple different lower layers. All of the lower layers consist of a Physical Layer and a Link Layer. The requirements for the Link Layer are very often closely related to a specific Physical Layer.

In order to define full protocol stacks, which are needed for meter interchangeability, the lower layers shall be specified/ selected as well. Some lower layers have been selected/ adopted, and new lower layers will be added as amendments in the future when new technologies mature.

An overall diagram with all of the elements needed and their relationships is shown in Figure 11.

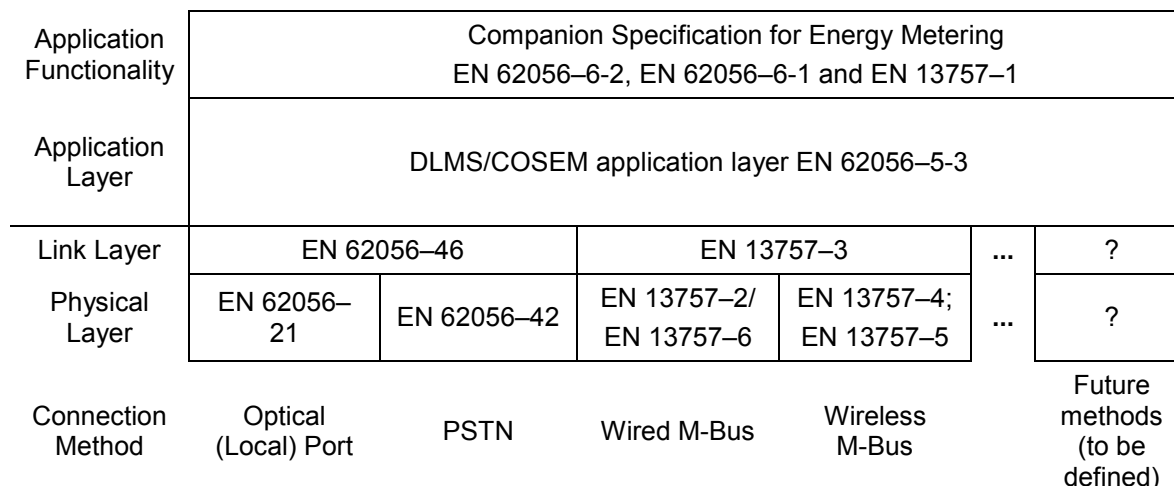


Figure 11 — Full protocol stack

As can be seen from the figure above, the Application Layer and the Application functionality remain unchanged, even if the connection method changes.

7 Data Exchange

7.1 General

This subclause describes a number of lower layers and stacks that are to be used in implementing smart metering. Because of the speed of evolution of communications media, and the use cases to which they will be put, this document does not promote any one of these. The document now also provides a secure interface to allow innovative communications media to be used with the EN 13757 series of standards, in accordance with the M/441 mandate.

7.2 Data exchange using direct local connection

7.2.1 General

This clause handles the reading of meters directly connected to a readout device. One interface of this type has been adopted, EN 62056-21. This standard specifies the physical connection adopted between meter and reading device:

- an optical interface;
- an electrical current loop interface;
- an electrical V.24/ V.28 interface.

All interfaces use the same protocol. Data are exchanged using a character oriented protocol (ASCII). Different communication modes are described in EN 62056-21. Modes A to D use ASCII transfer only, Mode E is able to switch over to a HDLC oriented binary data exchange. Provisions for battery operated devices are given in EN 62056-21:2002, B.1 and B.2.

NOTE This is for use with a hand-held terminal and is not intended as an H1 interface for in-home display.

7.2.2 Security

Physical access to this interface is governed by the location of the meter. The meter design should take account of the need for security of this interface, perhaps by means of a pre-shared key to ensure that the user of the terminal used to connect directly to the meter is suitably accredited.

7.2.3 Physical layer

7.2.3.1 Optical interface

This is a very common interface for Hand Held Units. It supports one meter at a time using half-duplex communication. It communicates with the meter using IR light via a standardized optical reading head, to be plugged magnetically to the meter. An interface of this type shall fulfil the requirements of EN 62056-21:2002, 4.3.

7.2.3.2 Electrical current loop interface

This interface is the 'classical' 20 mA current loop. Two- as well as four-wire configurations are available. One master unit may support up to eight meters. An interface of this type shall fulfil the requirements of EN 62056-21:2002, 4.1.

