

ISA-100.11a-2009

An ISA Standard

5

Wireless systems for industrial automation: Process control and related applications

10

15

20

25

30

	INTRODUCTION.....	24
	REVISION HISTORY	
	1 Scope.....	27
5	2 Normative references	27
	3 Terms, definitions, abbreviated terms, acronyms, and conventions	28
	3.1 (N)-layer and other terms and definitions from the open systems interconnection basic reference model	28
	3.2 Other terms and definitions.....	34
10	3.3 Symbols	50
	3.4 Abbreviated terms and acronyms	51
	3.5 IEC service table conventions.....	58
	4 Overview	60
	4.1 General	60
15	4.2 Interoperability	60
	4.3 Quality of service	60
	4.4 Worldwide applicability	60
	4.5 Network architecture	60
	4.6 Network characteristics	62
20	5 Systems	68
	5.1 General	68
	5.2 Devices	68
	5.3 Networks	75
	5.4 Protocol suite structure.....	85
25	5.5 Data flow	86
	5.6 Time reference.....	91
	5.7 Firmware upgrades	92
	5.8 Wireless backbones and other infrastructures.....	92
	6 System management.....	94
30	6.1 General	94
	6.2 Device management application process.....	96
	6.3 System manager	119
	7 Security	167
	7.1 General	167
35	7.2 Security services.....	168
	7.3 Data link layer frame security.....	170
	7.4 Transport layer transmission security functionality	184
	7.5 The join process	197
	7.6 Session establishment.....	220
40	7.7 Key update	224
	7.8 Security manager functionality	231
	7.9 Security policies.....	233
	7.10 Security functions available to the application layer	236
	7.11 Security statistics collection, threat detection, and reporting	239
45	7.12 Device security management object functionality	239
	8 Physical layer	247

	8.1	General	247
	8.2	Default physical layer	247
	9	Data link layer	249
	9.1	General	249
5	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	338
	9.5	Data link layer methods	380
	9.6	Data link layer alerts	382
10	10	Network layer	385
	10.1	General	385
	10.2	Network layer functionality overview	385
	10.3	Network layer data services	403
	10.4	Network layer management object	406
15	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 entity	422
20	11.4	Transport data entity	422
	11.5	Transport layer protocol data unit encoding	426
	11.6	Transport layer model	428
	12	Application layer	439
	12.1	General	439
25	12.2	Energy considerations	439
	12.3	Legacy control system considerations	439
	12.4	Introduction to object-oriented modeling	440
	12.5	Object model	442
	12.6	Object attribute model	443
30	12.7	Method model	446
	12.8	Alert model	446
	12.9	Alarm state model	447
	12.10	Event state model	448
	12.11	Alert reporting	448
35	12.12	Communication interaction model	450
	12.13	Application layer addressing	460
	12.14	Management objects	464
	12.15	User objects	464
	12.16	Data types	494
40	12.17	Application services provided by application sub-layer	501
	12.18	Application layer flow use to lower layer services	537
	12.19	Application layer management	538
	12.20	Process control industry standard data structures	558
	12.21	Additional tables	561
45	12.22	Coding	562
	12.23	Syntax	583
	12.24	Detailed coding examples (INFORMATIVE)	596
	13	Gateway	598

	13.1	General	598
	13.2	Service access point	602
	13.3	Protocol.....	645
	14	Provisioning.....	666
5	14.1	General	666
	14.2	Terms and definitions	666
	14.3	Provisioning procedures	667
	14.4	Pre-installed symmetric keys	668
	14.5	Provisioning using out-of-band mechanisms	668
10	14.6	Provisioning networks	669
	14.7	State transition diagrams.....	671
	14.8	Device management application protocol objects for provisioning	676
	14.9	Management objects	678
	14.10	Device provisioning service object	683
15	14.11	Provisioning functions	690
	Annex A (INFORMATIVE)	Protocol implementation conformance statement proforma	694
	A.1	Introduction	694
	A.2	System.....	697
	A.3	System management.....	700
20	A.4	Security manager	704
	A.5	Physical layer	705
	A.6	Data link layer.....	707
	A.7	Network layer.....	708
	A.8	Transport layer	710
25	A.9	Application layer	711
	A.10	Gateway	720
	A.11	Provisioning.....	722
	Annex B (NORMATIVE)	Role profiles.....	724
	B.1	Introduction	724
30	B.2	System.....	725
	B.3	System manager	725
	B.4	Security manager	726
	B.5	Physical layer	726
	B.6	Data link layer.....	727
35	B.7	Network layer.....	731
	B.8	Transport layer	732
	B.9	Application layer	732
	B.10	Gateway	732
	B.11	Provisioning.....	733
40	Annex C (INFORMATIVE)	Background information	735
	C.1	Industrial needs	735
	C.2	Usage classes	736
	C.3	Other uploading and downloading- alarms (human or automated action)	737
	C.4	The open systems interconnection basic reference model	737
45	Annex D (NORMATIVE)	Configuration defaults.....	741
	D.1	General	741
	D.2	System management.....	741

	D.3	Security	742
	D.4	Data link layer.....	743
	D.5	Network layer.....	744
	D.6	Transport layer	745
5	D.7	Application layer	745
	D.8	Gateway	747
	D.9	Provisioning.....	747
	Annex E (INFORMATIVE) Use of backbone networks		749
	E.1	General	749
10	E.2	Recommended characteristics	749
	E.3	Internet protocol backbones.....	749
	Annex F (NORMATIVE) Basic security concepts – Notation and representation		752
	F.1	Strings and string operations	752
	F.2	Integers, octets, and their representation	752
15	F.3	Entities.....	752
	Annex G (INFORMATIVE) Using certificate chains for over-the-air provisioning		753
	Annex H (NORMATIVE) Security building blocks		754
	H.1	Symmetric key cryptographic building blocks	754
	H.2	Asymmetric key cryptographic building blocks	755
20	H.3	Keying information	755
	H.4	Key agreement schemes	757
	H.5	Keying information schemes	758
	H.6	Challenge domain parameter generation and validation.....	759
	H.7	Challenge validation primitive	759
25	H.8	Secret key generation (SKG) primitive.....	760
	H.9	Block-cipher-based cryptographic hash function	760
	H.10	Symmetric-key authenticated key agreement scheme	761
	H.11	Elliptic curve cryptography manual certificate scheme.....	765
	H.12	Symmetric-key manual keying information scheme	768
30	Annex I (INFORMATIVE) Definition templates		771
	I.1	Object type template	771
	I.2	Standard object attributes template.....	771
	I.3	Standard object methods.....	772
	I.4	Standard object alert reporting template.....	773
35	I.5	Data structure definition	774
	Annex J (INFORMATIVE) Operations on attributes		776
	J.1	Operations on attributes	776
	J.2	Synchronized cutover	779
	Annex K (NORMATIVE) Standard object types		780
40	Annex L (NORMATIVE) Standard data types.....		786
	Annex M (NORMATIVE) Protocol identification values		789
	Annex N (INFORMATIVE) Tunneling and native object mapping.....		790
	N.1	Overview	790
	N.2	Tunneling	790
45	N.3	Foreign protocol application communication	790
	N.4	Native object mapping.....	791
	N.5	Tunneling and native object mapping tradeoffs	791

