



Deji Chen  
Mark Nixon  
Aloysius Mok

# WirelessHART™

Real-Time Mesh Network  
for Industrial Automation

 Springer

WirelessHART™

Deji Chen • Mark Nixon  
Aloysius Mok

# WirelessHART™

Real-Time Mesh Network for Industrial  
Automation

 Springer

Deji Chen  
Emerson Process Management  
12301 Research Blvd.  
Research Park Plaza, Bldg. III  
Austin, TX 78759  
USA  
deji.chen@emerson.com

Mark Nixon  
Emerson Process Management  
12301 Research Blvd.  
Research Park Plaza, Bldg. III  
Austin, TX 78759  
USA  
mark.nixon@emerson.com

Aloysius Mok  
Department of Computer Sciences  
The University of Texas at Austin  
Austin, TX 78712  
USA  
mok@cs.utexas.edu

ISBN 978-1-4419-6046-7 e-ISBN 978-1-4419-6047-4  
DOI 10.1007/978-1-4419-6047-4  
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2010925230

© Springer Science+Business Media, LLC 2010

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper

Springer is part of Springer Science+Business Media ([www.springer.com](http://www.springer.com))

*To my father Zhengcai Chen, my mother Jiangen Wang, my wife Qing Li, and my newborn daughter Daphne Chen.*

Deji Chen

*To Joshua and Jordan.*

Mark Nixon

*To my family especially my wife Amy who has been a great companion in life's adventures.*

Aloysius Mok

## **Acknowledgements**

We would like to thank the following persons without whom this book will not be possible. First we thank Jose Gutierrez, Ron Helson, and Quan Wang for their encouragement for starting the book. We owe a special gratitude to Wally Pratt, the chief engineer at the HCF, and the members of the specification team consisting of Eric Rotvold, Robin Pramanik, and Tomas Lennvall. Without all of your hard work this book would not have been possible. We also thank Veena Gondhalekar, Jianping Song, Song Han, Xiuming Zhu, Terry Blevins, Willy Wojsznis, and Greg McMillan for cooperating with us on the WirelessHART related research and development effort which provided the material for this book. Song Han and Xiuming also provided valuable feedback to the initial draft of the book. We thank Kelly Orth for important input to the book. We thank Mike Sheldon for much needed advices. And finally, we thank Susan Lagerstrom-Fife and Jennifer Maurer for their understanding in working with us closely to bring this book to reality.

# Table of Contents

<b>Introduction .....</b>	<b>xix</b>
<b>PART I WirelessHART in a Nutshell.....</b>	<b>1</b>
<b>Chapter 1 Overview .....</b>	<b>3</b>
1.1 About the HART Standard .....	3
1.2 About the WirelessHART Standard .....	4
1.3 The Layers .....	7
1.4 A Simple Example.....	12
<b>Chapter 2 Physical Layer .....</b>	<b>15</b>
2.1 Physical Layer Services.....	16
2.1.1 Message SPs.....	16
2.1.2 Management SPs.....	16
<b>Chapter 3 Data Link Layer .....</b>	<b>19</b>
3.1 Data Link Layer Services .....	20
3.1.1 Message SPs.....	20
3.1.2 Management SPs.....	21
3.2 Logical Link Control .....	23
3.2.1 The DLPDU .....	23
3.2.2 DLPDU Types.....	24
3.2.3 DLPDU Priority and Flow Control.....	24
3.2.4 Error Detection Coding and Security.....	25
3.3 Media Access Control.....	25
3.3.1 Slot Timing.....	25
3.3.2 Communication Tables and Buffers .....	27
3.3.3 Link Scheduling.....	27
<b>Chapter 4 Network Layer and Transport Layer .....</b>	<b>29</b>
4.1 Overview.....	29
4.1.1 Communication Traffic.....	29
4.1.2 Routing.....	30
4.1.3 Security .....	31
4.2 Network Layer Services .....	32
4.2.1 Network Layer Message SPs .....	32
4.2.2 Network Layer Management Services.....	33
4.3 Network Layer Specification.....	34
4.3.1 Network Layer PDUs.....	34