7.2.3.3 Electrical V.24/V.28 interface

This interface is the well-known "RS232 port" in a three-wire configuration (Rx, Tx, GND). An interface of this type shall fulfil the requirements of EN 62056-21:2002, 4.2.

7.2.4 Link Layer

The requirements of EN 62056-21 apply. Although no explicit layering is mentioned in this standard, the following relevant standards are referenced:

The character-oriented Link Layer uses:

- the ISO 7-bit coded character set as defined in ISO/IEC 646;
- the use of longitudinal parity (7E1) as defined in ISO 1155;
- the start/stop character-oriented transmission as defined in ISO 1177;
- the basic mode control procedures as defined in ISO 1745.

Binary data exchange (mode E) is based on:

- EN 62056-46 Data Link layer using HDLC protocol (see EN 62056-21:2002, Annex E).

7.3 Data exchange using wired local area network (LAN)

7.3.1 General

This is represented on the M/441 architecture, as interface M. See Figure 5.

This clause handles the reading of meters connected to a wired metering local area network. The network has a single master station, and one or more slave stations. Three types of interfaces have been adopted.

- EN 13757-2, the classical "M-Bus" for fixed installations,

- EN 13757-6, “Local bus” a limited subset of the M-Bus for non-fixed reading,
- EN 62056-3-1, the “Euridis” setup.

They are specified in the following subclauses.

7.3.2 Twisted pair, baseband signalling

7.3.2.1 General

This type of interface is standardized by EN 13757-2. It is a ‘multi-drop’ type connection with one master unit and one or more slave units. The master unit in the network can support energy to the interface part of the slave unit. A network may have up to 250 meters connected. The meter shall be a slave unit. This connection is applicable to COSEM as well as to M-Bus based Application Layers.

7.3.2.2 Physical layer

An interface of this type shall fulfil all the requirements of EN 13757-2:2004, Clause 4.

7.3.2.3 Link layer

An interface of this type shall fulfil all the requirements of EN 13757-2:2004, Clause 5.

7.3.3 Twisted pair, baseband limited systems

This type of interface is standardized by EN 13757-6. It is a limited version of EN 13757-2. It has a simple concentrator only able to support up to 5 meters. The standard only specifies the physical layers. The link layer is identical to the one used in EN 13757-2. This data exchange is only intended for M-Bus based Application Layer.

7.3.4 Twisted pair, carrier signalling

This interface shall comply with EN 62056-3-1. It is a multi-drop connection with one master unit and one or more slave units. A master unit is named a Primary Station. A slave unit is named a Secondary Station. The meter shall be a Secondary Station. The network is able to supply energy to the interface part of the slave unit. This data exchange is only intended for DLMS COSEM Application Layer.

7.4 Data exchange using wide area network (WAN)

7.4.1 General

This clause lists protocol stacks applicable for a direct connection from the meter to the processing centre using wide area networks, WAN, without intermediate processing. The public switched telephone network, PSTN is gradually being replaced by TCP/IP based data networks and Mobile telephone networks. Two standards have been identified for transfer across the wide area network. The one is based on the use of PSTN, the other is based on the use of a TCP/IP or UDP/IP based network. These connections are only applicable to DLMS/COSEM application Layers.

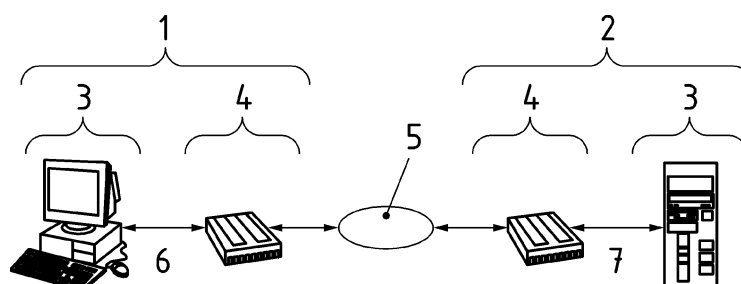
7.4.2 PSTN based connection

7.4.2.1 General

Meters using PSTN Connection shall comply with the relevant requirements of EN 62056-42 and EN 62056-46 for the lower layers. These are parts of the COSEM (Companion Specification for Energy Metering) three-layer connected oriented profile for asynchronous data communication. Normal asynchronous MODEM connection is used, based on intelligent Hayes modems.

