

CONSOLIDATED VERSION

VERSION CONSOLIDÉE



**Industrial networks –
Wireless communication network and communication profiles – ISA 100.11a**

**Réseaux industriels –
Réseau de communication sans fil et profils de communication – ISA 100.11a**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2019 IEC, Geneva, Switzerland

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

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

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

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

About the IEC

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

About IEC publications

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

IEC publications search - webstore.iec.ch/advsearchform

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

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

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

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

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

A propos de l'IEC

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

A propos des publications IEC

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

Recherche de publications IEC -

webstore.iec.ch/advsearchform

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

IEC Just Published - webstore.iec.ch/justpublished

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

Service Clients - webstore.iec.ch/csc

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

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

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

CONSOLIDATED VERSION

VERSION CONSOLIDÉE



**Industrial networks –
Wireless communication network and communication profiles – ISA 100.11a**

**Réseaux industriels –
Réseau de communication sans fil et profils de communication – ISA 100.11a**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 33.160.60; 33.170

ISBN 978-2-8322-7238-1

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

REDLINE VERSION

VERSION REDLINE



Industrial networks –

Wireless communication network and communication profiles – ISA 100.11a

Réseaux industriels –

Réseau de communication sans fil et profils de communication – ISA 100.11a

CONTENTS

FOREWORD.....	21
0 Introduction	23
0.1 General.....	23
0.2 Document structure.....	23
0.3 Potentially relevant patents.....	23
1 Scope.....	25
2 Normative references	25
3 Terms, definitions, abbreviated terms, acronyms, and conventions.....	26
3.1 Terms and definitions.....	26
3.2 Abbreviated terms and acronyms	55
3.3 Conventions.....	61
4 Overview	63
4.1 General.....	63
4.2 Interoperability and related issues	63
4.3 Quality of service	64
4.4 Worldwide applicability	64
4.5 Network architecture	64
4.6 Network characteristics	70
5 System	78
5.1 General.....	78
5.2 Devices.....	78
5.3 Networks	86
5.4 Protocol suite structure	96
5.5 Data flow	97
5.6 Time reference.....	104
5.7 Firmware upgrades	105
5.8 Wireless backbones and other infrastructures	105
6 System management role	105
6.1 General.....	105
6.2 DMAP	107
6.3 System manager	131
7 Security.....	188
7.1 General.....	188
7.2 Security services	189
7.3 PDU security.....	194
7.4 Joining process.....	227
7.5 Session establishment	259
7.6 Key update	265
7.7 Functionality of the security manager role	271
7.8 Security policies.....	273
7.9 Security functions available to the AL	276
7.10 Security statistics collection, threat detection, and reporting	279
7.11 DSMO functionality	280
8 Physical layer	287
8.1 General.....	287

8.2	Default physical layer.....	288
9	Data-link layer.....	289
9.1	General.....	289
9.2	DDSAP.....	359
9.3	Data DPDU and ACK/NAK DPDU.....	362
9.4	DL management information base.....	390
9.5	DLE methods.....	440
9.6	DL alerts.....	442
10	Network layer.....	445
10.1	General.....	445
10.2	NL functionality overview.....	445
10.3	NLE data services.....	465
10.4	NL management object.....	468
10.5	NPDU formats.....	476
11	Transport layer.....	484
11.1	General.....	484
11.2	TLE reference model.....	485
11.3	Transport security entity.....	485
11.4	Transport data entity.....	486
11.5	TPDU encoding.....	491
11.6	TL model.....	493
12	Application layer.....	503
12.1	General.....	503
12.2	Energy considerations.....	504
12.3	Legacy control system considerations.....	504
12.4	Overview of object-oriented modeling.....	505
12.5	Object model.....	507
12.6	Object attribute model.....	508
12.7	Method model.....	510
12.8	Alert model.....	511
12.9	Alarm state model.....	511
12.10	Event state model.....	512
12.11	Alert reporting.....	513
12.12	Communication interaction model.....	515
12.13	AL addressing.....	525
12.14	Management objects.....	528
12.15	User objects.....	529
12.16	Data types.....	562
12.17	Application services provided by application sublayer.....	569
12.18	AL flow use of lower layer services.....	605
12.19	AL management.....	606
12.20	Process control industry standard data structures.....	624
12.21	Additional tables.....	627
12.22	Coding.....	628
12.23	Syntax.....	652
12.24	Detailed coding examples (informative).....	664
13	Provisioning.....	665
13.1	General.....	665

13.2	Terms and definitions for devices with various roles or states	665
13.3	Provisioning procedures.....	667
13.4	Pre-installed symmetric keys	667
13.5	Provisioning using out-of-band mechanisms	668
13.6	Provisioning networks	668
13.7	State transition diagrams	671
13.8	Device management application protocol objects used during provisioning	675
13.9	Management objects	678
13.10	Device provisioning service object	684
13.11	Provisioning functions (informative)	692
Annex A (informative)	User layer/application profiles	696
Annex B (normative)	Communication role profiles	698
Annex C (informative)	Background information	710
Annex D (normative)	Configuration defaults	716
Annex E (informative)	Use of backbone networks	723
Annex F (normative)	Basic security concepts – Notation and representation	726
Annex G (informative)	Using certificate chains for over-the-air provisioning	727
Annex H (normative)	Security building blocks	728
Annex I (informative)	Definition templates	738
Annex J (informative)	Operations on attributes.....	743
Annex K (normative)	Standard object types	748
Annex L (informative)	Standard data types	753
Annex M (normative)	Identification of tunneled legacy fieldbus protocols	755
Annex N (informative)	Tunneling and native object mapping	756
Annex O (informative)	Generic protocol translation	758
Annex P (informative)	Exemplary GIAP adaptations for this standard.....	762
Annex Q (informative)	Exemplary GIAP adaptations for IEC 62591	767
Annex R (informative)	Host system interface to standard-compliant devices via a gateway	776
Annex S (informative)	Symmetric-key operation test vectors	782
Annex T (informative)	Data-link and network headers for join requests	785
Annex U (informative)	Gateway role.....	787
Annex V (informative)	Compliance with ETSI EN 300 328- ~~v1.8.1~~ v2.1.1	855
Bibliography.....		860
Figure 1 – Standard-compliant network		66
Figure 2 – Typical single-layer PDU without fragmenting or blocking.....		68
Figure 3 – Full multi-layer PDU structure used by this standard		68
Figure 4 – Physical devices versus roles		81
Figure 5 – Notional representation of device phases		85
Figure 6 – Simple star topology		87
Figure 7 – Simple hub-and-spoke topology		88
Figure 8 – Mesh topology.....		89
Figure 9 – Simple star-mesh topology		90
Figure 10 – Example where network and D-subnet overlap		91

Figure 11 – Example where network and D-subnet differ.....	92
Figure 12 – Network with multiple gateways.....	93
Figure 13 – Basic network with backup gateway	94
Figure 14 – Network with backbone	95
Figure 15 – Network with backbone – Device roles	96
Figure 16 – Reference model used by this standard.....	97
Figure 17 – Basic data flow.....	98
Figure 18 – Data flow between I/O devices	99
Figure 19 – Data flow with legacy I/O device.....	100
Figure 20 – Data flow with backbone-resident device.....	101
Figure 21 – Data flow between I/O devices via backbone subnet	102
Figure 22 – Data flow to standard-aware control system	103
Figure 23 – Management architecture.....	106
Figure 24 – DMAP	109
Figure 25 – Example of management SAP flow through standard protocol suite.....	111
Figure 26 – System manager architecture concept.....	132
Figure 27 – UAP-system manager interaction during contract establishment.....	154
Figure 28 – Contract-related interaction between DMO and SCO	157
Figure 29 – Contract source, destination, and intermediate devices	170
Figure 30 – Contract establishment example.....	180
Figure 31 – Contract ID usage in source	181
Figure 32 – Contract termination.....	185
Figure 33 – Contract modification with immediate effect.....	187
Figure 34 – Examples of DPDU and TPDU scope	189
Figure 35 – Keys and associated lifetimes	191
Figure 36 – Key lifetimes	193
Figure 37 – DPDU structure	196
Figure 38 – DLE and DLS processing for a D-transaction initiator	197
Figure 39 – Received DPDU – DLE and DSC	199
Figure 40 – TPDU structure and protected coverage.....	212
Figure 41 – TMIC parameters	212
Figure 42 – TL and TSC interaction, outgoing TPDU.....	214
Figure 43 – TL and TSC interaction, incoming TPDU	215
Figure 44 – Example: Overview of the symmetric-key joining process	232
Figure 45 – Example: Overview of the symmetric-key joining process of a backbone device.....	233
Figure 46 – Asymmetric-key-authenticated key agreement scheme.....	243
Figure 47 – Example: Overview of the asymmetric-key joining process for a device with a DL.....	246
Figure 48 – Example: Overview of the asymmetric-key joining process of a backbone device.....	247
Figure 49 – Device state transitions for joining process and device lifetime	259
Figure 50 – High-level example of session establishment	260
Figure 51 – Key update protocol overview.....	265

Figure 52 – Device key establishment and key update state transition	271
Figure 53 – DL protocol suite and PhPDU/DPDU structure.....	291
Figure 54 – Graph routing example	294
Figure 55 – Inbound and outbound graphs	296
Figure 56 – Slotted-channel-hopping	300
Figure 57 – Slow-channel-hopping	301
Figure 58 – Hybrid operation.....	301
Figure 59 – Radio spectrum usage	302
Figure 60 – Predefined channel-hopping-pattern1	304
Figure 61 – Two groups of DLEs with different channel-hopping-pattern-offsets.....	305
Figure 62 – Interleaved channel-hopping-pattern1 with sixteen different channel-hopping-pattern-offsets	306
Figure 63 – Example timeslot allocation for slotted-channel-hopping.....	307
Figure 64 – Example timeslot allocation for slow-channel-hopping	308
Figure 65 – Hybrid mode with slotted-channel-hopping and slow-channel-hopping.....	309
Figure 66 – Combining slow-channel-hopping and slotted-channel-hopping	309
Figure 67 – Example of a three-timeslot superframe and how it repeats.....	310
Figure 68 – Superframes and links.....	310
Figure 69 – Multiple superframes with aligned timeslots.....	311
Figure 70 – Example superframe for slotted-channel-hopping	315
Figure 71 – Example superframe for slow-channel-hopping	316
Figure 72 – Components of a slow-channel-hopping superframe.....	316
Figure 73 – Example configuration for avoiding collisions among routers	317
Figure 74 – Hybrid configuration	318
Figure 75 – Timeslot allocation and message queue	320
Figure 76 – 250 ms alignment intervals.....	323
Figure 77 – Timeslot durations and timing.....	324
Figure 78 – Clock source acknowledges receipt of a Data DPDU	329
Figure 79 – Transaction timing attributes	331
Figure 80 – Dedicated and shared transaction timeslots	332
Figure 81 – Unicast transaction	333
Figure 82 – PDU wait time (PWT)	336
Figure 83 – Duocast support in the standard.....	337
Figure 84 – Duocast transaction	338
Figure 85 – Shared timeslots with active CSMA/CA	339
Figure 86 – Transaction during slow-channel-hopping periods	340
Figure 87 – DL management SAP flow through standard protocol suite.....	343
Figure 88 – PhPDU and DPDU structure.....	362
Figure 89 – Typical ACK/NAK DPDU layout	372
Figure 90 – Relationship among DLMO indexed attributes	412
Figure 91 – Address translation process	448
Figure 92 – Fragmentation process.....	450
Figure 93 – Reassembly process	451