	Annex O (INFORMATIVE) Generic protocol translation	792
	O.1 Overview	792
	O.2 Publish	792
	O.3 Subscribe	793
5	O.4 Client	794
	O.5 Server	795
	Annex P (INFORMATIVE) Gateway service access point adaptations for this standard.....	796
	P.1 General	796
	P.2 Parameters	796
10	P.3 Session	796
	P.4 Lease	796
	P.5 Device list report	797
	P.6 Topology report.....	797
	P.7 Schedule report	797
15	P.8 Device health report	797
	P.9 Neighbor health report.....	797
	P.10 Network health report.....	797
	P.11 Time.....	797
	P.12 Client/server	797
20	P.13 Publish/subscribe	798
	P.14 Bulk transfer	799
	P.15 Alert	800
	P.16 Gateway configuration	800
	P.17 Device configuration.....	800
25	Annex Q (INFORMATIVE) Gateway service access point adaptations for WirelessHART™	801
	Q.1 General	801
	Q.2 Parameters	802
	Q.3 Session	802
30	Q.4 Lease	803
	Q.5 Device list report	803
	Q.6 Topology report.....	804
	Q.7 Schedule report	804
	Q.8 Device health report	804
35	Q.9 Neighbor health report.....	805
	Q.10 Network health report.....	805
	Q.11 Time.....	806
	Q.12 Client/server	806
	Q.13 Publish/subscribe	807
40	Q.14 Bulk transfer	808
	Q.15 Alert	808
	Q.16 Gateway configuration	809
	Q.17 Device configuration.....	809
45	Annex R (INFORMATIVE) Host system interface to standard-compliant devices via a gateway.....	810
	R.1 Background	810
	R.2 Device application data integration with host systems	811
	R.3 Host system configuration tool	811

	R.4	Field device / distributed control systems integration.....	813
	R.5	Gateway	814
	R.6	Asset management application support	814
		Bibliography	816
5			
		Table 1 – Standard management object types in DMAP	98
		Table 2 – Meta_Data_Attribute data structure.....	100
10		Table 3 – Alert types for communication diagnostic category.....	101
		Table 4 – Alert types for security alert category	102
		Table 5 – Alert types for device diagnostic alert category	102
		Table 6 – Alert types for process alert category	102
		Table 7 – ARMO attributes	104
15		Table 8 – ARMO alerts.....	108
		Table 9 – Alarm_Recovery method	109
		Table 10 – DMO attributes	112
		Table 11 – DMO alerts	117
		Table 12 – System management object types.....	121
20		Table 13 – DSO attributes	123
		Table 14 – Address_Translation_Row data structure	123
		Table 15 – Read_Address_Row method.....	124
		Table 16 – Input argument usage	125
		Table 17 – Output argument usage	125
25		Table 18 – Attributes of SMO in system manager	127
		Table 19 – Proxy_System_Manager_Join method.....	128
		Table 20 – Proxy_System_Manager_Contract method	129
		Table 21 – Attributes of DMSO in system manager	131
		Table 22 – System_Manager_Join method	132
30		Table 23 – System_Manager_Contract method.....	133
		Table 24 – Attributes of STSO in system manager.....	137
		Table 25 – Attributes of SCO in system manager.....	140
		Table 26 – SCO method for contract establishment, modification, or renewal	143
		Table 27 – Input argument usage	148
35		Table 28 – Output argument usage	149
		Table 29 – Contract_Data data structure	152
		Table 30 – New_Device_Contract_Response data structure.....	155
		Table 31 – SCO method for contract termination, deactivation and reactivation.....	161
		Table 32 – DMO method to terminate contract.....	161
40		Table 33 – DMO method to modify contract.....	164
		Table 34 – Structure of security control field.....	171
		Table 35 – Security levels	172
		Table 36 – Sec.DpduPrep.Request elements.....	175

	Table 37 – Sec.DpduPrep.Response elements	176
	Table 38 – Sec.DLAckCheck.Request elements	176
	Table 39 – Sec. DLAckCheck.Response elements	177
	Table 40 – Sec.DpduCheck.Request elements	178
5	Table 41 – Sec.DpduCheck.Response elements.....	179
	Table 42 – Sec.DLAckPrep.Request elements.....	179
	Table 43 – Sec.DLAckPrep.Response elements	180
	Table 44 – Structure of the WISN DPDU nonce	181
	Table 45 – Structure of the 32-bit truncated TAI time	181
10	Table 46 – Sec.TpduOutCheck.Request elements	187
	Table 47 – Sec.TpduOutCheck.Response elements.....	187
	Table 48 – Sec.TpduSecure.Request elements	188
	Table 49 – Sec. TpduSecure.Response elements.....	189
	Table 50 – Sec.TpduInCheck.Request elements.....	190
15	Table 51 – Sec.TpduInCheck.Response elements	190
	Table 52 – Sec.TpduVerify.Request elements	191
	Table 53 – Sec.TpduVerify.Response elements.....	192
	Table 54 – Structure of TL security header.....	193
	Table 55 – Structure of the TPDU nonce	193
20	Table 56 – Structure of 32-bit nominal TAI time	194
	Table 57 – Proxy_Security_Sym_Join method	202
	Table 58 – Security_Sym_Join method	203
	Table 59 – Security_Confirm method	203
	Table 60 – Security_Sym_Join_Request data structure.....	204
25	Table 61 – Security_Sym_Join_Response data structure	205
	Table 62 – Structure of compressed Policy field	206
	Table 63 – Security_Sym_Confirm data structure	207
	Table 64 – Proxy_Security_Pub_Join method.....	212
	Table 65 – Security_Pub_Join method	212
30	Table 66 – Proxy_Security_Pub_Confirm method	213
	Table 67 – Security_Pub_Confirm method.....	213
	Table 68 – Format of asymmetric join request internal structure	214
	Table 69 – Format of the protocol control field.....	214
	Table 70 – Algorithm identifier	215
35	Table 71 – Format of asymmetric join response internal structure	215
	Table 72 – Format of first join confirmation internal structure	216
	Table 73 – Format of join confirmation response internal structure	217
	Table 74 – Join process and device lifetime state machine	219
	Table 75 – Security_New_Session method.....	221
40	Table 76 – Security_New_Session_Request data structure	222
	Table 77 – Security_New_Session_Response data structure	223
	Table 78 – New_Key method	226