7.4.2.2 Physical Layer EN 62056-42

From the external point of view, the physical layer provides the interface between the Data Terminal Equipment (DTE) and the Data Communication Equipment (DCE). Figure 12 shows a typical configuration for data exchange through a Wide Area Network, for example the PSTN.

**Key**

1	COSEM Client	5	transmission network
2	COSEM Server	6	DTE to DCE ITU-T V. Series EIA RS232, RS485 Hayes, etc
3	DTE	7	DCE to DTE ITU-T V. Series EIA RS232, RS485 Hayes, etc
4	DCE		

Figure 12 — Typical PSTN configuration

From the physical connection point of view, all communications involve two sets of equipment represented by the terms Caller system and Called system, as defined in 4.1.

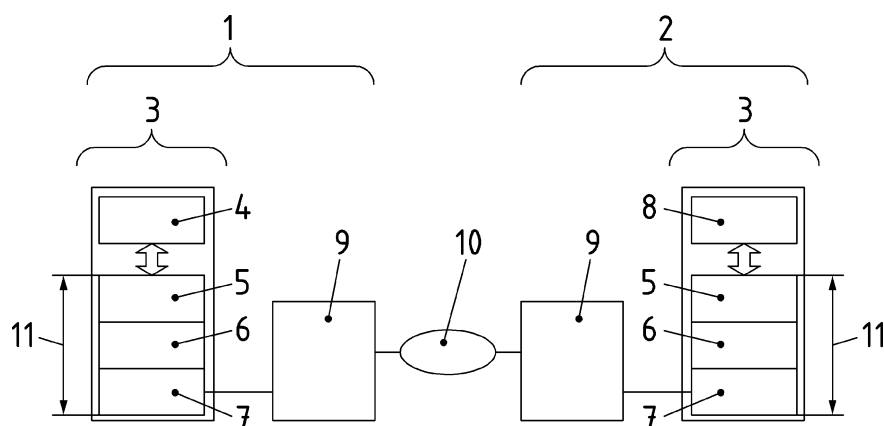
From the data link point of view the central station normally acts as a master, taking the initiative and controlling the data flow. The tariff device is the slave, responding to the master station.

From the application point of view the central station normally acts as a client asking for services, and the tariff device acts as a server delivering the requested services.

For the purposes of local data exchange, two DTEs can be directly connected using appropriate connections.

To allow using a wide variety of media, this standard does not specify the physical layer signals and their characteristics. However, the following assumptions are made:

- the communication is point to point or point to multipoint;
- both half-duplex and full-duplex connections are possible;
- asynchronous transmission with 1 start bit, 8 data bits, no parity and 1 stop bit (8N1);
- from the internal point of view, the physical layer is the lowest layer in the protocol stack – see Figure 13.



Key

1	COSEM Client	7	Physical Layer
2	COSEM Server	8	server application
3	DTE	9	Data Comm. Equipment (DCE)
4	client application	10	transmission network
5	Application Layer	11	protocol
6	Data Link Layer		

Figure 13 — The location of the Physical Layer

This standard defines the services of the physical layer towards its peer layer(s) and the upper layers, and the protocol of the physical layer.

7.4.2.3 Link Layer EN 62056-46

7.4.2.3.1 Introduction

This part of EN 62056 specifies the Data Link Layer for a connection-oriented, HDLC-based, asynchronous communication profile.

In order to ensure a coherent Data Link Layer service specification for both connection-oriented and connectionless operation modes, the Data Link Layer is divided into two sub-layers: the Logical Link Control (LLC) sub-layer and the Medium Access Control (MAC) sub-layer.

This specification supports the following communication environments:

- point-to-point and point-to-multipoint configurations;
- dedicated and switched data transmission facilities;
- half-duplex and full-duplex connections;
- asynchronous start/stop transmission, with 1 start bit, 8 data bits, no parity, 1 stop bit.

Two special procedures are also defined:

- transferring of separately received Service User layer PDU parts from the Server to the Client in a transparent manner. The Server side Service User layer can give its PDU to the Data Link layer in fragments and the Data Link Layer can hide this fragmentation from the Client;
- event reporting, by sending UI frames from the secondary station to the primary station.