- 4.3.2 Transport Layer PDU ..... 37
- Chapter 5 Application Layer ..... 39**
  - 5.1 Application Layer Interface..... 39
  - 5.2 Dynamic and Device Variables ..... 44
  - 5.3 Host Conformance Classifications ..... 44
- Chapter 6 WirelessHART Network ..... 45**
  - 6.1 Field Devices ..... 46
    - 6.1.1 General Requirements..... 46
    - 6.1.2 Maintenance Port ..... 46
    - 6.1.3 WirelessHART Device Interface ..... 47
  - 6.2 Router Device ..... 48
  - 6.3 Adapter ..... 48
  - 6.4 Handheld..... 49
  - 6.5 Gateway and Access Point ..... 50
    - 6.5.1 General Requirements..... 50
    - 6.5.2 Gateway Model..... 51
  - 6.6 Network Manager and Security Manager ..... 55
    - 6.6.1 Core Network Functions..... 55
    - 6.6.2 Network Manager Requirements ..... 58
    - 6.6.3 Scheduling..... 60
- PART II WirelessHART in Depth..... 63**
- Chapter 7 An Example ..... 65**
  - 7.1 Network Management and Host Request..... 66
  - 7.2 Process Measurement ..... 69
  - 7.3 Scheduling Example – Single Hop..... 70
  - 7.4 Scheduling Example – Multiple Hop ..... 71
- Chapter 8 Discourses on the Stack ..... 73**
  - 8.1 Physical Layer ..... 73
    - 8.1.1 Physical Channel and Maximum Bandwidth..... 73
    - 8.1.2 Packet Length versus Reliability ..... 74
    - 8.1.3 Channel Hopping ..... 74
    - 8.1.4 Health Report ..... 75
  - 8.2 Data Link Layer..... 76
    - 8.2.1 Timeslot ..... 76
    - 8.2.2 Links..... 78
    - 8.2.3 Synchronization ..... 79
    - 8.2.4 Keep Alive Interval..... 80
    - 8.2.5 Clock Drift and Precision..... 82
    - 8.2.6 Broadcast Messages ..... 82



8.3 Network and Transport Layer.....	83
8.3.1 Session and Transport Table, Who Owns Who? .....	83
8.3.2 The Security Layer .....	84
8.3.3 Broadcast and Response.....	84
8.3.4 Block Data Transfer .....	84
8.3.5 Transport Type Codes .....	85
8.4 Application Layer .....	85
8.4.1 Commands and Messages .....	85
8.4.2 Wireless versus Wired Command Formats .....	86
8.4.3 Some Interesting Commands .....	87
8.4.4 Burst Data and Delayed Response .....	88
8.5 Topics that Cross Layers .....	89
8.5.1 The Encryption Algorithm .....	89
8.5.2 Message Life Time.....	97
8.5.3 Retry .....	98
8.5.4 MSB and LSB, Big Endian and Small Endian .....	99
8.5.5 Short Address and Long Address.....	100
8.5.6 Nonce Counter and Sequence Numbers .....	100
8.5.7 Timestamp and ASN Time .....	103
8.5.8 Master and Slave .....	103
8.5.9 Broadcast and Unicast.....	104
8.6 Other Topics .....	104
8.6.1 Memory Footprint .....	104
8.6.2 Key Change.....	105
<b>Chapter 9 Discourses on the Mesh Network.....</b>	<b>107</b>
9.1 The Birth of a WirelessHART Mesh.....	107
9.2 Device Life Cycle in the Network.....	107
9.2.1 Pre-configure the New Device.....	108
9.2.2 Network Device Advertise .....	108
9.2.3 New Device Synchronize.....	109
9.2.4 Join Request .....	110
9.2.5 Join Reply.....	111
9.2.6 More Configurations .....	112
9.2.7 Keep in the Network .....	113
9.2.8 Disconnect.....	113
9.2.9 Rejoin .....	113
9.3 Routing .....	114
9.3.1 Source Routing .....	114
9.3.2 Graph Routing.....	114
9.3.3 Mixed Routing .....	115
9.3.4 Superframe Routing .....	116
9.3.5 Proxy Routing .....	117
9.3.6 Broadcast Routing.....	118

