

<b>STN</b>	<b>Priemyselné komunikačné siete. Bezdrôtová komunikačná sieť a komunikačné profily - ISA 100.11a.</b>	<b>STN EN 62734</b>  18 4022
------------	--	--

Industrial networks - Wireless communication network and communication profiles - ISA 100.11a

Táto norma obsahuje anglickú verziu európskej normy.  
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 06/15

Obsahuje: EN 62734:2015, IEC 62734:2014

**120874**

---

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, odbor SÚTN, 2015  
Podľa zákona č. 264/1999 Z. z. v znení neskorších predpisov sa môžu slovenské technické normy rozmnožovať a rozširovať iba so súhlasom Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

EUROPEAN STANDARD

**EN 62734**

NORME EUROPÉENNE

EUROPÄISCHE NORM

January 2015

ICS 25.040; 33.040; 35.100

English Version

**Industrial networks - Wireless communication network and  
communication profiles - ISA 100.11a  
(IEC 62734:2014)**

Réseaux industriels - Réseau de communication sans fil et  
profils de communication - ISA 100.11a  
(IEC 62734:2014)

Industrielle Kommunikationsnetze - Drahtlose  
Kommunikationsnetze und Kommunikationsprofile - ISA  
100.11a  
(IEC 62734:2014)

This European Standard was approved by CENELEC on 2014-12-02. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

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

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



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

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

## Foreword

The text of document 65C/778/FDIS, future edition 1 of IEC 62734, prepared by SC 65C "Industrial networks" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62734:2015.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2015-09-02
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2017-12-02

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

## Endorsement notice

The text of the International Standard IEC 62734:2014 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61158 Series	NOTE	Harmonized as EN 61158 Series.
IEC 61499-4:2005	NOTE	Harmonized as EN 61499-4:2006 <sup>1)</sup> (not modified).
IEC 61512-1	NOTE	Harmonized as EN 61512-1.
IEC 61804-3	NOTE	Harmonized as EN 61804-3.
IEC 62264-1:2013	NOTE	Harmonized as EN 62264-1:2013 (not modified).
IEC 62591	NOTE	Harmonized as EN 62591.
ISO 3166-1	NOTE	Harmonized as EN ISO 3166-1.

---

<sup>1)</sup> Superseded by EN 61499-4:2013 (IEC 61499-4:2013): DOW = 2016-03-06.

## Annex ZA (normative)

### Normative references to international publications with their corresponding European publications

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

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: [www.cenelec.eu](http://www.cenelec.eu)

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
ISO/IEC 646	-	Information technology; ISO 7-bit coded character set for information interchange	-	-
ISO/IEC 10731	-	Information technology - Open Systems Interconnection - Basic Reference Model - Conventions for the definition of OSI services	-	-
ISO/IEC 18033-3	-	Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers	-	-
ISO/IEC 19772	-	Information technology - Security techniques - Authenticated encryption	-	-
ANSI X 9.63	2011	Public Key Cryptography for Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography	-	-
IETF RFC 2460	1998	Internet Protocol - Version 6 (IPv6) - Specification	-	-
IETF RFC 2464	-	Transmission of IPv6 Packets over Ethernet Networks	-	-
IETF RFC 2529	-	Transmission of IPv6 over IPv4 Domains without Explicit Tunnels	-	-
IETF RFC 3168	-	The Addition of Explicit Congestion Notification (ECN) to IP	-	-
IETF RFC 4213	-	Basic Transition Mechanisms for IPv6 Hosts and Routers	-	-
IETF RFC 4291	2006	IP Version 6 Addressing Architecture	-	-
IETF RFC 4944	-	Transmission of IPv6 Packets over IEEE 802.15.4 Networks	-	-
IETF RFC 6282	2011	Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks	-	-
IETF RFC 6298	-	Computing TCP's Retransmission Timer	-	-

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEEE 802.15.4	2011	IEEE Standard for Local and metropolitan area networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANS)	-	-
SEC 1	2009	Elliptic Curve Cryptography, version 2		
SEC 4		Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV), version 0.97		



IEC 62734

Edition 1.0 2014-10

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE



---

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

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





**THIS PUBLICATION IS COPYRIGHT PROTECTED**  
**Copyright © 2014 IEC, Geneva, Switzerland**

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

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

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

Tel.: +41 22 919 02 11  
 Fax: +41 22 919 03 00  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)

#### About the IEC

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

#### About IEC publications

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

#### IEC Catalogue - [webstore.iec.ch/catalogue](http://webstore.iec.ch/catalogue)

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

#### IEC publications search - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

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

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

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

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

#### IEC Glossary - [std.iec.ch/glossary](http://std.iec.ch/glossary)

More than 55 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

#### IEC Customer Service Centre - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: [csc@iec.ch](mailto:csc@iec.ch).

#### A propos de l'IEC

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

#### A propos des publications IEC

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

#### Catalogue IEC - [webstore.iec.ch/catalogue](http://webstore.iec.ch/catalogue)

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

#### Recherche de publications IEC - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

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

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

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

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 14 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

#### Glossaire IEC - [std.iec.ch/glossary](http://std.iec.ch/glossary)

Plus de 55 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

#### Service Clients - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: [csc@iec.ch](mailto:csc@iec.ch).



IEC 62734

Edition 1.0 2014-10

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE



---

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

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

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

PRICE CODE **XH**  
CODE PRIX

---

ICS 25.040; 33.040; 35.100

ISBN 978-2-8322-1874-7

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



## CONTENTS

FOREWORD.....	31
0 Introduction .....	33
0.1 General.....	33
0.2 Document structure.....	33
0.3 Potentially relevant patents.....	33
1 Scope.....	35
2 Normative references .....	35
3 Terms, definitions, abbreviated terms, acronyms, and conventions.....	36
3.1 Terms and definitions.....	36
3.1.1 (N)-layer and other terms and definitions from the open systems interconnection Basic Reference Model .....	36
3.1.2 Other terms and definitions.....	45
3.1.3 Symbols for symmetric keys, and for asymmetric keys and certificates .....	63
3.1.4 Terms used to describe device behavior .....	64
3.2 Abbreviated terms and acronyms .....	65
3.3 Conventions.....	71
3.3.1 Service interfaces.....	71
3.3.2 Table cells.....	72
3.3.3 Italics.....	72
3.3.4 Bold face .....	73
3.3.5 Informal declarations of named constants .....	73
4 Overview .....	73
4.1 General.....	73
4.2 Interoperability and related issues .....	73
4.3 Quality of service .....	74
4.4 Worldwide applicability .....	74
4.5 Network architecture.....	74
4.5.1 Interfaces .....	74
4.5.2 Data structures .....	75
4.5.3 Network description .....	76
4.5.4 Generic protocol data unit construction.....	77
4.5.5 Abstract data and concrete representations .....	78
4.6 Network characteristics.....	80
4.6.1 General .....	80
4.6.2 Scalability.....	80
4.6.3 Extensibility .....	81
4.6.4 Simple operation .....	81
4.6.5 Site-license-exempt operation .....	81
4.6.6 Robustness in the presence of interference, including from other wireless systems .....	81
4.6.7 Determinism and contention-free media access .....	81
4.6.8 Self-organizing networking with support for redundancy .....	82
4.6.9 Internet-protocol-compatible NL.....	82
4.6.10 Coexistence with other radio frequency systems.....	82
4.6.11 Time-slotted assigned-channel D-transactions as the basis for communication .....	84

4.6.12	Robust and flexible security .....	86
4.6.13	System management .....	87
4.6.14	Application process using standard objects .....	87
4.6.15	Tunneling .....	87
5	System .....	87
5.1	General.....	87
5.2	Devices.....	88
5.2.1	General .....	88
5.2.2	Device interworkability.....	88
5.2.3	Profiles .....	88
5.2.4	Quality of service.....	88
5.2.5	Device worldwide applicability .....	88
5.2.6	Device description .....	89
5.2.7	Device addressing .....	93
5.2.8	Device phases .....	93
5.2.9	Device energy sources .....	95
5.3	Networks .....	95
5.3.1	General .....	95
5.3.2	Minimal network.....	95
5.3.3	Basic network topologies supported.....	96
5.3.4	Network configurations .....	99
5.3.5	Gateway, system manager, and security manager .....	104
5.4	Protocol suite structure .....	105
5.5	Data flow .....	106
5.5.1	General .....	106
5.5.2	Native communications.....	107
5.5.3	Basic data flow .....	107
5.5.4	Data flow between I/O devices.....	108
5.5.5	Data flow with legacy I/O device .....	108
5.5.6	Data flow with backbone.....	112
5.5.7	Data flow between I/O devices via backbone .....	112
5.5.8	Data flow to a standard-aware control system or device .....	112
5.6	Time reference.....	113
5.6.1	General .....	113
5.6.2	Time synchronization.....	114
5.7	Firmware upgrades .....	114
5.8	Wireless backbones and other infrastructures .....	114
6	System management role .....	114
6.1	General.....	114
6.1.1	Overview .....	114
6.1.2	Components and architecture .....	115
6.1.3	Management functions.....	116
6.2	DMAP .....	116
6.2.1	General .....	116
6.2.2	Architecture of device management.....	117
6.2.3	Definition of management objects .....	117
6.2.4	Management objects in DMAP.....	117
6.2.5	Communications services provided to device management objects.....	119
6.2.6	Attributes of management objects.....	120