7.4.2.3.2 The MAC sub-layer

The MAC sub-layer – the major part of this Data Link Layer specification – is based on ISO/IEC 13239 concerning high-level data link control (HDLC) procedures.

The MAC sub-layer is specified in EN 62056-46:2002, Clause 6. This standard includes a number of enhancements compared to the original HDLC, for example in the areas of addressing, error protection and segmentation. These enhancements have been incorporated in a new frame format, which meets the requirements of the environment found in telemetry applications for electricity metering and similar industries.

7.4.2.3.3 The LLC sub-layer

In the connection-oriented profile the only role of the LLC sub-layer is to ensure consistent Data Link Addressing. It can be considered that the LLC sub-layer, defined in ISO/IEC 8802-2, is used in an extended Class I operation, where the LLC sub-layer provides the standard connectionless data services via a connection-oriented MAC sub-layer.

The LLC sub-layer provides Data Link (DL) connection/disconnection services to the Service User layer, but it uses the services of the MAC sub-layer to execute these services.

The LLC sub-layer is specified in EN 62056-46:2002, Clause 5.

7.4.2.3.4 Specification method

Both sub-layers of the Data Link Layer are specified in terms of **services** and **protocol**.

Service specifications cover the services required of, or by, the given sub-layer at the logical interfaces with the neighbouring other sub-layer or layer, using connection oriented procedures. Services are the standard way to specify communications between protocol layers. Through the use of four types of transactions, commonly known as service primitives (Request, Indication, Response and Confirm) the service provider coordinates and manages the communication between the users. Using service primitives is an abstract, implementation-independent way to specify the transactions between protocol layers. Given this abstract nature of the primitives, their use makes good sense for the following reasons:

- they permit a common convention to be used between layers, without regard to specific operating systems and specific languages;
- they give the implementers a choice of how to implement the service primitives on a specific machine.

Service primitives include service parameters. There are three classes of service parameters:

- parameters transmitted to the peer layer, becoming part of the transmitted frame, e.g. addresses, control information;
- parameters which have only local significance (e.g. `Physical_Connection_Type`);
- parameters which are transmitted transparently across the data link layer to the user of the data link layer.

This document specifies values for parameters of the first category only.

The **protocol** specification for a protocol layer includes:

- the specification of the procedures for the transmission of the set of messages exchanged between peer-layer;
- the procedures for the correct interpretation of protocol control information;

- the layer behaviour.

The protocol specification for a protocol layer does not include:

- the structure and the meaning of the information which is transmitted by means of the layer (Information Field);
- the identity of the Service User layer;
- the manner in which the Service User layer operation is accomplished as a result of exchanging Data Link messages;
- the interactions that are the result of using the protocol layer.

7.4.3 IP connection

7.4.3.1 General

The internet protocol is the principal communications protocol used to relay datagrams across a wide area network. It uses a slightly different structure to the OSI 7-layer model, in that it consists of application, transport, internet and link layers.

COSEM on IP is currently fully defined for IPv4, in that the standard data model has support for IPv4 addressing, using the COSEM Application Layer, with ACSE and xDLMS to communicate via UDP or TCP.