9.4 Communication with the Host.....	119
9.5. Network Management .....	120
9.5.1 Superframe Lengths .....	120
9.5.2 Allocating Bandwidth for the Host Application .....	120
9.5.3 Some Comments .....	121
9.6 Redundancy .....	122
9.6.1 Device Redundancy .....	122
9.6.2 Path Redundancy .....	123
9.6.3 Broadcast Redundancy.....	127
9.7 Scalability .....	127
9.8 Low Power Mode and Battery Life.....	127
9.9 Interoperability and Interchangeability .....	129
9.10 Unwanted Access to a WirelessHART Mesh.....	129
9.10.1 Jamming.....	129
9.10.2 Key Discovery .....	131
<b>Chapter 10 Discourses in General .....</b>	<b>133</b>
10.1 The WirelessHART Standard and the ISO OSI Standard.....	133
10.2 Radio Basics .....	135
10.2.1 Radio Basics.....	135
10.2.2 Spread Spectrum Modulation .....	138
10.2.3 Media Access Control.....	139
10.2.4 The Reason for 2.4GHz Band.....	141
10.3 Why Centralized Control.....	141
10.4 Field Survey.....	143
10.5 The WirelessHART Standard and the IEEE 802.15.4 Standard.....	144
10.5.1 WirelessHART Values in IEEE 802.15.4 Header Fields .....	144
10.5.2 The Security Method.....	145
10.5.3 Maximum MAC Payload.....	146
10.5.4 Other Comparisons .....	146
10.5.5 Some Added Benefits with the IEEE 802.15.4 Standard .....	147
10.5.6 Beacon.....	147
10.5.7 Configure IEEE 802.15.4 Stack for WirelessHART Stack .....	149
10.6 Coexistence.....	150
10.6.1 The IEEE 802.15.4 Standard .....	151
10.6.2 The IEEE 802.11 Standard .....	151
10.6.3 Other Standards.....	153
10.6.4 Coexistence Test Scenarios.....	153
10.7 The HART Standard and Other Fieldbus Standards.....	154
10.8 What the WirelessHART Standard Does Not .....	155
10.9 Security and Reliability .....	155
10.10 Do I Need to Know All These to Use WirelessHART Technology?...	156

<b>PART III WirelessHART in Practice.....</b>	<b>157</b>
<b>Chapter 11 Test and Diagnostic Tools.....</b>	<b>159</b>
11.1 The Wi-Analys Tool.....	160
11.2 The Wi-HTest Tool.....	163
11.2.1 WirelessHART Test Specification and Test Scripts.....	164
11.2.2 Wi-HTest Architecture.....	166
11.3 The Post Process Suite.....	173
<b>Chapter 12 A Fast Approach to Equip a HART Device with WirelessHART Capability .....</b>	<b>175</b>
12.1 The WirelessHART Adapter .....	175
12.2 A WirelessHART Adapterlite .....	175
<b>Chapter 13 Development Recommendations.....</b>	<b>177</b>
13.1 OS or No OS.....	177
13.2 Timestamping Incoming Messages .....	178
13.3 Realizing Network Layers in the Stack .....	178
13.4 API between Adjacent Network Layers in the Stack .....	179
13.5 A Timer Module .....	179
13.5.1 Timeslots in the WirelessHART Standard.....	180
13.5.2 Standard-Conscious Timer Module .....	180
13.5.3 The Implementation .....	182
13.6 Hardware Considerations .....	183
13.7 Miscellaneous Comments.....	184
<b>Chapter 14 Deployment Recommendations .....</b>	<b>187</b>
14.1 Scope the Network.....	187
14.2 Design the Network .....	187
14.3 Deploy the Network.....	189
14.4 More Comments .....	191
<b>PART IV WirelessHART in the Bigger Picture.....</b>	<b>193</b>
<b>Chapter 15 Why WirelessHART .....</b>	<b>195</b>
15.1 The WirelessHART Standard Is Based on Proven Solutions.....	195
15.2 The WirelessHART Standard Embraces the Best Technology.....	196
15.3 The WirelessHART Standard Has an Easy Adoption Path.....	197
<b>Chapter 16 Wireless and Real-Time Industrial Process Control.....</b>	<b>201</b>
16.1 Challenges of Wireless Control.....	201
16.1.1 Process Control Networks and their Wireless Counterparts.....	202
16.1.2 Process Control with Sensor Networks.....	204
16.2 Improving PID Control with Unreliable Communications .....	208
16.2.1 The Control Loop.....	209
16.2.2 The Standard PID Algorithm .....	209

