

# *The Internet of Things*

Key Applications and Protocols

OLIVIER HERSENT | DAVID BOSWARTHICK | OMAR ELLOUMI

 **WILEY**

**ETSI**  World Class Standards



# THE INTERNET OF THINGS



# THE INTERNET OF THINGS

## KEY APPLICATIONS AND PROTOCOLS

**Olivier Hersent**

*Actility, France*

**David Boswarthick**

*ETSI, France*

**Omar Elloumi**

*Alcatel-Lucent, France*



A John Wiley & Sons, Ltd., Publication

This edition first published 2012  
© 2012 John Wiley & Sons Ltd

*Registered office*

John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at [www.wiley.com](http://www.wiley.com).

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. 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, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

ETSI logo reproduced by kind permission of © ETSI, All Rights Reserved.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

*Library of Congress Cataloging-in-Publication Data*

Hersent, Olivier.

The internet of things : key applications and protocols / Olivier Hersent,  
David Boswarthick, Omar Elloumi.

p. cm.

Includes bibliographical references and index.

ISBN 978-1-119-99435-0 (hardback)

1. Intelligent buildings. 2. Smart power grids. 3. Sensor networks. I. Boswarthick, David.

II. Elloumi, Omar. III. Title.

TH6012.H47 2012

681'.2—dc23

2011037210

A catalogue record for this book is available from the British Library.

ISBN: 9781119994350 (H/B)

Typeset in 10.5/13pt Times by Aptara Inc., New Delhi, India

# Contents

<b>List of Acronyms</b>	<b>xv</b>
-------------------------	-----------

<b>Introduction</b>	<b>xxiii</b>
---------------------	--------------

## **Part I      M2M AREA NETWORK PHYSICAL LAYERS**

<b>1</b>	<b>IEEE 802.15.4</b>	<b>3</b>
1.1	The IEEE 802 Committee Family of Protocols	3
1.2	The Physical Layer	3
1.2.1	<i>Interferences with Other Technologies</i>	5
1.2.2	<i>Choice of a 802.15.4 Communication Channel, Energy Detection, Link Quality Information</i>	7
1.2.3	<i>Sending a Data Frame</i>	8
1.3	The Media-Access Control Layer	8
1.3.1	<i>802.15.4 Reduced Function and Full Function Devices, Coordinators, and the PAN Coordinator</i>	9
1.3.2	<i>Association</i>	12
1.3.3	<i>802.15.4 Addresses</i>	13
1.3.4	<i>802.15.4 Frame Format</i>	13
1.3.5	<i>Security</i>	14
1.4	Uses of 802.15.4	16
1.5	The Future of 802.15.4: 802.15.4e and 802.15.4g	17
1.5.1	<i>802.15.4e</i>	17
1.5.2	<i>802.15.4g</i>	21
<b>2</b>	<b>Powerline Communication for M2M Applications</b>	<b>23</b>
2.1	Overview of PLC Technologies	23
2.2	PLC Landscape	23
2.2.1	<i>The Historical Period (1950–2000)</i>	24
2.2.2	<i>After Year 2000: The Maturity of PLC</i>	24

2.3	Powerline Communication: A Constrained Media	27
2.3.1	<i>Powerline is a Difficult Channel</i>	27
2.3.2	<i>Regulation Limitations</i>	27
2.3.3	<i>Power Consumption</i>	32
2.3.4	<i>Lossy Network</i>	33
2.3.5	<i>Powerline is a Shared Media and Coexistence is not an Optional Feature</i>	35
2.4	The Ideal PLC System for M2M	37
2.4.1	<i>Openness and Availability</i>	38
2.4.2	<i>Range</i>	38
2.4.3	<i>Power Consumption</i>	38
2.4.4	<i>Data Rate</i>	39
2.4.5	<i>Robustness</i>	39
2.4.6	<i>EMC Regulatory Compliance</i>	40
2.4.7	<i>Coexistence</i>	40
2.4.8	<i>Security</i>	40
2.4.9	<i>Latency</i>	40
2.4.10	<i>Interoperability with M2M Wireless Services</i>	40
2.5	Conclusion	40
	References	41

## **Part II    LEGACY M2M PROTOCOLS FOR SENSOR NETWORKS, BUILDING AUTOMATION AND HOME AUTOMATION**

<b>3</b>	<b>The BACnet™ Protocol</b>	<b>45</b>
3.1	Standardization	45
3.1.1	<i>United States</i>	46
3.1.2	<i>Europe</i>	46
3.1.3	<i>Interworking</i>	46
3.2	Technology	46
3.2.1	<i>Physical Layer</i>	47
3.2.2	<i>Link Layer</i>	47
3.2.3	<i>Network Layer</i>	47
3.2.4	<i>Transport and Session Layers</i>	49
3.2.5	<i>Presentation and Application Layers</i>	49
3.3	BACnet Security	55
3.4	BACnet Over Web Services (Annex N, Annex H6)	55
3.4.1	<i>The Generic WS Model</i>	56
3.4.2	<i>BACnet/WS Services</i>	58
3.4.3	<i>The Web Services Profile for BACnet Objects</i>	59
3.4.4	<i>Future Improvements</i>	59