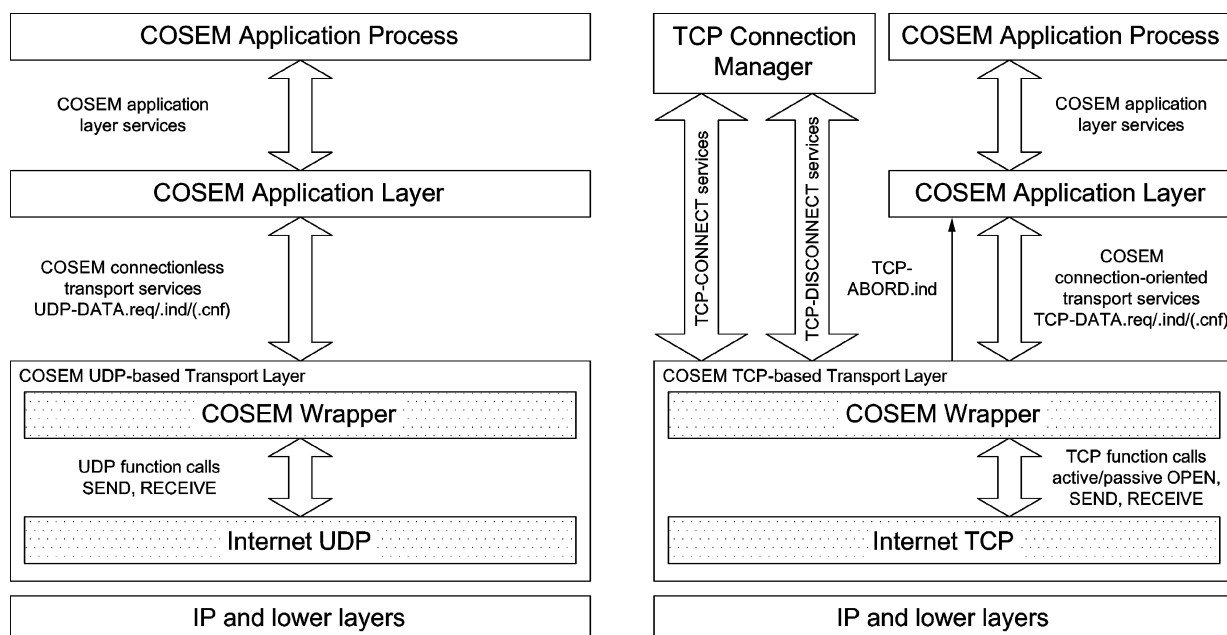


Figure 14 — COSEM over IP

Figure 14 shows the layers utilized in communication over IP networks. Where COSEM is to be transported over IP, the layers below the IP layer shall be capable of transporting the data between the client and the server. While this will often be on the internet, this could be over a private IP network. Technologies that can support this transport include PSTN, xDSL, PLC and a range of radio technologies including GPRS.

7.4.3.2 IPv4 based connection

The internet based connection is based on the “Internet” protocol suite. There are no limitations to the Physical Layer and Link Layer protocols, except that they shall provide the services needed by the “IPv4”

network layer. Typical connection methods applicable are optical fibre, LAN cabling, ADSL and wireless services. The network layer is specified by IETF RFC 791. Two possible Transport Layer standards are available, IETF RFC 793, TCP and IETF RFC 768 UDP. The adaptation to the COSEM Application layer is specified in EN 62056-47. This standard is as well applicable as the connection method across a LAN to a concentrator. The biggest restriction in IPv4 is the lack of availability of static IP addresses, and this is leading a move to IPv6 technology for the future. The shortage of IPv4 addresses means that the vast majority of meters cannot be allocated individual IP addresses, and therefore the meter needs to initialize a communications session to gain a temporary IP address, either as result of a scheduled event, a response to an event within the meter, or by a communications stimulus (for example, a SMS message to a GPRS modem).

7.4.3.3 IPv6 based connection

This is the latest version of the Internet Protocol. There are no limitations to the Physical Layer and Link Layer protocols that may be applied, except that they shall provide the services needed by the "IPv6" network layer. Typical connection methods applicable are optical fibre, LAN cabling, ADSL, Power Line Carrier, and radio services. The IPsec security layer was designed to be used on IPv6. The core standard for IPv6 is IETF RFC 2460. The key difference between IPv6 and IPv4 is that IPv6 uses 128 bit addressing, which provides for $(3,4 \times 10^{38})$ possible addresses, where IPv4 was limited to just over 4 billion addresses.

7.4.3.4 IP security

7.4.3.4.1 General

There are a number of methods that can be used for IP security. While any or all of the methods described here can be used with or without the application layer client security requirements in 4.3.4, evaluation of the value of the data and costs of security is necessary to select the correct methods to ensure a secure solution. There is a temptation to simply insist on security at three levels, where this will be burdensome and costly to manage, and may provide little better protection than protection at one or two layers.

7.4.3.4.2 IPsec

IPsec is an end-to-end security scheme operating in the Internet layer. It can be used in protecting data flows between a pair of hosts (*host-to-host*) or between a security gateway and a host (*network-to-host*). IPsec is documented principally in IETF RFC 4301. IPsec provides both encryption and authentication.

If IPsec is used on IPv4 networks then Tunnelling Mode shall be applied, to avoid network address translation issues.

7.4.3.4.3 TLS

TLS is a secure transport/application layer security protocol that can be used alongside TCP or UDP. While one of its features is the ability to use a variety of encryption, hashing and key handling techniques, the additional handling required to negotiate the security is not optimal for networks where small data sets are moved over frequent sessions. TLS is documented fully in IETF RFC 5246.