Figure 94 – Processing of an NSDU received from a TLE	453
Figure 95 – Processing of a received NPDU	454
Figure 96 – Processing of a NPDU received by a NLE from the backbone	456
Figure 97 – Delivery of a received NPDU at its final destination NLE	457
Figure 98 – Routing from a field device direct to a field-connected gateway without backbone routing	458
Figure 99 – Protocol suite diagram for routing from a field device direct to a field-connected gateway without backbone routing	459
Figure 100 – Routing an NPDU from a field device to a gateway via a backbone router	460
Figure 101 – Protocol suite diagram for routing an APDU from a field device to a gateway via a backbone router	461
Figure 102 – Routing from a field device on one D-subnet to another field device on a different D-subnet	462
Figure 103 – Protocol suite diagram for routing from an I/O device on one D-subnet to another I/O device on a different D-subnet	463
Figure 104 – Example of routing over an Ethernet backbone network	464
Figure 105 – Example of routing over a fieldbus backbone network	465
Figure 106 – Distinguishing between NPDU header formats	477
Figure 107 – TLE reference model	485
Figure 108 – UDP pseudo-header for IPv6	487
Figure 109 – TPDU structure	491
Figure 110 – User application objects in a UAP	506
Figure 111 – Alarm state model	512
Figure 112 – Event model	513
Figure 113 – A successful example of multiple outstanding requests, with response concatenation	518
Figure 114 – An example of multiple outstanding unordered requests, with second write request initially unsuccessful	519
Figure 115 – An example of multiple outstanding ordered requests, with second write request initially unsuccessful	520
Figure 116 – Send window example 1, with current send window smaller than maximum send window	522
Figure 117 – Send window example 2, with current send window the same size as maximum send window, and non-zero usable send window width	522
Figure 118 – Send window example 3, with current send window the same size as maximum send window, and usable send window width of zero	523
Figure 119 – General addressing model	525
Figure 120 – UAP management object state diagram	532
Figure 121 – Alert report reception state diagram	534
Figure 122 – Alert-reporting example	534
Figure 123 – UploadDownload object download state diagram	551
Figure 124 – UploadDownload object upload state diagram	551
Figure 125 – Publish sequence of service primitives	572
Figure 126 – Client/server model two-part interactions	577
Figure 127 – Client/server model four-part interactions: Successful delivery	577
Figure 128 – Client/server model four-part interactions: Request delivery failure	578

Figure 129 – Client/server model four-part interactions: Response delivery failure.....	578
Figure 130 – AlertReport and AlertAcknowledge, delivery success.....	593
Figure 131 – AlertReport, delivery failure	593
Figure 132 – AlertReport, acknowledgment failure	594
Figure 133 – Concatenated response for multiple outstanding write requests (no message loss)	601
Figure 134 – Management and handling of malformed APDUs received from device X	607
Figure 135 – The provisioning network.....	669
Figure 136 – State transition diagrams outlining provisioning steps during a device lifecycle	671
Figure 137 – State transition diagram showing various paths to joining a secured network.....	674
Figure 138 – Provisioning objects and interactions	676
Figure C.1 – OSI Basic Reference Model	712
Figure O.1 – Generic protocol translation publish diagram	758
Figure O.2 – Generic protocol translation subscribe diagram	759
Figure O.3 – Generic protocol translation client/server transmission diagram.....	760
Figure O.4 – Generic protocol translation client/server reception diagram	761
Figure R.1 – Host integration reference model	776
Figure R.2 – Configuration using an electronic device definition.....	778
Figure R.3 – Configuration using FDT/DTM approach	779
Figure U.1 – Gateway scenarios	789
Figure U.2 – Basic gateway model.....	790
Figure U.3 – Internal sequence of primitives for session interface.....	794
Figure U.4 – Internal sequence of primitives for lease management interface	794
Figure U.5 – Internal sequence of primitives for system report interfaces.....	795
Figure U.6 – Internal sequence of primitives for time interface	795
Figure U.7 – Internal sequence of primitives for client/server interface initiated from gateway to an adapter device	796
Figure U.8 – Internal sequence of primitives for publish interface initiated from gateway to an adapter device	796
Figure U.9 – Internal sequence of primitives for subscribe interface initiated from an adapter device	797
Figure U.10 – Internal sequence of primitives for publisher timer initiated from gateway to an adapter device	797
Figure U.11 – Internal sequence of primitives for subscriber timers initiated from an adapter device	797
Figure U.12 – Internal sequence of primitives for the bulk transfer interface	798
Figure U.13 – Internal sequence of primitives for the alert subscription interface	798
Figure U.14 – Internal sequence of primitives for the alert notification interface	799
Figure U.15 – Internal sequence of primitives for gateway management interfaces	799
Figure U.16 – Tunnel object model	835
Figure U.17 – Distributed tunnel endpoints	836
Figure U.18 – Multicast, broadcast, and one-to-many messaging.....	837
Figure U.19 – Tunnel object buffering	838
Figure U.20 – Publish/subscribe publisher CoSt flowchart.....	841

Figure U.21 – Publish/subscribe publisher periodic flowchart	841
Figure U.22 – Publish/subscribe subscriber common periodic and CoSt flowchart.....	842
Figure U.23 – Network address mappings.....	843
Figure U.24 – Connection_Info usage in protocol translation.....	844
Figure U.25 – Transaction_Info usage in protocol translation	845
Figure U.26 – Interworkable tunneling mechanism overview diagram	846
Figure U.27 – Bulk transfer model.....	849
Figure U.28 – Alert model	850
Figure U.29 – Alert cascading	851
Figure U.30 – Native publish/subscribe and client/server access	852
Table 1 – Standard management object types in DMAP	109
Table 2 – Metadata_attribute data structure	112
Table 3 – Alert types for communication diagnostic category	114
Table 4 – Alert types for security alert category	114
Table 5 – Alert types for device diagnostic alert category.....	114
Table 6 – Alert types for process alert category	114
Table 7 – ARMO attributes (1 of 3)	116
Table 8 – ARMO alerts	119
Table 9 – Alarm_Recovery method	120
Table 10 – DMO attributes (1 of 8).....	122
Table 11 – DMO alerts	130
Table 12 – System management object types	133
Table 13 – DSO attributes.....	135
Table 14 – Address_Translation_Row data structure	136
Table 15 – Read_Address_Row method	136
Table 16 – Input argument usage for Read_Address_Row method	138
Table 17 – Output argument usage for Read_Address_Row method.....	138
Table 18 – Attributes of SMO in system manager.....	140
Table 19 – Proxy_System_Manager_Join method	142
Table 20 – Proxy_System_Manager_Contract method	144
Table 21 – Effect of different join commands on attribute sets	146
Table 22 – Attributes of DMSO in the system manager	146
Table 23 – System_Manager_Join method.....	147
Table 24 – System_Manager_Contract method.....	149
Table 25 – Attributes of STSO in the system manager	153
Table 26 – Attributes of SCO in the system manager	156
Table 27 – SCO method for contract establishment, modification, or renewal (1 of 8)	160
Table 28 – Input argument usage for SCO method for contract establishment, modification, or renewal.....	168
Table 29 – Output argument usage for SCO method for contract establishment, modification, or renewal.....	169
Table 30 – Contract_Data data structure (1 of 3)	172
Table 31 – New_Device_Contract_Response data structure (1 of 2)	176

Table 32 – SCO method for contract termination, deactivation and reactivation	183
Table 33 – DMO method to notify of contract termination	184
Table 34 – DMO method to notify of contract modification	186
Table 35 – Security levels	194
Table 36 – Structure of the security control field	194
Table 37 – Sec.DpduPrep.Request elements	200
Table 38 – Sec.DpduPrep.Response elements	201
Table 39 – Sec.DAckCheck.Request elements	202
Table 40 – Sec.DAckCheck.Response elements	203
Table 41 – Sec.DInitialCheck.Request elements	204
Table 42 – Sec.DInitialCheck.Response elements	205
Table 43 – Sec.DAckPrep.Request elements	205
Table 44 – Sec.DAckPrep.Response elements	206
Table 45 – Structure of the WISN DPDU nonce	207
Table 46 – Structure of the 32-bit truncated TAI time used in the D-nonce	208
Table 47 – TSC pseudo-header structure	213
Table 48 – Sec.TpduOutCheck.Request elements	216
Table 49 – Sec.TpduOutCheck.Response elements	216
Table 50 – Sec.TpduSecure.Request elements	217
Table 51 – Sec. TpduSecure.Response elements	218
Table 52 – Sec.TpduInCheck.Request elements	219
Table 53 – Sec.TpduInCheck.Response elements	220
Table 54 – Sec.TpduVerify.Request elements	221
Table 55 – Sec.TpduVerify.Response elements	222
Table 56 – Structure of TL security header	222
Table 57 – Structure of the TPDU nonce	223
Table 58 – Structure of 32-bit truncated nominal TAI time used in the T-nonce	223
Table 59 – Proxy_Security_Sym_Join method	235
Table 60 – Security_Sym_Join method	236
Table 61 – Security_Confirm method	236
Table 62 – Security_Sym_Join_Request data structure	237
Table 63 – Security_Sym_Join_Response data structure	238
Table 64 – Structure of compressed security level field	239
Table 65 – Master key security level	240
Table 66 – Security_Sym_Confirm data structure	240
Table 67 – Implicit certificate format	242
Table 68 – Usage_serial_number structure	242
Table 69 – Proxy_Security_Pub_Join method	249
Table 70 – Security_Pub_Join method	250
Table 71 – Proxy_Security_Pub_Confirm method	251
Table 72 – Security_Pub_Confirm method	251
Table 73 – Network_Information_Confirmation method	252
Table 74 – Format of asymmetric join request internal structure	253