<b>4</b>	<b>The LonWorks® Control Networking Platform</b>	<b>61</b>
4.1	Standardization	61
4.1.1	<i>United States of America</i>	61
4.1.2	<i>Europe</i>	62
4.1.3	<i>China</i>	62
4.2	Technology	62
4.2.1	<i>Physical Layer</i>	63
4.2.2	<i>Link Layer</i>	64
4.2.3	<i>Network Layer</i>	65
4.2.4	<i>Transport Layer</i>	66
4.2.5	<i>Session Layer</i>	67
4.2.6	<i>Presentation Layer</i>	67
4.2.7	<i>Application Layer</i>	71
4.3	Web Services Interface for LonWorks Networks: Echelon SmartServer	72
4.4	A REST Interface for LonWorks	73
4.4.1	<i>LonBridge REST Transactions</i>	74
4.4.2	<i>Requests</i>	74
4.4.3	<i>Responses</i>	75
4.4.4	<i>LonBridge REST Resources</i>	75
<b>5</b>	<b>ModBus</b>	<b>79</b>
5.1	Introduction	79
5.2	ModBus Standardization	80
5.3	ModBus Message Framing and Transmission Modes	80
5.4	ModBus/TCP	81
<b>6</b>	<b>KNX</b>	<b>83</b>
6.1	The Konnex/KNX Association	83
6.2	Standardization	83
6.3	KNX Technology Overview	84
6.3.1	<i>Physical Layer</i>	84
6.3.2	<i>Data Link and Routing Layers, Addressing</i>	87
6.3.3	<i>Transport Layer</i>	89
6.3.4	<i>Application Layer</i>	89
6.3.5	<i>KNX Devices, Functional Blocks and Interworking</i>	89
6.4	Device Configuration	92
<b>7</b>	<b>ZigBee</b>	<b>93</b>
7.1	Development of the Standard	93
7.2	ZigBee Architecture	94

7.2.1	<i>ZigBee and 802.15.4</i>	94
7.2.2	<i>ZigBee Protocol Layers</i>	94
7.2.3	<i>ZigBee Node Types</i>	96
7.3	<i>Association</i>	96
7.3.1	<i>Forming a Network</i>	96
7.3.2	<i>Joining a Parent Node in a Network Using 802.15.4 Association</i>	97
7.3.3	<i>Using NWK Rejoin</i>	99
7.4	<i>The ZigBee Network Layer</i>	99
7.4.1	<i>Short-Address Allocation</i>	99
7.4.2	<i>Network Layer Frame Format</i>	100
7.4.3	<i>Packet Forwarding</i>	101
7.4.4	<i>Routing Support Primitives</i>	101
7.4.5	<i>Routing Algorithms</i>	102
7.5	<i>The ZigBee APS Layer</i>	105
7.5.1	<i>Endpoints, Descriptors</i>	106
7.5.2	<i>The APS Frame</i>	106
7.6	<i>The ZigBee Device Object (ZDO) and the ZigBee Device Profile (ZDP)</i>	109
7.6.1	<i>ZDP Device and Service Discovery Services (Mandatory)</i>	109
7.6.2	<i>ZDP Network Management Services (Mandatory)</i>	110
7.6.3	<i>ZDP Binding Management Services (Optional)</i>	111
7.6.4	<i>Group Management</i>	111
7.7	<i>ZigBee Security</i>	111
7.7.1	<i>ZigBee and 802.15.4 Security</i>	111
7.7.2	<i>Key Types</i>	113
7.7.3	<i>The Trust Center</i>	114
7.7.4	<i>The ZDO Permissions Table</i>	116
7.8	<i>The ZigBee Cluster Library (ZCL)</i>	116
7.8.1	<i>Cluster</i>	116
7.8.2	<i>Attributes</i>	117
7.8.3	<i>Commands</i>	117
7.8.4	<i>ZCL Frame</i>	117
7.9	<i>ZigBee Application Profiles</i>	119
7.9.1	<i>The Home Automation (HA) Application Profile</i>	119
7.9.2	<i>ZigBee Smart Energy 1.0 (ZSE or AMI)</i>	122
7.10	<i>The ZigBee Gateway Specification for Network Devices</i>	129
7.10.1	<i>The ZGD</i>	130
7.10.2	<i>GRIP Binding</i>	131
7.10.3	<i>SOAP Binding</i>	132
7.10.4	<i>REST Binding</i>	132
7.10.5	<i>Example IPHA–ZGD Interaction Using the REST Binding</i>	134