7.5 Data exchange using M-Bus radio communication

7.5.1 General

This clause handles the reading of meters connected to a wireless metering network. There are networks with a basic architecture as well as networks with routing capabilities. The networks are specified in EN 13757-4 and EN 13757-5.

7.5.2 Basic M- Bus radio networks

EN 13757-4 specifies radio network with a number of different modes. It uses the basic architecture from Clause 5. It has a number of different modes, each applicable to a different operating environments. EN 13757-4 is updated periodically to ensure that new radio modes are standardized.

EN 13757-4 specifies physical and link layers based on EN 60870-5-2. This connection provided is applicable to COSEM as well as to M-Bus based Application Layers.

7.5.3 Routed M-Bus radio networks

EN 13757-5 specifies the forwarding of data from basic radio networks using gateways or routers. It contains three different modes all having Network Layer functionality:

- the forwarding of data from basic networks using gateways, based on Mode R from EN 13757-4;
- the forwarding of data using routers, using an adapted Mode R2 Link Layer protocol and a Network Layer;
- a mode optimized for the handling of precise timing.

All three modes are able to handle COSEM as well as M-Bus Application Layer data.

7.6 Data Exchange using HDLC for some innovative communications technologies and local interfaces

7.6.1 General

This subclause handles the reading of meters where there is as yet no formal stack, and is designed to allow innovation in communications media using a standardized approach to the upper layers.

Data should be exchanged using a character oriented protocol (ASCII). Mode E, as described in EN 62056-21:2002, 6.4.5, shall be used as it is able to switch over to a HDLC oriented binary data exchange. Provisions for battery operated devices are given in EN 62056-21:2002, B.1 and B.2.

7.6.2 Security

As a minimum, low level authentication security shall be applied. See 4.3.4 for more information.

If the electrical interface can be accessed by unauthorized persons without causing an error condition in the system, then:

- 1) high level application layer security shall be applied;
- 2) traffic over the interface shall be encrypted and signed.

7.6.3 Physical layer

7.6.3.1 General

The physical layers specified below may be used to provide local interfaces to the meter, but innovative communications media will be determined by the media specification.

7.6.3.2 Electrical current loop interface

This interface is the 'classical' 20 mA current loop. Two- as well as four-wire configurations are available. One master unit may support up to eight meters, however, this application of the interface shall restrict users to a

single master and a single slave. An interface of this type shall fulfil the requirements of EN 62056-21:2002, 4.1.

7.6.3.3 Electrical V.24/V.28 interface

This interface is the well-known “RS232 port” in a three-wire configuration (Rx, Tx, GND). An interface of this type shall fulfil the requirements of EN 62056-21:2002, 4.2.

7.6.4 Link Layer

The requirements of EN 62056-21 apply. Although no explicit layering is mentioned in this standard, the following relevant standards are referenced:

The character-oriented Link Layer uses:

- the ISO 7-bit coded character set as defined in ISO/IEC 646;
- the use of longitudinal parity (7E1) as defined in ISO 1155;
- the start/stop character-oriented transmission as defined in ISO 1177;
- the basic mode control procedures as defined in ISO 1745.

Binary data exchange (mode E) is based on EN 62056-46 Data Link layer using HDLC protocol (see EN 62056-21:2002, Annex E).

8 Upper Layer Protocols

8.1 Introduction

This clause covers the upper layer protocols for COSEM based connections. The requirements are split into the following sub-layers:

- transport;
- application.

NOTE Upper layer protocols for M-Bus based connections are handled in EN 13757-3.

8.2 Transport sub-layer

8.2.1 Introduction

The Transport sub-layer is the first one to handle direct connections between the systems at the ends of the links. All the connections set up at this level and those at higher levels can be considered as end-to-end links. This end-to-end notion indicates that the transport entities offer services completely independent of the physical networks.

The most important properties of the Transport sub-layer are; end-to-end transport (mentioned above), transparency (any binary configuration shall be accepted by the transport protocol and delivered without modification, whatever its format or size, this may require segmenting/reassembling functionality in the sub-layer) and application layer addressing (multiplexing of multiple logical connections on one physical connection).