Table 75 – Format of the protocol control field	253
Table 76 – Format of asymmetric join response internal structure	254
Table 77 – Format of first join confirmation internal structure	255
Table 78 – Format of join confirmation response internal structure	256
Table 79 – Joining process and device lifetime state machine	258
Table 80 – Security_New_Session method	261
Table 81 – Security_New_Session_Request data structure	262
Table 82 – Security_New_Session_Response data structure	264
Table 83 – New_Key method	266
Table 84 – Security_Key_and_Policies data structure	267
Table 85 – Security_Key_Update_Status data structure	269
Table 86 – T-key and D-key state transition	270
Table 87 – Attributes of PSMO in the system manager	271
Table 88 – Structure of policy field	274
Table 89 – Key_Type	274
Table 90 – Key_Usage	275
Table 91 – Granularity	275
Table 92 – DSMO attributes	280
Table 93 – KeyDescriptor	282
Table 94 – T-keyLookupData OctetString fields	283
Table 95 – Delete key method	284
Table 96 – Key_Policy_Update method	285
Table 97 – DSMO alerts	287
Table 98 – Timing requirements	288
Table 99 – Graph table on ND20	294
Table 100 – Graph table on ND21	294
Table 101 – Approximating nominal timing with 32 KiHz clock	325
Table 102 – DL_Config_Info structure	351
Table 103 – CountryCode	357
Table 104 – DD-DATA.request parameters	360
Table 105 – DD-DATA.confirm parameters	361
Table 106 – Value set for status parameter	361
Table 107 – DD-DATA.indication parameters	362
Table 108 – ExtDLUInt, one-octet variant	364
Table 109 – ExtDLUInt, two-octet variant	365
Table 110 – Data DPDU MHR	366
Table 111 – Data DPDU DHDR	367
Table 112 – Data DPDU DMXHR	368
Table 113 – DROUT structure, compressed variant	369
Table 114 – DROUT structure, uncompressed variant	370
Table 115 – DADDR structure	371
Table 116 – ACK/NAK DPDU MHR	372
Table 117 – ACK/NAK DPDU DHR	373

Table 118 – ACK/NAK DPDU DHDR	374
Table 119 – Advertisement DAUX structure	375
Table 120 – Advertisement selections elements.....	376
Table 121 – Advertisement selections.....	377
Table 122 – Advertisement time synchronization elements	377
Table 123 – Advertisement time synchronization structure.....	377
Table 124 – Join superframe information subfields	379
Table 125 – Join superframe information structure.....	379
Table 126 – Superframe derived from advertisement	380
Table 127 – Join information elements.....	381
Table 128 – Join information structure	381
Table 129 – Defaults for links created from advertisements	383
Table 130 – dlmo.Neighbor entry created from advertisements	384
Table 131 – dlmo.Graph entry created from advertisements.....	384
Table 132 – dlmo.Route entry created from advertisements	384
Table 133 – Solicitation header subfields.....	387
Table 134 – Solicitation header structure	387
Table 135 – Solicitation DAUX fields.....	388
Table 136 – Solicitation DAUX structure	388
Table 137 – Activate link DAUX fields	389
Table 138 – Activate link DAUX structure.....	390
Table 139 – Report received signal quality DAUX fields.....	390
Table 140 – Report received signal quality DAUX structure	390
Table 141 – DLMO attributes (1 of 7)	391
Table 142 – D-subnet filter octets	401
Table 143 – dlmo.TaiAdjust OctetString fields.....	402
Table 144 – dlmo.TaiAdjust OctetString structure	402
Table 145 – dlmo.EnergyDesign OctetString fields.....	402
Table 146 – dlmo.EnergyDesign OctetString structure	402
Table 147 – dlmo.DeviceCapability OctetString fields	403
Table 148 – dlmo.DeviceCapability OctetString structure	404
Table 149 – dlmo.DiscoveryAlert fields	406
Table 150 – dlmo.DiscoveryAlert structure	406
Table 151 – dlmo.Candidates OctetString fields.....	407
Table 152 – dlmo.Candidates structure.....	407
Table 153 – dlmo.SmoothFactors OctetString fields.....	408
Table 154 – dlmo.SmoothFactors structure.....	408
Table 155 – dlmo.QueuePriority fields	409
Table 156 – dlmo.QueuePriority structure	410
Table 157 – dlmo.ChannelDiag fields.....	411
Table 158 – dlmo.ChannelDiag structure	411
Table 159 – dlmo.Ch fields	413
Table 160 – dlmo.Ch structure	413

Table 161 – Transaction receiver template fields	416
Table 162 – Transaction receiver template structure	416
Table 163 – Transaction initiator template fields	417
Table 164 – Transaction initiator template structure	418
Table 165 – Default transaction responder template, used during joining process	418
Table 166 – Default transaction initiator template, used during joining process	419
Table 167 – Default transaction responder template, used during joining process	419
Table 168 – dlmo.Neighbor fields	421
Table 169 – dlmo.Neighbor structure	422
Table 170 – ExtendGraph fields	423
Table 171 – ExtGraph structure	424
Table 172 – dlmo.NeighborDiagReset fields	424
Table 173 – dlmo.NeighborDiagReset structure	424
Table 174 – dlmo.Superframe fields	425
Table 175 – dlmo.Superframe structure	426
Table 176 – dlmo.SuperframeIdle fields	430
Table 177 – dlmo.SuperframeIdle structure	430
Table 178 – dlmo.Graph	431
Table 179 – dlmo.Graph structure	431
Table 180 – dlmo.Link fields	432
Table 181 – dlmo.Link structure	433
Table 182 – dlmo.Link[].Type structure	434
Table 183 – Allowed dlmo.Link[].Type combinations	435
Table 184 – Values for dlmo.Link[].Schedule	436
Table 185 – dlmo.Route fields	436
Table 186 – dlmo.Route structure	437
Table 187 – dlmo.NeighborDiag fields	438
Table 188 – Diagnostic summary OctetString fields	438
Table 189 – Diagnostic summary OctetString structure	439
Table 190 – Diagnostic ClockDetail OctetString fields	439
Table 191 – Diagnostic ClockDetail OctetString structure	440
Table 192 – Read_Row method	441
Table 193 – Write_Row method	441
Table 194 – Write_Row_Now method	442
Table 195 – dlmo.AlertPolicy fields	443
Table 196 – dlmo.AlertPolicy OctetString structure	443
Table 197 – DL_Connectivity alert	444
Table 198 – DL_Connectivity alert OctetString	444
Table 199 – NeighborDiscovery alert	445
Table 200 – Link-local address structure	446
Table 201 – Address translation table (ATT)	447
Table 202 – Example of a routing table	452
Table 203 – N-DATA.request elements	466

Table 204 – N-DATA.confirm elements.....	467
Table 205 – N-DATA.indication elements	468
Table 206 – NLMO attributes (1 of 3)	469
Table 207 – Contract table structure	472
Table 208 – Route table elements.....	473
Table 209 – Address translation table structure	473
Table 210 – NLMO structured MIB manipulation methods	475
Table 211 – Alert to indicate dropped PDU/PDU error.....	476
Table 212 – Common header patterns	478
Table 213 – Basic NL header format	478
Table 214 – Contract-enabled NL header format.....	480
Table 215 – 6LoWPAN_IPHC encoding format.....	480
Table 216 – IPv6 NL header format	481
Table 217 – Full NL header in the DL.....	482
Table 218 – NL header format for fragmented NPDUs	483
Table 219 – Format of first fragment header	483
Table 220 – Format of second and subsequent fragment headers.....	484
Table 221 – UDP header encoding	488
Table 222 – UDP 6LoWPAN_NHC-for-UDP encoding octet.....	492
Table 223 – Optimal UDP header encoding.....	492
Table 224 – UDP header encoding with checksum and compressed port numbers.....	493
Table 225 – T-DATA.request elements.....	494
Table 226 – T-DATA.confirm elements.....	495
Table 227 – T-DATA.confirm status codes	495
Table 228 – T-DATA.indication elements	496
Table 229 – TLMO attributes (1 of 2)	497
Table 230 – TL management object methods – Reset.....	499
Table 231 – TL management object methods – Halt.....	500
Table 232 – TL management object methods – PortRangeInfo.....	500
Table 233 – TL management object methods – GetPortInfo	501
Table 234 – TL management object methods – GetNextPortInfo	502
Table 235 – TL management object alert types – Illegal use of port	502
Table 236 – TL management object alert types – TPDU received on unregistered port	503
Table 237 – TL management object alert types – TPDU does not match security policies	503
Table 238 – State table for alarm transitions.....	512
Table 239 – State table for event transitions	513
Table 240 – UAP management object attributes (1 of 2)	530
Table 241 – State table for UAP management object	532
Table 242 – UAP management object methods	532
Table 243 – Alert-receiving object attributes	533
Table 244 – State table for handling an AlertReport reception.....	534
Table 245 – AlertReceiving object methods	535

Table 246 – UploadDownload object attributes (1 of 4)	536
Table 247 – UploadDownload object methods.....	541
Table 248 – UploadDownload object StartDownload method.....	542
Table 249 – UploadDownload object DownloadData method.....	543
Table 250 – UploadDownload object EndDownload method.....	545
Table 251 – UploadDownload object StartUpload method	546
Table 252 – UploadDownload object UploadData method	547
Table 253 – UploadDownload object EndUpload method	548
Table 254 – Download state table for unicast operation mode (1 of 2)	549
Table 255 – Upload state table for unicast operation mode (1 of 2).....	552
Table 256 – Concentrator object attributes (1 of 2)	554
Table 257 – Concentrator object methods.....	555
Table 258 – Dispersion object attributes (1 of 2)	556
Table 259 – Dispersion object methods	557
Table 260 – Tunnel object attributes (1 of 3).....	558
Table 261 – Tunnel object methods	560
Table 262 – Interface object attributes	561
Table 263 – Interface object methods	561
Table 264 – Data type: ObjectAttributeIndexAndSize	563
Table 265 – Data type: Communication association endpoint (1 of 2).....	564
Table 266 – Data type: Communication contract data	566
Table 267 – Data type: Alert communication endpoint.....	567
Table 268 – Data type: Tunnel endpoint.....	567
Table 269 – Data type: Alert report descriptor.....	568
Table 270 – Data type: Process control alarm report descriptor for analog with single reference condition	568
Table 271 – Data type: ObjectIDandType.....	569
Table 272 – Data type: UnscheduledCorrespondent.....	569
Table 273 – AL services	570
Table 274 – Publish service	574
Table 275 – Read service	580
Table 276 – Write service	585
Table 277 – Execute service	589
Table 278 – AlertReport service.....	595
Table 279 – AlertAcknowledge service.....	598
Table 280 – Tunnel service.....	602
Table 281 – Application flow characteristics.....	605
Table 282 – AL service primitive to TL service primitive mapping.....	606
Table 283 – ASLMO attributes (1 of 2)	608
Table 284 – Application sublayer management object methods.....	609
Table 285 – Reset method	610
Table 286 – ASLMO alerts	611
Table 287 – Analog input object attributes	614