	Table 79 – Security_Key_and_Policies data structure	227
	Table 80 – Security_Key_Update_Status data structure	229
	Table 81 – Device session state transition	230
	Table 82 – Attributes of PSMO in the system manager.....	232
5	Table 83 – Structure of Policy field	234
	Table 84 – Key types	234
	Table 85 – Key usage	234
	Table 86 – Granularity	235
	Table 87 – Device security management object attributes	240
10	Table 88 – KeyDescriptor [INFORMATIVE].....	242
	Table 89 – TL KeyLookupData OctetString fields.....	243
	Table 90 – Delete key method	244
	Table 91 – Key_Policy_Update method	245
	Table 92 – DSMO Alerts.....	246
15	Table 93 – Timing requirements	247
	Table 94 – Graph table on ND20	253
	Table 95 – Graph table on ND21	253
	Table 96 – DL_Config_Info structure.....	308
	Table 97 – DD-DATA.request parameters.....	315
20	Table 98 – DD-DATA.confirm parameters.....	316
	Table 99 – Value set for status parameter	316
	Table 100 – DD-DATA.indication parameters.....	317
	Table 101 – ExtDLUInt, one-octet variant	319
	Table 102 – ExtDLUInt, two-octet variant	319
25	Table 103 – Data frame MHR	320
	Table 104 – DHDR frame control octet.....	321
	Table 105 – Data frame DMXHR.....	321
	Table 106 – DROUT structure, compressed variant	322
	Table 107 – DROUT structure, uncompressed variant.....	323
30	Table 108 – DADDR structure	324
	Table 109 – Acknowledgement frame MHR	325
	Table 110 – Acknowledgement frame DHR.....	326
	Table 111 – DHR ACK/NACK frame control.....	327
	Table 112 – Advertisement DAUX structure.....	328
35	Table 113 – Advertisement selections elements	329
	Table 114 – Advertisement selections	329
	Table 115 – Advertisement time synchronization elements.....	329
	Table 116 – Advertisement time synchronization structure	330
	Table 117 – Join superframe information subfields	331
40	Table 118 – Join superframe information field	331
	Table 119 – Join information elements.....	332
	Table 120 – Join information structure	332
	Table 121 – Defaults for links created from advertisements.....	333

	Table 122 – dlmo11a.Neighbor entry created from advertisements	334
	Table 123 – dlmo11a.Graph entry created from advertisements	334
	Table 124 – dlmo11a.Route entry created from advertisements.....	334
	Table 125 – Solicitation header subfields	336
5	Table 126 – Solicitation header structure	336
	Table 127 – Solicitation DAUX fields.....	336
	Table 128 – Solicitation DAUX structure.....	337
	Table 129 – Activate link DAUX fields	337
	Table 130 – Activate link DAUX structure	338
10	Table 131 – Reporting received signal quality DAUX fields	338
	Table 132 – Report received signal quality DAUX structure.....	338
	Table 133 – DLMO attributes.....	339
	Table 134 – Subnet filter octets	346
	Table 135 – dlmo11a.TaiAdjust OctetString fields.....	347
15	Table 136 – dlmo11a.TaiAdjust OctetString structure.....	347
	Table 137 – dlmo11a.EnergyDesign OctetString fields	348
	Table 138 – dlmo11a.EnergyDesign OctetString structure.....	348
	Table 139 – dlmo11a.DeviceCapability OctetString fields.....	348
	Table 140 – dlmo11a.DeviceCapability OctetString structure.....	349
20	Table 141 – dlmo11a.Candidates OctetString fields	351
	Table 142 – dlmo11a.Candidates structure	351
	Table 143 – dlmo11a.SmoothFactors OctetString fields	352
	Table 144 – dlmo11a.SmoothFactors structure.....	352
	Table 145 – dlmo11a.QueuePriority fields	353
25	Table 146 – dlmo11a.QueuePriority structure	353
	Table 147 – dlmo11a.ChannelDiag fields	354
	Table 148 – dlmo11a.ChannelDiag structure	354
	Table 149 – dlmo11a.Ch fields	356
	Table 150 – dlmo11a.Ch structure	356
30	Table 151 – Receive template fields	359
	Table 152 – Receive template structure	359
	Table 153 – Transmit template fields	360
	Table 154 – Transmit template structure	360
	Table 155 – Default receive template.....	361
35	Table 156 – Default transmit template.....	361
	Table 157 – Default receive template for scanning.....	361
	Table 158 – dlmo11a.Neighbor fields	363
	Table 159 – dlmo11a.Neighbor structure	363
	Table 160 – ExtendGraph fields.....	365
40	Table 161 – ExtGraph structure	365
	Table 162 – dlmo11a.NeighborDiagReset fields	365
	Table 163 – dlmo11a.NeighborDiagReset structure	365