The Transport sub-layer accepts the messages from the Application sub-layer. As the size of these messages is dictated by the application, the Transport sub-layer shall be able to segment them into packets (called TPDU, transport protocol data units) with a size supported by the lower layers and transmit them to the

corresponding Transport sub-layer at the other end. Reciprocally, it shall be able to receive the packets from the corresponding Transport sub-layer and assemble them into coherent messages for the Application sub-layer.

The Transport sub-layer protocol shall be able to transmit data in full duplex or half duplex modes, Caller-Called and Called-Caller. Moreover, the multiplexing of transport connections on the same virtual circuit means that several application associations can coexist in a given communication.

Whatever their origin, the Transport Protocol Data Units, TPDU are transmitted using the services of the Data Link Layer. Of course, the Data Link is not aware of the multiplexing implemented at the higher level.

8.2.2 EN 62056-46 related Transport sub-layer

For connection methods using the HDLC based link layers, the use of the EPA model has been foreseen. The transport layer services needed has been integrated into the link layer.

In COSEM, there are two mechanisms provided for segmentation:

- The data link layer provides segmentation for messages between the slave and the master station only. This is transparent for the application layer. It is supported by the segmentation feature of HDLC (I frames). See EN 62056-46:2002, 6.4.4.5;
- The application layer provides segmentation in both directions, using the xDLMS services GET, SET, ACTION (DataBlock-G, DataBlock-SA).

Multiple Application Associations are supported by the DLMS/COSEM application layer and the COSEM Association objects, provided that the HDLC layer supports multiple data link connections

NOTE For details of establishing and releasing application associations, see EN 62056-5-3. For details of transferring long data, see EN 62056-46 and EN 62056-5-3.

8.2.3 EN 62056-47 related Transport sub-layer.

For connections based on IP TCP provides the handling of segmentation. The TCP-UDP/IP transport layer is specified in EN 62056-47, EN 13757-2 and EN 13757-4.

8.2.4 Transport sub-layer

For connection methods based on the EN 60870-5-2, link layer, transport sub-layer services are not included. For these connection methods, the Transport Protocol Data Unit (TPDU) shall consist of the following fields:

- a Control Information, (CI) field of 1 byte;
- a Source Transport Service Access Point (Address), STSAP field of 2 bytes;
- a Destination Transport Service Access Point (Address), DTSAP field of 2 bytes;
- a data field, of up to 248 bytes in size.

The fields shall be in the sequence shown in Figure 15.

NOTE 1 The maximum size of the data field is determined by the size limitations of the EN 60870-5-2 link level packets.



Figure 15 — EN 60870-5-2-related Transport PDU format

The CI field of the Transport PDU shall be as shown in Figure 16 and coded in the following way:

Bit 8, Bit 7, Bit 6	Always '000'
Bit 5 'FIN'	Set to '1' in the last 'TPDU' as a part of a 'APDU'
Bit 4, Bit 3, Bit 2, Bit 1	Fragment count, set to '0000' in the first 'TPDU' for a session and incremented for each 'TPDU' sent.

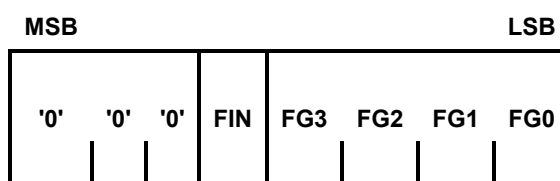


Figure 16 — CI field format

The coding of bit 8, bit 7 and bit 6 of the CI field ensures that DLMS oriented frames can coexist with existing meter communication from an EN 1434-3 or EN 13757-3 based bus system.

The FIN (finish) bit indicates the last segment of an APDU from the Application sub-layer. The FIN bit shall be set in the last TPDU of a APDU. This makes it possible to reassemble the data reliably at the receiving end.

In short messages, with only one segment, the FIN bit should be set as well in the first (and only) TPDU.

A fragment counter, FG3 - FG0 shall be available in the Transport sub-layer, as EN 60870-5-2 has no mechanism to identify double packet in responses from the meter to the central station. The fragment counter shall be '0000' in the first TPDU of every APDU from the Application sub-Layer. The fragment counter shall be incremented for every TPDU.

NOTE 2 Usually there will be one fragment counter for each concurrent connection.

The STSAP field shall contain the Logical Device Address of the caller. Most significant byte is sent first.