16.2.3 The Enhanced PID Algorithm .....	212
16.2.4 Experiments and Results .....	214
16.2.5 Active Traffic Reduction to Increase Battery Life .....	219
16.2.6 Comments .....	220
<b>Chapter 17 Research in Real-Time Wireless Mesh Networks .....</b>	<b>223</b>
17.1 Real-Time Systems .....	223
17.2 Selected Topics .....	224
<b>Chapter 18 Future of Wireless and the WirelessHART Standard.....</b>	<b>227</b>
18.1 Wireless Sensor Network in Process Automation.....	227
18.1.1 Wireless Mesh Applications .....	227
18.1.2 Wireless Products.....	228
18.2 Location Awareness .....	230
18.2.1 Location Awareness Techniques .....	230
18.2.2 A WirelessHART Location-Determination Application .....	232
18.3 Cyber-Physical Systems and WirelessHART Systems .....	234
18.4 What's next for the WirelessHART Standard? .....	239
18.4.1 Discrete Devices and Values .....	241
18.4.2 Location .....	242
18.4.3 Handhelds.....	242
18.4.4 Public/Private Key for Handheld .....	243
18.4.5 Control over Wireless .....	243
<b>PART V Appendices .....</b>	<b>245</b>
<b>Chapter 19 Attribute and Field Values.....</b>	<b>247</b>
19.1 Comments on Message Field Values .....	247
19.2 WirelessHART Message Fields .....	248
<b>Chapter 20 Symbols and Abbreviations .....</b>	<b>253</b>
<b>Chapter 21 Definitions .....</b>	<b>257</b>
<b>Chapter 22 References .....</b>	<b>267</b>
22.1 HART 7 Protocol Specifications .....	267
22.2 Related HART Documents.....	268
22.3 Related Documents Cited by HART .....	268
22.4 Other References .....	269
<b>Index .....</b>	<b>273</b>