	Table 164 – dlmo11a.Superframe fields	367
	Table 165 – dlmo11a.Superframe structure	367
	Table 166 –dlmo11a.SuperframeIdle fields.....	370
	Table 167 – dlmo11a.SuperframeIdle structure.....	371
5	Table 168 – dlmo11a.Graph	371
	Table 169 – dlmo11a.Graph structure	372
	Table 170 – dlmo11a.Link fields	373
	Table 171 – dlmo11a.Link structure	373
	Table 172 – dlmo11a.Link[].Type structure	374
10	Table 173 – Values for dlmo11a.Link[].Schedule	376
	Table 174 – dlmo11a.Route fields.....	376
	Table 175 – dlmo11a.Route structure	377
	Table 176 – dlmo11a.NeighborDiag fields	378
	Table 177 – Diagnostic Summary OctetString fields.....	378
15	Table 178 – Diagnostic Summary OctetString structure.....	379
	Table 179 – Diagnostic ClockDetail OctetString fields.....	379
	Table 180 – Diagnostic ClockDetail OctetString structure.....	379
	Table 181 – Read_Row method	380
	Table 182 – Write_Row method	381
20	Table 183 – Write_Row_Now method.....	381
	Table 184 – dlmo11a.AlertPolicy fields.....	382
	Table 185 – dlmo11a.AlertPolicy OctetString structure.....	382
	Table 186 – DL_Connectivity alert	383
	Table 187 – DL_Connectivity alert OctetString	384
25	Table 188 – NeighborDiscovery alert	384
	Table 189 – Link local address structure	386
	Table 190 – Address translation table (ATT).....	386
	Table 191 – Example of a routing table	391
	Table 192 – N-DATA.request elements	404
30	Table 193 – N-DATA.confirm elements.....	404
	Table 194 – N-DATA.indication elements	405
	Table 195 – NLMO attributes.....	407
	Table 196 – Contract table structure	409
	Table 197 – Route table elements	410
35	Table 198 – Address translation table structure	410
	Table 199 – NLMO structured MIB manipulation methods	412
	Table 200 – Alert to indicate dropped PDU /PDU error.....	413
	Table 201 – Common header patterns	414
	Table 202 – Basic network layer header format	415
40	Table 203 – Contract-enabled network layer header format.....	416
	Table 204 – 6LoWPAN_IPHC encoding format	417
	Table 205 – IPv6 network layer header format.....	418
	Table 206 – Full network layer header in the DL.....	419

	Table 207 – Network layer header format for fragmented NPDUs	419
	Table 208 – First fragment header format.....	420
	Table 209 – Second and subsequent fragment header format	420
	Table 210 – UDP LowPAN_NHC encoding	426
5	Table 211 – Optimal UDP header encoding	427
	Table 212 – UDP header encoding with checksum.....	427
	Table 213 – T-DATA.request elements	429
	Table 214 – T-DATA.confirm elements	430
	Table 215 – T-DATA.confirm status codes.....	430
10	Table 216 – T-DATA.indication elements.....	431
	Table 217 – TLMO attributes	433
	Table 218 – Transport layer management object methods – Reset	435
	Table 219 – Transport layer management object methods – Halt.....	435
	Table 220 – Transport layer management object methods – PortRangeInfo	436
15	Table 221 – Transport layer management object methods – GetPortInfo.....	436
	Table 222 – Transport layer management object methods – GetNextPortInfo	437
	Table 223 – Transport layer management object alert types – Illegal use of port	437
	Table 224 – Transport layer management object alert types – TPDU received on unregistered port	438
20	Table 225 – Transport layer management object alert types – TPDU does not match security policies.....	438
	Table 226 – State table for alarm transitions	447
	Table 227 – State table for event transitions	448
	Table 228 – UAP management object attributes	465
25	Table 229 – State table for UAP management object	467
	Table 230 – UAP management object methods.....	467
	Table 231 – Alert receiving object attributes.....	468
	Table 232 – State table for handling an AlertReport reception	469
	Table 233 – AlertReceiving object methods.....	470
30	Table 234 – UploadDownload object attributes	471
	Table 235 – UploadDownload object methods	475
	Table 236 – UploadDownload object StartDownload method	475
	Table 237 – UploadDownload object DownloadData method	477
	Table 238 – UploadDownload object EndDownload method	478
35	Table 239 – UploadDownload object StartUpload method	479
	Table 240 – UploadDownload object UploadData method	480
	Table 241 – UploadDownload object EndUpload method.....	482
	Table 242 – Download state table for unicast operation mode	483
	Table 243 – Upload state table for unicast operation mode	485
40	Table 244 – Concentrator object attributes	487
	Table 245 – Concentrator object methods	488
	Table 246 – Dispersion object attributes	489
	Table 247 – Dispersion object methods.....	490

	Table 248 – Tunnel object attributes	491
	Table 249 – Tunnel object methods	493
	Table 250 – Interface object attributes	494
	Table 251 – Interface object methods	494
5	Table 252 – Data type: ObjectAttributeIndexAndSize	495
	Table 253 – Data type: Communication association endpoint	496
	Table 254 – Data type: Communication contract data	497
	Table 255 – Data type: Alert communication endpoint.....	498
	Table 256 – Data type: Tunnel endpoint.....	498
10	Table 257 – Data type: Alert report descriptor	499
	Table 258 – Data type: Process control alarm report descriptor for analog with single reference condition	499
	Table 259 – Data type: ObjectIDandType	500
	Table 260 – Data type: Unscheduled correspondent	500
15	Table 261 – Data type: PublishingSource	501
	Table 262 – AL services	502
	Table 263 – Publish service	506
	Table 264 – Read service.....	513
	Table 265 – Write service.....	517
20	Table 266 – Execute service	521
	Table 267 – AlertReport service.....	527
	Table 268 – AlertAcknowledge service.....	530
	Table 269 – Tunnel service	534
	Table 270 – Application flow characteristics	537
25	Table 271 – Application service primitive to transport service primitive mapping.....	538
	Table 272 – ASLMO attributes.....	540
	Table 273 – Application sub-layer management object methods	541
	Table 274 –Reset method	542
	Table 275 – ASLMO alerts	543
30	Table 276 – Analog input object attributes.....	546
	Table 277 – Analog input object methods.....	547
	Table 278 – Analog input alerts	548
	Table 279 – Analog output attributes.....	550
	Table 280 – Analog output object methods.....	551
35	Table 281 – Analog output alerts	552
	Table 282 – Binary input object attributes	554
	Table 283 – Binary input object methods.....	555
	Table 284 – Binary input alerts	555
	Table 285 – Binary output attributes	556
40	Table 286 – Binary output object methods.....	557
	Table 287 – Binary output alerts	557
	Table 288 – Status bitstring.....	559
	Table 289 – Data type: Process value and status for analog value	559