6.2.7	Definitions of management objects in DMAP .....	121
6.2.8	Functions of device management and layer management .....	130
6.3	System manager .....	140
6.3.1	General .....	140
6.3.2	System management architecture .....	140
6.3.3	Standard system management object types .....	141
6.3.4	Security management .....	142
6.3.5	Addresses and address allocation .....	143
6.3.6	Firmware upgrade .....	147
6.3.7	System performance monitoring .....	148
6.3.8	Device provisioning service .....	149
6.3.9	Device management services .....	149
6.3.10	System time services .....	158
6.3.11	System communication configuration .....	162
6.3.12	Redundancy management .....	195
6.3.13	System management protocols .....	196
6.3.14	Management policies and policy administration .....	196
6.3.15	Operational interaction with plant operations or maintenance personnel .....	196
7	Security .....	196
7.1	General .....	196
7.2	Security services .....	197
7.2.1	Overview .....	197
7.2.2	Keys .....	198
7.3	PDU security .....	202
7.3.1	General .....	202
7.3.2	DPDU security .....	203
7.3.3	TL security functionality .....	218
7.4	Joining process .....	234
7.4.1	General .....	234
7.4.2	Prerequisites .....	234
7.4.3	Desired device end state and properties .....	235
7.4.4	Joining process steps common for symmetric-key and asymmetric-key approaches .....	235
7.4.5	Symmetric-key joining process .....	238
7.4.6	Asymmetric-key joining process .....	248
7.4.7	Joining process and device lifetime failure recovery .....	264
7.5	Session establishment .....	266
7.5.1	General .....	266
7.5.2	Description .....	266
7.5.3	Application protocol data unit protection using the master key .....	268
7.5.4	Proxy security management object methods related to the session establishment .....	268
7.6	Key update .....	271
7.6.1	General .....	271
7.6.2	Description .....	271
7.6.3	Device security management object methods related to T-key update .....	272
7.6.4	Failure recovery .....	276
7.7	Functionality of the security manager role .....	278
7.7.1	Proxy security management object .....	278

7.7.2	Authorization of network devices and generation or derivation of initial master keys .....	279
7.7.3	Interaction with device security management objects .....	279
7.7.4	Management of operational keys .....	279
7.8	Security policies.....	280
7.8.1	Definition of security policy .....	280
7.8.2	Policy extent.....	280
7.8.3	Unconstrained security policy choices .....	281
7.8.4	Policy structures .....	281
7.9	Security functions available to the AL .....	283
7.9.1	Parameters on transport service requests that relate to security .....	283
7.9.2	Direct access to cryptographic primitives .....	284
7.9.3	Symmetric-key cryptography.....	285
7.10	Security statistics collection, threat detection, and reporting .....	286
7.11	DSMO functionality .....	287
7.11.1	General .....	287
7.11.2	DSMO attributes .....	287
7.11.3	KeyDescriptor.....	288
7.11.4	DSMO alerts .....	293
8	Physical layer .....	294
8.1	General.....	294
8.2	Default physical layer.....	295
8.2.1	General requirements .....	295
8.2.2	Additional requirements of IEEE 802.15.4.....	295
8.2.3	Exceptions to the IEEE 802.15.4 physical layer .....	296
9	Data-link layer .....	296
9.1	General.....	296
9.1.1	Overview .....	296
9.1.2	Coexistence strategies in the DL .....	297
9.1.3	Allocation of digital bandwidth .....	297
9.1.4	Structure of the DPDU .....	298
9.1.5	The DL and the IEEE 802.15.4 MAC .....	298
9.1.6	Routes and graphs .....	299
9.1.7	Slotted-channel-hopping, slow-channel-hopping, and timeslots .....	306
9.1.8	Superframes .....	317
9.1.9	DL time keeping.....	329
9.1.10	D-subnet addressing.....	348
9.1.11	DL management service .....	349
9.1.12	Relationship between DLE and DSC .....	351
9.1.13	DLE neighbor discovery .....	352
9.1.14	Neighbor discovery and joining – DL considerations .....	355
9.1.15	Radio link control and quality measurement.....	360
9.1.16	DLE roles and options .....	365
9.1.17	DLE energy considerations .....	365
9.2	DDSAP .....	366
9.2.1	General .....	366
9.2.2	DD-DATA.request .....	366
9.2.3	DD-DATA.confirm .....	368
9.2.4	DD-DATA.indication .....	368

9.3	Data DPDU and ACK/NAK DPDU	369
9.3.1	General	369
9.3.2	Octet and bit ordering	370
9.3.3	Media access control headers	371
9.3.4	MAC acknowledgment DPDU	378
9.3.5	DL auxiliary subheader	381
9.4	DL management information base	396
9.4.1	General	396
9.4.2	DL management object attributes	396
9.4.3	DLMO attributes (indexed OctetStrings)	416
9.5	DLE methods	445
9.5.1	Method for synchronized cutover of DLE attributes	445
9.5.2	Methods to access indexed OctetString attributes	445
9.6	DL alerts	447
9.6.1	DL_Connectivity alert	447
9.6.2	NeighborDiscovery alert	449
10	Network layer	450
10.1	General	450
10.2	NL functionality overview	450
10.2.1	General	450
10.2.2	Addressing	451
10.2.3	Address translation	451
10.2.4	Network protocol data unit headers	453
10.2.5	Fragmentation and reassembly	453
10.2.6	Routing	456
10.2.7	Routing examples	462
10.3	NLE data services	470
10.3.1	General	470
10.3.2	N-DATA.request	471
10.3.3	N-DATA.confirm	472
10.3.4	N-DATA.indication	472
10.4	NL management object	473
10.4.1	NL management information base	473
10.4.2	Structured management information bases	477
10.4.3	NL management object methods	478
10.5	NPDU formats	481
10.5.1	General	481
10.5.2	Basic header format for NL	483
10.5.3	Contract-enabled network header format	484
10.5.4	Full header (IPv6) format	486
10.5.5	Fragmentation header format	488
11	Transport layer	489
11.1	General	489
11.2	TLE reference model	490
11.3	Transport security entity	490
11.3.1	General	490
11.3.2	Securing the TL	490
11.4	Transport data entity	491
11.4.1	General	491

11.4.2	UDP over IPv6.....	492
11.4.3	UDP header transmission and compression.....	492
11.4.4	TSAPs and UDP ports .....	495
11.4.5	Good network citizenship.....	496
11.5	TPDU encoding.....	496
11.5.1	General .....	496
11.5.2	Header compression – User datagram protocol encoding .....	496
11.5.3	TPDU security header.....	498
11.6	TL model .....	498
11.6.1	General .....	498
11.6.2	Data services.....	498
12	Application layer.....	507
12.1	General.....	507
12.2	Energy considerations .....	508
12.3	Legacy control system considerations.....	508
12.4	Overview of object-oriented modeling .....	509
12.4.1	General .....	509
12.4.2	Object-to-object communication concept.....	509
12.4.3	AL structure.....	510
12.4.4	UAP structure .....	510
12.5	Object model .....	511
12.6	Object attribute model.....	512
12.6.1	General .....	512
12.6.2	Attributes of standard objects .....	513
12.6.3	Attribute classification.....	513
12.6.4	Attribute accessibility.....	514
12.7	Method model .....	514
12.8	Alert model .....	515
12.9	Alarm state model.....	515
12.10	Event state model.....	516
12.10.1	General .....	516
12.10.2	State table and transitions .....	516
12.11	Alert reporting.....	517
12.11.1	General .....	517
12.11.2	Alert types .....	517
12.11.3	Alert report information .....	518
12.11.4	Alarm state recovery.....	519
12.12	Communication interaction model .....	519
12.12.1	General .....	519
12.12.2	Buffered unidirectional publication communication.....	519
12.12.3	Queued unidirectional communication .....	520
12.12.4	Queued bidirectional communication .....	520
12.12.5	Communication service contract .....	528
12.13	AL addressing.....	529
12.13.1	General .....	529
12.13.2	Object addressing.....	529
12.13.3	Object attribute addressing.....	530
12.13.4	Object attribute addressing.....	530
12.13.5	Object method addressing .....	532