<b>8</b>	<b>Z-Wave</b>	<b>139</b>
8.1	History and Management of the Protocol	139
8.2	The Z-Wave Protocol	140
8.2.1	<i>Overview</i>	140
8.2.2	<i>Z-Wave Node Types</i>	140
8.2.3	<i>RF and MAC Layers</i>	142
8.2.4	<i>Transfer Layer</i>	143
8.2.5	<i>Routing Layer</i>	145
8.2.6	<i>Application Layer</i>	148

### **Part III LEGACY M2M PROTOCOLS FOR UTILITY METERING**

<b>9</b>	<b>M-Bus and Wireless M-Bus</b>	<b>155</b>
9.1	Development of the Standard	155
9.2	M-Bus Architecture	156
9.2.1	<i>Physical Layer</i>	156
9.2.2	<i>Link Layer</i>	156
9.2.3	<i>Network Layer</i>	157
9.2.4	<i>Application Layer</i>	158
9.3	Wireless M-Bus	160
9.3.1	<i>Physical Layer</i>	160
9.3.2	<i>Data-Link Layer</i>	162
9.3.3	<i>Application Layer</i>	162
9.3.4	<i>Security</i>	163
<b>10</b>	<b>The ANSI C12 Suite</b>	<b>165</b>
10.1	Introduction	165
10.2	C12.19: The C12 Data Model	166
10.2.1	<i>The Read and Write Minimum Services</i>	167
10.2.2	<i>Some Remarkable C12.19 Tables</i>	167
10.3	C12.18: Basic Point-to-Point Communication Over an Optical Port	168
10.4	C12.21: An Extension of C12.18 for Modem Communication	169
10.4.1	<i>Interactions with the Data-Link Layer</i>	170
10.4.2	<i>Modifications and Additions to C12.19 Tables</i>	171
10.5	C12.22: C12.19 Tables Transport Over Any Networking Communication System	171
10.5.1	<i>Reference Topology and Network Elements</i>	171
10.5.2	<i>C12.22 Node to C12.22 Network Communications</i>	173
10.5.3	<i>C12.22 Device to C12.22 Communication Module Interface</i>	174
10.5.4	<i>C12.19 Updates</i>	176

10.6	Other Parts of ANSI C12 Protocol Suite	176
10.7	RFC 6142: C12.22 Transport Over an IP Network	176
10.8	REST-Based Interfaces to C12.19	177
<b>11</b>	<b>DLMS/COSEM</b>	<b>179</b>
11.1	DLMS Standardization	179
11.1.1	<i>The DLMS UA</i>	179
11.1.2	<i>DLMS/COSEM, the Colored Books</i>	179
11.1.3	<i>DLMS Standardization in IEC</i>	180
11.2	The COSEM Data Model	181
11.3	The Object Identification System (OBIS)	182
11.4	The DLMS/COSEM Interface Classes	184
11.4.1	<i>Data-Storage ICs</i>	185
11.4.2	<i>Association ICs</i>	185
11.4.3	<i>Time- and Event-Bound ICs</i>	186
11.4.4	<i>Communication Setup Channel Objects</i>	186
11.5	Accessing COSEM Interface Objects	186
11.5.1	<i>The Application Association Concept</i>	186
11.5.2	<i>The DLMS/COSEM Communication Framework</i>	187
11.5.3	<i>The Data Communication Services of COSEM Application Layer</i>	189
11.6	End-to-End Security in the DLMS/COSEM Approach	191
11.6.1	<i>Access Control Security</i>	191
11.6.2	<i>Data-Transport Security</i>	192

## Part IV THE NEXT GENERATION: IP-BASED PROTOCOLS

<b>12</b>	<b>6LoWPAN and RPL</b>	<b>195</b>
12.1	Overview	195
12.2	What is 6LoWPAN? 6LoWPAN and RPL Standardization	195
12.3	Overview of the 6LoWPAN Adaptation Layer	196
12.3.1	<i>Mesh Addressing Header</i>	197
12.3.2	<i>Fragment Header</i>	198
12.3.3	<i>IPv6 Compression Header</i>	198
12.4	Context-Based Compression: IPHC	200
12.5	RPL	202
12.5.1	<i>RPL Control Messages</i>	204
12.5.2	<i>Construction of the DODAG and Upward Routes</i>	204
12.6	Downward Routes, Multicast Membership	206
12.7	Packet Routing	207
12.7.1	<i>RPL Security</i>	208