	Table 290 – Data type: Process value and status for binary value	560
	Table 291 – Data type: Process control mode.....	560
	Table 292 – Data type: Process control mode bitstring.....	561
	Table 293 – Data type: Process control scaling	561
5	Table 294 – Process control standard objects	562
	Table 295 – Services	562
	Table 296 – Application messaging format	563
	Table 297 – Concatenated APDUs in a single TSDU.....	563
	Table 298 – Object addressing	563
10	Table 299 – Four-bit addressing mode APDU header construction.....	564
	Table 300 – Eight-bit addressing mode APDU header construction.....	564
	Table 301 – Sixteen-bit addressing mode APDU header construction	564
	Table 302 – Inferred addressing use case example	565
	Table 303 – Inferred addressing mode APDU header construction	565
15	Table 304 – Six-bit attribute identifier, not indexed	566
	Table 305 – Six-bit attribute identifier, singly indexed, with seven-bit index.....	566
	Table 306 – Six-bit attribute identifier, singly indexed, with fifteen-bit index	566
	Table 307 – Six-bit attribute identifier, doubly indexed, with two seven-bit indices	566
	Table 308 – Six-bit attribute identifier, doubly indexed, with two fifteen-bit indices.....	567
20	Table 309 – Six-bit attribute identifier, doubly indexed, with first index seven-bits long and second index fifteen bits long	567
	Table 310 – Six-bit attribute bit attribute identifier, doubly indexed, with first index fifteen bits long and second index seven bits long	567
	Table 311 – Twelve-bit attribute identifier, not indexed	567
25	Table 312 – Twelve-bit attribute identifier, singly indexed with seven-bit index.....	568
	Table 313 – Twelve-bit attribute identifier, singly indexed with fifteen bit identifier.....	568
	Table 314 – Twelve-bit attribute identifier, doubly indexed with two seven bit indices	568
	Table 315 – Twelve-bit attribute identifier, doubly indexed with two fifteen bit indices.....	568
30	Table 316 – Twelve-bit attribute identifier, doubly indexed with first index seven-bits long and second index fifteen-bits long	569
	Table 317 – Twelve-bit attribute identifier, doubly indexed with the first index fifteen bits long and the second index seven bits long	569
	Table 318 – Twelve-bit attribute identifier, reserved form	569
	Table 319 – Coding rules for read service request.....	569
35	Table 320 – Coding rules for read service response with 7-bit length field	570
	Table 321 – Coding rules for read service response with 15-bit length field.....	570
	Table 322 – Coding rules for write service request with seven bit length field.....	570
	Table 323 – Coding rules for write service request with fifteen-bit length field	570
	Table 324 – Coding rules for write service response	571
40	Table 325 – Coding rules for execute service request with seven-bit length field	571
	Table 326 – Coding rules for execute service request with fifteen-bit length field.....	571
	Table 327 – Coding rules for execute service response with 7-bit length field	571
	Table 328 – Coding rules for execute service response with 15-bit length field.....	572

	Table 329 – Coding rules for tunnel service request with seven-bit length field.....	572
	Table 330 – Coding rules for tunnel service request with fifteen-bit length field	572
	Table 331 – Coding rules for tunnel service response with seven-bit length field	572
	Table 332 – Coding rules for tunnel service response with fifteen-bit length field.....	573
5	Table 333 – Coding rules for AlertReport service with 7-bit length field.....	573
	Table 334 – Coding rules for AlertReport service with 15-bit length field	573
	Table 335 – Coding rules for AlertAcknowledge service	574
	Table 336 – Coding rules for publish service for a native single value.....	574
	Table 337 – Coding rules for publish service for a native sequence of values.....	574
10	Table 338 – Coding rules for publish service – non-native (for tunnel support)	574
	Table 339 – Coding rules for concatenate service.....	574
	Table 340 – General coding rule for size-invariant application data	575
	Table 341 – Coding rules for application data of varying size	575
	Table 342 – Coding rules for Boolean data – true	575
15	Table 343 – Coding rules for Boolean data – false.....	575
	Table 344 – Coding rules for Unsigned8.....	576
	Table 345 – Coding rules for Unsigned16.....	577
	Table 346 – Coding rules for Unsigned32.....	577
	Table 347 – Coding rules for Unsigned64.....	577
20	Table 348 – Coding rules for Unsigned128.....	578
	Table 349 – Coding rules for Float.....	578
	Table 350 – Coding rules for double-precision float	579
	Table 351 – Coding rules for VisibleString.....	579
	Table 352 – Coding rules for OctetString.....	579
25	Table 353 – Example: Coding rules for Bitstring of size 8.....	580
	Table 354 – Coding rules for Bitstring	580
	Table 355 – Coding rules for TAIDifference.....	580
	Table 356 – Coding rules for TAINetworkTimeValue	581
	Table 357 – Coding rules for TAIRounded	581
30	Table 358 – Coding example: Read request for a non-indexed attribute.....	596
	Table 359 – Coding example: Read response (corresponding to request contained in the preceding table).....	597
	Table 360 – Coding example: Tunnel service request	597
	Table 361 – Summary of gateway high side interface services	603
35	Table 362 – Primitive G_Session parameter usage.....	612
	Table 363 – GS_Status for G_Session confirm.....	613
	Table 364 – Primitive G_Lease parameter usage.....	614
	Table 365 – GS_Lease_Type for G_Lease request.....	615
	Table 366 – GS_Status for G_Lease confirm.....	616
40	Table 367 – Primitive G_Device_List_Report parameter usage.....	617
	Table 368 – GS_Status for G_Device_List_Report confirm.....	618
	Table 369 – Primitive G_Topology_Report parameter usage	618
	Table 370 – GS_Status for G_Topology_Report confirm	619

	Table 371 – Primitive G_Schedule_Report parameter usage	620
	Table 372 – GS_Status for G_Schedule_Report confirm	621
	Table 373 – Primitive G_Device_Health_Report parameter usage	622
	Table 374 – GS_Status for G_Device_Health_Report confirm	622
5	Table 375 – Primitive G_Neighbor_Health_Report parameter usage	623
	Table 376 – GS_Status for G_Device_Health_Report confirm	624
	Table 377 – Primitive G_Network_Health_Report parameter usage	625
	Table 378 – GS_Status for G_Network_Health_Report confirm	626
	Table 379 – Primitive G_Time parameter usage	627
10	Table 380 – GS_Status for G_Time confirm	627
	Table 381 – Primitive G_Client_Server parameter usage	628
	Table 382 – GS_Status for G_Client_Server confirm.....	629
	Table 383 – Primitive G_Publish parameter usage.....	631
	Table 384 – GS_Status for G_Publish confirm.....	632
15	Table 385 – Primitive G_Subscribe parameter usage	632
	Table 386 – GS_Status for G_Subscribe confirm	633
	Table 387 – Primitive G_Publish_Timer parameter usage	633
	Table 388 – Primitive G_Subscribe_Timer parameter usage	633
	Table 389 – Primitive G_Publish_Watchdog parameter usage	634
20	Table 390 – Primitive G_Bulk_Open parameter usage	635
	Table 391 – GS_Status for G_Bulk_Open confirm	636
	Table 392 – Primitive G_Bulk_Transfer parameter usage	636
	Table 393 – GS_Status for G_Bulk_Transfer confirm	636
	Table 394 – Primitive G_Bulk_Close parameter usage	637
25	Table 395 – GS_Status for G_Bulk_Close confirm	637
	Table 396 – Primitive G_Alert_Subscription parameter usage	638
	Table 397 – GS_Status for G_Alert_Subscription confirm.....	639
	Table 398 – Primitive G_Alert_Notification parameter usage	639
	Table 399 – Primitive G_Read_Gateway_Configuration parameter usage	640
30	Table 400 – GS_Attribute_Identifier values	641
	Table 401 – GS_Status for G_Read_Gateway_Configuration confirm	641
	Table 402 – Primitive G_Write_Gateway_Configuration parameter usage	641
	Table 403 – GS_Attribute_Identifier values	642
	Table 404 – GS_Status for G_Write_Gateway_Configuration confirm	642
35	Table 405 – Primitive G_Write_Device_Configuration parameter usage	643
	Table 406 – GS_Status for G_Write_Device_Configuration confirm	644
	Table 407 – Primitive G_Read_Device_Configuration parameter usage	644
	Table 408 – GS_Status for G_Read_Device_Configuration confirm	645
	Table 409 – UAP management object extended attributes.....	665
40	Table 410 – Factory default settings	673
	Table 411 – Device provisioning object	679
	Table 412 – Reset_To_Default method	682

	Table 413 – Write symmetric join key method.....	682
	Table 414 – Device provisioning service object	684
	Table 415 – DPSO structured attributes	687
	Table 416 – Array manipulation table	688
5	Table 417 – DPSO alert to indicate join by a device not on the WhiteList	689
	Table 418 – DPSO alert to indicate inadequate device join capability	689
	Table 419 – Field media type	697
	Table 420 – Protocol layer support	697
	Table 421 – Device PICS	698
10	Table 422 – PICS for device implementing I/O role	698
	Table 423 – PICS for device implementing router role.....	698
	Table 424 – PICS for backbone router	698
	Table 425 – PICS for gateway	699
	Table 426 – PICS for system manager	699
15	Table 427 – PICS for provisioning device.....	699
	Table 428 – PICS for security manager.....	699
	Table 429 – PICS for device implementing system time source role.....	700
	Table 430 – System PICS	700
	Table 431 – Device PICS	701
20	Table 432 – Router and backbone router PICS.....	701
	Table 433 – PICS for system time source.....	702
	Table 434 – PICS for system manager	703
	Table 435 – PICS for provisioning role	703
	Table 436 – Device PICS	704
25	Table 437 – PICS for provisioning role	705
	Table 438 – PICS for security manager	705
	Table 439 – PhL roles	706
	Table 440 – PhL frequency of operation.....	706
	Table 441 – PhL functions.....	706
30	Table 442 – PhL packet	707
	Table 443 – DL roles.....	707
	Table 444 – DL PICS for device implementing I/O role.....	707
	Table 445 – DL PICS for device implementing router role	707
	Table 446 – DL PICS for device implementing backbone router role	708
35	Table 447 – PICS for devices implementing I/O role	708
	Table 448 – PICS for device implementing router role.....	709
	Table 449 – PICS for devices implementing backbone router role.....	709
	Table 450 – PICS for device implementing I/O role	710
	Table 451 – PICS for routing device.....	710
40	Table 452 – PICS for backbone router	710
	Table 453 – AL implementation option	711
	Table 454 – PICS part 2: Optional industry-independent objects	712
	Table 455 – PICS part 2: Supported standard services for I/O device role.....	713

	Table 456 – PICS part 2: Supported standard services for system manager role	714
	Table 457 – PICS part 2: Supported standard services for gateway role when supporting native access	715
5	Table 458 – PICS part 2: Supported standard services for gateway role when supporting interoperable tunneling and for adapters	716
	Table 459 – PICS part 2: Supported standard services for routing device role	717
	Table 460 – PICS part 2: Supported standard services for backbone router role	718
	Table 461 – PICS part 2: Supported standard services for provisioning role	719
	Table 462 – PICS part 2: Supported standard services for system time source role	719
10	Table 463 – Process control conformance: Supported objects	719
	Table 464 – Process control conformance: Supported alerts	720
	Table 465 – PICS: Gateway	721
	Table 466 – PICS: I/O devices, routing devices, gateways, and backbone routers	723
	Table 467 – PICS: Provisioning devices	723
15	Table 468 – Protocol layer device roles	725
	Table 469 – Over-the-air upgrades	725
	Table 470 – Contract support profiles	726
	Table 471 – Baseline profiles	726
	Table 472 – PhL roles	726
20	Table 473 – DL required for listed roles	727
	Table 474 – Role profiles: General DLMO attributes	728
	Table 475 – Role profiles: dlmo11a.Device_Capability	729
	Table 476 – Role profiles: dlmo.11a.Ch (channel hopping)	729
	Table 477 – Role profiles: dlmo11a.TsTemplate	730
25	Table 478 – Role profiles: dlmo11a.Neighbor	730
	Table 479 – Role profiles: dlmo11a.Diagnostic	730
	Table 480 – Role profiles: dlmo11a.Superframe	730
	Table 481 – Role profiles: dlmo11a.Graph	731
	Table 482 – Role profiles: dlmo11a.Link	731
30	Table 483 – Role profiles: dlmo11a.Route	731
	Table 484 – Role profiles: dlmo11a.Queue_Priority	731
	Table 485 – Routing table size	732
	Table 486 – Address table size	732
	Table 487 – Port support size	732
35	Table 488 – APs	732
	Table 489 – Role profile: Gateway	733
	Table 490 – Role profile: Gateway native access	733
	Table 491 – Role profile: Gateway interoperable tunnel mechanism	733
	Table 492 – Role profiles: I/O, routers, gateways, and backbone routers	734
40	Table 493 – Usage classes	736
	Table 494 – System management configuration defaults	742
	Table 495 – Security configuration defaults	743
	Table 496 – DL configuration defaults	744

	Table 497 – Network configuration defaults	745
	Table 498 – Transport configuration defaults	745
	Table 499 – Application configuration defaults	746
	Table 500 – Gateway configuration defaults	747
5	Table 501 – Provisioning configuration defaults	748
	Table 502 – Table of standard object types	771
	Table 503 – Template for standard object attributes	772
	Table 504 – Template for standard object methods	773
	Table 505 – Template for standard object alert reporting	774
10	Table 506 – Template for data structures	775
	Table 507 – Scheduled_Write method template	776
	Table 508 – Read_Row method template	777
	Table 509 – Write_Row method template	777
	Table 510 – Reset_Row method template	778
15	Table 511 – Delete_Row method template	779
	Table 512 – Standard object types	782
	Table 513 – Standard object instances	784
	Table 514 – Standard data types	787
	Table 515 – Protocol identification values	789
20		
	Figure 1 – Standard-compliant network	61
	Figure 2 – Single protocol data unit	62
25	Figure 3 – Full protocol data unit	62
	Figure 4 – Physical devices versus roles	70
	Figure 5 – Notional representation of device phases	74
	Figure 6 – Simple star topology	76
	Figure 7 – Simple hub-and-spoke topology	77
30	Figure 8 – Mesh topology	78
	Figure 9 – Simple star-mesh topology	79
	Figure 10 – Network and DL subnet overlap	80
	Figure 11 – Network and DL subnet differ	81
	Figure 12 – Network with multiple gateways	82
35	Figure 13 – Basic network with backup gateway	83
	Figure 14 – Network with backbone	84
	Figure 15 – Network with backbone – device roles	85
	Figure 16 – Reference model	86
	Figure 17 – Basic data flow	87
40	Figure 18 – Data flow between I/O devices	88
	Figure 19 – Data flow with legacy I/O device	89
	Figure 20 – Data flow with backbone	89
	Figure 21 – Data flow between I/O devices via backbone	90

	Figure 22 – Data flow to standard-aware control system	91
	Figure 23 – Management architecture	94
	Figure 24 – DMAP	97
	Figure 25 – Example of management SAP flow through standard protocol suite	99
5	Figure 26 – System manager architecture concept	120
	Figure 27 – UAP-system manager interaction during contract establishment.....	138
	Figure 28 – Contract-related interaction between DMO and SCO.....	140
	Figure 29 – Contract source, destination, and intermediate devices.....	150
	Figure 30 – Contract establishment example	158
10	Figure 31 – Contract ID usage in source	159
	Figure 32 – Contract termination.....	162
	Figure 33 – Contract modification with immediate effect.....	165
	Figure 34 – Examples of DPDU and TPDU scope	167
	Figure 35 – Keys and associated lifetimes.....	169
15	Figure 36 – DLPDU structure.....	171
	Figure 37 – Outgoing messages – DL and security	172
	Figure 38 – Incoming messages- DL and security.....	174
	Figure 39 – Transport layer and security sub-layer interaction, outgoing TPDU	185
	Figure 40 – Transport layer and security sub-layer interaction, incoming TPDU.....	186
20	Figure 41 – Example: Overview of the join process.....	201
	Figure 42 – Asymmetric key-authenticated key agreement scheme	208
	Figure 43 – Asymmetric-key based join protocol message sequence chart.....	211
	Figure 44 – Device state transitions for join process and device lifetime	219
	Figure 45 – High-level example of session establishment.....	220
25	Figure 46 – Key update protocol overview.....	225
	Figure 47 – Device session establishment and key update state transition	231
	Figure 48 – DL protocol suite and PhPDU/DPDU structure.....	250
	Figure 49 – Graph routing example	253
	Figure 50 – Inbound and outbound graphs	255
30	Figure 51 – Slotted hopping	258
	Figure 52 – Slow hopping.....	259
	Figure 53 – Hybrid operation	259
	Figure 54 – Radio spectrum usage	260
	Figure 55 – Default hopping pattern 1	262
35	Figure 56 – Two groups of devices with different hopping pattern offsets	263
	Figure 57 – Interleaved hopping pattern 1 with 16 different hopping pattern offsets	264
	Figure 58 – Slotted hopping	265
	Figure 59 – Slow hopping.....	266
	Figure 60 – Hybrid mode with slotted and slow hopping	267
40	Figure 61 – Combining slotted hopping and slow hopping	267
	Figure 62 – Example of a three-timeslot superframe	268
	Figure 63 – Superframes and links	268

	Figure 64 – Multiple superframes, with timeslots aligned.....	269
	Figure 65 – Slotted hopping	273
	Figure 66 – Slow hopping.....	274
	Figure 67 – Components of a slow hop	274
5	Figure 68 – Avoiding collisions among routers.....	275
	Figure 69 – Hybrid configuration	275
	Figure 70 – Timeslot allocation and the message queue	278
	Figure 71 – 250 ms alignment intervals.....	281
	Figure 72 – Timeslot durations and timing	282
10	Figure 73 – Clock source acknowledges receipt of DPDU	286
	Figure 74 – Transaction timing attributes	288
	Figure 75 – Dedicated and shared transaction timeslots	289
	Figure 76 – Unicast transaction	290
	Figure 77 – PDU wait time (PWT)	293
15	Figure 78 – Duocast support in the standard	294
	Figure 79 – Duocast transaction	295
	Figure 80 – Shared timeslots with CSMA-CA.....	296
	Figure 81 – Transaction during slow-hopping periods	297
	Figure 82 – DL management SAP flow through standard protocol suite.....	300
20	Figure 83 – Response to solicitation	305
	Figure 84 – PhPDU and DPDU structure	317
	Figure 85 – Typical acknowledgement frame layout	325
	Figure 86 – Relationship among DLMO indexed attributes	355
	Figure 87 – Address translation process	387
25	Figure 88 – Fragmentation process.....	389
	Figure 89 – Reassembly process	390
	Figure 90 – Processing of a NSDU received from the transport layer	392
	Figure 91 – Processing of an incoming NPDU	393
	Figure 92 – Processing of a NPDU received from the backbone	394
30	Figure 93 – Delivery of an incoming NPDU at its final destination	395
	Figure 94 – Routing from a field device to a gateway on field – no backbone routing	396
	Figure 95 – Protocol suite diagram for routing from a field device to a gateway on field – no backbone routing.....	397
	Figure 96 – Routing a PDU from a field device to a gateway via a backbone router	398
35	Figure 97 – Protocol suite diagram for routing a PDU from a field device to a gateway via a backbone router	399
	Figure 98 – Routing from a field device on one subnet to another field device on a different subnet	400
40	Figure 99 – Protocol suite diagram for routing from an I/O device on one subnet to another I/O device on a different subnet.....	401
	Figure 100 – Routing over an Ethernet backbone network.....	402
	Figure 101 – Routing over a fieldbus backbone network.....	403
	Figure 102 – Distinguishing between NPDU header formats	414
	Figure 103 – Transport layer reference model	421

	Figure 104 – IPv6 pseudo-header	423
	Figure 105 –Pseudo-header	424
	Figure 106 – Transport layer protocol data unit	426
	Figure 107 – User application objects in a user application process.....	442
5	Figure 108 – Alarm state model	447
	Figure 109 – Event model	448
	Figure 110 – A successful example of multiple outstanding requests, with response concatenation	453
10	Figure 111 – An example of multiple outstanding unordered requests, with second write request initially unsuccessful.....	454
	Figure 112 – An example of multiple outstanding ordered requests, with second write request initially unsuccessful	455
	Figure 113 – Send window example 1, with current send window smaller than maximum send window	457
15	Figure 114 – Send window example 2, with current send window the same size as maximum send window, and non-zero usable send window width	458
	Figure 115 – Send window example 3, with current send window the same size as maximum send window, and usable send window width of zero (0).....	458
	Figure 116 – General addressing model.....	461
20	Figure 117 – UAP management object state diagram.....	467
	Figure 118 – Alert report reception state diagram	469
	Figure 119 – Alert reporting example	469
	Figure 120 – Upload/Download object download state diagram	484
	Figure 121 – Upload/Download object upload state diagram.....	486
25	Figure 122 – Publish sequence of service primitives	504
	Figure 123 – Client/server model two-part interactions.....	509
	Figure 124 – Client/server model four-part interactions: Successful delivery	510
	Figure 125 – Client/server model four-part interactions: Request delivery failure	510
	Figure 126 – Client/server model four-part interactions: Response delivery failure	511
30	Figure 127 – AlertReport and AlertAcknowledge, delivery success	525
	Figure 128 – AlertReport, delivery failure	526
	Figure 129 – Alert Report, acknowledgment failure	526
	Figure 130 – Concatenated response for multiple outstanding write requests (no message loss)	533
35	Figure 131 – Management and handling of malformed APDUs received from device X	539
	Figure 132 – Gateway scenarios.....	600
	Figure 133 – Basic gateway model	601
	Figure 134 – Sequence of primitives for session service	604
	Figure 135 – Sequence of primitives for lease management service	604
40	Figure 136 – Sequence of primitives for system report services	605
	Figure 137 – Sequence of primitives for time service	605
	Figure 138 – Sequence of primitives for client/server service initiated from gateway	606
	Figure 139 – Sequence of primitives for publish service initiated from gateway	606
	Figure 140 – Sequence of primitives for subscribe service initiated from device	607

	Figure 141 – Sequence of primitives for publisher timer initiated from gateway	607
	Figure 142 – Sequence of primitives for subscriber timers initiated from device	607
	Figure 143 – Sequence of primitives for the bulk transfer service	608
	Figure 144 – Sequence of primitives for the alert subscription service	608
5	Figure 145 – Sequence of primitives for the alert notification service	609
	Figure 146 – Sequence of primitives for gateway management services	609
	Figure 147 – Tunnel object model	646
	Figure 148 – Distributed tunnel endpoints	647
	Figure 149 – Multicast, broadcast, and one-to-many messaging	648
10	Figure 150 – Tunnel object buffering	649
	Figure 151 – Publish/subscribe publisher CoSt flowchart	652
	Figure 152 – Publish/subscribe publisher periodic flowchart	652
	Figure 153 – Publish/subscribe subscriber common periodic and CoSt flowchart	653
	Figure 154 – Network address mappings	654
15	Figure 155 – Connection_Info usage in protocol translation	655
	Figure 156 – Transaction_Info usage in protocol translation	656
	Figure 157 – Interoperable tunneling mechanism overview diagram	657
	Figure 158 – Bulk transfer model	660
	Figure 159 – Alert model	661
20	Figure 160 – Alert cascading	662
	Figure 161 – Native P/S and C/S access	663
	Figure 162 – The provisioning network	670
	Figure 163 – State transition diagrams outlining provisioning steps during a device life cycle	672
25	Figure 164 – State transition diagram showing various paths to joining a secured network	675
	Figure 165 – Provisioning objects and interactions	677
	Figure 166 – Basic reference model	738
	Figure 167 – Symmetric key authenticated key agreement scheme	762
30	Figure 168 – Generic protocol translation publish diagram	792
	Figure 169 – Generic protocol translation subscribe diagram	793
	Figure 170 – Generic protocol translation client/server transmission diagram	794
	Figure 171 – Generic protocol translation client/server reception diagram	795
	Figure 172 – Host integration reference model	810
35	Figure 173 – Configuration using an electronic device definition	812
	Figure 174 – Configuration using FDT/DTM approach	813

INTRODUCTION

0.1 General

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

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

10 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.

15 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 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
20 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,
25 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.

30 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

35 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 are used in this document to describe device behavior:

- 40 • 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).
- 45 • 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).

5 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.

10 0.3 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

45 Email: standards@isa.org

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

ISBN: 978-1-936007-26-4

Copyright © 2009 by 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.

An ISA Standard

ISA100.11a-2009

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

1 Scope

10 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.

15 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;
- 20 • 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;
- 25 • 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

30 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.

35 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

40 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