12.14	Management objects .....	532
12.15	User objects .....	533
12.15.1	General .....	533
12.15.2	Industry-independent objects .....	533
12.16	Data types .....	566
12.16.1	Basic data types .....	566
12.16.2	Derived atomic data types .....	566
12.16.3	Industry-independent standard data structures .....	566
12.17	Application services provided by application sublayer .....	573
12.17.1	General .....	573
12.17.2	Publish/subscribe application communication model .....	574
12.17.3	Scheduled periodic buffered communication .....	575
12.17.4	Client/server interactions .....	580
12.17.5	Unscheduled acyclic queued unidirectional messages (source/sink) .....	596
12.17.6	Client/server and source/sink commonalities .....	603
12.18	AL flow use of lower layer services .....	609
12.18.1	General .....	609
12.18.2	AL use of TDSAPs .....	609
12.18.3	Mapping AL service primitives to TL service primitives .....	609
12.19	AL management .....	610
12.19.1	General .....	610
12.19.2	Application sublayer handling of malformed application protocol data units .....	610
12.19.3	Application sublayer management object attributes .....	611
12.19.4	Application sublayer management object methods .....	613
12.19.5	Application sublayer management object alerts .....	614
12.19.6	DMAP services invoked by application sublayer .....	615
12.19.7	Process industries standard objects .....	616
12.19.8	Factory automation industries profile .....	627
12.20	Process control industry standard data structures .....	628
12.20.1	General .....	628
12.20.2	Status for analog information .....	628
12.20.3	Value and status for analog information .....	629
12.20.4	Value and status for binary information .....	629
12.20.5	Process control mode .....	630
12.20.6	Scaling .....	631
12.21	Additional tables .....	631
12.21.1	Process control profile standard objects .....	631
12.21.2	Services .....	632
12.22	Coding .....	632
12.22.1	General .....	632
12.22.2	Coding rules for application protocol data units .....	632
12.22.3	Coding of application data .....	646
12.22.4	Time-related data types .....	653
12.23	Syntax .....	656
12.23.1	Application protocol data unit .....	656
12.23.2	Alert reports and acknowledgments .....	663
12.23.3	Service feedback code .....	665
12.23.4	Read, write, and execute .....	667

12.23.5	Tunnel .....	667
12.23.6	End of contained module .....	668
12.24	Detailed coding examples (informative).....	668
12.24.1	Read .....	668
12.24.2	Tunnel .....	668
13	Provisioning.....	669
13.1	General.....	669
13.2	Terms and definitions for devices with various roles or states .....	669
13.3	Provisioning procedures.....	671
13.4	Pre-installed symmetric keys .....	671
13.5	Provisioning using out-of-band mechanisms .....	672
13.6	Provisioning networks .....	672
13.6.1	General .....	672
13.6.2	Provisioning over-the-air using asymmetric cryptography.....	673
13.6.3	Provisioning over-the-air using an open symmetric join key .....	674
13.7	State transition diagrams .....	675
13.8	Device management application protocol objects used during provisioning .....	679
13.9	Management objects.....	682
13.9.1	Device provisioning object .....	682
13.9.2	Device provisioning object methods and alerts .....	687
13.10	Device provisioning service object .....	688
13.10.1	Device provisioning service object attributes .....	688
13.10.2	Device provisioning service object structured attributes .....	692
13.10.3	Device provisioning service object methods.....	694
13.10.4	Device provisioning service object alerts .....	695
13.10.5	Summary of attributes that can be provisioned .....	696
13.11	Provisioning functions (informative) .....	696
13.11.1	General .....	696
13.11.2	Examples of provisioning methods.....	697
Annex A (informative)	User layer/application profiles .....	700
A.1	Overview .....	700
A.2	User layer .....	700
A.3	Application profile .....	700
Annex B (normative)	Communication role profiles .....	702
B.1	Overview .....	702
B.1.1	General .....	702
B.1.2	Purpose.....	702
B.1.3	System size.....	702
B.1.4	Abbreviations and special symbols .....	702
B.1.5	Role profiles .....	702
B.2	System .....	703
B.3	System manager.....	703
B.4	Security manager.....	704
B.5	Physical layer .....	705
B.6	Data-link layer .....	705
B.6.1	General .....	705
B.6.2	Role profiles .....	706
B.7	Network layer.....	710
B.8	Transport layer .....	711



B.9	Application layer .....	711
B.10	Provisioning .....	712
B.11	Gateway (informative) .....	712
Annex C (informative) Background information .....		714
C.1	Industrial needs .....	714
C.2	Usage classes .....	714
C.2.1	General .....	714
C.2.2	Class examples .....	715
C.2.3	Other uploading and downloading alarms (human or automated action) .....	716
C.3	The Open Systems Interconnection Basic Reference Model .....	716
C.3.1	Overview .....	716
C.3.2	Application layer .....	717
C.3.3	Transport layer .....	718
C.3.4	Network layer .....	718
C.3.5	Data-link layer .....	718
C.3.6	Physical layer .....	718
Annex D (normative) Configuration defaults .....		720
D.1	General .....	720
D.2	System management .....	720
D.3	Security .....	721
D.4	Data-link layer .....	721
D.5	Network layer .....	723
D.6	Transport layer .....	723
D.7	Application layer .....	723
D.8	Provisioning .....	725
D.9	Gateway (informative) .....	726
Annex E (informative) Use of backbone networks .....		727
E.1	General .....	727
E.2	Recommended characteristics .....	727
E.3	Internet protocol backbones .....	727
E.3.1	Methods of IPv6 protocol data unit transmission .....	727
E.3.2	Backbone router peer device discovery .....	728
E.3.3	Security .....	728
Annex F (normative) Basic security concepts – Notation and representation .....		730
F.1	Strings and string operations .....	730
F.2	Integers, octets, and their representation .....	730
F.3	Entities .....	730
Annex G (informative) Using certificate chains for over-the-air provisioning .....		731
Annex H (normative) Security building blocks .....		732
H.1	Symmetric key cryptographic building blocks .....	732
H.1.1	Overview .....	732
H.1.2	Symmetric key domain parameters .....	732
H.1.3	Block cipher .....	732
H.1.4	Mode of operation .....	732
H.1.5	Cryptographic hash function .....	732
H.1.6	Keyed hash function for message authentication .....	732
H.1.7	Specialized keyed hash function for message authentication .....	733
H.1.8	Challenge domain parameters .....	733

H.2	Asymmetric-key cryptographic building blocks .....	733
H.2.1	General .....	733
H.2.2	Elliptic curve domain parameters .....	733
H.2.3	Elliptic curve point representation .....	733
H.2.4	Elliptic curve public-key pair .....	733
H.3	Keying information .....	733
H.3.1	General .....	733
H.3.2	Elliptic curve cryptography implicit certificates .....	734
H.3.3	Elliptic curve cryptography manual certificates.....	734
H.3.4	Additional information .....	735
H.4	Key agreement schemes.....	735
H.4.1	Symmetric-key key agreement scheme .....	735
H.4.2	Asymmetric-key key agreement scheme .....	735
H.5	Keying information schemes .....	735
H.5.1	Implicit certificate scheme .....	735
H.5.2	Manual certificate scheme .....	736
H.6	Challenge domain parameter generation and validation .....	736
H.6.1	Overview .....	736
H.6.2	Challenge domain parameter generation .....	736
H.6.3	Challenge domain parameter verification .....	736
H.7	Challenge validation primitive .....	737
H.8	Secret key generation (SKG) primitive .....	737
H.9	Block-cipher-based cryptographic hash function .....	738
H.10	Elliptic curve cryptography manual certificate scheme.....	739
H.10.1	Overview .....	739
H.10.2	Elliptic curve cryptography manual certificate generation transformation.....	740
H.10.3	Elliptic curve cryptography manual certificate processing transformation .....	740
Annex I (informative)	Definition templates .....	742
I.1	Object type template .....	742
I.2	Standard object attributes template.....	742
I.3	Standard object methods .....	743
I.4	Standard object alert reporting template .....	744
I.5	Data structure definition .....	745
Annex J (informative)	Operations on attributes.....	747
J.1	Operations on attributes.....	747
J.1.1	General .....	747
J.1.2	Attribute classification.....	747
J.1.3	Retrieving, setting, and resetting attributes.....	747
J.1.4	Retrieving and setting structured attributes.....	748
J.1.5	Resetting structured attribute values.....	750
J.1.6	Deleting structured attribute values .....	750
J.2	Synchronized cutover .....	751
Annex K (normative)	Standard object types .....	752
Annex L (informative)	Standard data types .....	757
Annex M (normative)	Identification of tunneled legacy fieldbus protocols .....	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.....	764
O.5	Server.....	765
Annex P (informative) Exemplary GIAP 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.12.1	General .....	767
P.12.2	Native access .....	767
P.12.3	Foreign access .....	768
P.13	Publish/subscribe.....	768
P.13.1	General .....	768
P.13.2	Native access .....	768
P.13.3	Foreign access .....	769
P.14	Bulk transfer .....	769
P.15	Alert.....	769
P.16	Gateway configuration .....	770
P.17	Device configuration .....	770
Annex Q (informative) Exemplary GIAP adaptations for IEC 62591 .....		771
Q.1	General.....	771
Q.1.1	Overview .....	771
Q.1.2	Reference.....	771
Q.1.3	Addressing .....	771
Q.1.4	Stack interface .....	771
Q.1.5	Tunneling .....	772
Q.1.6	Entities .....	772
Q.1.7	Delayed response.....	772
Q.2	Parameters .....	772
Q.3	Session.....	772
Q.4	Lease .....	773
Q.5	Device list report.....	773
Q.6	Topology report .....	773
Q.7	Schedule report .....	774
Q.8	Device health report.....	774

Q.9	Neighbor health report .....	775
Q.10	Network health report.....	775
Q.11	Time .....	776
Q.12	Client/server .....	776
Q.13	Publish/subscribe.....	777
Q.13.1	General .....	777
Q.13.2	Lease establishment.....	777
Q.13.3	Buffering.....	778
Q.14	Bulk transfer .....	778
Q.15	Alert.....	778
Q.16	Gateway configuration .....	779
Q.17	Device configuration .....	779
Annex R (informative)	Host system interface to standard-compliant devices via a gateway.....	780
R.1	Background .....	780
R.1.1	Host system integration reference model .....	780
R.1.2	Asset management tools .....	780
R.1.3	Configuration tools .....	780
R.1.4	Distributed control system .....	781
R.1.5	Gateway .....	781
R.2	Device application data integration with host systems .....	781
R.2.1	General .....	781
R.2.2	Native protocol integration via mapping .....	781
R.2.3	Legacy device protocol integration via tunneling .....	781
R.3	Host system configuration tool .....	781
R.3.1	General .....	781
R.3.2	Host configuration using electronic device description language .....	781
R.3.3	Host configuration using field device tool/device type manager.....	782
R.4	Field device/distributed control systems integration .....	783
R.4.1	General .....	783
R.4.2	Foundation Fieldbus High Speed Ethernet.....	783
R.4.3	Modbus .....	783
R.4.4	Open connectivity for industrial automation .....	783
R.5	Gateway .....	784
R.5.1	General .....	784
R.5.2	Devices supported.....	784
R.5.3	Data subscription.....	784
R.5.4	Data publication.....	784
R.5.5	Client/server access .....	784
R.5.6	Alerts reception .....	784
R.6	Asset management application support.....	784
R.6.1	General .....	784
R.6.2	Field device tool / device type manager .....	785
R.6.3	HART .....	785
R.6.4	OPC .....	785
Annex S (informative)	Symmetric-key operation test vectors .....	786
S.1	DPDU samples .....	786
S.1.1	General .....	786
S.1.2	DPDU with expected DMIC32 .....	786

S.1.3	DPDU with expected ENC-DMIC32 .....	786
S.2	TPDU samples .....	787
S.2.1	General .....	787
S.2.2	TPDU with expected ENC-TMIC-32: .....	787
S.2.3	TPDU with expected TMIC-32: .....	787
Annex T (informative)	Data-link and network headers for join requests .....	789
T.1	Overview .....	789
T.2	MAC header (MHR) .....	789
T.3	DL header (DHR) .....	789
T.4	NL header .....	790
Annex U (informative)	Gateway role .....	791
U.1	General .....	791
U.1.1	Overview .....	791
U.1.2	Notional gateway protocol suite diagrams for native devices and adapters .....	792
U.1.3	Gateway scenarios .....	792
U.1.4	Basic gateway model .....	794
U.2	Notional GIAP .....	795
U.2.1	Summary of interfaces and primitives .....	795
U.2.2	Sequence of primitives .....	798
U.2.3	Detailed description of parameters .....	803
U.2.4	Detailed description of interfaces .....	805
U.3	Example uses of WISN standard services and objects .....	839
U.3.1	Tunneling .....	839
U.3.2	Bulk transfer .....	852
U.3.3	Alerts .....	853
U.3.4	Native publish/subscribe and client/server access .....	855
U.3.5	Time management .....	856
U.3.6	Security .....	857
U.3.7	Configuration .....	857
U.3.8	Provisioning and joining .....	858
Annex V (informative)	Compliance with ETSI EN 300 328 v1.8.1 .....	859
Bibliography	.....	863
Figure 1	– Standard-compliant network .....	76
Figure 2	– Typical single-layer PDU without fragmenting or blocking .....	77
Figure 3	– Full multi-layer PDU structure used by this standard .....	77
Figure 4	– Physical devices versus roles .....	90
Figure 5	– Notional representation of device phases .....	94
Figure 6	– Simple star topology .....	96
Figure 7	– Simple hub-and-spoke topology .....	97
Figure 8	– Mesh topology .....	98
Figure 9	– Simple star-mesh topology .....	99
Figure 10	– Example where network and D-subnet overlap .....	100
Figure 11	– Example where network and D-subnet differ .....	101
Figure 12	– Network with multiple gateways .....	102
Figure 13	– Basic network with backup gateway .....	103

Figure 14 – Network with backbone .....	104
Figure 15 – Network with backbone – Device roles .....	105
Figure 16 – Reference model used by this standard.....	106
Figure 17 – Basic data flow.....	107
Figure 18 – Data flow between I/O devices .....	108
Figure 19 – Data flow with legacy I/O device.....	109
Figure 20 – Data flow with backbone-resident device.....	110
Figure 21 – Data flow between I/O devices via backbone subnet .....	111
Figure 22 – Data flow to standard-aware control system .....	112
Figure 23 – Management architecture .....	115
Figure 24 – DMAP .....	118
Figure 25 – Example of management SAP flow through standard protocol suite.....	120
Figure 26 – System manager architecture concept.....	141
Figure 27 – UAP-system manager interaction during contract establishment.....	163
Figure 28 – Contract-related interaction between DMO and SCO .....	166
Figure 29 – Contract source, destination, and intermediate devices .....	179
Figure 30 – Contract establishment example.....	188
Figure 31 – Contract ID usage in source .....	189
Figure 32 – Contract termination.....	193
Figure 33 – Contract modification with immediate effect.....	195
Figure 34 – Examples of DPDU and TPDU scope .....	197
Figure 35 – Keys and associated lifetimes .....	199
Figure 36 – Key lifetimes .....	201
Figure 37 – DPDU structure .....	204
Figure 38 – DLE and DLS processing for a D-transaction initiator .....	205
Figure 39 – Received DPDUs – DLE and DSC .....	207
Figure 40 – TPDU structure and protected coverage.....	219
Figure 41 – TMIC parameters .....	220
Figure 42 – TL and TSC interaction, outgoing TPDU.....	221
Figure 43 – TL and TSC interaction, incoming TPDU .....	222
Figure 44 – Example: Overview of the symmetric-key joining process .....	239
Figure 45 – Example: Overview of the symmetric-key joining process of a backbone device.....	240
Figure 46 – Asymmetric-key-authenticated key agreement scheme.....	250
Figure 47 – Example: Overview of the asymmetric-key joining process for a device with a DL.....	253
Figure 48 – Example: Overview of the asymmetric-key joining process of a backbone device.....	254
Figure 49 – Device state transitions for joining process and device lifetime .....	266
Figure 50 – High-level example of session establishment .....	267
Figure 51 – Key update protocol overview.....	272
Figure 52 – Device key establishment and key update state transition .....	278
Figure 53 – DL protocol suite and PhPDU/DPDU structure.....	298
Figure 54 – Graph routing example .....	301

Figure 55 – Inbound and outbound graphs .....	303
Figure 56 – Slotted-channel-hopping .....	307
Figure 57 – Slow-channel-hopping .....	308
Figure 58 – Hybrid operation.....	308
Figure 59 – Radio spectrum usage .....	309
Figure 60 – Predefined channel-hopping-pattern1 .....	311
Figure 61 – Two groups of DLEs with different channel-hopping-pattern-offsets.....	312
Figure 62 – Interleaved channel-hopping-pattern1 with sixteen different channel-hopping-pattern-offsets .....	313
Figure 63 – Example timeslot allocation for slotted-channel-hopping.....	314
Figure 64 – Example timeslot allocation for slow-channel-hopping .....	315
Figure 65 – Hybrid mode with slotted-channel-hopping and slow-channel-hopping.....	316
Figure 66 – Combining slow-channel-hopping and slotted-channel-hopping .....	316
Figure 67 – Example of a three-timeslot superframe and how it repeats.....	317
Figure 68 – Superframes and links.....	317
Figure 69 – Multiple superframes with aligned timeslots.....	318
Figure 70 – Example superframe for slotted-channel-hopping .....	322
Figure 71 – Example superframe for slow-channel-hopping .....	323
Figure 72 – Components of a slow-channel-hopping superframe.....	323
Figure 73 – Example configuration for avoiding collisions among routers .....	324
Figure 74 – Hybrid configuration .....	325
Figure 75 – Timeslot allocation and message queue .....	327
Figure 76 – 250 ms alignment intervals.....	330
Figure 77 – Timeslot durations and timing.....	331
Figure 78 – Clock source acknowledges receipt of a Data DPDU .....	336
Figure 79 – Transaction timing attributes .....	338
Figure 80 – Dedicated and shared transaction timeslots .....	339
Figure 81 – Unicast transaction .....	340
Figure 82 – PDU wait time (PWT) .....	343
Figure 83 – Duocast support in the standard.....	344
Figure 84 – Duocast transaction .....	345
Figure 85 – Shared timeslots with active CSMA/CA .....	346
Figure 86 – Transaction during slow-channel-hopping periods .....	347
Figure 87 – DL management SAP flow through standard protocol suite.....	350
Figure 88 – PhPDU and DPDU structure.....	369
Figure 89 – Typical ACK/NAK DPDU layout .....	378
Figure 90 – Relationship among DLMO indexed attributes .....	416
Figure 91 – Address translation process .....	453
Figure 92 – Fragmentation process.....	455
Figure 93 – Reassembly process .....	456
Figure 94 – Processing of an NSDU received from a TLE .....	458
Figure 95 – Processing of a received NPDU .....	459
Figure 96 – Processing of a NPDU received by a NLE from the backbone .....	461