Table 288 – Analog input object methods.....	615
Table 289 – Analog input alerts	616
Table 290 – Analog output attributes (1 of 2)	617
Table 291 – Analog output object methods	618
Table 292 – Analog output alerts	619
Table 293 – Binary input object attributes	620
Table 294 – Binary input object methods	621
Table 295 – Binary input alerts	621
Table 296 – Binary output attributes	622
Table 297 – Binary output object methods	623
Table 298 – Binary output alerts	623
Table 299 – Status octet	625
Table 300 – Data type: Process control value and status for analog value	625
Table 301 – Data type: Process control value and status for binary value	626
Table 302 – Data type: Process control mode	626
Table 303 – Data type: Process control mode bitstring.....	626
Table 304 – Data type: Process control scaling.....	627
Table 305 – Process control standard objects.....	627
Table 306 – Services	628
Table 307 – Application messaging format.....	628
Table 308 – Concatenated APDUs in a single TSDU.....	629
Table 309 – Object addressing	629
Table 310 – Four-bit addressing mode APDU header construction.....	630
Table 311 – Eight-bit addressing mode APDU header construction	630
Table 312 – Sixteen-bit addressing mode APDU header construction	630
Table 313 – Inferred addressing use case example	631
Table 314 – Inferred addressing mode APDU header construction.....	631
Table 315 – Six-bit attribute identifier, not indexed	632
Table 316 – Six-bit attribute identifier, singly indexed, with 7-bit index.....	632
Table 317 – Six-bit attribute identifier, singly indexed, with 15-bit index	632
Table 318 – Six-bit attribute identifier, doubly indexed, with two 7-bit indices.....	633
Table 319 – Six-bit attribute identifier, doubly indexed, with two 15-bit indices.....	633
Table 320 – Six-bit attribute identifier, doubly indexed, with first index seven bits long and second index fifteen bits long	633
Table 321 – Six-bit attribute identifier, doubly indexed, with first index fifteen bits long and second index seven bits long.....	633
Table 322 – Twelve-bit attribute identifier, not indexed	634
Table 323 – Twelve-bit attribute identifier, singly indexed with 7-bit index.....	634
Table 324 – Twelve-bit attribute identifier, singly indexed with 15-bit index.....	634
Table 325 – Twelve-bit attribute identifier, doubly indexed with two 7-bit indices.....	634
Table 326 – Twelve-bit attribute identifier, doubly indexed with two 15-bit indices.....	635
Table 327 – Twelve-bit attribute identifier, doubly indexed with first index 7 bits long and second index 15 bits long.....	635

Table 328 – Twelve-bit attribute identifier, doubly indexed with the first index 15 bits long and the second index 7 bits long	635
Table 329 – Twelve-bit attribute identifier, reserved form	635
Table 330 – Coding rules for read service request	636
Table 331 – Coding rules for read service response with 7-bit size field.....	636
Table 332 – Coding rules for read service response with 15-bit size field.....	636
Table 333 – Coding rules for write service request with 7-bit size field.....	637
Table 334 – Coding rules for write service request with 15-bit size field.....	637
Table 335 – Coding rules for write service response	637
Table 336 – Coding rules for execute service request with 7-bit size field	638
Table 337 – Coding rules for execute service request with 15-bit size field	638
Table 338 – Coding rules for execute service response with 7-bit size field	638
Table 339 – Coding rules for execute service response with 15-bit size field.....	639
Table 340 – Coding rules for tunnel service request with 7-bit size field.....	639
Table 341 – Coding rules for tunnel service request with 15-bit size field.....	639
Table 342 – Coding rules for tunnel service response with 7-bit size field	639
Table 343 – Coding rules for tunnel service response with 15-bit size field	640
Table 344 – Coding rules for AlertReport service with 7-bit associated-data size field.....	640
Table 345 – Coding rules for AlertReport service with 15-bit associated-data size field.....	640
Table 346 – Coding rules for AlertAcknowledge service	641
Table 347 – Coding rules for publish service for a native sequence of values	641
Table 348 – Coding rules for publish service – non-native (for tunnel support).....	641
Table 349 – Coding rules for concatenate service	641
Table 350 – General coding rule for size-invariant application data.....	642
Table 351 – General coding rule for size-varying application data of 0..255 octets.....	642
Table 352 – Coding rules for Unsigned8	644
Table 353 – Coding rules for Unsigned16	644
Table 354 – Coding rules for Unsigned32	645
Table 355 – Coding rules for Unsigned64	645
Table 356 – Coding rules for Unsigned128	646
Table 357 – Coding rules for single-precision float.....	647
Table 358 – Coding rules for double-precision float	647
Table 359 – Coding rules for VisibleString	648
Table 360 – Coding rules for OctetString	648
Table 361 – Coding rules for BitString	649
Table 362 – Coding rules for TAINetworkTime, and for TAIDifference when interpreted as a modulo difference	650
Table 363 – Coding rules for TAIRounded	650
Table 364 – Coding example: Read request for a non-indexed attribute	664
Table 365 – Coding example: Read response for a non-indexed attribute	664
Table 366 – Coding example: Tunnel service request	664
Table 367 – Factory default settings	672
Table 368 – Device provisioning object (1 of 6).....	678
Table 369 – Reset_To_Default method	683

Table 370 – Write symmetric join key method	684
Table 371 – Device provisioning service object (1 of 4)	685
Table 372 – DPSOWhiteListTbl data structure (1 of 2)	689
Table 373 – Array manipulation table	691
Table 374 – DPSO alert to indicate join by a device not on the WhiteList	691
Table 375 – DPSO alert to indicate inadequate device join capability	692
Table B.1 – Protocol layer device roles	699
Table B.2 – Over-the-air upgrades	699
Table B.3 – Session support profiles	700
Table B.4 – Baseline profiles	701
Table B.5 – PhL roles	701
Table B.6 – DL required for listed roles	702
Table B.7 – Role profiles: General DLMO attributes	703
Table B.8 – Role profiles: dlmo.Device_Capability	703
Table B.9 – Role profiles: dlmo.Ch (channel-hopping)	704
Table B.10 – Role profiles: dlmo.TsTemplate	704
Table B.11 – Role profiles: dlmo.Neighbor	704
Table B.12 – Role profiles: dlmo.NeighborDiag	705
Table B.13 – Role profiles: dlmo.Superframe	705
Table B.14 – Role profiles: dlmo.Graph	705
Table B.15 – Role profiles: dlmo.Link	706
Table B.16 – Role profiles: dlmo.Route	706
Table B.17 – Role profiles: dlmo.Queue_Priority	706
Table B.18 – Routing table size	707
Table B.19 – Address table size	707
Table B.20 – Port support size	707
Table B.21 – APs	707
Table B.22 – Role profiles: I/O, routers, gateways, and backbone routers	708
Table B.23 – Role profile: Gateway	708
Table B.24 – Role profile: Gateway native access	708
Table B.25 – Role profile: Gateway interworkable tunnel mechanism	709
Table C.1 – Usage classes	711
Table D.1 – System management configuration defaults	716
Table D.2 – Security configuration defaults	717
Table D.3 – DLE configuration defaults	718
Table D.4 – NLE configuration defaults	719
Table D.5 – TLE configuration defaults	719
Table D.6 – ALE configuration defaults	720
Table D.7 – Provisioning configuration defaults	722
Table D.8 – Gateway configuration defaults	722
Table I.1 – Table of standard object types	738
Table I.2 – Template for standard object attributes	739
Table I.3 – Template for standard object methods	740

Table I.4 – Template for standard object alert reporting	741
Table I.5 – Template for data structures.....	742
Table J.1 – Scheduled_Write method template	744
Table J.2 – Read_Row method template	745
Table J.3 – Write_Row method template	745
Table J.4 – Reset_Row method template	746
Table J.5 – Delete_Row method template	747
Table K.1 – Standard object types	749
Table K.2 – Standard object instances	751
Table L.1 – Standard data types	753
Table M.1 – Identification of tunneled legacy fieldbus protocols	755
Table T.1 – Sample MHR for join request.....	785
Table T.2 – Sample DHR for join request.....	786
Table T.3 – Network header for join messages	786
Table U.1 – Summary of notional gateway high-side interface examples.....	792
Table U.2 – Primitive G_Session parameter usage	801
Table U.3 – GS_Status for G_Session confirm.....	803
Table U.4 – Primitive G_Lease parameter usage	804
Table U.5 – GS_Lease_Type for G_Lease request	805
Table U.6 – GS_Status for G_Lease confirm.....	806
Table U.7 – Primitive G_Device_List_Report parameter usage	807
Table U.8 – GS_Status for G_Device_List_Report confirm.....	808
Table U.9 – Primitive G_Topology_Report parameter usage	808
Table U.10 – Primitive G_Schedule_Report parameter usage	810
Table U.11 – Primitive G_Device_Health_Report parameter usage	812
Table U.12 – Primitive G_Neighbor_Health_Report parameter usage	813
Table U.13 – Primitive G_Network_Health_Report parameter usage	815
Table U.14 – Primitive G_Time parameter usage	817
Table U.15 – GS_Status for G_Time confirm	817
Table U.16 – Primitive G_Client_Server parameter usage.....	818
Table U.17 – GS_Status for G_Client_Server confirm	819
Table U.18 – Primitive G_Publish parameter usage	821
Table U.19 – GS_Status for G_Publish confirm.....	822
Table U.20 – Primitive G_Subscribe parameter usage	822
Table U.21 – GS_Status for G_Subscribe confirm.....	823
Table U.22 – Primitive G_Publish_Timer parameter usage.....	823
Table U.23 – Primitive G_Subscribe_Timer parameter usage.....	823
Table U.24 – Primitive G_Publish_Watchdog parameter usage	824
Table U.25 – Primitive G_Bulk_Open parameter usage.....	825
Table U.26 – GS_Status for G_Bulk_Open confirm	826
Table U.27 – Primitive G_Bulk_Transfer parameter usage	826
Table U.28 – GS_Status for G_Bulk_Transfer confirm	826
Table U.29 – Primitive G_Bulk_Close parameter usage	827