<b>13</b>	<b>ZigBee Smart Energy 2.0</b>	<b>209</b>
13.1	REST Overview	209
13.1.1	<i>Uniform Interfaces, REST Resources and Resource Identifiers</i>	209
13.1.2	<i>REST Verbs</i>	210
13.1.3	<i>Other REST Constraints, and What is REST After All?</i>	211
13.2	ZigBee SEP 2.0 Overview	212
13.2.1	<i>ZigBee IP</i>	213
13.2.2	<i>ZigBee SEP 2.0 Resources</i>	214
13.3	Function Sets and Device Types	217
13.3.1	<i>Base Function Set</i>	218
13.3.2	<i>Group Enrollment</i>	221
13.3.3	<i>Meter</i>	223
13.3.4	<i>Pricing</i>	223
13.3.5	<i>Demand Response and Load Control Function Set</i>	224
13.3.6	<i>Distributed Energy Resources</i>	227
13.3.7	<i>Plug-In Electric Vehicle</i>	227
13.3.8	<i>Messaging</i>	230
13.3.9	<i>Registration</i>	231
13.4	ZigBee SE 2.0 Security	232
13.4.1	<i>Certificates</i>	232
13.4.2	<i>IP Level Security</i>	232
13.4.3	<i>Application-Level Security</i>	235
<b>14</b>	<b>The ETSI M2M Architecture</b>	<b>237</b>
14.1	Introduction to ETSI TC M2M	237
14.2	System Architecture	238
14.2.1	<i>High-Level Architecture</i>	238
14.2.2	<i>Reference Points</i>	239
14.2.3	<i>Service Capabilities</i>	240
14.3	ETSI M2M SCL Resource Structure	242
14.3.1	<i>SCL Resources</i>	244
14.3.2	<i>Application Resources</i>	244
14.3.3	<i>Access Right Resources</i>	248
14.3.4	<i>Container Resources</i>	248
14.3.5	<i>Group Resources</i>	250
14.3.6	<i>Subscription and Notification Channel Resources</i>	251
14.4	ETSI M2M Interactions Overview	252
14.5	Security in the ETSI M2M Framework	252
14.5.1	<i>Key Management</i>	252
14.5.2	<i>Access Lists</i>	254

14.6	Interworking with Machine Area Networks	255
14.6.1	<i>Mapping M2M Networks to ETSI M2M Resources</i>	256
14.6.2	<i>Interworking with ZigBee 1.0</i>	257
14.6.3	<i>Interworking with C.12</i>	262
14.6.4	<i>Interworking with DLMS/COSEM</i>	264
14.7	Conclusion on ETSI M2M	266

## **Part V KEY APPLICATIONS OF THE INTERNET OF THINGS**

<b>15</b>	<b>The Smart Grid</b>	<b>271</b>
15.1	Introduction	271
15.2	The Marginal Cost of Electricity: Base and Peak Production	272
15.3	Managing Demand: The Next Challenge of Electricity Operators . . . and Why M2M Will Become a Key Technology	273
15.4	Demand Response for Transmission System Operators (TSO)	274
15.4.1	<i>Grid-Balancing Authorities: The TSOs</i>	274
15.4.2	<i>Power Shedding: Who Pays What?</i>	276
15.4.3	<i>Automated Demand Response</i>	277
15.5	Case Study: RTE in France	277
15.5.1	<i>The Public-Network Stabilization and Balancing Mechanisms in France</i>	277
15.5.2	<i>The Bidding Mechanisms of the Tertiary Adjustment Reserve</i>	281
15.5.3	<i>Who Pays for the Network-Balancing Costs?</i>	283
15.6	The Opportunity of Smart Distributed Energy Management	285
15.6.1	<i>Assessing the Potential of Residential and Small-Business Power Shedding (Heating/Cooling Control)</i>	286
15.6.2	<i>Analysis of a Typical Home</i>	287
15.6.3	<i>The Business Case</i>	293
15.7	Demand Response: The Big Picture	300
15.7.1	<i>From Network Balancing to Peak-Demand Suppression</i>	300
15.7.2	<i>Demand Response Beyond Heating Systems</i>	304
15.8	Conclusion: The Business Case of Demand Response and Demand Shifting is a Key Driver for the Deployment of the Internet of Things	305
<b>16</b>	<b>Electric Vehicle Charging</b>	<b>307</b>
16.1	Charging Standards Overview	307
16.1.1	<i>IEC Standards Related to EV Charging</i>	310
16.1.2	<i>SAE Standards</i>	317
16.1.3	<i>J2293</i>	318
16.1.4	<i>CAN – Bus</i>	319

16.1.5	<i>J2847: The New “Recommended Practice” for High-Level Communication Leveraging the ZigBee Smart Energy Profile 2.0</i>	320
16.2	Use Cases	321
16.2.1	<i>Basic Use Cases</i>	321
16.2.2	<i>A More Complex Use Case: Thermal Preconditioning of the Car</i>	323
16.3	Conclusion	324
<b>Appendix A</b>	<b>Normal Aggregate Power Demand of a Set of Identical Heating Systems with Hysteresis</b>	<b>327</b>
<b>Appendix B</b>	<b>Effect of a Decrease of <math>T_{\text{ref}}</math>. The Danger of Correlation</b>	<b>329</b>
<b>Appendix C</b>	<b>Changing <math>T_{\text{ref}}</math> without Introducing Correlation</b>	<b>331</b>
C.1	Effect of an Increase of $T_{\text{ref}}$	331
<b>Appendix D</b>	<b>Lower Consumption, A Side Benefit of Power Shedding</b>	<b>333</b>
<b>Index</b>		<b>337</b>