Figure 97 – Delivery of a received NPDU at its final destination NLE .....	462
Figure 98 – Routing from a field device direct to a field-connected gateway without backbone routing .....	463
Figure 99 – Protocol suite diagram for routing from a field device direct to a field-connected gateway without backbone routing .....	464
Figure 100 – Routing an NPDU from a field device to a gateway via a backbone router .....	465
Figure 101 – Protocol suite diagram for routing an APDU from a field device to a gateway via a backbone router .....	466
Figure 102 – Routing from a field device on one D-subnet to another field device on a different D-subnet .....	467
Figure 103 – Protocol suite diagram for routing from an I/O device on one D-subnet to another I/O device on a different D-subnet .....	468
Figure 104 – Example of routing over an Ethernet backbone network .....	469
Figure 105 – Example of routing over a fieldbus backbone network .....	470
Figure 106 – Distinguishing between NPDU header formats .....	482
Figure 107 – TLE reference model .....	490
Figure 108 – UDP pseudo-header for IPv6 .....	492
Figure 109 – TPDU structure .....	496
Figure 110 – User application objects in a UAP .....	510
Figure 111 – Alarm state model .....	516
Figure 112 – Event model .....	517
Figure 113 – A successful example of multiple outstanding requests, with response concatenation .....	521
Figure 114 – An example of multiple outstanding unordered requests, with second write request initially unsuccessful .....	523
Figure 115 – An example of multiple outstanding ordered requests, with second write request initially unsuccessful .....	524
Figure 116 – Send window example 1, with current send window smaller than maximum send window .....	526
Figure 117 – Send window example 2, with current send window the same size as maximum send window, and non-zero usable send window width .....	526
Figure 118 – Send window example 3, with current send window the same size as maximum send window, and usable send window width of zero .....	527
Figure 119 – General addressing model .....	529
Figure 120 – UAP management object state diagram .....	536
Figure 121 – Alert report reception state diagram .....	538
Figure 122 – Alert-reporting example .....	538
Figure 123 – UploadDownload object download state diagram .....	555
Figure 124 – UploadDownload object upload state diagram .....	555
Figure 125 – Publish sequence of service primitives .....	576
Figure 126 – Client/server model two-part interactions .....	581
Figure 127 – Client/server model four-part interactions: Successful delivery .....	581
Figure 128 – Client/server model four-part interactions: Request delivery failure .....	582
Figure 129 – Client/server model four-part interactions: Response delivery failure .....	582
Figure 130 – AlertReport and AlertAcknowledge, delivery success .....	597
Figure 131 – AlertReport, delivery failure .....	597



Figure 132 – AlertReport, acknowledgment failure .....	598
Figure 133 – Concatenated response for multiple outstanding write requests (no message loss) .....	605
Figure 134 – Management and handling of malformed APDUs received from device X .....	611
Figure 135 – The provisioning network.....	673
Figure 136 – State transition diagrams outlining provisioning steps during a device lifecycle .....	675
Figure 137 – State transition diagram showing various paths to joining a secured network.....	678
Figure 138 – Provisioning objects and interactions .....	680
Figure C.1 – OSI Basic Reference Model.....	716
Figure O.1 – Generic protocol translation publish diagram .....	762
Figure O.2 – Generic protocol translation subscribe diagram .....	763
Figure O.3 – Generic protocol translation client/server transmission diagram.....	764
Figure O.4 – Generic protocol translation client/server reception diagram.....	765
Figure R.1 – Host integration reference model .....	780
Figure R.2 – Configuration using an electronic device definition.....	782
Figure R.3 – Configuration using FDT/DTM approach .....	783
Figure U.1 – Gateway scenarios .....	793
Figure U.2 – Basic gateway model.....	794
Figure U.3 – Internal sequence of primitives for session interface.....	798
Figure U.4 – Internal sequence of primitives for lease management interface .....	798
Figure U.5 – Internal sequence of primitives for system report interfaces.....	799
Figure U.6 – Internal sequence of primitives for time interface .....	799
Figure U.7 – Internal sequence of primitives for client/server interface initiated from gateway to an adapter device .....	800
Figure U.8 – Internal sequence of primitives for publish interface initiated from gateway to an adapter device .....	800
Figure U.9 – Internal sequence of primitives for subscribe interface initiated from an adapter device .....	801
Figure U.10 – Internal sequence of primitives for publisher timer initiated from gateway to an adapter device .....	801
Figure U.11 – Internal sequence of primitives for subscriber timers initiated from an adapter device .....	801
Figure U.12 – Internal sequence of primitives for the bulk transfer interface .....	802
Figure U.13 – Internal sequence of primitives for the alert subscription interface .....	802
Figure U.14 – Internal sequence of primitives for the alert notification interface .....	803
Figure U.15 – Internal sequence of primitives for gateway management interfaces .....	803
Figure U.16 – Tunnel object model .....	839
Figure U.17 – Distributed tunnel endpoints .....	840
Figure U.18 – Multicast, broadcast, and one-to-many messaging.....	841
Figure U.19 – Tunnel object buffering .....	842
Figure U.20 – Publish/subscribe publisher CoSt flowchart.....	845
Figure U.21 – Publish/subscribe publisher periodic flowchart.....	845
Figure U.22 – Publish/subscribe subscriber common periodic and CoSt flowchart.....	846
Figure U.23 – Network address mappings.....	847

Figure U.24 – Connection_Info usage in protocol translation.....	848
Figure U.25 – Transaction_Info usage in protocol translation.....	849
Figure U.26 – Interworkable tunneling mechanism overview diagram.....	850
Figure U.27 – Bulk transfer model.....	853
Figure U.28 – Alert model.....	854
Figure U.29 – Alert cascading.....	855
Figure U.30 – Native publish/subscribe and client/server access.....	856
Table 1 – Standard management object types in DMAP.....	118
Table 2 – Metadata_attribute data structure.....	121
Table 3 – Alert types for communication diagnostic category.....	123
Table 4 – Alert types for security alert category.....	123
Table 5 – Alert types for device diagnostic alert category.....	123
Table 6 – Alert types for process alert category.....	123
Table 7 – ARMO attributes (1 of 3).....	125
Table 8 – ARMO alerts.....	128
Table 9 – Alarm_Recovery method.....	129
Table 10 – DMO attributes (1 of 8).....	131
Table 11 – DMO alerts.....	139
Table 12 – System management object types.....	142
Table 13 – DSO attributes.....	144
Table 14 – Address_Translation_Row data structure.....	145
Table 15 – Read_Address_Row method.....	145
Table 16 – Input argument usage for Read_Address_Row method.....	147
Table 17 – Output argument usage for Read_Address_Row method.....	147
Table 18 – Attributes of SMO in system manager.....	149
Table 19 – Proxy_System_Manager_Join method.....	151
Table 20 – Proxy_System_Manager_Contract method.....	153
Table 21 – Effect of different join commands on attribute sets.....	155
Table 22 – Attributes of DMSO in the system manager.....	155
Table 23 – System_Manager_Join method.....	156
Table 24 – System_Manager_Contract method.....	158
Table 25 – Attributes of STSO in the system manager.....	162
Table 26 – Attributes of SCO in the system manager.....	165
Table 27 – SCO method for contract establishment, modification, or renewal (1 of 8).....	169
Table 28 – Input argument usage for SCO method for contract establishment, modification, or renewal.....	177
Table 29 – Output argument usage for SCO method for contract establishment, modification, or renewal.....	178
Table 30 – Contract_Data data structure (1 of 3).....	181
Table 31 – New_Device_Contract_Response data structure (1 of 2).....	185
Table 32 – SCO method for contract termination, deactivation and reactivation.....	191
Table 33 – DMO method to notify of contract termination.....	192
Table 34 – DMO method to notify of contract modification.....	194

Table 35 – Security levels.....	202
Table 36 – Structure of the security control field .....	202
Table 37 – Sec.DpduPrep.Request elements .....	208
Table 38 – Sec.DpduPrep.Response elements .....	209
Table 39 – Sec.DAckCheck.Request elements.....	209
Table 40 – Sec.DAckCheck.Response elements .....	210
Table 41 – Sec.DInitialCheck.Request elements .....	211
Table 42 – Sec.DInitialCheck.Response elements .....	212
Table 43 – Sec.DAckPrep.Request elements .....	213
Table 44 – Sec.DAckPrep.Response elements .....	214
Table 45 – Structure of the WISN DPDU nonce .....	215
Table 46 – Structure of the 32-bit truncated TAI time used in the D-nonce .....	215
Table 47 – TSC pseudo-header structure.....	220
Table 48 – Sec.TpduOutCheck.Request elements .....	223
Table 49 – Sec.TpduOutCheck.Response elements.....	223
Table 50 – Sec.TpduSecure.Request elements.....	224
Table 51 – Sec. TpduSecure.Response elements .....	225
Table 52 – Sec.TpduInCheck.Request elements .....	226
Table 53 – Sec.TpduInCheck.Response elements .....	227
Table 54 – Sec.TpduVerify.Request elements.....	228
Table 55 – Sec.TpduVerify.Response elements .....	229
Table 56 – Structure of TL security header .....	229
Table 57 – Structure of the TPDU nonce.....	230
Table 58 – Structure of 32-bit truncated nominal TAI time used in the T-nonce .....	230
Table 59 – Proxy_Security_Sym_Join method .....	242
Table 60 – Security_Sym_Join method .....	243
Table 61 – Security_Confirm method .....	243
Table 62 – Security_Sym_Join_Request data structure.....	244
Table 63 – Security_Sym_Join_Response data structure .....	245
Table 64 – Structure of compressed security level field.....	246
Table 65 – Master key security level .....	247
Table 66 – Security_Sym_Confirm data structure.....	247
Table 67 – Implicit certificate format .....	249
Table 68 – Usage_serial_number structure .....	249
Table 69 – Proxy_Security_Pub_Join method .....	256
Table 70 – Security_Pub_Join method .....	257
Table 71 – Proxy_Security_Pub_Confirm method .....	258
Table 72 – Security_Pub_Confirm method .....	258
Table 73 – Network_Information_Confirmation method .....	259
Table 74 – Format of asymmetric join request internal structure .....	260
Table 75 – Format of the protocol control field .....	260
Table 76 – Format of asymmetric join response internal structure.....	261
Table 77 – Format of first join confirmation internal structure .....	262

Table 78 – Format of join confirmation response internal structure.....	263
Table 79 – Joining process and device lifetime state machine .....	265
Table 80 – Security_New_Session method .....	268
Table 81 – Security_New_Session_Request data structure.....	269
Table 82 – Security_New_Session_Response data structure .....	270
Table 83 – New_Key method .....	273
Table 84 – Security_Key_and_Policies data structure .....	274
Table 85 – Security_Key_Update_Status data structure.....	276
Table 86 – T-key and D-key state transition .....	277
Table 87 – Attributes of PSMO in the system manager .....	278
Table 88 – Structure of policy field.....	281
Table 89 – Key_Type .....	281
Table 90 – Key_Usage.....	282
Table 91 – Granularity .....	282
Table 92 – DSMO attributes.....	287
Table 93 – KeyDescriptor.....	289
Table 94 – T-keyLookupData OctetString fields .....	290
Table 95 – Delete key method .....	291
Table 96 – Key_Policy_Update method.....	292
Table 97 – DSMO alerts.....	294
Table 98 – Timing requirements.....	295
Table 99 – Graph table on ND20.....	301
Table 100 – Graph table on ND21.....	301
Table 101 – Approximating nominal timing with 32 KiHz clock .....	332
Table 102 – DL_Config_Info structure.....	358
Table 103 – CountryCode .....	364
Table 104 – DD-DATA.request parameters .....	367
Table 105 – DD-DATA.confirm parameters.....	368
Table 106 – Value set for status parameter.....	368
Table 107 – DD-DATA.indication parameters .....	368
Table 108 – ExtDLUInt, one-octet variant.....	371
Table 109 – ExtDLUInt, two-octet variant .....	371
Table 110 – Data DPDU MHR.....	372
Table 111 – Data DPDU DHDR.....	374
Table 112 – Data DPDU DMXHR .....	374
Table 113 – DROUT structure, compressed variant .....	375
Table 114 – DROUT structure, uncompressed variant.....	376
Table 115 – DADDR structure.....	377
Table 116 – ACK/NAK DPDU MHR .....	378
Table 117 – ACK/NAK DPDU DHR .....	379
Table 118 – ACK/NAK DPDU DHDR .....	380
Table 119 – Advertisement DAUX structure .....	381
Table 120 – Advertisement selections elements.....	382

Table 121 – Advertisement selections.....	383
Table 122 – Advertisement time synchronization elements .....	383
Table 123 – Advertisement time synchronization structure .....	383
Table 124 – Join superframe information subfields .....	385
Table 125 – Join superframe information structure.....	385
Table 126 – Superframe derived from advertisement .....	386
Table 127 – Join information elements.....	387
Table 128 – Join information structure .....	387
Table 129 – Defaults for links created from advertisements .....	388
Table 130 – dlmo.Neighbor entry created from advertisements .....	389
Table 131 – dlmo.Graph entry created from advertisements.....	389
Table 132 – dlmo.Route entry created from advertisements .....	390
Table 133 – Solicitation header subfields.....	392
Table 134 – Solicitation header structure .....	393
Table 135 – Solicitation DAUX fields.....	393
Table 136 – Solicitation DAUX structure .....	393
Table 137 – Activate link DAUX fields .....	395
Table 138 – Activate link DAUX structure.....	395
Table 139 – Report received signal quality DAUX fields .....	395
Table 140 – Report received signal quality DAUX structure .....	396
Table 141 – DLMO attributes ( <i>1 of 7</i> ).....	396
Table 142 – D-subnet filter octets .....	406
Table 143 – dlmo.TaiAdjust OctetString fields.....	406
Table 144 – dlmo.TaiAdjust OctetString structure .....	407
Table 145 – dlmo.EnergyDesign OctetString fields.....	407
Table 146 – dlmo.EnergyDesign OctetString structure .....	407
Table 147 – dlmo.DeviceCapability OctetString fields .....	408
Table 148 – dlmo.DeviceCapability OctetString structure .....	408
Table 149 – dlmo.DiscoveryAlert fields .....	410
Table 150 – dlmo.DiscoveryAlert structure .....	410
Table 151 – dlmo.Candidates OctetString fields.....	411
Table 152 – dlmo.Candidates structure.....	412
Table 153 – dlmo.SmoothFactors OctetString fields.....	413
Table 154 – dlmo.SmoothFactors structure .....	413
Table 155 – dlmo.QueuePriority fields .....	414
Table 156 – dlmo.QueuePriority structure .....	414
Table 157 – dlmo.ChannelDiag fields.....	415
Table 158 – dlmo.ChannelDiag structure .....	416
Table 159 – dlmo.Ch fields .....	418
Table 160 – dlmo.Ch structure .....	418
Table 161 – Transaction receiver template fields .....	421
Table 162 – Transaction receiver template structure.....	421
Table 163 – Transaction initiator template fields .....	422

Table 164 – Transaction initiator template structure .....	422
Table 165 – Default transaction responder template, used during joining process .....	423
Table 166 – Default transaction initiator template, used during joining process .....	423
Table 167 – Default transaction responder template, used during joining process .....	424
Table 168 – dlmo.Neighbor fields .....	426
Table 169 – dlmo.Neighbor structure .....	427
Table 170 – ExtendGraph fields .....	428
Table 171 – ExtGraph structure .....	428
Table 172 – dlmo.NeighborDiagReset fields .....	429
Table 173 – dlmo.NeighborDiagReset structure .....	429
Table 174 – dlmo.Superframe fields .....	430
Table 175 – dlmo.Superframe structure .....	431
Table 176 – dlmo.Superframeldle fields .....	435
Table 177 – dlmo.Superframeldle structure .....	435
Table 178 – dlmo.Graph .....	436
Table 179 – dlmo.Graph structure .....	436
Table 180 – dlmo.Link fields .....	437
Table 181 – dlmo.Link structure .....	438
Table 182 – dlmo.Link[ ].Type structure .....	439
Table 183 – Allowed dlmo.Link[ ].Type combinations .....	440
Table 184 – Values for dlmo.Link[ ].Schedule .....	441
Table 185 – dlmo.Route fields .....	441
Table 186 – dlmo.Route structure .....	442
Table 187 – dlmo.NeighborDiag fields .....	443
Table 188 – Diagnostic summary OctetString fields .....	443
Table 189 – Diagnostic summary OctetString structure .....	444
Table 190 – Diagnostic ClockDetail OctetString fields .....	444
Table 191 – Diagnostic ClockDetail OctetString structure .....	445
Table 192 – Read_Row method .....	446
Table 193 – Write_Row method .....	446
Table 194 – Write_Row_Now method .....	447
Table 195 – dlmo.AlertPolicy fields .....	448
Table 196 – dlmo.AlertPolicy OctetString structure .....	448
Table 197 – DL_Connectivity alert .....	449
Table 198 – DL_Connectivity alert OctetString .....	449
Table 199 – NeighborDiscovery alert .....	450
Table 200 – Link-local address structure .....	451
Table 201 – Address translation table (ATT) .....	452
Table 202 – Example of a routing table .....	457
Table 203 – N-DATA.request elements .....	471
Table 204 – N-DATA.confirm elements .....	472
Table 205 – N-DATA.indication elements .....	473
Table 206 – NLMO attributes (1 of 3) .....	474

Table 207 – Contract table structure .....	477
Table 208 – Route table elements.....	478
Table 209 – Address translation table structure .....	478
Table 210 – NLMO structured MIB manipulation methods .....	480
Table 211 – Alert to indicate dropped PDU/PDU error.....	481
Table 212 – Common header patterns .....	483
Table 213 – Basic NL header format .....	483
Table 214 – Contract-enabled NL header format.....	485
Table 215 – 6LoWPAN_IPHC encoding format.....	485
Table 216 – IPv6 NL header format .....	486
Table 217 – Full NL header in the DL.....	487
Table 218 – NL header format for fragmented NPDU's .....	488
Table 219 – Format of first fragment header .....	488
Table 220 – Format of second and subsequent fragment headers.....	489
Table 221 – UDP header encoding .....	493
Table 222 – UDP 6LoWPAN_NHC-for-UDP encoding octet.....	497
Table 223 – Optimal UDP header encoding.....	497
Table 224 – UDP header encoding with checksum and compressed port numbers.....	498
Table 225 – T-DATA.request elements.....	499
Table 226 – T-DATA.confirm elements .....	500
Table 227 – T-DATA.confirm status codes .....	500
Table 228 – T-DATA.indication elements .....	501
Table 229 – TLMO attributes (1 of 2) .....	502
Table 230 – TL management object methods – Reset.....	504
Table 231 – TL management object methods – Halt.....	504
Table 232 – TL management object methods – PortRangeInfo.....	505
Table 233 – TL management object methods – GetPortInfo .....	505
Table 234 – TL management object methods – GetNextPortInfo .....	506
Table 235 – TL management object alert types – Illegal use of port.....	506
Table 236 – TL management object alert types – TPDU received on unregistered port .....	507
Table 237 – TL management object alert types – TPDU does not match security policies .....	507
Table 238 – State table for alarm transitions .....	515
Table 239 – State table for event transitions .....	516
Table 240 – UAP management object attributes (1 of 2) .....	534
Table 241 – State table for UAP management object .....	536
Table 242 – UAP management object methods .....	536
Table 243 – Alert-receiving object attributes .....	537
Table 244 – State table for handling an AlertReport reception.....	538
Table 245 – AlertReceiving object methods .....	539
Table 246 – UploadDownload object attributes (1 of 4).....	540
Table 247 – UploadDownload object methods.....	545
Table 248 – UploadDownload object StartDownload method.....	546

Table 249 – UploadDownload object DownloadData method .....	547
Table 250 – UploadDownload object EndDownload method .....	549
Table 251 – UploadDownload object StartUpload method .....	550
Table 252 – UploadDownload object UploadData method .....	551
Table 253 – UploadDownload object EndUpload method .....	552
Table 254 – Download state table for unicast operation mode (1 of 2) .....	553
Table 255 – Upload state table for unicast operation mode (1 of 2).....	556
Table 256 – Concentrator object attributes (1 of 2) .....	558
Table 257 – Concentrator object methods .....	559
Table 258 – Dispersion object attributes (1 of 2).....	560
Table 259 – Dispersion object methods .....	561
Table 260 – Tunnel object attributes (1 of 3).....	562
Table 261 – Tunnel object methods .....	564
Table 262 – Interface object attributes .....	565
Table 263 – Interface object methods .....	565
Table 264 – Data type: ObjectAttributeIndexAndSize .....	567
Table 265 – Data type: Communication association endpoint (1 of 2).....	568
Table 266 – Data type: Communication contract data .....	570
Table 267 – Data type: Alert communication endpoint.....	571
Table 268 – Data type: Tunnel endpoint.....	571
Table 269 – Data type: Alert report descriptor.....	572
Table 270 – Data type: Process control alarm report descriptor for analog with single reference condition .....	572
Table 271 – Data type: ObjectIDandType.....	573
Table 272 – Data type: UnscheduledCorrespondent.....	573
Table 273 – AL services .....	574
Table 274 – Publish service .....	578
Table 275 – Read service .....	584
Table 276 – Write service .....	589
Table 277 – Execute service .....	593
Table 278 – AlertReport service.....	599
Table 279 – AlertAcknowledge service.....	602
Table 280 – Tunnel service.....	606
Table 281 – Application flow characteristics.....	609
Table 282 – AL service primitive to TL service primitive mapping.....	610
Table 283 – ASLMO attributes (1 of 2).....	612
Table 284 – Application sublayer management object methods.....	613
Table 285 – Reset method .....	614
Table 286 – ASLMO alerts .....	615
Table 287 – Analog input object attributes .....	618
Table 288 – Analog input object methods.....	619
Table 289 – Analog input alerts .....	620
Table 290 – Analog output attributes (1 of 2) .....	621



Table 291 – Analog output object methods .....	622
Table 292 – Analog output alerts .....	623
Table 293 – Binary input object attributes .....	624
Table 294 – Binary input object methods .....	625
Table 295 – Binary input alerts .....	625
Table 296 – Binary output attributes .....	626
Table 297 – Binary output object methods .....	627
Table 298 – Binary output alerts .....	627
Table 299 – Status octet .....	629
Table 300 – Data type: Process control value and status for analog value .....	629
Table 301 – Data type: Process control value and status for binary value .....	630
Table 302 – Data type: Process control mode .....	630
Table 303 – Data type: Process control mode bitstring.....	630
Table 304 – Data type: Process control scaling.....	631
Table 305 – Process control standard objects.....	631
Table 306 – Services .....	632
Table 307 – Application messaging format.....	632
Table 308 – Concatenated APDUs in a single TSDU.....	633
Table 309 – Object addressing .....	633
Table 310 – Four-bit addressing mode APDU header construction.....	634
Table 311 – Eight-bit addressing mode APDU header construction .....	634
Table 312 – Sixteen-bit addressing mode APDU header construction .....	634
Table 313 – Inferred addressing use case example .....	635
Table 314 – Inferred addressing mode APDU header construction.....	635
Table 315 – Six-bit attribute identifier, not indexed .....	636
Table 316 – Six-bit attribute identifier, singly indexed, with 7-bit index.....	636
Table 317 – Six-bit attribute identifier, singly indexed, with 15-bit index.....	636
Table 318 – Six-bit attribute identifier, doubly indexed, with two 7-bit indices.....	637
Table 319 – Six-bit attribute identifier, doubly indexed, with two 15-bit indices.....	637
Table 320 – Six-bit attribute identifier, doubly indexed, with first index seven bits long and second index fifteen bits long.....	637
Table 321 – Six-bit attribute bit attribute identifier, doubly indexed, with first index fifteen bits long and second index seven bits long.....	637
Table 322 – Twelve-bit attribute identifier, not indexed .....	638
Table 323 – Twelve-bit attribute identifier, singly indexed with 7-bit index.....	638
Table 324 – Twelve-bit attribute identifier, singly indexed with 15-bit index.....	638
Table 325 – Twelve-bit attribute identifier, doubly indexed with two 7-bit indices.....	638
Table 326 – Twelve-bit attribute identifier, doubly indexed with two 15-bit indices.....	639
Table 327 – Twelve-bit attribute identifier, doubly indexed with first index 7 bits long and second index 15 bits long.....	639
Table 328 – Twelve-bit attribute identifier, doubly indexed with the first index 15 bits long and the second index 7 bits long .....	639
Table 329 – Twelve-bit attribute identifier, reserved form .....	639
Table 330 – Coding rules for read service request .....	640