Table U.30 – Primitive G_Alert_Subscription parameter usage	828
Table U.31 – GS_Status for G_Alert_Subscription confirm	829
Table U.32 – Primitive G_Alert_Notification parameter usage	829
Table U.33 – Primitive G_Read_Gateway_Configuration parameter usage	830
Table U.34 – GS_Attribute_Identifier values for G_Read_Gateway_Configuration request	831
Table U.35 – Primitive G_Write_Gateway_Configuration parameter usage	831
Table U.36 – GS_Attribute_Identifier values for G_Write_Gateway_Configuration request	832
Table U.37 – GS_Status for G_Write_Gateway_Configuration confirm	832
Table U.38 – Primitive G_Write_Device_Configuration parameter usage	833
Table U.39 – GS_Status for G_Write_Device_Configuration confirm	834
Table U.40 – Primitive G_Read_Device_Configuration parameter usage	834
Table U.41 – Example of gateway configuration management attributes	854

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL NETWORKS – WIRELESS COMMUNICATION NETWORK AND COMMUNICATION PROFILES – ISA 100.11A

FOREWORD

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

DISCLAIMER

This Consolidated version is not an official IEC Standard and has been prepared for user convenience. Only the current versions of the standard and its amendment(s) are to be considered the official documents.

This Consolidated version of IEC 62734 bears the edition number 1.1. It consists of the first edition (2014-10) [documents 65C/778/FDIS and 65C/788/RVD] and its amendment 1 (2019-07) [documents 65C/965/FDIS and 65C/970/RVD]. The technical content is identical to the base edition and its amendment.

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendment 1. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.

International Standard IEC 62734 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation.

This International Standard is based on ISA 100.11a:2011.

The reader's attention is drawn to the fact that Annex V lists all of the "in-some-country" clauses on differing practices of a less permanent nature relating to the subject of this standard.

This first edition constitutes a technical revision.

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

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

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

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

0 Introduction

0.1 General

This standard provides specifications in accordance with the OSI Basic Reference Model, ISO/IEC 7498–1, (e.g., PhL, DL, etc.), and also provides security and management (including network and device configuration) specifications for wireless devices serving Annex C's usage classes 1 through 5, and potentially class 0, for fixed, portable, and moving devices.

This standard is intended to provide reliable and secure wireless operation for non-critical monitoring, alerting, supervisory control, open loop control, and closed loop control applications. This standard defines a protocol suite, including system management, gateway considerations, and security specifications, for low-data-rate wireless connectivity with fixed, portable, and slowly-moving devices, often operating under severe energy and power constraints. The application focus is the performance needs of process automation monitoring and control where end-to-end communication latencies on the order of at least 100 ms can be tolerated.

To meet the needs of industrial wireless users and operators, the technology specified in this document provides robustness in the presence of interference found in harsh industrial environments or caused by wireless systems not covered by this international standard. As described in Clause 4, this standard addresses coexistence with other wireless devices anticipated in the industrial workspace, such as cell phones and devices based on IEC 62591 (based on WirelessHART™¹), IEC 62601 (based on WIA-PA), IEEE 802.11 (WiFi), IEEE 802.15, IEEE 802.16 (WiMax), and other relevant standards. Furthermore, this standard supports interoperability of devices compliant with this international standard, as described in Clause 5, in those aspects of operation that are covered by this international standard.

This standard does not define or specify plant infrastructure or its security or performance characteristics. However, it is important that the security of the plant infrastructure be assured by the end user.

0.2 Document structure

This document is organized into clauses focused on unique network functions and protocol suite layers. The clauses describe system, system management, security management, physical layer, data-link layer, network layer, transport layer, application layer, and provisioning. Generic considerations that apply to protocol gateways are also included, though specifications of specific protocol gateways are not. Each clause describes a functionality or protocol layer and dictates the behavior required for proper operation. When a clause describes behaviors related to another function or layer, a reference to the appropriate other clause is supplied for further information.

The mandatory and optional communication protocols defined by this document are referred to as native protocols, while those protocols used by other networks such as legacy fieldbus communication protocols are referred to as foreign protocols.

0.3 Potentially relevant patents

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of multiple patents:

- a) concerning elliptic curve (asymmetric) cryptography, given in 7.4.6 and 7.2.2.3;

¹ Property of the HART Communication Foundation. This information is given for the convenience of users of the standard and does not constitute an endorsement of the trademark holder or any related products. Compliance to this profile does not require use of the registered trademark. Use of the trademarks requires permission of the trade name holder.

- b) concerning synchronizing clocks and assessing link quality, given in 9.1.9.3 and 9.1.15;
- c) concerning unspecified subject areas;
- d) concerning wireless provisioning, and selection and routing among multiple gateways.

IEC takes no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured the IEC that they are willing to negotiate licences either free of charge (free) or under reasonable and non-discriminatory terms and conditions (RAND) with applicants throughout the world. In this respect, the statements of the following holders of those patent rights are registered with IEC.

Information on these patent rights and their licensing may be obtained from:

a)	Certicom Corporation 4701 Tahoe Blvd, Bldg A L4W 0B5 Mississauga, ON CANADA Attn: Patent licensing Licensing terms: presumably RAND Relevant patents: unknown; not stated by patent holder	b)	NIVIS LLC 1000 Circle 75 Pkwy, Suite 300 Atlanta, GA 30339-6051 USA Attn: Patent licensing Licensing terms: RAND Relevant patents: – US 20100027437 – US 20100098204
c)	General Electric 1 Research Cir Schenectady, NY 12309-1027 USA Attn: Patent licensing Licensing terms: presumably RAND, reciprocity Relevant patents: unknown; not stated by patent holder	d)	Yokogawa Electric Corporation 2-9-32 Nakachou, ~~Musashina~~ Musashino-shi Tokyo JAPAN Attn: Patent licensing Licensing terms: RAND, reciprocity Relevant patents: – JP 4129749 – US 8005514 – US 8031727 – US 8305927 – US 2009080394
The above patent holders, patents, and licensing terms are those declared to the IEC as relevant to IEC 62734, as of the date of preparation of this text.			

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. IEC shall not be held responsible for identifying any or all such patent rights.

ISO (<http://www.iso.org/patents>) and IEC (<http://patents.iec.ch>) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult these databases for the most up-to-date information concerning patents.

INDUSTRIAL NETWORKS – WIRELESS COMMUNICATION NETWORK AND COMMUNICATION PROFILES – ISA 100.11A

1 Scope

This International Standard specifies a method of reliable and secure wireless operation for non-critical monitoring, alerting, supervisory control, open loop control, and closed loop control applications. This standard defines a protocol suite, including system management, gateway considerations, and security specifications, for low-data-rate wireless connectivity with fixed, portable, and slowly-moving devices, often operating under severe energy and power constraints. The application focus of this standard is the performance needs of process automation monitoring and control, where end-to-end communication delays on the order of 100 ms can be tolerated.

This standard specifies the following:

- physical layer service definition and protocol specification;
- data-link layer service definition and protocol specification;
- network layer service definition and protocol specification;
- transport layer service definition and protocol specification;
- application layer service definition and protocol specification, including support for protocol tunneling and gateways;
- security and security management;
- provisioning and configuration;
- network management; and
- additive communication role profiles (i.e., one or more can be selected concurrently).

Functionality above the application layer of the OSI Basic Reference Model, such as the so-called User Layer and different profiles for functionality at that layer, is not addressed. However, it is discussed briefly in Annex A.

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.

NOTE See the Bibliography for non-normative references.

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

ISO/IEC 10731, *Information technology – Open Systems Interconnection – Basic Reference Model – Conventions for the definition of OSI services*

ISO/IEC 18033-3, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*

ISO/IEC 19772, *Information technology – Security techniques – Authenticated encryption*

ANSI X9.63:2011, *Public Key Cryptography for the Financial Services Industry – Key Agreement and Key Transport Using Elliptic Curve Cryptography*

IETF RFC 2460:1998, *Internet Protocol, Version 6 (IPv6) Specification*

IETF RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*

IETF RFC 2529, *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*

IETF RFC 3168, *The Addition of Explicit Congestion Notification (ECN) to IP*

IETF RFC 4213, *Basic Transition Mechanisms for IPv6 Hosts and Routers*

IETF RFC 4291:2006, *IP Version 6 Addressing Architecture*

IETF RFC 4944, *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*

IETF RFC 6282:2011, *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*

IETF RFC 6298, *Computing TCP's Retransmission Timer*

IEEE Std 802.15.4™:2011/2015², ~~IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANS)~~ *IEEE Standard for Low-Rate Wireless Networks*

SEC 1:2009, *Elliptic Curve Cryptography, version 2*, available at <http://www.secg.org>

SEC 4, *Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV), version 0.97*, available at <http://www.secg.org>

3 Terms, definitions, abbreviated terms, acronyms, and conventions

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

3.1 Terms and definitions

3.1.1 (N)-layer and other terms and definitions from the open systems interconnection Basic Reference Model

3.1.1.1

abstract syntax

specification of (N)-PDUs by using notation rules which are independent of the encoding technique used to represent them

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 7.1.1.2, modified – generalized to any layer]

² Property of IEEE, <http://www.ieee.org>.

3.1.1.2

accountability

property that ensures that the actions of an entity may be traced uniquely to the entity

[SOURCE: ISO 7498-2:1989, 3.3.3]

3.1.1.3

acknowledgment

function of the (N)-layer which allows a receiving (N)-entity to inform a sending (N)-entity of the receipt of an (N)-PDU

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.16]

3.1.1.4

application-entity

active element, within an application process, embodying a set of capabilities that is pertinent to OSI and that is defined for the AL, that corresponds to a specific application-entity-type (without any extra capabilities being used)

Note 1 to entry: This is a slight specialization of (N)-entity, because the AL includes non-OSI-relevant application functions. Each application-entity represents one and only one process in the open system interconnection environment.

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 7.1.1.1]

3.1.1.5

application-management

functions in the AL related to management of OSI application-processes

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 8.1.1]

3.1.1.6

association

cooperative relationship between system entities, usually for the purpose of transferring information between them

[SOURCE: IEC TS 62443-1-1:2009, 3.2.7]

3.1.1.7

(N)-association

cooperative relationship among (N)-entity-invocations

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.3.1.1]

3.1.1.8

authorization

granting of rights, which includes the granting of access based on access rights

[SOURCE: ISO 7498-2:1989, 3.3.10]

3.1.1.9

availability

property of being accessible and useable upon demand by an authorized entity

[SOURCE: ISO 7498-2:1989, 3.3.11]

3.1.1.10 blocking

function performed by an (N)-entity to map multiple (N)-SDUs into one (N)-PDU

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.11]

3.1.1.11 centralized-multi-endpoint-connection

multi-endpoint-connection where data sent by the entity associated with the central-connection-endpoint is received by all other entities, while data sent by the other entities is received by only the central entity

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.2]

3.1.1.12 ciphertext

data produced through the use of encipherment so that the semantic content of the resulting data is not available

Note 1 to entry: See cleartext, plaintext.

Note 2 to entry: Relative to a PDU, ciphertext is information in a PDU that is subject to obscuration by encryption, in its post-encryption pre-decryption obscured form.

[SOURCE: ISO 7498-2:1989, 3.3.1]

3.1.1.13 cleartext

<generic> intelligible data, the semantic content of which is available

[SOURCE: ISO 7498-2:1989, 3.3.15]

3.1.1.14 cleartext

<communications-protocol-specific> information in a PDU that is not subject to obscuration by encryption

Note 1 to entry: Relative to a PDU, cleartext is information in the PDU that is not subject to obscuration by encryption, that when present in the PDU is always present in its unobscured form.

3.1.1.15 compromise

violation of computer security whereby programs or data may have been modified, destroyed, or made available to unauthorized entities

[SOURCE: ISO/IEC 2382-8:1998, 08.05.11]

3.1.1.16 concatenation

function performed by an (N)-entity to map multiple (N)-PDUs into one (N-1)-SDU

Note 1 to entry: Blocking and concatenation, though similar (they both permit grouping of data-units) serve different purposes. For instance, concatenation permits the (N)-layer to group one or several acknowledgment (N)-PDUs with one (or several) (N)-PDUs containing user-data. This would not be possible with the blocking function only. Note also that the two functions are combinable so that the (N)-layer performs blocking and concatenation.

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.13]

3.1.1.17

concrete syntax

those aspects of the rules used in the specification of data which embody a specific representation of that data

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 7.2.1.1]

3.1.1.18

confidentiality

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Note 1 to entry: In a general information security context, confidentiality preserves authorized restrictions on information access and disclosure, including means for preserving personal privacy and proprietary information.

[SOURCE: ISO 7498-2:1989, 3.3.16]

3.1.1.19

(N)-connection

association requested by an (N+1)-layer entity for the transfer of data between two or more (N+1)-entities

Note 1 to entry: The association is established by the (N)-layer and provides explicit identification of a set of (N)-data-transmissions and agreement concerning the (N)-data-transmission services to be provided for the set.

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.3.1.2]

3.1.1.20

(N)-connection endpoint

terminator at one end of an (N)-connection within an (N)-service-access-point

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.3.1.3]

3.1.1.21

(N)-connection-endpoint-identifier

identifier of an (N)-connection-endpoint which can be used to identify the corresponding (N)-connection at an (N)-SAP

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.4.1.5]

3.1.1.22

(N)-connection-endpoint-suffix

that part of an (N)-connection-endpoint-identifier which is unique within the scope of an (N)-SAP

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.4.1.6]

3.1.1.23

(N)-connection-mode-transmission

(N)-data-transmission in the context of an (N)-connection

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.3.1.17]

3.1.1.24

(N)-connectionless-mode-transmission

(N)-data-transmission not in the context of an (N)-connection and not required to maintain any logical relationship between (N)-SDUs

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.3.1.18]

3.1.1.25

correspondent-(N)-entities

(N)-entities with an (N-1)-connection between them

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.3.1.5]

3.1.1.26

cryptanalysis

analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext

[SOURCE: ISO 7498-2:1989, 3.3.18]

3.1.1.27

data integrity

property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1989, 3.3.21]

3.1.1.28

data-origin authentication

corroboration that the source of data received is as claimed

[SOURCE: ISO 7489-2:1989, 3.3.22]

3.1.1.29

(N)-data transmission

(N)-facility that conveys SDUs from one (N+1) layer entity to one or more (N+1) entities

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.3.1.9]

3.1.1.30

deblocking

function performed by an (N)-entity to identify multiple (N)-SDUs which are contained in one (N)-PDU

Note 1 to entry: In the absence of error, deblocking is the reverse function of blocking.

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.12]

3.1.1.31

decentralized-multi-endpoint-connection

multi-endpoint-connection where data sent by an entity associated with a connection-endpoint is received by all other entities

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.3]

3.1.1.32

decryption

reversal of a corresponding reversible encipherment

[SOURCE: ISO 7498-2:1989, 3.3.23]

3.1.1.33

demultiplexing

function performed by an (N)-entity which identifies (N)-PDUs for more than one (N)-connection within an (N-1)-connection

Note 1 to entry: In the absence of error, demultiplexing is the reverse function of multiplexing.

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.5]

3.1.1.34

digital signature

data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

[SOURCE: ISO 7498-2:1989, 3.3.26]

3.1.1.35

(N)-entity

active element within an (N)-subsystem embodying a set of capabilities defined for the (N)-layer that corresponds to a specific (N)-entity-type (without any extra capabilities being used)

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.2.1.11]

3.1.1.36

(N)-entity-invocation

specific utilization of part or all of the capabilities of a given (N)-entity (without any extra capabilities being used)

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.2.1.12]

3.1.1.37

(N)-entity-type

description of a class of (N)-entities in terms of a set of capabilities defined for the (N)-layer

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.2.1.10]

3.1.1.38

(N)-interface-control-information

information transferred locally between an (N+1)-entity and an (N)-entity to coordinate their joint operation

3.1.1.39

(N)-layer

subdivision of the OSI architecture, constituted by subsystems of the same rank (N)

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.2.1.2]

3.1.1.40

(N)-layer-management

functions related to the management of the (N)-layer partly performed in the (N)-layer itself according to the (N)-protocol of the layer (activities such as activation and error control) and partly performed as a subset of systems-management

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 8.1.6]

3.1.1.41

multi-endpoint-connection

connection with more than two connection-endpoints

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.3.1.4]

3.1.1.42

multiplexing

function performed by an (N)-entity in which one (N-1)-connection is used to support more than one (N)-connection

Note 1 to entry: The term multiplexing is also used in a more restricted sense to the function performed by the sending (N)-entity while the term demultiplexing is used to the function performed by the receiving (N)-entity.

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.4]

3.1.1.43

password

confidential authentication information, usually composed of a string of characters

[SOURCE: ISO 7498-2:1989, 3.3.39]

3.1.1.44

peer-(N)-entities

entities within the same (N)-layer

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.2.1.3]

3.1.1.45

peer-entity authentication

corroboration that a peer entity in an association is the one claimed

[SOURCE: ISO 7489-2:1989, 3.3.40]

3.1.1.46

(N)-protocol

set of rules and formats (semantic and syntactic) that determines the communication behavior of (N)-entities in the performance of (N)-functions

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.2.1.9]

3.1.1.47

(N)-protocol-addressing-information

those elements of (N)-PCI which contain addressing information

[SOURCE: ISO/IEC 7498-3:1997, 3.4.20]

3.1.1.48

(N)-protocol-control-information

information exchanged between (N)-entities to coordinate their joint operation

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.6.1.1]

3.1.1.49

(N)-protocol-data-unit

unit of data specified in an (N)-protocol and consisting of (N)-protocol-control-information and possibly (N)-user-data

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.6.1.3]

3.1.1.50

(N)-protocol-version-identifier

identifier conveyed between correspondent (N)-entities which allows the selection of the version of an (N)-protocol

Note 1 to entry: The definition of a new (N)-protocol-version-identifier presupposes a minimal common knowledge of the (N)-protocol identified by the preceding (N)-protocol-version-identifier. When such a minimal common knowledge cannot be achieved, the (N)-protocols are considered to be independent and different.

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.18]

3.1.1.51

quality of service

<generic> collective effect of service performance which determines the degree of satisfaction of a user of the service

Note 1 to entry: The quality of service is characterized by the combined aspects of service support performance, service operability performance, serviceability performance, service integrity and other factors specific to each service.

Note 2 to entry: ISO defines quality as the ability of a product or service to satisfy users' needs.

[SOURCE: IEC 61907:2009, 3.1.15]

3.1.1.52

quality of service

<data link service> negotiated parameters for a link, including

- priority;
- time windows for control messaging;
- acceptability of out-of-order message delivery; and
- acceptability of message delivery in partial increments

3.1.1.53

reassembling

function performed by an (N)-entity to map multiple (N)-PDUs into one (N)-SDU

Note 1 to entry: In the absence of error, reassembling is the reverse function of segmenting.

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.10]

3.1.1.54

recombining

function performed by an (N)-entity which identifies (N)-PDUs for a single (N)-connection in (N-1)-SDUs received on more than one (N-1)-connection

Note 1 to entry: In the absence of error, recombining is the reverse function of splitting.

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.7]

3.1.1.55

(N)-relay

(N)-function by means of which an (N)-entity forwards data received from one peer (N)-entity to another peer (N)-entity

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.3.1.6]

3.1.1.56

reset

function that sets the corresponding (N)-entities to a predefined state with a possible loss or duplication of data

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.17]

3.1.1.57

security label

marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource

[SOURCE: ISO 7498-2:1989, 3.3.49]

3.1.1.58

segmenting

function performed by an (N)-entity to map one (N)-SDU into multiple (N)-PDUs

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.9]

3.1.1.59

(N)-selector

that part of an (N)-address that is specific to the addressed (N)-subsystem, i.e., which identifies one or more (N)-SAPs within an end open system once that end open system is unambiguously identified

Note 1 to entry: Since the end open system is implicitly known at the Network layer, (N)-selectors are used above the Network layer, along with local information, to address the desired (N+1)-entity within the open system. (N)-selector values are exchanged between open systems as part of the (N)-PAI.

[SOURCE: ISO/IEC 7498-3:1997, 6.2.3]

3.1.1.60

separation

function performed by an (N)-entity to identify multiple (N)-PDUs which are contained in one (N-1)-SDU

Note 1 to entry: In the absence of error, separation is the reverse function of concatenation.

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.14]

3.1.1.61

sequencing

function performed by the (N)-layer to preserve the order of (N)-SDUs that were submitted to the (N)-layer

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.15]

3.1.1.62

(N)-service

capability of the (N)-layer and the layers beneath it, which is provided to (N+1) entities at the boundary between the (N)-layer and the (N+1) layer

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.2.1.5]

3.1.1.63

(N)-service access point

point at which (N)-services are provided by an (N)-entity to an (N+1)-entity

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.2.1.8]

3.1.1.64

(N)-service-access-point-address

(N)-address that is used to identify a single (N)-SAP

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.4.1.2]

3.1.1.65

(N)-service-data-unit

amount of information whose identity is preserved when transferred between peer (N+1)-entities and which is not interpreted by the supporting (N)-entities

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.6.1.4]

3.1.1.66

splitting

function within the (N)-layer by which more than one (N-1)-connection is used to support one (N)-connection

Note 1 to entry: The term splitting is also used in a more restricted sense to see the function performed by the sending (N)-entity while the term recombining is used to see the function performed by the receiving (N)-entity.

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.8.1.6]

3.1.1.67

system management

functions in the AL related to management of various OSI resources and their status across all layers of the OSI architecture

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 8.1.4]

3.1.1.68

transfer syntax

abstract and concrete syntax used in the transfer of data between open systems

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 7.2.1.2]

3.1.1.69

user application process

active process within the highest portion of the AL that is the user of OSI services

Note 1 to entry: The aspects of a UAP that need to be taken into account for the purpose of OSI are represented by one or more application-entities, of one or more application-entity-types, defined in ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 7.1.2.2 and 7.1.2.3.

Note 2 to entry: The collection of UAPs is sometimes referred to as the user layer, even though ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 7.1.2.1 states that the AL has no boundary with a higher layer. In the OSI Basic Reference Model, the AL includes the UAPs.

3.1.1.70

(N)-user-data

data transferred between (N)-entities on behalf of the (N+1)-entities for which the (N)-entities are providing services

[SOURCE: ISO/IEC 7498-1:1994 as corrected and reprinted in 1996, 5.6.1.2]

3.1.2 Other terms and definitions

NOTE Sources of definitions that are otherwise unreferenced by this standard can be found in the Bibliography.

3.1.2.1

access control

means to ensure that access to assets is authorized and restricted based on business and security requirements

[SOURCE: ISO/IEC 27000:2014, 2.1]

3.1.2.2

adapter

specialization of a device that internally converts the protocol in the attached legacy device(s) to that of a network device compliant with this standard

3.1.2.3

alarm

condition that maintains a state until the condition clears, reported on change of state

EXAMPLE The occurrence of an alarm or of a return-to-normal condition that is of potential significance to a correspondent UAP.

3.1.2.4

alert

action of reporting an event condition or an alarm condition

3.1.2.5

end application

application

system or problem to which a computer is applied

3.1.2.6

application program

application

program that provides functionality to end users

3.1.2.7

application layer

application

highest protocol layer in the ISO/IEC Basic Reference Model in which types of applications are classified according to criticality

3.1.2.8

application process

element that performs the information processing for a particular application

3.1.2.9

asymmetric-key algorithm

asymmetric-key cryptographic algorithm

public key cryptographic algorithm

<information security> algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ

[SOURCE: ISO/IEC 10181-1:1996, 3.3.1]

3.1.2.10

authentication

<information security> verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system

Note 1 to entry: See data-origin authentication (3.1.1.28) and/or peer-entity authentication (3.1.1.45).

3.1.2.11

authentication code

<information security> full or truncated cryptographic checksum based on an appropriate security function

Note 1 to entry: See 3.1.2.97.

Note 2 to entry: This is also known as a message authentication code (MAC). It is called a message integrity code (MIC) when used in contexts where the acronym MAC has an alternate definition, such as in local area network standards.

[SOURCE: ISO/IEC 19790:2012, 3.8, modified by the “full or truncated” prefix]

3.1.2.12

backbone network

backbone subnet

network not specified by this standard, generally using IPv6 or IPv4 network technology, that is used for routing between the wireless industrial sensor (and actuator) network (WISN) of this standard and

- a) connected back-end devices that are specified in part by this standard, such as system managers, security managers, and protocol gateways;
- b) devices that natively support the wireless TL, AL and management protocols of this standard; and
- c) other backbone routers on the same backbone subnet

3.1.2.13

backbone router

router that forwards between the wireless network of this standard and a higher-speed backbone network

3.1.2.14

backup

procedure, technique, or hardware used to help recover lost or destroyed data or to keep a system operating

[SOURCE: ISO 2382-12:1988, 12.01.17]

3.1.2.15

bandwidth

<analog domain> numerical difference between the upper and lower frequencies of a band of frequencies

Note 1 to entry: Analog bandwidth is expressed in Hz.

3.1.2.16

bandwidth

<digital domain> amount of data that can be passed along a communications channel within a given period of time

Note 1 to entry: Digital bandwidth is expressed in bit/s.

3.1.2.17

black channel

communication channel of a safety system that provides no safety functionality in addition to its basic communication capability

3.1.2.18

blacklist

list of RF channels upon which transmission is prohibited

Note 1 to entry: A blacklist is temporary or permanent, local or network-wide.

3.1.2.19

block cipher

<information security> cryptographic primitive that uses a symmetric key to create a key-dependent pseudorandom permutation of a fixed-size bit string

3.1.2.20

broadcast

transmission intended for all nodes

Note 1 to entry: Broadcast reception often is limited to specific layers, e.g., MAC or network layer.

Note 2 to entry: Many lower layer protocols do not provide an acknowledgment for broadcasts.

3.1.2.21

canonical transfer syntax

full transfer syntax

full encoding of an object for transfer between devices, before any compression

3.1.2.22

cipher

<information security> cryptographic technique used to protect the confidentiality of data, consisting of three component processes: an encryption algorithm, a decryption algorithm, and a method for generating keys

[SOURCE: attributed in other ISO/IEC standards to an unknown edition of ISO/IEC 18033-1, modified – slightly edited for readability.]

3.1.2.23

coexistence

ability of multiple systems to perform their tasks in a given environment where they may or may not be using a similar set of rules

3.1.2.24

compressed transfer syntax

encoding of an object for transfer between devices, after any compression

3.1.2.25

communications latency

delay between an initial communications event, such as making a transmit request, and a related subsequent communications event, such as message delivery at an intended recipient

3.1.2.26

communications reliability

degree to which messages reach their final destination complete and uncorrupted and within acceptable latency

3.1.2.27

communications throughput

capacity of a communications channel, usually measured in message/s or octet/s

3.1.2.28

construction option

set of features that a device designer may choose to include in, or exclude from, a device

3.1.2.29

contract

agreement between the system manager and a device in the network involving the allocation of network resources by the system manager to support a particular communication need of that device

3.1.2.30

cryptographic algorithm

<information security> algorithm based upon the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms

Note 1 to entry: Examples of cryptographic algorithms are block and stream ciphers and keyed hashes. An unkeyed hash is not formally a cryptographic algorithm, although it often is a one-way function that has similar resistance to attack, and often is constructed from a cryptographic algorithm with a fixed key. The SHA family of hashes is so constructed.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.34, modified – a note has been added.]

3.1.2.31

cryptographic key

key

<information security> mathematical value that is used

- a) in an algorithm to generate ciphertext from plaintext or vice versa, and
- b) to determine the operation of a cryptographic function (e.g., the synchronized generation of keying material), or a digital signature computation or validation

[SOURCE: IEC TS 62351-2:2008, 2.2.64]

3.1.2.32

cryptographic key component

key component

<information security> parameter(s) used in a security function to perform a cryptographic function

[SOURCE: ISO/IEC 19790:2012, 3.24]

3.1.2.33

cryptographic module

<information security> set of hardware, software, and/or firmware that implements appropriate security functions and is contained within the cryptographic boundary

[SOURCE: ISO/IEC 19790:2012, 3.25]

3.1.2.34

cryptoperiod

<information security> time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect

[SOURCE: ISO/IEC 11568-4:2007, 3.9]

3.1.2.35

data authenticity

<information security> assurance about the source of information

[SOURCE: IEEE 802-15-4:2011, 3.1]

3.1.2.36

data key

data authenticating key

data encrypting key

<information security> cryptographic key used for the encipherment, decipherment or authentication of data

[SOURCE: ISO/IEC 11568-2:2012, 3.5]

3.1.2.37

deployment option

set of features that a device designer includes in a device, but which the end-user or their agent (e.g., a network security manager) can elect to employ or not employ

3.1.2.38

derived key

<information security> symmetric key that is derived from a prior symmetric key

Note 1 to entry: Such keys are usable to limit the cryptoperiod of any single key while meeting key archive requirements, provided that the independent key from which the derived key was derived (perhaps through many generations of derivation) has previously met those archive requirements.

3.1.2.39

key destruction

destruction

<information security> zeroisation or physical destruction of keying material so that it cannot be recovered

3.1.2.40

deterministic random bit generator

<information security> process used to generate an unpredictable series of bits that are random in the sense that there is no way to describe the generator's output that is more efficient than simply listing each entire output string

Note 1 to entry: Deterministic random bit generators have provable properties. The unpredictability of their output depends on the unpredictability of their initial seed and, for hybrid generators, the rate at which new unpredictable (high entropy) input is included relative to the number of output bits generated. See note to entry 1 of 3.1.2.102, non-deterministic random bit generator, for common sources of such unpredictability.

3.1.2.41

device security management object

application software within a device that acts as a local peer of a security manager

3.1.2.42

duocast

variant of unicast, wherein a second receiver is scheduled to overhear the DPDU and provides a second acknowledgment within a single D-transaction

Note 1 to entry: Duocast is shown graphically in Figure 84.

3.1.2.43

encrypted key

<information security> cryptographic key that has been encrypted using an approved security function with a key encryption key

Note 1 to entry: This process is used in order to disguise the value of the underlying plaintext key.

[SOURCE: ISO/IEC 19790:2012, 3.36]

3.1.2.44
encryption

<information security> reversible operation by a cryptographic algorithm converting data into ciphertext so as to hide the information content of the data

[SOURCE: ISO/IEC 9798-1:2010, 3.13]

3.1.2.45
entity

individual (person), organization, device or process

3.1.2.46
ephemeral key

<information security> cryptographic key that is generated for each execution of a key establishment process and that meets other requirements of the key type (e.g., unique to each message exchange or session)

Note 1 to entry: In some cases ephemeral keys are used more than once, within a single session (e.g., broadcast applications) where the originator generates only one ephemeral key pair per message and the private key (of that pair) is combined separately with each recipient's public key.

3.1.2.47
event

transient (i.e., stateless) condition, used to report when something happened

EXAMPLE The occurrence of an alarm or a return-to-normal condition that is of potential significance to a correspondent UAP.

3.1.2.48
field device

physical device designed to meet the rigors of plant operation that communicates via DPDU's and higher-layer protocols conforming to this standard

Note 1 to entry: These include routing devices, sensors, and actuators.

3.1.2.49
field network

configuration of two or more field devices interconnected by the wireless protocol defined by this standard

3.1.2.50
field router

router that is also a field device (i.e., not a backbone router), existing within a field network

3.1.2.51
foreign protocol application communication

optimized conveyance of PDUs or portions of PDUs from a first protocol within a second protocol by selective usage of caching, compression, address translation and proxy techniques

3.1.2.52
fragment, verb
segment

to break or separate into contiguous disjoint parts

Note 1 to entry: Fragment and fragmentation are the terms used by the IETF in internet protocol specifications to describe the OSI concepts of segment and segmentation. In this standard the terms fragment and segment are essentially synonymous, with fragment usually used at the network layer and sometimes at other protocol layers, while segment is usually used at the application layer and sometimes at other protocol layers.

3.1.2.53

fragment, noun
segment

one of the (N)-protocol-data-units resulting from the operation of segmenting

Note 1 to entry: Fragment and fragmentation are the terms used by the IETF in internet protocol specifications to describe the OSI concepts of segment and segmentation. In this standard the terms fragment and segment are essentially synonymous, with fragment usually used at the network layer and sometimes at other protocol layers, while segment is usually used at the application layer and sometimes at other protocol layers.

3.1.2.54 gateway

role (of a device) that acts as a protocol translator between an AE conforming to this standard and other, different AEs

3.1.2.55

hash-based message authentication code

<information security> message authentication code that uses an appropriate keyed-hash function

Note 1 to entry: This definition is generalized from the second construction of ISO/IEC 9797-2, which refers to the HMAC construction that is also specified in [US] FIPS 198.

[SOURCE: ISO/IEC 9797-2:2011, modified – generalized.]

3.1.2.56

hash function

<information security> function which maps strings of bits to fixed-size strings of bits, satisfying the following two properties: for a given output, it is computationally infeasible to find an input which maps to this output; for a given input, it is computationally infeasible to find a second input which maps to the same output

Note 1 to entry: Computational feasibility depends on the specific security requirements and environment.

Note 2 to entry: See the note 1 to entry of 3.1.2.30.

[SOURCE: ISO/IEC 9796-2:2010, 3.6, modified – notes to entry have been added.]

3.1.2.57

hash value

<information security> full or truncated result of applying a hash function to information

3.1.2.58

identity

distinguishing character or personality of an individual or entity

3.1.2.59

independent key

<information security> symmetric key that is derived from a high entropy bit source and not from a prior key

3.1.2.60

infrastructure

technical structures that support data communications within a facility

EXAMPLE Parts of a plant's IT network, perhaps using IEEE 802.3 or IEEE 802.11, or IEC 61158 Type 10 (PROFINet) or IEC 61158 Type 9 (FOUNDATION™ Fieldbus HSE).³

³ PROFINet and FOUNDATION Fieldbus are the trademarks of various trade organizations. This information is given for the convenience of users of the standard and does not constitute an endorsement of the trademark holders or any of their products. Compliance to this profile does not require use of the registered trademark. Use of the trademarks requires permission of the trade name holder.

3.1.2.61

initialization vector

<information security> block of bits that is required to allow a cryptographic cipher in a streaming mode of operation to produce a unique stream independent from other streams produced under the same encryption key

3.1.2.62

interoperable

able to work together to perform a specific role in one or more distributed application programs

Note 1 to entry: In this case parameters and their application-related functionality fit together both syntactically and semantically. Interoperability is achieved when the devices support complementary sets of parameters and functions belonging to the same profile.

[SOURCE: IEC TR 62390:2005, 6.2.2.6, modified – adapted.]

3.1.2.63

interworkable

able to transfer parameters among correspondents

Note 1 to entry: In addition to the communication protocol, communication interface and data access, the parameter data types are the same.

[SOURCE: IEC TR 62390:2005, 6.2.2.5, modified – adapted.]

3.1.2.64

kerberos protocol

specific network authentication protocol that allows individuals communicating over an insecure network to prove their identity to one another in a secure manner

3.1.2.65

key agreement

<information security> process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key

[SOURCE: ISO/IEC 11770-1:2010, 2.13]

3.1.2.66

key archive

key management archive

<information security> encryption system with a backup decryption capability that allows authorized persons, under certain prescribed conditions, to decrypt ciphertext with the help of information supplied by one or more trusted parties which hold special data recovery keys

3.1.2.67

key center

<information security> centralized key distribution process, usually a separate computer system, that uses key-encrypting keys (master keys) to encrypt and distribute T-keys needed by a community of users

Note 1 to entry: Key centers generally are certified, traceable to an accredited independent testing agency, as meeting the requirements of ISO/IEC 19790 (similar to FIPS 140-2) for a Level 3 or Level 4 cryptographic module.

3.1.2.68

key confirmation

<information security> assurance for one entity that another identified entity is in possession of the correct key

[SOURCE: ISO/IEC 11770-1:2010, 2.16]

3.1.2.69

key de-registration

<information security> marking of all keying material records and associations to indicate that the key is no longer in use

3.1.2.70

key derivation

<information security> process by which one or more keys are derived from a shared secret and other information

3.1.2.71

key distribution

<information security> transport of a key and other keying material from an entity that either owns the key or generates the key to another entity that is intended to use the key

3.1.2.72

key distribution center

entity that is trusted to generate or acquire keys and to distribute the keys to communicating parties and that shares a unique symmetric key with each of the parties

[SOURCE: ISO/IEC 11770-1:2010, 2.22]

3.1.2.73

key encrypting key

<information security> cryptographic key that is used for the encryption or decryption of other keys

Note 1 to entry: Best practice is to limit use of symmetric (secret) KEKs to key wrapping and not use them for key transport or session (i.e., data) keys.

Note 2 to entry: KEKs may form a hierarchy. In this standard KEKs are often referred to as “master keys”, although the two concepts are not synonymous.

3.1.2.74

key escrow

<information security> process of recording keys and any related essential key recovery information in a key archive

3.1.2.75

key establishment

<information security> process by which cryptographic keys are securely distributed among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consisting of key transport plus key agreement)

3.1.2.76

keying material installation

<information security> installation of keying material for operational use

3.1.2.77

key management

<information security> administration and use of generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy

[SOURCE: ISO/IEC 11770-1:2010, 2.28]

3.1.2.78

key management infrastructure

<information security> framework and services that provide for the generation, production, distribution, control, accounting, and destruction of all cryptographic material, including symmetric keys, as well as public key signing and generation of its own static and ephemeral asymmetric-key pairs

Note 1 to entry: This includes all elements (hardware, software, other equipment, and documentation); facilities; personnel; procedures; standards; and information products that form the system that distributes, manages, and supports the delivery of cryptographic products and services to end users.

Note 2 to entry: Key management services include key ordering, distribution, re-key, update of keying material attributes, certificate revocation, key recovery and the distribution, accounting, tracking, and control of software that performs either keying material security or cryptographic functions.

3.1.2.79

key manager

<information security> key management infrastructure device that provides key management services

3.1.2.80

key pair

asymmetric key pair

<information security> pair of related keys where the private key defines the private transformation and the public key defines the public transformation

Note 1 to entry: A key pair is used with asymmetric-key cryptographic algorithms.

[SOURCE: ISO/IEC 11770-1:2010, 2.2]

3.1.2.81

key recovery

<information security> mechanisms and processes that allow authorized entities to retrieve keying material from secure key backup or archive storage

3.1.2.82

key registration

<information security> process of officially recording the keying material by a registration authority

3.1.2.83

key revocation

<information security> process whereby a notice is made available to affected entities that keying material should be removed from operational use prior to the end of the established cryptoperiod of that keying material

3.1.2.84

key transport

<information security> process of transferring a key from one entity to another entity, suitably protected

Note 1 to entry: When used in conjunction with a public key (asymmetric) algorithm, the keying material is encrypted using the public key of the receiver and subsequently decrypted using the private key of the receiver. When used in conjunction with a symmetric algorithm, the keying material is wrapped with a key encrypting key shared by the two parties.

[SOURCE: ISO/IEC 11770-1:2010, 2.33]

3.1.2.85

key update

<information security> function performed on a cryptographic key in order to compute a new but related key

3.1.2.86

key usage period

<information security> either the originator usage period or the recipient usage period of a symmetric key

3.1.2.87

key wrapping

<information security> method of encrypting keys (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric key

3.1.2.88

key wrapping key

<information security> (symmetric-key) key encryption key

3.1.2.89

keying material

<information security> data necessary to establish and maintain cryptographic keying relationships

EXAMPLE Keys, initialization values, periods of validity.

[SOURCE: ISO/IEC 11770-1:2010, 2.27]

3.1.2.90

latency

delay from when data is created at a data source device to when it is available to be consumed at the destination device

Note 1 to entry: The designated points of measurement are a) physical devices, or b) layer boundaries within multi-layer software (e.g., from sending transport to receiving transport functionality, or from sending application to sending modem).

3.1.2.91

lease

per-session fine-grained communication resource allocation occurring at a GIAP

3.1.2.92

least privilege

<information security> security principle that restricts the access privileges (e.g., program execution privileges, file modification privileges) of authorized personnel and their cyber agents to the minimum necessary to perform their jobs

3.1.2.93

link

momentary or persistent interconnecting path between two or more devices for the purpose of transmitting and receiving messaging

3.1.2.94

master key

<information security> cryptographic key that is used for deriving other keys

Note 1 to entry: Best practice prohibits using master keys as session (i.e., data) keys, which would ease their cryptanalysis. They may be used as KEKs, often at the top of a KEK hierarchy.

3.1.2.95

mesh topology

network topology in which redundant physically-diverse routing paths are available between each pair of network nodes