# List of Acronyms

6LoWPAN	6LoWPAN is the acronym of IPv6 over Low power Wireless Personal Area Networks and the name of a working group in IETF
ACL	Access Control List
ACSE	Association Control Service Element
AER	All Electric Range
AFE	Analog Front End
AIB	Application Layer Information Base
AIS	Application Interworking Specification
AMI	Automatic Metering Infrastructure
ANSI	American National Standards Institute
AODV	Advanced Ad-Hoc On-Demand Distance Vectoring
AP	Application Process
APDU	Application Protocol Data Unit
API	Application Programming Interface
aPoC	Application Point of Contact
APS	Application Support Sublayer
APSDE-SAP	Application Support Sublayer Data Entity Service Access Point
APSME-SAP	Application Support Sublayer Management Entity Service Access Point
APSSE-SAP	Application Support Sublayer Security Entity Service Access Point
ARIB	Association of Radio Industries and Businesses is a standardization organization in Japan
ASDU	Aps Service Data Unit
ASK	Amplitude-Shift Keying
BbC	KNX Backbone Controller
BCI	Batibus Club International
BEV	Battery Electric Vehicle
BO	Beacon Order
BPSK	Binary Phase Shift Keying
BTT	Broadcast Transaction Table

CAN	Controller Area Network
CAP	Contention Access Period
CBC MAC	CBC Message Authentication Code
CC	Consistency Check
CCA	Clear Channel Assessment
CCM*	Extension of Counter with CBC-MAC Mode of Operation
CD range	Charge Depleting Range
CENELEC	European Committee for Electrotechnical Standardization
CER	Communication Error Rate
CFP	Contention Free Period
CI	Control Information
CNF	M-Bus CONFIRM Message
CRC	Cyclical Redundancy Check
CRL	X.509 Certificate Revocation List
CRUD	Create, Read, Update, Delete
CS mode	Charge Sustaining Mode
CSL	Coordinated Sampled Listening
CSMA	Carrier-Sense, Multiple Access
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection
D device	ETSI M2M device without local M2M capabilities and interfaced to a gateway via the mId interface
D' device	ETSI M2M device implementing ETSI M2M capabilities and the mId interface to the network domain (does not interface via a gateway)
DA	Device Application
DAG	Direct Acyclic Graph
DAG root	A Node within the DAG that has no outgoing edge
DAO	Destination Advertisement Object
DER	Distinguished Encoding Rule
dIa	ETSI M2M Reference point between an application and ETSI M2M service capabilities
DIB	Data Information Block
DIO	DODAG Information Object
DIS	DODAG Information Solicitation
DLL	Data Link Layer the layer 2 specified in the seven-layer OSI model
DLMS	Device Language Message Specification is a specification for Data exchange for meter reading, tariff and load control
DODAG	Oriented Direct Acyclic Graph
DODAG Version	Specific iteration (“Version”) of a DODAG with a given DODAGID
DODAGID	The identifier of a DODAG Root
DR	Demand Response

DRH	Data Record Header
DSSS	Direct Spread Spectrum Destination
DTSN	Destination Advertisement Trigger Sequence Number
ED	Energy Detection
EFF	Extended Frame Format
EHS	European Home System
EIB	European Installation Bus
EIBA	The European Installation Bus Association
EMC	Electromagnetic Compatibility
EMS	Energy Management System
EN 50065-1	CENELEC standard for Powerline transmission on low-voltage electrical installations in the frequency range 3 to 148,5 kHz
EP	Enforcement Point
EPID	Extended PAN ID
ESI	Energy Services Interface
ESP	Energy Service Portal
eTag	Entity Tag
ETSI	European Telecommunications Standards Institute is an independent, nonprofit, standardization organization in the telecommunications industry
ETSI PLT	The ETSI Powerline working group
EUI	Extended Unique Identifier
EV	Electric Vehicle
EVCC	Electric Vehicle Communication Controller
EVSE	Electric Vehicle Charging Equipment
EXI	Efficient XML Interchange Encoding
FCC	Federal Communications Commission
FFD	Full Function Device
FHSS	Frequency Hopping Spread Spectrum
FLiRS	Frequently Listening Routing Slave
FSK	Frequency-shift keying is a frequency modulation scheme in which digital information is transmitted through discrete frequency changes of a carrier wave
GA	Gateway Application
GBA	Generic Bootstrapping Architecture
GCM	Galois/Counter Mode
GMO	Gateway Management Object
GO	Group Object
GRE	Gestionnaire de réseau de transport
GRIP	Gateway Remote Interface Protocol
HC	Header Compression
HEV	Hybrid Electric Vehicle

HLS	High-Level Security
HomePlug Alliance	The HomePlug Alliance is a group of electronics manufacturers, service providers, and retailers that establishes standards for power line communication
IANA	Internet Assigned Number Authority
I-Band	Industrial Band, see ISM
IC	Interface Class
IEC TC13	International Electrotechnical Commission, Technical Committee 13
IEEE	The Institute of Electrical and Electronics Engineers
IEEE 1901	IEEE 1901 is an IEEE working group developing a global standard for high speed Powerline communications
IEEE 802.15.4	IEEE 802.15.4-2006 is a standard that specifies the physical layer and media access control for low-rate wireless personal area networks
IEEE P1901.2	IEEE 1901.2 is an IEEE working group developing a Powerline communications standard for metering applications
IETF	Internet Engineering Task Force
IHD	In Home Display
IID	Interface Id
IO	Interface Object
IPHA	IP Host Application
IPHC	IP Header Compression
IPSO	Internet Protocol for Smart Objects is a industry alliance promoting Internet of Objects
ISM	Industrial Scientific and Medical
ISO	International Organization for Standardization
ISP	Intersystem Protocol
ITS	Intelligent Transport System
ITU	International Telecommunication Union is the specialized agency of the United Nations which is responsible for information and communication technologies
ITU G.9972	ITU G.9972 (also known as G.cx) is a recommendation developed by ITU-T that specifies a coexistence mechanism for networking transceivers
ITU G.hn	G.hn is the common name for ITU recommendation G.9960, a home network technology standard being developed under the International Telecommunication Union
ITU G.hnem	An ITU project addressing the home networking aspects of energy management
LC	Line Coupler
LDN	Logical Device Name

LLC	Logical Link Control layer
LLN	Low Bitrate and Lossy Network
LLS	Low-Level Security
LN	Logical Name
LonWorks	LonWorks is a networking platform created to control applications The platform is built on a protocol created by Echelon Corporation
LowPAN	Low-power Wireless Personal Area Networks
LQI	Link Quality Information
LRWBS	Low Rate Wide Band Services are emerging services on Powerline transmitting in the 2–4 MHz band
LV-MV	Low Voltage (less than 600 Volts) and Medium Voltage (in the order of magnitude of 20 000 Volts)
M2M	Machine-to-Machine
MAC	Media Access Control
MAS	M2M Authentication Server
MCPS	MAC Common Part Sublayer
MCPS-SAP	MAC Common Part Service Access Point
MDU	Multidwelling Unit
mIa	Reference Point between a M2M application and the M2M Service Capabilities in the Networks and Applications Domain
MIC	Message Integrity Protection Code
mId	Reference point between an M2M Device or M2M Gateway and the M2M Service Capabilities in the Network and Applications Domain
MLDE	MAC Layer Management Entity
MLME-SAP	MAC Layer Management Entity Service Access Point
MP2P	Multipoint To Point Traffic
MSBF	M2M Service Bootstrap Function
MSP	Manufacturer Specific Profile
MTU	Maximum Transmission Unit
NA	Network Application
NAN	Neighborhood Area Network
NAPT	Network Address and Port Translation
NIB	Network Information Base
NIF	Node Information Frame
NIP	Network Interworking Proxy
NIST	National Institute of Standards and Technology is a measurement standards laboratory in USA
NLDE-SAP	Network Layer Data Entity Service Access Point
NLME	Network Layer Management Entity
NLME-SAP	Network Layer Management Entity Service Access Point
NLSE-SAP	Network Layer Security Entity Service Access Point

---

NREL	National Renewable Energy Laboratory
NRZ	Nonreturn to Zero
NUD	Neighbor Unreachability Detection
OBIS	Object Identification System
OCP	Objective Code Point
OF	Objective Function
OFDM	Orthogonal Frequency-Division Multiplexing
OOK	On-off keying the simplest form of modulation that represents digital data as the presence or absence of a carrier wave
O-QPSK	Offset-Quadrature Phase-Shift Keying
OSI	Open Systems Interconnections
OTA	Over-the-Air
OUI	Organizationally Unique Identifier
P2MP	Point to Multipoint Traffic
PAA	PANA Authentication Agent
PaC	PANA Client
PAN	Personal Area Network
PAN ID	Personal Area Network Identifier
PANA	Protocol for Carrying Authentication for Network Access
PCT	Programmable Communicating Thermostat
PEV	Plug-in Electric Vehicle
PHEV	Plug-in Hybrid Electric Vehicle
PHR	Physical Header
PHY	Physical Layer
PIB	PAN Information Base
PIO	Prefix Information Option
PLC	Powerline Communication
PLT	Powerline Technology
PN	Parent Node
PoC	Point of Contact
PRE	PANA Relay Element
PRIME	Powerline Intelligent Metering Evolution
PSDU	Physical Service Data Unit
PSEM	Protocol Specification for Electric Metering
PSSS	Parallel Spread Spectrum modulation
PWM	Pulse Width Modulation
Rank	A node's individual position relative to other nodes with respect to a DODAG root
REQ	M-Bus REQUEST message
REST	Representational State Transfer
RFD	Reduced Function Device
RIT	Receiver-Initiated Transmission

ROLL	Routing over Low-power and Lossy network
RPF	Reverse Power Flow
RPL	RPL IPv6 Routing Protocol over Low-power and Lossy Networks
RPL Instance	A set of one or more DODAGs that share a RPLInstanceID
RPLInstanceID	A unique identifier within a RPL LLN. DODAGs with the same RPLInstanceID share the same Objective Function
RSP	M-Bus RESPOND Message
RTE	Réseau Transport Electricité
RTU	Remote Terminal Unit
RZtime	Rendezvous Time
SA	Secure Association
SAP	Service Access Point
S-Band	Scientific Band, <i>see</i> ISM
SCDE	Secured Connection Protocol
SCL	Service Capability Layer
SCME	SCoP Management Entity
SCoP	SCoP Data Entity
SCPT	Standard Configuration Property Type
SCSS	SCoP Security Service
SDP	SECC Discovery Protocol
SDU	Service Data Unit
SECC	Supply Equipment Communication Controller
SFD	Start Frame Delimiter
SHR	Synchronous Header
SKKE	Symmetric-Key Key Exchange
SLAAC	IPv6 Stateless Address Autoconfiguration
SN	Short Name
SND	M-Bus SEND Message
SNVT	Standard Network Variable Type
SoC	System on Chip
SUN	Smart Utility Network
TDMA	Time division multiple access is a channel access method for shared medium networks
TL	Transport Layer
TLS	Transport Layer Security
ToU	Time of Use
TP1	KNX Twisted Pair Physical Media
TSCH	Time-Synchronized Channel Hopping
TSO	Transmission System Operator
UC	Upgrade Client
UID	Unique Node Identifier
U-NII	Unlicensed National Information Infrastructure

---

UNVT	User Network Variable Type
US	Upgrade Server
V2GTP	Vehicle to Grid Transfer Protocol
VIB	Value Information Block
VIF	Value Information field, see M-Bus
WADL	Web Application Description Language
xAE	Application Enablement M2M Service Capability
xBC	Compensation Broker M2M Service Capability
XCAP	Extensible Markup Language (XML) Configuration Access Protocol (RFC 4825)
xCS	Communication Selection M2M Service Capability
xHDR	History and Data Retention M2M Service Capability
xIP	Interworking Proxy M2M Service Capability
xRAR	Reachability, Addressing and Repository M2M Service Capability
xREM	Remote Entity Management M2M Service Capability
xSEC	Security M2M Service Capability
xTM	Transaction Management M2M Service Capability
xTOE	Telco Operator Exposure M2M Service Capability
ZBD	ZigBee Bridge Device
ZC	ZigBee Coordinator
ZCL	ZigBee Cluster Library
ZCP	ZigBee Compliant Platform
ZDO	ZigBee Device Object
ZDP	ZigBee Device Profile
ZED	ZigBee End Device
Zero-crossing	In alternating current, the zero-crossing is the instantaneous point at which there is no voltage present
ZGD	ZigBee Gateway Device
ZigBee Alliance	ZigBee Alliance is a group of companies that maintain and publish the ZigBee standard
ZIPT	ZigBee IP Tunneling Protocol
ZR	ZigBee Router
ZSE	ZigBee Smart Energy



# Introduction

Innovation rarely comes where it is expected. Many governments have been spending billions to increase the Internet bandwidth available to end users . . . only to discover that there are only a limited number of HD movies one can watch at a given time. In fact, there are also a limited number of human beings on Earth.

The Internet is about to bring us another ten years of surprises, as it morphs into the “Internet of Things” (IoT). Your mobile phone and your PC are already connected to the Internet, maybe even your car GPS too. In the coming years your car, office, house and all the appliances it contains, including your electricity, gas and water meters, street lights, sprinklers, bathroom scales, tensiometers and even walls<sup>1</sup> will be connected to the IoT. Tomorrow, several improvements will be made to these appliances such as not heating your house if hot weather is forecast, watering your garden automatically only if it doesn’t rain, getting assistance immediately on the road, and so on. These improvements will facilitate our lives and utilize natural resources more efficiently.

Why is this happening now? As always, there is a combination of small innovations that, together, have reached a critical mass:

- Fieldbus technologies, using proprietary protocols and standards (LON, KNX, DALI, CAN, ModBus, M-Bus, ZigBee, Zwave . . .), have explored many vertical domains. Gradually, these domains have started to overlap as use cases expanded to more complex situations, and protocols have emerged to facilitate interoperability (e.g., BACnet). But in many ways, current fieldbus deployments continue to use parallel networks that do not collaborate. The need for a common networking technology that would run over any physical layer, like IP, has become very clear.
- Despite the need for a layer 2 independent networking technology for fieldbuses, IP was not considered as a possible candidate for low-bitrate physical layers typically used in fieldbus networks, due to its large overheads. But the wait is now over: with 6LoWPAN not only has IP technology found its way onto low-bitrate networks but – surprise, surprise – it is IPv6 ! As an additional bonus, the technology comes with a state-of-the-art, standardized IP level mesh networking protocol, which makes multiply

---

<sup>1</sup> Sensors for structural monitoring.

mesh networking a reality: finally different layer 2 fieldbus technologies can collaborate and form larger networks.

- Today, local fieldbus networks optimize the HVAC<sup>2</sup> regulation in your office and perhaps your home, with sophisticated algorithms. The energy-efficiency regulation for new building construction has created a need for even more sophisticated algorithms, like predictive regulation that takes into account weather forecasts or load shifting that incorporates the CO<sub>2</sub> content of electricity. In many automation sectors, the current state-of-the-art tool requires the local fieldbus to collaborate with hosted centralized applications and data sources. The technology required to enable this progressed in steps: oBix introduced the concept of a uniform (REST) interface to sensor networks, ETSI M2M added the management of security and additional improvements required in large-scale public networks.

The industry was only missing a really, really compelling business case to trigger the enormous amount of R&D that will be required to integrate all these technologies and build a bulletproof Internet of Things.

This business case is coming from the energy sector:

- The accelerated introduction of renewable-energy sources in the overall electricity production park brings an increasing degree of randomness to the traditionally deterministic supply side.
- In parallel, the mass introduction of rechargeable electric and hybrid vehicles is making the demand side more complex: EVs are roaming objects that will need to authenticate to the network, and will require admission control protocols.

The current credo of electricity operators “demand is unpredictable, and our expertise is to adapt production to demand”, is about to be reversed into “production is unpredictable, and our expertise is to adapt demand to production”.

As the rules of the game change, the key assets of an energy operator will no longer be the means of production, but the next-generation communication network and information system, which they still need to build entirely, creating an enormous market for mission-critical M2M technology. This dramatic change of how electricity will be distributed prefigures the more general evolution of the Internet towards the Internet of Things, where telecom operators and network-based application developers will have an increasing impact on our everyday lives, including the things that we touch and use.

This book targets an audience of engineers who are involved or want to get involved in large-scale automation and smart-grid projects and need to get a feel for the “big picture”.

Many such projects will involve interfaces with existing systems. We included detailed overviews of many legacy fieldbus and automation technologies: BACnet, CAN, LON, M-Bus/wMBUS, ModBus, LON, KNX, ZigBee, Z-Wave, as well as C.12 and

---

<sup>2</sup> Heating, ventilation and air conditioning.

DLMS/COSEM metering standards. We also cover in detail two common fieldbus physical layers: 802.15.4 and PLC.

This book will not make you an expert on any of these technologies, but provides enough information to understand what each technology can or cannot do, and the fast-track descriptions should make it much easier to learn the details by yourself.

The future of fieldbus protocols is IP: we introduce 6LoWPAN and RPL, as well as the first automation protocol to have been explicitly designed for 6LoWPAN networks: ZigBee SE 2.0. We also provide an introduction to the emerging ETSI M2M standard, which is the much-awaited missing piece for service providers willing to provide a general-purpose public M2M infrastructure, shared by all applications.

I would like to thank Paul Bertrand, the inventor of the lowest-power PLC fieldbus technology to date (WPC) and designer of the first port of 6LoWPAN to PLC for accepting to write – guess what – the Powerline Communications chapter of this book. I am also grateful for the C.12 and DLMS chapters that were provided by Jean-Marc Ballot (Alcatel), and required a lot of documentation work.

Despite my efforts, there are probably quite a few errors remaining in the text, but there would have been many more without the help of the expert reviewers of this book: Cedric Chauvenet for 6LoWPAN/RPL, Mathieu Pouillot for ZigBee, Juan Perez (EPEX) for the smart-grid section, François Collet (Renault) for EV charging, Alexandre Ouimet-Storrs for his insights on energy trading, and the companies who provided internal documentation or reviews: Echelon for LON (with special thanks to Bob Dolin, Jeff Lund, Larry Colton and Mark Ossel), and Sigma Designs for Z-Wave. I am also grateful to Benoit Guennec and Baptiste Vial (Connected Object), who supplied me with the temperature and consumption profiles of their homes and shared their field experience with Z-Wave. Please let me know of remaining errors, so that we can improve the next edition of this book, at [olivier.hersent@actility.com](mailto:olivier.hersent@actility.com).

Gathering and reading the documentation for this book has been an amazing experience discovering new horizons and perspectives. I hope you will enjoy reading this book as much as I enjoyed writing it.

Olivier Hersent



# **Part One**

## **M2M Area Network Physical Layers**