Table 331 – Coding rules for read service response with 7-bit size field.....	640
Table 332 – Coding rules for read service response with 15-bit size field.....	640
Table 333 – Coding rules for write service request with 7-bit size field.....	641
Table 334 – Coding rules for write service request with 15-bit size field.....	641
Table 335 – Coding rules for write service response .....	641
Table 336 – Coding rules for execute service request with 7-bit size field .....	642
Table 337 – Coding rules for execute service request with 15-bit size field .....	642
Table 338 – Coding rules for execute service response with 7-bit size field .....	642
Table 339 – Coding rules for execute service response with 15-bit size field.....	643
Table 340 – Coding rules for tunnel service request with 7-bit size field.....	643
Table 341 – Coding rules for tunnel service request with 15-bit size field.....	643
Table 342 – Coding rules for tunnel service response with 7-bit size field .....	643
Table 343 – Coding rules for tunnel service response with 15-bit size field .....	644
Table 344 – Coding rules for AlertReport service with 7-bit associated-data size field.....	644
Table 345 – Coding rules for AlertReport service with 15-bit associated-data size field.....	644
Table 346 – Coding rules for AlertAcknowledge service .....	645
Table 347 – Coding rules for publish service for a native sequence of values .....	645
Table 348 – Coding rules for publish service – non-native (for tunnel support).....	645
Table 349 – Coding rules for concatenate service .....	645
Table 350 – General coding rule for size-invariant application data.....	646
Table 351 – General coding rule for size-varying application data of 0..255 octets.....	646
Table 352 – Coding rules for Unsigned8 .....	648
Table 353 – Coding rules for Unsigned16 .....	648
Table 354 – Coding rules for Unsigned32 .....	649
Table 355 – Coding rules for Unsigned64 .....	649
Table 356 – Coding rules for Unsigned128 .....	650
Table 357 – Coding rules for single-precision float.....	651
Table 358 – Coding rules for double-precision float .....	651
Table 359 – Coding rules for VisibleString .....	652
Table 360 – Coding rules for OctetString .....	652
Table 361 – Coding rules for BitString .....	653
Table 362 – Coding rules for TAINetworkTime, and for TAITimeDifference when interpreted as a modulo difference .....	654
Table 363 – Coding rules for TAITimeRounded.....	654
Table 364 – Coding example: Read request for a non-indexed attribute.....	668
Table 365 – Coding example: Read response for a non-indexed attribute .....	668
Table 366 – Coding example: Tunnel service request .....	668
Table 367 – Factory default settings .....	676
Table 368 – Device provisioning object (1 of 6).....	682
Table 369 – Reset_To_Default method .....	687
Table 370 – Write symmetric join key method .....	688
Table 371 – Device provisioning service object (1 of 4).....	689
Table 372 – DPSOWhiteListTbl data structure (1 of 2).....	693

Table 373 – Array manipulation table .....	695
Table 374 – DPSO alert to indicate join by a device not on the WhiteList .....	695
Table 375 – DPSO alert to indicate inadequate device join capability .....	696
Table B.1 – Protocol layer device roles .....	703
Table B.2 – Over-the-air upgrades .....	703
Table B.3 – Session support profiles .....	704
Table B.4 – Baseline profiles .....	705
Table B.5 – PhL roles .....	705
Table B.6 – DL required for listed roles .....	706
Table B.7 – Role profiles: General DLMO attributes .....	707
Table B.8 – Role profiles: dlmo.Device_Capability .....	707
Table B.9 – Role profiles: dlmo.Ch (channel-hopping) .....	708
Table B.10 – Role profiles: dlmo.TsTemplate .....	708
Table B.11 – Role profiles: dlmo.Neighbor .....	708
Table B.12 – Role profiles: dlmo.NeighborDiag .....	709
Table B.13 – Role profiles: dlmo.Superframe .....	709
Table B.14 – Role profiles: dlmo.Graph .....	709
Table B.15 – Role profiles: dlmo.Link .....	710
Table B.16 – Role profiles: dlmo.Route .....	710
Table B.17 – Role profiles: dlmo.Queue_Priority .....	710
Table B.18 – Routing table size .....	711
Table B.19 – Address table size .....	711
Table B.20 – Port support size .....	711
Table B.21 – APs .....	711
Table B.22 – Role profiles: I/O, routers, gateways, and backbone routers .....	712
Table B.23 – Role profile: Gateway .....	712
Table B.24 – Role profile: Gateway native access .....	712
Table B.25 – Role profile: Gateway interworkable tunnel mechanism .....	713
Table C.1 – Usage classes .....	715
Table D.1 – System management configuration defaults .....	720
Table D.2 – Security configuration defaults .....	721
Table D.3 – DLE configuration defaults .....	722
Table D.4 – NLE configuration defaults .....	723
Table D.5 – TLE configuration defaults .....	723
Table D.6 – ALE configuration defaults .....	724
Table D.7 – Provisioning configuration defaults .....	726
Table D.8 – Gateway configuration defaults .....	726
Table I.1 – Table of standard object types .....	742
Table I.2 – Template for standard object attributes .....	743
Table I.3 – Template for standard object methods .....	744
Table I.4 – Template for standard object alert reporting .....	745
Table I.5 – Template for data structures .....	746
Table J.1 – Scheduled_Write method template .....	748

Table J.2 – Read_Row method template .....	749
Table J.3 – Write_Row method template .....	749
Table J.4 – Reset_Row method template .....	750
Table J.5 – Delete_Row method template .....	751
Table K.1 – Standard object types .....	753
Table K.2 – Standard object instances .....	755
Table L.1 – Standard data types .....	757
Table M.1 – Identification of tunneled legacy fieldbus protocols .....	759
Table T.1 – Sample MHR for join request.....	789
Table T.2 – Sample DHR for join request.....	790
Table T.3 – Network header for join messages .....	790
Table U.1 – Summary of notional gateway high-side interface examples.....	796
Table U.2 – Primitive G_Session parameter usage .....	805
Table U.3 – GS_Status for G_Session confirm.....	807
Table U.4 – Primitive G_Lease parameter usage .....	808
Table U.5 – GS_Lease_Type for G_Lease request .....	809
Table U.6 – GS_Status for G_Lease confirm.....	810
Table U.7 – Primitive G_Device_List_Report parameter usage .....	811
Table U.8 – GS_Status for G_Device_List_Report confirm.....	812
Table U.9 – Primitive G_Topology_Report parameter usage .....	812
Table U.10 – Primitive G_Schedule_Report parameter usage .....	814
Table U.11 – Primitive G_Device_Health_Report parameter usage .....	816
Table U.12 – Primitive G_Neighbor_Health_Report parameter usage .....	817
Table U.13 – Primitive G_Network_Health_Report parameter usage.....	819
Table U.14 – Primitive G_Time parameter usage .....	821
Table U.15 – GS_Status for G_Time confirm .....	821
Table U.16 – Primitive G_Client_Server parameter usage.....	822
Table U.17 – GS_Status for G_Client_Server confirm .....	823
Table U.18 – Primitive G_Publish parameter usage .....	825
Table U.19 – GS_Status for G_Publish confirm.....	826
Table U.20 – Primitive G_Subscribe parameter usage .....	826
Table U.21 – GS_Status for G_Subscribe confirm.....	827
Table U.22 – Primitive G_Publish_Timer parameter usage.....	827
Table U.23 – Primitive G_Subscribe_Timer parameter usage.....	827
Table U.24 – Primitive G_Publish_Watchdog parameter usage .....	828
Table U.25 – Primitive G_Bulk_Open parameter usage.....	829
Table U.26 – GS_Status for G_Bulk_Open confirm .....	830
Table U.27 – Primitive G_Bulk_Transfer parameter usage .....	830
Table U.28 – GS_Status for G_Bulk_Transfer confirm .....	830
Table U.29 – Primitive G_Bulk_Close parameter usage .....	831
Table U.30 – Primitive G_Alert_Subscription parameter usage .....	832
Table U.31 – GS_Status for G_Alert_Subscription confirm.....	833
Table U.32 – Primitive G_Alert_Notification parameter usage .....	833

Table U.33 – Primitive G_Read_Gateway_Configuration parameter usage .....	834
Table U.34 – GS_Attribute_Identifier values for G_Read_Gateway_Configuration request .....	835
Table U.35 – Primitive G_Write_Gateway_Configuration parameter usage .....	835
Table U.36 – GS_Attribute_Identifier values for G_Write_Gateway_Configuration request .....	836
Table U.37 – GS_Status for G_Write_Gateway_Configuration confirm .....	836
Table U.38 – Primitive G_Write_Device_Configuration parameter usage .....	837
Table U.39 – GS_Status for G_Write_Device_Configuration confirm .....	838
Table U.40 – Primitive G_Read_Device_Configuration parameter usage .....	838
Table U.41 – Example of gateway configuration management attributes .....	858

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

---

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

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

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

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

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

This first edition cancels and replaces the IEC/PAS 62734 published in 2012. This edition constitutes a technical revision.

The text of this standard is based on the following documents:

FDIS	Report on voting
65C/778/FDIS	65C/788/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

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

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

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

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

## 0 Introduction

### 0.1 General

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

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

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

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

### 0.2 Document structure

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

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

### 0.3 Potentially relevant patents

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

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

---

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



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

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

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

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

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

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

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

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

## 1 Scope

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

This standard specifies the following:

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

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

## 2 Normative references

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

NOTE See the Bibliography for non-normative references.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IEEE 802.15.4™:2011<sup>2</sup>, *IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANS)*

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

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

**koniec náhľadu – text ďalej pokračuje v platenej verzii STN**

---

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