The DTSAP field shall contain the Logical Device Address of the called. A DTSAP of FFFFh is a broadcast address, and the data shall be distributed to all logical devices in the called unit. Most significant byte is sent first.

The DTSAP of 0001h is in COSEM pre-assigned to the management application, and should always be present. In a simple meter, this can be the only DTSAP assigned. The Management Logical Device should support an Application Association with lowest security level to a Public Client with a STSAP of 0010h.

Detection of errors in the communication of the Transport sub-layer will cause the following actions:

- an abort indication will be sent to the Application sub-layer;
- a request to abort is sent to the Link Layer;
- a re-initialization of the Transport sub-layer.

Care should be taken to avoid confusing caller and called with DLMS-COSEM client and server.

8.3 Application sub-layer

8.3.1 Introduction

EN 62056-5-3 applies. This document specifies the COSEM Application Layer in terms of structure, services and protocols, for COSEM Clients and Servers.

8.3.2 Application layer structure

The main component of the Client and Server COSEM Application Layer is the COSEM Application Service Object (ASO), which provides services to the COSEM Application process and uses services provided by the supporting lower layer.

Both the Client and Server side COSEM ASO contains three mandatory components, as follows:

- Association Control Service Element (ACSE). The task of this element is to establish, maintain and release application associations. For the purpose of the connection-oriented profile, the connection-oriented ACSE, specified in ISO/IEC 15953 and ISO/IEC 15954 is used;
- the Extended DLMS Application Service Element (xDLMS_ASE). The task of this element is to provide data communication services to remote COSEM equipment;
- the Control Function (CF). This element specifies how the ASO services invoke the appropriate service primitives of the ACSE and the xDLMS ASE-s and the services of the supporting layer.

Both the Client and the Server COSEM ASO may contain other optional application protocol components. Figure 17 shows a 'minimal' COSEM ASO-s, containing only the three mandatory components.

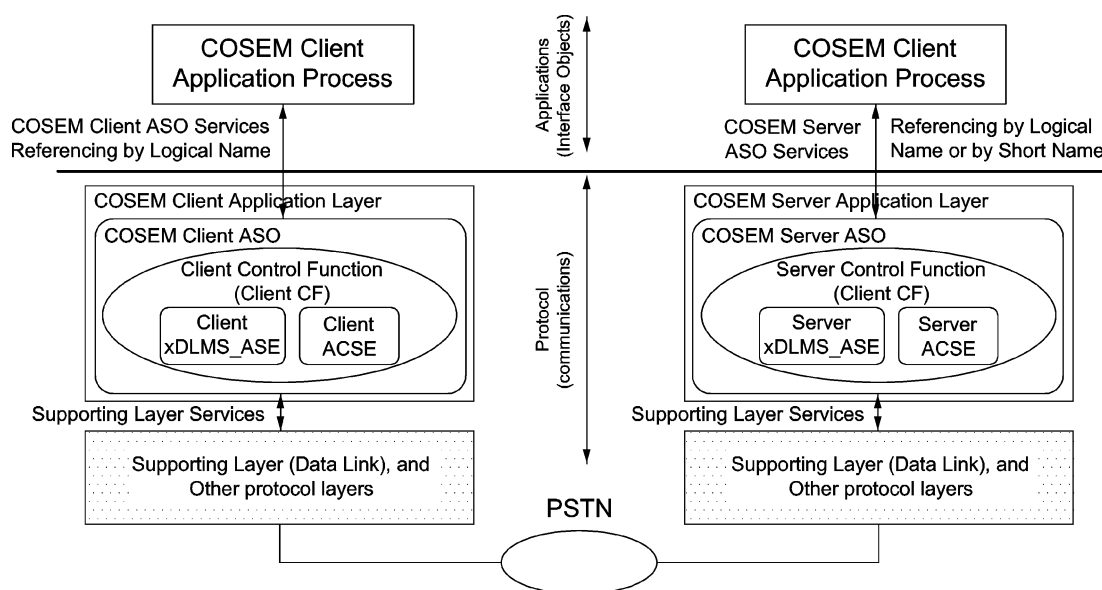


Figure 17 — The structure of the COSEM Application Layers

8.3.3 Service specification

Service specification covers the services required of or by, the Client and Server COSEM Application Processes at the logical interfaces with the respective COSEM Application Layer, using connection oriented procedures.

Services provided by the COSEM ASO fall in three categories: