

STANDARD

ISA-100.11a-2011

**Wireless systems for industrial automation:
Process control and related applications**

Approved 4 May 2011

ISA-100.11a-2011

Wireless systems for industrial automation: Process control and related applications

ISBN: 978-1-936007-96-7

Copyright © 2011 by the International Society of Automation (ISA). All rights reserved. Not for resale. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic mechanical, photocopying, recording, or otherwise), without the prior written permission of the Publisher.

ISA
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, North Carolina 27709

Preface

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-100.11a-2011.

This document has been prepared as part of the service of ISA toward a goal of uniformity in the field of instrumentation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA; 67 Alexander Drive; P. O. Box 12277; Research Triangle Park, NC 27709; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

The ISA Standards and Practices Department is aware of the growing need for attention to the metric system of units in general, and the International System of Units (SI) in particular, in the preparation of instrumentation standards. The Department is further aware of the benefits to USA users of ISA standards of incorporating suitable references to the SI (and the metric system) in their business and professional dealings with other countries. Toward this end, this Department will endeavor to introduce SI-acceptable metric units in all new and revised standards, recommended practices, and technical reports to the greatest extent possible. *Standard for Use of the International System of Units (SI): The Modern Metric System*, published by the American Society for Testing & Materials as IEEE/ASTM SI 10-97, and future revisions, will be the reference guide for definitions, symbols, abbreviations, and conversion factors.

It is the policy of ISA to encourage and welcome the participation of all concerned individuals and interests in the development of ISA standards, recommended practices, and technical reports. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA, or of any of the standards, recommended practices, and technical reports that ISA develops.

CAUTION — ISA DOES NOT TAKE ANY POSITION WITH RESPECT TO THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS ASSERTED IN CONNECTION WITH THIS DOCUMENT, AND ISA DISCLAIMS LIABILITY FOR THE INFRINGEMENT OF ANY PATENT RESULTING FROM THE USE OF THIS DOCUMENT. USERS ARE ADVISED THAT DETERMINATION OF THE VALIDITY OF ANY PATENT RIGHTS, AND THE RISK OF INFRINGEMENT OF SUCH RIGHTS, IS ENTIRELY THEIR OWN RESPONSIBILITY.

PURSUANT TO ISA'S PATENT POLICY, ONE OR MORE PATENT HOLDERS OR PATENT APPLICANTS MAY HAVE DISCLOSED PATENTS THAT COULD BE INFRINGED BY USE OF THIS DOCUMENT AND EXECUTED A LETTER OF ASSURANCE COMMITTING TO THE GRANTING OF A LICENSE ON A WORLDWIDE, NON-DISCRIMINATORY BASIS, WITH A FAIR AND REASONABLE ROYALTY RATE AND FAIR AND REASONABLE TERMS AND CONDITIONS. FOR MORE INFORMATION ON SUCH DISCLOSURES AND LETTERS OF ASSURANCE, CONTACT ISA OR VISIT WWW.ISA.ORG/STANDARDSPATENTS.

OTHER PATENTS OR PATENT CLAIMS MAY EXIST FOR WHICH A DISCLOSURE OR LETTER OF ASSURANCE HAS NOT BEEN RECEIVED. ISA IS NOT RESPONSIBLE FOR IDENTIFYING PATENTS OR PATENT APPLICATIONS FOR WHICH A LICENSE MAY BE REQUIRED, FOR CONDUCTING INQUIRIES INTO THE LEGAL VALIDITY OR SCOPE OF PATENTS, OR DETERMINING WHETHER ANY LICENSING TERMS OR CONDITIONS PROVIDED IN CONNECTION WITH SUBMISSION OF A LETTER OF ASSURANCE, IF ANY, OR IN ANY LICENSING AGREEMENTS ARE REASONABLE OR NON-DISCRIMINATORY.

ISA REQUESTS THAT ANYONE REVIEWING THIS DOCUMENT WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE DOCUMENT NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER.

ADDITIONALLY, THE USE OF THIS DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES

ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS DOCUMENT MUST EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER MUST ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS DOCUMENT.

THE USER OF THIS DOCUMENT SHOULD BE AWARE THAT THIS DOCUMENT MAY BE IMPACTED BY ELECTRONIC SECURITY ISSUES. THE COMMITTEE HAS NOT YET ADDRESSED THE POTENTIAL ISSUES IN THIS VERSION.

INTRODUCTION.....	28
REVISION HISTORY	30
1 Scope.....	31
2 Normative references	31
3 Terms, definitions, abbreviated terms, acronyms, and conventions	32
3.1 (N)-layer and other terms and definitions from the open systems interconnection basic reference model	32
3.2 Other terms and definitions.....	37
3.3 Symbols	52
3.4 Abbreviated terms and acronyms	53
3.5 IEC service table conventions.....	59
4 Overview	61
4.1 General	61
4.2 Interoperability	61
4.3 Quality of service	61
4.4 Worldwide applicability	61
4.5 Network architecture	61
4.6 Network characteristics	63
5 Systems	68
5.1 General	68
5.2 Devices	68
5.3 Networks	74
5.4 Protocol suite structure.....	83
5.5 Data flow	84
5.6 Time reference.....	89
5.7 Firmware upgrades	90
5.8 Wireless backbones and other infrastructures.....	90
6 System management.....	91
6.1 General	91
6.2 Device management application process.....	93
6.3 System manager	114
7 Security	161
7.1 General	161
7.2 Security services.....	161
7.3 Frame security	165
7.4 The join process	194
7.5 Session establishment.....	222
7.6 Key update	229
7.7 Security manager functionality	236
7.8 Security policies.....	238
7.9 Security functions available to the application layer	240
7.10 Security statistics collection, threat detection, and reporting.....	243
7.11 Device security management object functionality	243
8 Physical layer	251
8.1 General	251
8.2 Default physical layer	251

9	Data link layer	253
9.1	General	253
9.2	Data link layer data service access point	315
9.3	Data frames and acknowledgements	317
9.4	Data link layer management information base	339
9.5	Data link layer methods	381
9.6	Data link layer alerts	383
10	Network layer	386
10.1	General	386
10.2	Network layer functionality overview	386
10.3	Network layer data services	404
10.4	Network layer management object	406
10.5	Network layer protocol data unit formats	413
11	Transport layer	421
11.1	General	421
11.2	Transport layer reference model	421
11.3	Transport security sub-layer	422
11.4	Transport data entity	422
11.5	Transport layer protocol data unit encoding	426
11.6	Transport layer model	428
12	Application layer	438
12.1	General	438
12.2	Energy considerations	438
12.3	Legacy control system considerations	438
12.4	Introduction to object-oriented modeling	439
12.5	Object model	441
12.6	Object attribute model	442
12.7	Method model	444
12.8	Alert model	444
12.9	Alarm state model	445
12.10	Event state model	446
12.11	Alert reporting	446
12.12	Communication interaction model	448
12.13	Application layer addressing	457
12.14	Management objects	461
12.15	User objects	461
12.16	Data types	491
12.17	Application services provided by application sub-layer	497
12.18	Application layer flow use to lower layer services	530
12.19	Application layer management	531
12.20	Process control industry standard data structures	551
12.21	Additional tables	554
12.22	Coding	555
12.23	Syntax	574
12.24	Detailed coding examples (INFORMATIVE)	587
13	Gateway	589
13.1	General	589
13.2	Service access point	593

13.3	Protocol.....	632
14	Provisioning.....	651
14.1	General	651
14.2	Terms and definitions	651
14.3	Provisioning procedures	653
14.4	Pre-installed symmetric keys	653
14.5	Provisioning using out-of-band mechanisms	654
14.6	Provisioning networks	654
14.7	State transition diagrams	656
14.8	Device management application protocol objects for provisioning	661
14.9	Management objects	663
14.10	Device provisioning service object	668
14.11	Provisioning functions (INFORMATIVE).....	677
Annex A	(INFORMATIVE) Protocol implementation conformance statement proforma	680
A.1	Introduction	680
A.2	System	682
A.3	System management.....	685
A.4	Security manager	688
A.5	Physical layer	689
A.6	Data link layer.....	691
A.7	Network layer.....	692
A.8	Transport layer	694
A.9	Application layer	695
A.10	Gateway	703
A.11	Provisioning.....	705
Annex B	(NORMATIVE) Role profiles.....	707
B.1	Introduction	707
B.2	System	708
B.3	System manager	708
B.4	Security manager	708
B.5	Physical layer	709
B.6	Data link layer.....	710
B.7	Network layer.....	715
B.8	Transport layer	716
B.9	Application layer	716
B.10	Gateway	716
B.11	Provisioning.....	717
Annex C	(INFORMATIVE) Background information	718
C.1	Industrial needs	718
C.2	Usage classes	718
C.3	Other uploading and downloading- alarms (human or automated action)	719
C.4	The open systems interconnection basic reference model	720
Annex D	(NORMATIVE) Configuration defaults.....	723
D.1	General	723
D.2	System management.....	723
D.3	Security	724
D.4	Data link layer.....	724
D.5	Network layer.....	725

D.6	Transport layer	726
D.7	Application layer	726
D.8	Gateway	728
D.9	Provisioning	728
Annex E (INFORMATIVE)	Use of backbone networks	730
E.1	General	730
E.2	Recommended characteristics	730
E.3	Internet protocol backbones	730
Annex F (NORMATIVE)	Basic security concepts – Notation and representation	732
F.1	Strings and string operations	732
F.2	Integers, octets, and their representation	732
F.3	Entities	732
Annex G (INFORMATIVE)	Using certificate chains for over-the-air provisioning	733
Annex H (NORMATIVE)	Security building blocks	734
H.1	Symmetric key cryptographic building blocks	734
H.2	Asymmetric key cryptographic building blocks	735
H.3	Keying information	735
H.4	Key agreement schemes	736
H.5	Keying information schemes	737
H.6	Challenge domain parameter generation and validation	738
H.7	Challenge validation primitive	738
H.8	Secret key generation (SKG) primitive	739
H.9	Block-cipher-based cryptographic hash function	739
H.10	Elliptic curve cryptography manual certificate scheme	740
Annex I (INFORMATIVE)	Definition templates	743
I.1	Object type template	743
I.2	Standard object attributes template	743
I.3	Standard object methods	744
I.4	Standard object alert reporting template	745
I.5	Data structure definition	746
Annex J (INFORMATIVE)	Operations on attributes	747
J.1	Operations on attributes	747
J.2	Synchronized cutover	750
Annex K (NORMATIVE)	Standard object types	751
Annex L (INFORMATIVE)	Standard data types	757
Annex M (NORMATIVE)	Protocol identification values	759
Annex N (INFORMATIVE)	Tunneling and native object mapping	760
N.1	Overview	760
N.2	Tunneling	760
N.3	Foreign protocol application communication	760
N.4	Native object mapping	761
N.5	Tunneling and native object mapping tradeoffs	761
Annex O (INFORMATIVE)	Generic protocol translation	762
O.1	Overview	762
O.2	Publish	762
O.3	Subscribe	763
O.4	Client	763

O.5	Server	764
Annex P (INFORMATIVE) Gateway service access point adaptations for this standard.....		766
P.1	General	766
P.2	Parameters.....	766
P.3	Session	766
P.4	Lease	766
P.5	Device list report.....	767
P.6	Topology report.....	767
P.7	Schedule report	767
P.8	Device health report.....	767
P.9	Neighbor health report.....	767
P.10	Network health report.....	767
P.11	Time.....	767
P.12	Client/server	767
P.13	Publish/subscribe.....	768
P.14	Bulk transfer	769
P.15	Alert	769
P.16	Gateway configuration.....	769
P.17	Device configuration.....	769
Annex Q (INFORMATIVE) Gateway service access point adaptations for WirelessHART®		770
Q.1	General	770
Q.2	Parameters.....	771
Q.3	Session	771
Q.4	Lease	771
Q.5	Device list report.....	772
Q.6	Topology report.....	772
Q.7	Schedule report	772
Q.8	Device health report.....	773
Q.9	Neighbor health report.....	773
Q.10	Network health report.....	774
Q.11	Time.....	774
Q.12	Client/server	774
Q.13	Publish/subscribe.....	775
Q.14	Bulk transfer	776
Q.15	Alert	776
Q.16	Gateway configuration.....	777
Q.17	Device configuration.....	777
Annex R (INFORMATIVE) Host system interface to standard-compliant devices via a gateway.....		778
R.1	Background	778
R.2	Device application data integration with host systems	779
R.3	Host system configuration tool	779
R.4	Field device / distributed control systems integration.....	781
R.5	Gateway	781
R.6	Asset management application support	782
Annex S (INFORMATIVE) Symmetric Key Operation Test Vectors		783
S.1	DPDU samples	783
S.2	TPDU samples.....	784

Annex T (INFORMATIVE) Data link header and network header for join requests	786
T.1 Overview	786
T.2 MAC header (MHR)	786
T.3 DL header (DHR)	786
T.4 NL header.....	786
Bibliography	788
Table 1 – Standard management object types in DMAP	95
Table 2 – Meta_Data_Attribute data structure.....	97
Table 3 – Alert types for communication diagnostic category.....	98
Table 4 – Alert types for security alert category	98
Table 5 – Alert types for device diagnostic alert category.....	98
Table 6 – Alert types for process alert category	99
Table 7 – ARMO attributes	100
Table 8 – ARMO alerts.....	103
Table 9 – Alarm_Recovery method	104
Table 10 – DMO attributes	107
Table 11 – DMO alerts	113
Table 12 – System management object types.....	116
Table 13 – DSO attributes	118
Table 14 – Address_Translation_Row data structure	118
Table 15 – Read_Address_Row method.....	120
Table 16 – Input argument usage	121
Table 17 – Output argument usage	121
Table 18 – Attributes of SMO in system manager	123
Table 19 – Proxy_System_Manager_Join method.....	124
Table 20 – Proxy_System_Manager_Contract method	125
Table 21 – Effect of Different Join Commands on Attribute Sets	127
Table 22 – Attributes of DMSO in system manager	127
Table 23 – System_Manager_Join method	128
Table 24 – System_Manager_Contract method.....	129
Table 25 – Attributes of STSO in system manager.....	133
Table 26 – Attributes of SCO in system manager.....	136
Table 27 – SCO method for contract establishment, modification, or renewal.....	138
Table 28 – Input argument usage	143
Table 29 – Output argument usage	144
Table 30 – Contract_Data data structure	147
Table 31 – New_Device_Contract_Response data structure.....	150
Table 32 – SCO method for contract termination, deactivation and reactivation.....	156
Table 33 – DMO method to terminate contract.....	156
Table 34 – DMO method to modify contract.....	158
Table 35 – Security levels	165

Table 36 – Structure of the security control field	166
Table 37 – Sec.DpduPrep.Request elements	170
Table 38 – Sec.DpduPrep.Response elements	171
Table 39 – Sec.DLAckCheck.Request elements	172
Table 40 – Sec. DLAckCheck.Response elements	172
Table 41 – Sec.DpduCheck.Request elements	173
Table 42 – Sec.DpduCheck.Response elements	174
Table 43 – Sec.DLAckPrep.Request elements	174
Table 44 – Sec.DLAckPrep.Response elements	175
Table 45 – Structure of the WISN DPDU nonce	176
Table 46 – Structure of the 32-bit truncated TAI time	176
Table 47 – TSS “pseudo-header” structure	181
Table 48 – Sec.TpduOutCheck.Request elements	184
Table 49 – Sec.TpduOutCheck.Response elements	184
Table 50 – Sec.TpduSecure.Request elements	185
Table 51 – Sec. TpduSecure.Response elements	186
Table 52 – Sec.TpduInCheck.Request elements	187
Table 53 – Sec.TpduInCheck.Response elements	187
Table 54 – Sec.TpduVerify.Request elements	188
Table 55 – Sec.TpduVerify.Response elements	189
Table 56 – Structure of TL security header	189
Table 57 – Structure of the TPDU nonce	190
Table 58 – Structure of 32-bit nominal TAI time	190
Table 59 – Proxy_Security_Sym_Join method	201
Table 60 – Security_Sym_Join method	201
Table 61 – Security_Confirm method	202
Table 62 – Security_Sym_Join_Request data structure	202
Table 63 – Security_Sym_Join_Response data structure	203
Table 64 – Structure of compressed Security level field	204
Table 65 – Master key security level	205
Table 66 – Structure of KeyHardLifeSpan field	205
Table 67 – Security_Sym_Confirm data structure	206
Table 68 – Implicit certificate format	207
Table 69 – Usage_Serial structure	208
Table 70 – Proxy_Security_Pub_Join method	213
Table 71 – Security_Pub_Join method	213
Table 72 – Proxy_Security_Pub_Confirm method	214
Table 73 – Security_Pub_Confirm method	214
Table 74 – Network_Information_Confirmation method	215
Table 75 – Format of asymmetric join request internal structure	216
Table 76 – Format of the protocol control field	216
Table 77 – Format of asymmetric join response internal structure	217
Table 78 – Format of first join confirmation internal structure	218

Table 79 – Format of join confirmation response internal structure	219
Table 80 – Join process and device lifetime state machine	221
Table 81 – Security_New_Session method.....	226
Table 82 – Security_New_Session_Request data structure	227
Table 83 – Security_New_Session_Response data structure	228
Table 84 – New_Key method	230
Table 85 – Security_Key_and_Policies data structure.....	232
Table 86 – Security_Key_Update_Status data structure	234
Table 87 – Session and DL key state transition	235
Table 88 – Attributes of PSMO in the system manager	236
Table 89 – Structure of Policy field	238
Table 90 – Key types	239
Table 91 – Key usage	239
Table 92 – Granularity	239
Table 93 – Device security management object attributes	244
Table 94 – KeyDescriptor (INFORMATIVE)	246
Table 95 – TL KeyLookupData OctetString fields	247
Table 96 – Delete key method	248
Table 97 – Key_Policy_Update method	249
Table 98 – DSMO Alerts.....	250
Table 99 – Timing requirements	251
Table 100 – Graph table on ND20.....	257
Table 101 – Graph table on ND21.....	257
Table 102 – Approximating nominal timing with 32 kHz clock (INFORMATIVE)	284
Table 103 – DL_Config_Info structure	308
Table 104 – DD-DATA.request parameters.....	315
Table 105 – DD-DATA.confirm parameters	316
Table 106 – Value set for status parameter	316
Table 107 – DD-DATA.indication parameters.....	317
Table 108 – ExtDLUInt, one-octet variant	319
Table 109 – ExtDLUInt, two-octet variant	319
Table 110 – Data frame MHR	320
Table 111 – DHDR frame control octet.....	321
Table 112 – Data frame DMXHR.....	321
Table 113 – DROUT structure, compressed variant	322
Table 114 – DROUT structure, uncompressed variant.....	323
Table 115 – DADDR structure	324
Table 116 – Acknowledgement frame MHR	325
Table 117 – Acknowledgement frame DHR	326
Table 118 – DHR ACK/NACK frame control.....	326
Table 119 – Advertisement DAUX structure.....	328
Table 120 – Advertisement selections elements	328
Table 121 – Advertisement selections.....	329

Table 122 – Advertisement time synchronization elements.....	329
Table 123 – Advertisement time synchronization structure	329
Table 124 – Join superframe information subfields	330
Table 125 – Join superframe information structure	330
Table 126 – Superframe derived from advertisement	331
Table 127 – Join information elements.....	331
Table 128 – Join information structure	332
Table 129 – Defaults for links created from advertisements.....	333
Table 130 – dlmo.Neighbor entry created from advertisements.....	334
Table 131 – dlmo.Graph entry created from advertisements.....	334
Table 132 – dlmo.Route entry created from advertisements	334
Table 133 – Solicitation header subfields	336
Table 134 – Solicitation header structure	336
Table 135 – Solicitation DAUX fields.....	336
Table 136 – Solicitation DAUX structure.....	336
Table 137 – Activate link DAUX fields	338
Table 138 – Activate link DAUX structure.....	338
Table 139 – Reporting received signal quality DAUX fields	338
Table 140 – Report received signal quality DAUX structure.....	338
Table 141 – DLMO attributes.....	340
Table 142 – Subnet filter octets	347
Table 143 – dlmo.TaiAdjust OctetString fields	348
Table 144 – dlmo.TaiAdjust OctetString structure	348
Table 145 – dlmo.EnergyDesign OctetString fields	348
Table 146 – dlmo.EnergyDesign OctetString structure	348
Table 147 – dlmo.DeviceCapability OctetString fields	349
Table 148 – dlmo.DeviceCapability OctetString structure	349
Table 149 – dlmo.DiscoveryAlert fields	351
Table 150 – dlmo.DiscoveryAlert structure	351
Table 151 – dlmo.Candidates OctetString fields	352
Table 152 – dlmo.Candidates structure	352
Table 153 – dlmo.SmoothFactors OctetString fields.....	353
Table 154 – dlmo.SmoothFactors structure	353
Table 155 – dlmo.QueuePriority fields.....	354
Table 156 – dlmo.QueuePriority structure	354
Table 157 – dlmo.ChannelDiag fields.....	355
Table 158 – dlmo.ChannelDiag structure.....	355
Table 159 – dlmo.Ch fields.....	357
Table 160 – dlmo.Ch structure.....	357
Table 161 – Receive template fields	360
Table 162 – Receive template structure	360
Table 163 – Transmit template fields	361
Table 164 – Transmit template structure	361

Table 165 – Default receive template	362
Table 166 – Default transmit template	362
Table 167 – Default receive template for scanning	362
Table 168 – dlmo.Neighbor fields	364
Table 169 – dlmo.Neighbor structure	364
Table 170 – ExtendGraph fields	366
Table 171 – ExtGraph structure	366
Table 172 – dlmo.NeighborDiagReset fields	366
Table 173 – dlmo.NeighborDiagReset structure	366
Table 174 – dlmo.Superframe fields	367
Table 175 – dlmo.Superframe structure	368
Table 176 – dlmo.SuperframeIdle fields	371
Table 177 – dlmo.SuperframeIdle structure	371
Table 178 – dlmo.Graph	372
Table 179 – dlmo.Graph structure	372
Table 180 – dlmo.Link fields	373
Table 181 – dlmo.Link structure	374
Table 182 – dlmo.Link[].Type structure	375
Table 183 – Allowed dlmo.Link[].Type combinations	376
Table 184 – Values for dlmo.Link[].Schedule	377
Table 185 – dlmo.Route fields	377
Table 186 – dlmo.Route structure	378
Table 187 – dlmo.NeighborDiag fields	379
Table 188 – Diagnostic Summary OctetString fields	379
Table 189 – Diagnostic Summary OctetString structure	380
Table 190 – Diagnostic ClockDetail OctetString fields	380
Table 191 – Diagnostic ClockDetail OctetString structure	381
Table 192 – Read_Row method	381
Table 193 – Write_Row method	382
Table 194 – Write_Row_Now method	382
Table 195 – dlmo.AlertPolicy fields	383
Table 196 – dlmo.AlertPolicy OctetString structure	383
Table 197 – DL_Connectivity alert	384
Table 198 – DL_Connectivity alert OctetString	384
Table 199 – NeighborDiscovery alert	385
Table 200 – Link local address structure	387
Table 201 – Address translation table (ATT)	387
Table 202 – Example of a routing table	393
Table 203 – N-DATA.request elements	404
Table 204 – N-DATA.confirm elements	405
Table 205 – N-DATA.indication elements	406
Table 206 – NLMO attributes	407
Table 207 – Contract table structure	410

Table 208 – Route table elements	411
Table 209 – Address translation table structure	411
Table 210 – NLMO structured MIB manipulation methods	412
Table 211 – Alert to indicate dropped PDU/PDU error.....	413
Table 212 – Common header patterns	414
Table 213 – Basic network layer header format	415
Table 214 – Contract-enabled network layer header format.....	416
Table 215 – 6LoWPAN_IPHC encoding format	417
Table 216 – IPv6 network layer header format.....	418
Table 217 – Full network layer header in the DL	419
Table 218 – Network layer header format for fragmented NPDUs	419
Table 219 – First fragment header format.....	419
Table 220 – Second and subsequent fragment header format	420
Table 221 – UDP header encoding	423
Table 222 – UDP LowPAN_NHC encoding	427
Table 223 – Optimal UDP header encoding	427
Table 224 – UDP header encoding with checksum.....	428
Table 225 – T-DATA.request elements.....	429
Table 226 – T-DATA.confirm elements	430
Table 227 – T-DATA.confirm status codes.....	430
Table 228 – T-DATA.indication elements.....	431
Table 229 – TLMO attributes	432
Table 230 – Transport layer management object methods – Reset	434
Table 231 – Transport layer management object methods – Halt.....	434
Table 232 – Transport layer management object methods – PortRangeInfo	435
Table 233 – Transport layer management object methods – GetPortInfo.....	435
Table 234 – Transport layer management object methods – GetNextPortInfo	436
Table 235 – Transport layer management object alert types – Illegal use of port	436
Table 236 – Transport layer management object alert types – TPDU received on unregistered port	437
Table 237 – Transport layer management object alert types – TPDU does not match security policies.....	437
Table 238 – State table for alarm transitions	445
Table 239 – State table for event transitions	446
Table 240 – UAP management object attributes	462
Table 241 – State table for UAP management object	463
Table 242 – UAP management object methods	464
Table 243 – Alert receiving object attributes.....	465
Table 244 – State table for handling an AlertReport reception.....	465
Table 245 – AlertReceiving object methods.....	466
Table 246 – UploadDownload object attributes	468
Table 247 – UploadDownload object methods	471
Table 248 – UploadDownload object StartDownload method.....	472
Table 249 – UploadDownload object DownloadData method	473

Table 250 – UploadDownload object EndDownload method	475
Table 251 – UploadDownload object StartUpload method	476
Table 252 – UploadDownload object UploadData method	477
Table 253 – UploadDownload object EndUpload method.....	478
Table 254 – Download state table for unicast operation mode	479
Table 255 – Upload state table for unicast operation mode	481
Table 256 – Concentrator object attributes	484
Table 257 – Concentrator object methods	485
Table 258 – Dispersion object attributes	486
Table 259 – Dispersion object methods.....	487
Table 260 – Tunnel object attributes	488
Table 261 – Tunnel object methods	490
Table 262 – Interface object attributes	491
Table 263 – Interface object methods	491
Table 264 – Data type: ObjectAttributeIndexAndSize	492
Table 265 – Data type: Communication association endpoint	493
Table 266 – Data type: Communication contract data	494
Table 267 – Data type: Alert communication endpoint.....	495
Table 268 – Data type: Tunnel endpoint.....	495
Table 269 – Data type: Alert report descriptor	496
Table 270 – Data type: Process control alarm report descriptor for analog with single reference condition	496
Table 271 – Data type: ObjectIDandType	497
Table 272 – Data type: Unscheduled correspondent	497
Table 273 – AL services.....	498
Table 274 – Publish service	501
Table 275 – Read service.....	508
Table 276 – Write service.....	512
Table 277 – Execute service	515
Table 278 – AlertReport service	521
Table 279 – AlertAcknowledge service.....	524
Table 280 – Tunnel service	527
Table 281 – Application flow characteristics	530
Table 282 – Application service primitive to transport service primitive mapping	531
Table 283 – ASLMO attributes.....	533
Table 284 – Application sub-layer management object methods	534
Table 285 –Reset method	535
Table 286 – ASLMO alerts	536
Table 287 – Analog input object attributes.....	539
Table 288 – Analog input object methods.....	540
Table 289 – Analog input alerts	541
Table 290 – Analog output attributes.....	543
Table 291 – Analog output object methods.....	544

Table 292 – Analog output alerts	545
Table 293 – Binary input object attributes	547
Table 294 – Binary input object methods.....	548
Table 295 – Binary input alerts	548
Table 296 – Binary output attributes	549
Table 297 – Binary output object methods.....	550
Table 298 – Binary output alerts	550
Table 299 – Status octet	551
Table 300 – Data type: Process value and status for analog value	552
Table 301 – Data type: Process value and status for binary value	552
Table 302 – Data type: Process control mode	553
Table 303 – Data type: Process control mode bitstring.....	553
Table 304 – Data type: Process control scaling	554
Table 305 – Process control standard objects	554
Table 306 – Services	554
Table 307 – Application messaging format	555
Table 308 – Concatenated APDUs in a single TSDU.....	555
Table 309 – Object addressing	556
Table 310 – Four-bit addressing mode APDU header construction	556
Table 311 – Eight-bit addressing mode APDU header construction.....	556
Table 312 – Sixteen-bit addressing mode APDU header construction	557
Table 313 – Inferred addressing use case example	557
Table 314 – Inferred addressing mode APDU header construction	557
Table 315 – Six-bit attribute identifier, not indexed	558
Table 316 – Six-bit attribute identifier, singly indexed, with seven-bit index.....	558
Table 317 – Six-bit attribute identifier, singly indexed, with fifteen-bit index	558
Table 318 – Six-bit attribute identifier, doubly indexed, with two seven-bit indices.....	559
Table 319 – Six-bit attribute identifier, doubly indexed, with two fifteen-bit indices.....	559
Table 320 – Six-bit attribute identifier, doubly indexed, with first index seven-bits long and second index fifteen bits long	559
Table 321 – Six-bit attribute bit attribute identifier, doubly indexed, with first index fifteen bits long and second index seven bits long	559
Table 322 – Twelve-bit attribute identifier, not indexed	559
Table 323 – Twelve-bit attribute identifier, singly indexed with seven-bit index.....	560
Table 324 – Twelve-bit attribute identifier, singly indexed with fifteen bit identifier.....	560
Table 325 – Twelve-bit attribute identifier, doubly indexed with two seven bit indices	560
Table 326 – Twelve-bit attribute identifier, doubly indexed with two fifteen bit indices.....	560
Table 327 – Twelve-bit attribute identifier, doubly indexed with first index seven-bits long and second index fifteen-bits long	560
Table 328 – Twelve-bit attribute identifier, doubly indexed with the first index fifteen bits long and the second index seven bits long	561
Table 329 – Twelve-bit attribute identifier, reserved form	561
Table 330 – Coding rules for read service request.....	561
Table 331 – Coding rules for read service response with seven bit length field.....	561

Table 332 – Coding rules for read service response with fifteen-bit length field	562
Table 333 – Coding rules for write service request with seven bit length field	562
Table 334 – Coding rules for write service request with fifteen-bit length field	562
Table 335 – Coding rules for write service response	562
Table 336 – Coding rules for execute service request with seven-bit length field	563
Table 337 – Coding rules for execute service request with fifteen-bit length field	563
Table 338 – Coding rules for execute service response with 7-bit length field	563
Table 339 – Coding rules for execute service response with 15-bit length field	563
Table 340 – Coding rules for tunnel service request with seven-bit length field	564
Table 341 – Coding rules for tunnel service request with fifteen-bit length field	564
Table 342 – Coding rules for tunnel service response with seven-bit length field	564
Table 343 – Coding rules for tunnel service response with fifteen-bit length field	564
Table 344 – Coding rules for AlertReport service with seven bit length field	565
Table 345 – Coding rules for AlertReport service with fifteen-bit length field	565
Table 346 – Coding rules for AlertAcknowledge service	565
Table 347 – Coding rules for publish service for a native sequence of values	565
Table 348 – Coding rules for publish service – non-native (for tunnel support)	566
Table 349 – Coding rules for concatenate service	566
Table 350 – General coding rule for size-invariant application data	566
Table 351 – Coding rules for application data of varying size	566
Table 352 – Coding rules for Boolean data – true	567
Table 353 – Coding rules for Boolean data – false	567
Table 354 – Coding rules for Unsigned8	568
Table 355 – Coding rules for Unsigned16	568
Table 356 – Coding rules for Unsigned32	568
Table 357 – Coding rules for Unsigned64	569
Table 358 – Coding rules for Unsigned128	569
Table 359 – Coding rules for Float	570
Table 360 – Coding rules for double-precision float	570
Table 361 – Coding rules for VisibleString	571
Table 362 – Coding rules for OctetString	571
Table 363 – Coding rules for Bitstring	571
Table 364 – Example of coding for Bitstring of size 8	571
Table 365 – Coding rules for TAIDifference	572
Table 366 – Coding rules for TAINetworkTimeValue	572
Table 367 – Coding rules for TAIRounded	573
Table 368 – Coding example: Read request for a non-indexed attribute	587
Table 369 – Coding example: Read response (corresponding to request contained in the preceding table)	588
Table 370 – Coding example: Tunnel service request	588
Table 371 – Summary of gateway high side interface services	594
Table 372 – Primitive G_Session parameter usage	603
Table 373 – GS_Status for G_Session confirm	604

Table 374 – Primitive G_Lease parameter usage.....	604
Table 375 – GS_Lease_Type for G_Lease request.....	605
Table 376 – GS_Status for G_Lease confirm.....	606
Table 377 – Primitive G_Device_List_Report parameter usage	607
Table 378 – GS_Status for G_Device_List_Report confirm.....	608
Table 379 – Primitive G_Topology_Report parameter usage	608
Table 380 – GS_Status for G_Topology_Report confirm	609
Table 381 – Primitive G_Schedule_Report parameter usage	609
Table 382 – GS_Status for G_Schedule_Report confirm	611
Table 383 – Primitive G_Device_Health_Report parameter usage	611
Table 384 – GS_Status for G_Device_Health_Report confirm	612
Table 385 – Primitive G_Neighbor_Health_Report parameter usage.....	612
Table 386 – GS_Status for G_Device_Health_Report confirm	613
Table 387 – Primitive G_Network_Health_Report parameter usage	614
Table 388 – GS_Status for G_Network_Health_Report confirm	615
Table 389 – Primitive G_Time parameter usage	616
Table 390 – GS_Status for G_Time confirm	616
Table 391 – Primitive G_Client_Server parameter usage	617
Table 392 – GS_Status for G_Client_Server confirm	618
Table 393 – Primitive G_Publish parameter usage.....	619
Table 394 – GS_Status for G_Publish confirm.....	620
Table 395 – Primitive G_Subscribe parameter usage.....	620
Table 396 – GS_Status for G_Subscribe confirm.....	621
Table 397 – Primitive G_Publish_Timer parameter usage	621
Table 398 – Primitive G_Subscribe_Timer parameter usage	621
Table 399 – Primitive G_Publish_Watchdog parameter usage.....	622
Table 400 – Primitive G_Bulk_Open parameter usage	623
Table 401 – GS_Status for G_Bulk_Open confirm	623
Table 402 – Primitive G_Bulk_Transfer parameter usage.....	624
Table 403 – GS_Status for G_Bulk_Transfer confirm	624
Table 404 – Primitive G_Bulk_Close parameter usage.....	624
Table 405 – GS_Status for G_Bulk_Close confirm.....	625
Table 406 – Primitive G_Alert_Subscription parameter usage	625
Table 407 – GS_Status for G_Alert_Subscription confirm.....	626
Table 408 – Primitive G_Alert_Notification parameter usage	627
Table 409 – Primitive G_Read_Gateway_Configuration parameter usage	628
Table 410 – GS_Attribute_Identifier values	628
Table 411 – GS_Status for G_Read_Gateway_Configuration confirm	629
Table 412 – Primitive G_Write_Gateway_Configuration parameter usage	629
Table 413 – GS_Attribute_Identifier values	629
Table 414 – GS_Status for G_Write_Gateway_Configuration confirm	630
Table 415 – Primitive G_Write_Device_Configuration parameter usage	630
Table 416 – GS_Status for G_Write_Device_Configuration confirm	631

Table 417 – Primitive G_Read_Device_Configuration parameter usage	631
Table 418 – GS_Status for G_Read_Device_Configuration confirm	632
Table 419 – UAP management object extended attributes.....	650
Table 420 – Factory default settings	658
Table 421 – Device provisioning object	664
Table 422 – Reset_To_Default method	668
Table 423 – Write symmetric join key method.....	668
Table 424 – Device provisioning service object	670
Table 425 – DPSOWhiteListTbl data structure	674
Table 426 – Array manipulation table.....	675
Table 427 – DPSO alert to indicate join by a device not on the WhiteList.....	676
Table 428 – DPSO alert to indicate inadequate device join capability	676
Table 429 – Field media type	682
Table 430 – Protocol layer support	683
Table 431 – Device PICS	683
Table 432 – PICS for device implementing I/O role.....	683
Table 433 – PICS for device implementing router role.....	684
Table 434 – PICS for backbone router	684
Table 435 – PICS for gateway	684
Table 436 – PICS for system manager	684
Table 437 – PICS for provisioning device.....	684
Table 438 – PICS for security manager	685
Table 439 – PICS for device implementing system time source role.....	685
Table 440 – System PICS	685
Table 441 – Device PICS	686
Table 442 – Router and backbone router PICS.....	686
Table 443 – PICS for system time source.....	687
Table 444 – PICS for system manager.....	687
Table 445 – PICS for provisioning role.....	688
Table 446 – Device PICS	688
Table 447 – PICS for provisioning role.....	689
Table 448 – PICS for security manager.....	689
Table 449 – PhL roles.....	690
Table 450 – PhL frequency of operation.....	690
Table 451 – PhL functions.....	690
Table 452 – PhL packet	691
Table 453 – DL roles.....	691
Table 454 – DL PICS for device implementing I/O role.....	691
Table 455 – DL PICS for device implementing router role	691
Table 456 – DL PICS for device implementing backbone router role	692
Table 457 – PICS for devices implementing I/O role	692
Table 458 – PICS for device implementing router role.....	693
Table 459 – PICS for devices implementing backbone router role.....	693

Table 460 – PICS for device implementing I/O role	694
Table 461 – PICS for routing device.....	694
Table 462 – PICS for backbone router	694
Table 463 – AL implementation option	695
Table 464 – PICS part 2: Optional industry-independent objects	695
Table 465 – PICS part 2: Supported standard services for I/O device role.....	696
Table 466 – PICS part 2: Supported standard services for system manager role	697
Table 467 – PICS part 2: Supported standard services for gateway role when supporting native access	698
Table 468 – PICS part 2: Supported standard services for gateway role when supporting interoperable tunneling and for adapters	699
Table 469 – PICS part 2: Supported standard services for routing device role.....	700
Table 470 – PICS part 2: Supported standard services for backbone router role	701
Table 471 – PICS part 2: Supported standard services for provisioning role.....	702
Table 472 – PICS part 2: Supported standard services for system time source role.....	702
Table 473 – Process control conformance: Supported objects.....	702
Table 474 – Process control conformance: Supported alerts	703
Table 475 – PICS: Gateway	704
Table 476 – PICS: I/O devices, routing devices, gateways, and backbone routers.....	706
Table 477 – PICS: Provisioning devices.....	706
Table 478 – Protocol layer device roles.....	708
Table 479 – Over-the-air upgrades	708
Table 480 – Session support profiles	709
Table 481 – Baseline profiles	709
Table 482 – PhL roles	710
Table 483 – DL required for listed roles	710
Table 484 – Role profiles: General DLMO attributes	711
Table 485 – Role profiles: dlmo.Device_Capability	712
Table 486 – Role profiles: dlmo.Ch (channel hopping)	713
Table 487 – Role profiles: dlmo.TsTemplate.....	713
Table 488 – Role profiles: dlmo.Neighbor.....	713
Table 489 – Role profiles: dlmo. NeighborDiag.....	714
Table 490 – Role profiles: dlmo.Superframe.....	714
Table 491 – Role profiles: dlmo.Graph	714
Table 492 – Role profiles: dlmo.Link	715
Table 493 – Role profiles: dlmo.Route	715
Table 494 – Role profiles: dlmo.Queue_Priority.....	715
Table 495 – Routing table size	715
Table 496 – Address table size.....	716
Table 497 – Port support size.....	716
Table 498 – APs	716
Table 499 – Role profile: Gateway	716
Table 500 – Role profile: Gateway native access.....	717
Table 501 – Role profile: Gateway interoperable tunnel mechanism	717

Table 502 – Role profiles: I/O, routers, gateways, and backbone routers	717
Table 503 – Usage classes	718
Table 504 – System management configuration defaults.....	723
Table 505 – Security configuration defaults	724
Table 506 – DL configuration defaults	725
Table 507 – Network configuration defaults	726
Table 508 – Transport configuration defaults	726
Table 509 – Application configuration defaults.....	727
Table 510 – Gateway configuration defaults	728
Table 511 – Provisioning configuration defaults.....	729
Table 512 – Table of standard object types	743
Table 513 – Template for standard object attributes	743
Table 514 – Template for standard object methods.....	744
Table 515 – Template for standard object alert reporting	745
Table 516 – Template for data structures	746
Table 517 – Scheduled_Write method template	747
Table 518 – Read_Row method template	748
Table 519 – Write_Row method template	748
Table 520 – Reset_Row method template	749
Table 521 – Delete_Row method template	750
Table 522 – Standard object types.....	753
Table 523 – Standard object instances	755
Table 524 – Standard data types	758
Table 525 – Protocol identification values	759
Table 526 – Sample MHR for join request	786
Table 527 – Sample DHR for join request	786
Table 528 – Network header for join messages	787
Figure 1 – Standard-compliant network	62
Figure 2 – Single protocol data unit	63
Figure 3 – Full protocol data unit	63
Figure 4 – Physical devices versus roles.....	70
Figure 5 – Notional representation of device phases.....	73
Figure 6 – Simple star topology	75
Figure 7 – Simple hub-and-spoke topology.....	76
Figure 8 – Mesh topology	77
Figure 9 – Simple star-mesh topology	77
Figure 10 – Network and DL subnet overlap	78
Figure 11 – Network and DL subnet differ	79
Figure 12 – Network with multiple gateways	80
Figure 13 – Basic network with backup gateway	81

Figure 14 – Network with backbone	82
Figure 15 – Network with backbone – device roles.....	83
Figure 16 – Reference model	84
Figure 17 – Basic data flow	85
Figure 18 – Data flow between I/O devices.....	86
Figure 19 – Data flow with legacy I/O device	87
Figure 20 – Data flow with backbone.....	87
Figure 21 – Data flow between I/O devices via backbone.....	88
Figure 22 – Data flow to standard-aware control system	89
Figure 23 – Management architecture	91
Figure 24 – DMAP	94
Figure 25 – Example of management SAP flow through standard protocol suite	96
Figure 26 – System manager architecture concept	115
Figure 27 – UAP-system manager interaction during contract establishment.....	134
Figure 28 – Contract-related interaction between DMO and SCO	136
Figure 29 – Contract source, destination, and intermediate devices.....	145
Figure 30 – Contract establishment example	153
Figure 31 – Contract ID usage in source	154
Figure 32 – Contract termination.....	157
Figure 33 – Contract modification with immediate effect.....	159
Figure 34 – Examples of DPDU and TPDU scope	161
Figure 35 – Keys and associated lifetimes.....	163
Figure 36 – Key lifetimes.....	164
Figure 37 – DPDU structure	167
Figure 38 – Outgoing messages – DL and security	168
Figure 39 – Incoming messages- DL and security.....	169
Figure 40 – TPDU structure and protected coverage.....	180
Figure 41 – TMIC parameters	180
Figure 42 – Transport layer and security sub-layer interaction, outgoing TPDU	182
Figure 43 – Transport layer and security sub-layer interaction, incoming TPDU.....	183
Figure 44 – Example: Overview of the symmetric key join process	198
Figure 45 – Example: Overview of the symmetric key join process of backbone device.....	199
Figure 46 – Asymmetric key-authenticated key agreement scheme	208
Figure 47 – Example: Overview of the asymmetric key join process for a device with a data link layer.....	211
Figure 48 – Example: Overview of the asymmetric key join process of a backbone device	212
Figure 49 – Device state transitions for join process and device lifetime	221
Figure 50 – High-level example of session establishment.....	222
Figure 51 – Key update protocol overview	230
Figure 52 – Device session establishment and key update state transition.....	236
Figure 53 – DL protocol suite and PPDU/DPDU structure.....	254
Figure 54 – Graph routing example.....	257
Figure 55 – Inbound and outbound graphs	259

Figure 56 – Slotted hopping	263
Figure 57 – Slow hopping	263
Figure 58 – Hybrid operation	264
Figure 59 – Radio spectrum usage	264
Figure 60 – Default hopping pattern 1	266
Figure 61 – Two groups of devices with different hopping pattern offsets	267
Figure 62 – Interleaved hopping pattern 1 with 16 different hopping pattern offsets	268
Figure 63 – Slotted hopping	269
Figure 64 – Slow hopping	269
Figure 65 – Hybrid mode with slotted and slow hopping	270
Figure 66 – Combining slotted hopping and slow hopping	270
Figure 67 – Example of a three-timeslot superframe	271
Figure 68 – Superframes and links	271
Figure 69 – Multiple superframes, with timeslots aligned	272
Figure 70 – Slotted hopping	275
Figure 71 – Slow hopping	276
Figure 72 – Components of a slow hop	276
Figure 73 – Avoiding collisions among routers	277
Figure 74 – Hybrid configuration	278
Figure 75 – Timeslot allocation and the message queue	280
Figure 76 – 250 ms alignment intervals	283
Figure 77 – Timeslot durations and timing	283
Figure 78 – Clock source acknowledges receipt of DPDU	288
Figure 79 – Transaction timing attributes	290
Figure 80 – Dedicated and shared transaction timeslots	291
Figure 81 – Unicast transaction	292
Figure 82 – PDU wait time (PWT)	294
Figure 83 – Duocast support in the standard	295
Figure 84 – Duocast transaction	296
Figure 85 – Shared timeslots with CSMA-CA	297
Figure 86 – Transaction during slow-hopping periods	298
Figure 87 – DL management SAP flow through standard protocol suite	300
Figure 88 – PPDU and DPDU structure	317
Figure 89 – Typical acknowledgement frame layout	324
Figure 90 – Relationship among DLMO indexed attributes	356
Figure 91 – Address translation process	389
Figure 92 – Fragmentation process	390
Figure 93 – Reassembly process	392
Figure 94 – Processing of a NSDU received from the transport layer	394
Figure 95 – Processing of an incoming NPDU	395
Figure 96 – Processing of a NPDU received from the backbone	396
Figure 97 – Delivery of an incoming NPDU at its final destination	397
Figure 98 – Routing from a field device to a gateway on field – no backbone routing	397

Figure 99 – Protocol suite diagram for routing from a field device to a gateway on field – no backbone routing.....	398
Figure 100 – Routing a PDU from a field device to a gateway via a backbone router	399
Figure 101 – Protocol suite diagram for routing a PDU from a field device to a gateway via a backbone router	399
Figure 102 – Routing from a field device on one subnet to another field device on a different subnet	401
Figure 103 – Protocol suite diagram for routing from an I/O device on one subnet to another I/O device on a different subnet.....	402
Figure 104 – Routing over an Ethernet backbone network.....	403
Figure 105 – Routing over a fieldbus backbone network.....	403
Figure 106 – Distinguishing between NPDU header formats.....	414
Figure 107 – Transport layer reference model	421
Figure 108 – UDP “pseudo-header” for IPv6.....	423
Figure 109 – Transport layer protocol data unit	426
Figure 110 – User application objects in a user application process.....	440
Figure 111 – Alarm state model	445
Figure 112 – Event model	446
Figure 113 – A successful example of multiple outstanding requests, with response concatenation.....	451
Figure 114 – An example of multiple outstanding unordered requests, with second write request initially unsuccessful.....	452
Figure 115 – An example of multiple outstanding ordered requests, with second write request initially unsuccessful	453
Figure 116 – Send window example 1, with current send window smaller than maximum send window	455
Figure 117 – Send window example 2, with current send window the same size as maximum send window, and non-zero usable send window width.....	455
Figure 118 – Send window example 3, with current send window the same size as maximum send window, and usable send window width of zero (0).....	456
Figure 119 – General addressing model.....	458
Figure 120 – UAP management object state diagram.....	464
Figure 121 – Alert report reception state diagram	466
Figure 122 – Alert reporting example	466
Figure 123 – Upload/Download object download state diagram	480
Figure 124 – Upload/Download object upload state diagram.....	482
Figure 125 – Publish sequence of service primitives.....	500
Figure 126 – Client/server model two-part interactions.....	504
Figure 127 – Client/server model four-part interactions: Successful delivery	505
Figure 128 – Client/server model four-part interactions: Request delivery failure	505
Figure 129 – Client/server model four-part interactions: Response delivery failure	506
Figure 130 – AlertReport and AlertAcknowledge, delivery success	519
Figure 131 – AlertReport, delivery failure	519
Figure 132 – Alert Report, acknowledgment failure.....	520
Figure 133 – Concatenated response for multiple outstanding write requests (no message loss)	526

Figure 134 – Management and handling of malformed APDUs received from device X	532
Figure 135 – Gateway scenarios.....	591
Figure 136 – Basic gateway model	592
Figure 137 – Sequence of primitives for session service	595
Figure 138 – Sequence of primitives for lease management service	595
Figure 139 – Sequence of primitives for system report services	596
Figure 140 – Sequence of primitives for time service	596
Figure 141 – Sequence of primitives for client/server service initiated from gateway	597
Figure 142 – Sequence of primitives for publish service initiated from gateway	597
Figure 143 – Sequence of primitives for subscribe service initiated from device	598
Figure 144 – Sequence of primitives for publisher timer initiated from gateway	598
Figure 145 – Sequence of primitives for subscriber timers initiated from device	598
Figure 146 – Sequence of primitives for the bulk transfer service	599
Figure 147 – Sequence of primitives for the alert subscription service	599
Figure 148 – Sequence of primitives for the alert notification service	600
Figure 149 – Sequence of primitives for gateway management services	600
Figure 150 – Tunnel object model.....	633
Figure 151 – Distributed tunnel endpoints	634
Figure 152 – Multicast, broadcast, and one-to-many messaging.....	635
Figure 153 – Tunnel object buffering.....	636
Figure 154 – Publish/subscribe publisher CoSt flowchart	638
Figure 155 – Publish/subscribe publisher periodic flowchart.....	639
Figure 156 – Publish/subscribe subscriber common periodic and CoSt flowchart.....	639
Figure 157 – Network address mappings.....	640
Figure 158 – Connection_Info usage in protocol translation	641
Figure 159 – Transaction_Info usage in protocol translation.....	642
Figure 160 – Interoperable tunneling mechanism overview diagram.....	643
Figure 161 – Bulk transfer model	645
Figure 162 – Alert model	646
Figure 163 – Alert cascading	647
Figure 164 – Native P/S and C/S access.....	648
Figure 165 – The provisioning network.....	655
Figure 166 – State transition diagrams outlining provisioning steps during a device life cycle	657
Figure 167 – State transition diagram showing various paths to joining a secured network	660
Figure 168 – Provisioning objects and interactions	662
Figure 169 – Basic reference model.....	720
Figure 170 – Generic protocol translation publish diagram	762
Figure 171 – Generic protocol translation subscribe diagram	763
Figure 172 – Generic protocol translation client/server transmission diagram.....	764
Figure 173 – Generic protocol translation client/server reception diagram.....	765
Figure 174 – Host integration reference model	778
Figure 175 – Configuration using an electronic device definition.....	780

ISA-100.11a-2011	- 27 -	4 May 2011
Figure 176 – Configuration using FDT/DTM approach.....		780

INTRODUCTION

0.1 General

The ISA100 Committee was established by ISA to address wireless manufacturing and control systems in areas including:

- The environment in which the wireless technology is deployed;
- Technology and life cycle for wireless equipment and systems; and
- The application of wireless technology.

The Committee's focus is to improve the confidence in, integrity of, and availability of components or systems used for manufacturing or control, and to provide criteria for procuring and implementing wireless technology in the control system environment. Compliance with the Committee's guidance will improve manufacturing and control system deployment and will help identify vulnerabilities and address them, thereby reducing the risk of compromising or causing manufacturing control systems degradation or failure.

This ISA 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 the protocol suite, system management, gateway, and security specifications for low-data-rate wireless connectivity with fixed, portable, and moving devices supporting very limited power consumption requirements. The application focus is to address the performance needs of applications such as monitoring and process control where latencies on the order of 100 ms can be tolerated, with optional behavior for shorter latency.

To meet the needs of industrial wireless users and operators, this standard provides robustness in the presence of interference found in harsh industrial environments and with legacy non-ISA100 compliant wireless systems. 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 IEEE 802.11x, IEEE 802.15x, IEEE 802.16x, and other relevant standards. Furthermore, this standard allows for interoperability of ISA100 devices, as described in Clause 5.

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 standard 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, gateway, and provisioning. 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 clause will be supplied for further information.

The following terms will be used in this document to describe device behavior:

- **Mandatory:** behavior or a protocol that is required for a device to state compliance with the standard (e.g., symmetrical keys).
- **Optional:** behavior or protocol defined in the standard that is not required for compliance to the standard but, if implemented, shall be compliant with the standard (e.g., asymmetrical keys).
- **Configuration:** setting of a parameter that will alter behavior and can be set by the system manager (e.g., network layer hop limit). Configurations where defaults are appropriate will state those defaults (e.g., network layer hop limit = 64).
- **Capability:** ability of device to perform to a specified level (e.g., number of children a router can support). Profiles will specify a minimum capability.
- **Feature:** notable characteristic of a device (e.g., battery powered).

Mandatory behavior (also referred to as normative behavior) is denoted by the use of the term "shall". Non-mandatory behavior (also referred to as informative behavior) is denoted by the use of the terms "may" or "recommended".

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

0.2 Disclaimers

ISA does not take any position with respect to the existence or validity of any patent rights asserted in connection with this document, and ISA disclaims liability for the infringement of any patent resulting from the use of this document. Users are advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

Pursuant to ISA's Patent Policy, one or more patent holders or patent applicants may have disclosed patents that could be infringed by use of this document and executed a Letter of Assurance committing to the granting of a license on a worldwide, non-discriminatory basis, with a fair and reasonable royalty rate and fair and reasonable terms and conditions. For more information on such disclosures and Letters of Assurance, contact ISA or visit www.isa.org/StandardsPatents.

Other patents or patent claims may exist for which a disclosure or Letter of Assurance has not been received. ISA is not responsible for identifying patents or patent applications for which a license may be required, for conducting inquiries into the legal validity or scope of patents, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory.

ISA requests that anyone reviewing this Document who is aware of any patents that may impact implementation of the Document notify the ISA Standards and Practices Department of the patent and its owner.

Additionally, the use of this standard may involve hazardous materials, operations or equipment. The standard cannot anticipate all possible applications or address all possible safety issues associated with use in hazardous conditions. The user of this standard must exercise sound professional judgment concerning its use and applicability under the user's particular circumstances. The user must also consider the applicability of any governmental regulatory limitations and established safety and health practices before implementing this standard.

NOTE The ISA100 standards development committee, which developed this ISA standard, is seeking feedback on its content and usefulness. If you have comments on the value of this document or suggestions for improvements or additional topics, please send those comments by email, fax, post, or phone to:

ISA100

ISA Standards

67 Alexander Drive

Research Triangle Park, NC 27709 USA

Email: standards@isa.org

Tel: +1 919 990 9200 Fax: +1 919 549 8288

REVISION HISTORY

ISA100.11a-2009		First approved version
ISA100.11a-rev		Revision of first approved version

ISA

ISA100.11a

Wireless systems for industrial automation: Process control and related applications

1 Scope

This project will define the OSI layer specifications (e.g., PhL, DL, etc.), security specifications, and management (including network and device configuration) specifications for wireless devices serving application classes 1 through 5 and optionally class 0 for fixed, portable, and moving devices.

NOTE Usage classes are described in Annex C.

The project's application focus will address performance needs for periodic monitoring and process control where latencies on the order of 100 ms can be tolerated, with optional behavior for shorter latency.

This project will address:

- Low energy consumption devices, and also those applications that have latency and latency variability constraints, with the ability to scale to address large installations;
- Wireless infrastructure, interfaces to legacy infrastructure and applications, security, and network management requirements in a functionally scalable manner;
- Robustness in the presence of interference found in harsh industrial environments and with legacy systems;
- Coexistence with other wireless devices anticipated in the industrial work space, such as IEEE 802.11x, IEEE 802.16x, cell phones, and other relevant standards; and
- Interoperability of ISA100 devices.

2 Normative references

The following standards and specifications contain provisions which, through references in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision and may be changed without notice, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the references listed below.

For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE See the bibliography for non-normative references.

ANSI X9.63-2001, *Public key cryptography for the financial services industry - Key agreement and key transport using elliptic curve cryptography*. American Bankers Association, November 20, 2001

FIPS 197, *Advanced encryption standard (AES)*, Federal Information Processing Standards Publication 197, US Department of Commerce/N.I.S.T., Springfield, Virginia, November 26, 2001

FIPS 198, *The keyed-hash message authentication code (HMAC)*, Federal Information Processing Standards Publication 198, US Department of Commerce/N.I.S.T., Springfield, Virginia, March 6, 2002

IEEE Std 802.15.4™:2006, *Wireless medium access control (MAC) and physical layer (PhL) specifications for low rate wireless personal area networks (WPANs)*