# Table of Figures

Fig. 1.1 The Evolution of HART. ....	4
Fig. 1.2 Example of a WirelessHART Network. ....	5
Fig. 1.3 WirelessHART Communication Stack. ....	6
Fig. 1.4 Architecture of HART Communication Protocol. ....	7
Fig. 1.5 WirelessHART Data Link Layer Architecture. ....	9
Fig. 1.6 WirelessHART Network Layer Architecture. ....	10
Fig. 1.7 WirelessHART Application Layer Architecture. ....	11
Fig. 1.8 Keying Model. ....	13
Fig. 3.1 Data-Link Layer Scope. ....	19
Fig. 3.2 DLPDU Structure. ....	23
Fig. 3.3 DLPDU Specifier. ....	24
Fig. 3.4 Slot Timing. ....	26
Fig. 4.1 Network Layer Scope. ....	30
Fig. 4.2 Summary of PDU Format. ....	31
Fig. 4.3 WirelessHART NPDU Structure. ....	35
Fig. 4.4 Network Control Byte. ....	35
Fig. 4.5 Security Control Byte. ....	37
Fig. 4.6 Transport Layer. ....	38
Fig. 4.7 Transport Byte. ....	38
Fig. 4.8 WirelessHART Command Format. ....	38
Fig. 7.1 Bio-reactor process. ....	65
Fig. 7.2 Network Management Frames. ....	67
Fig. 7.3 Network Management Frames/Graph Transferred to C4. ....	68
Fig. 7.4 Synchronize Measurement Processing and Transmission. ....	70
Fig. 7.5 Batch Bio-Rractor Example – Single Hop. ....	70
Fig. 7.6 Multiple Frames for Different Update Rates – Single Hop. ....	71
Fig. 7.7 Bio-Reactor Example – Multiple Hops. ....	71
Fig. 7.8 Multiple Frames for Different Update Rates – Multiple Hops. ....	72
Fig. 8.1 Calculating Keep Alive Interval. ....	81
Fig. 9.1 Graph Routing. ....	115
Fig. 9.2 Single Failure in a Graph. ....	123
Fig. 9.3 Redundant Graph. ....	125
Fig. 10.1 The Fresnel Zones. ....	137
Fig. 11.1 Wi-Analys. ....	160
Fig. 11.2 Wi-Analys Screen Capture. ....	161
Fig. 11.3 Wi-HTest Tool. ....	166
Fig. 11.4 Wi-HTest High Level Architecture. ....	167
Fig. 11.5 Wi-HTest Host Architecture. ....	168
Fig. 11.6 Wi-HTest Architecture on RF Interface. ....	171
Fig. 13.1. WirelessHART Timer Module. ....	181
Fig. 14.1. Connecting the Gateway to the Control System. ....	190

**Fig. 14.2. Integration with DCS System. .... 191**  
**Fig. 16.1 A Process Control System. .... 202**  
**Fig. 16.2 A Wireless Process Control System. .... 203**  
**Fig. 16.3 Control Data Sampling Rate. .... 204**  
**Fig. 16.4 Sensor Networks in Process Control Systems (Large System). 205**  
**Fig. 16.5 Sensor Networks in Process Control Systems (Small System). 206**  
**Fig. 16.6 Tank Level Control with Fieldbus. .... 207**  
**Fig. 16.7 Tank Level Control with Sensor Network. .... 208**  
**Fig. 16.8 PID Block. .... 209**  
**Fig. 16.9 Standard PID Block with Lost Input. .... 210**  
**Fig. 16.10 Standard PID Block with Lost Output. .... 212**  
**Fig. 16.11 The enhanced PID algorithm application. .... 213**  
**Fig. 16.12 Experimental Setup. .... 215**  
**Fig. 16.13 Lost Inputs coupled with a setpoint change. .... 216**  
**Fig. 16.14 Lost Inputs coupled with unmeasured disturbances. .... 217**  
**Fig. 16.15 Missed Outputs with a setpoint change. .... 218**  
**Fig. 16.16 Missed Outputs with unmeasured disturbances. .... 219**

# List of Tables

Table I.1 Terms used describing message flow within the stack. ....	1
Table 1.1 The Superframe Configuration. ....	13
Table 2.1 Local Device Management Commands. ....	17
Table 3.1 Local Device Management Commands. ....	21
Table 3.2 Slot Timing Symbols. ....	26
Table 4.1 Transport Type Codes. ....	33
Table 4.2 Local Device Management Commands. ....	34
Table 5.1 HART Command Number Partitions. ....	40
Table 5.2 WirelessHART Commands. ....	41
Table 5.3 Host Conformance Classes. ....	44
Table 6.1 Network Manager Requirements. ....	58
Table 6.2 Scheduler Requirements. ....	60
Table 7.1 Instrument and Valve List for the Bio-Reactor. ....	66
Table 7.2 Measurements and Scan Rates for the Bio-Reactor. ....	69
Table 8.1 2.4GHz IEEE 802.15.4 Timing and Specifications (excerpt). ....	80
Table 8.2 CCM Encryption Symbols. ....	90
Table 8.3 Minimum Table and Buffer Space Requirement. ....	105
Table 8.4 Minimum Table Space Requirement. ....	105
Table 10.1 IEEE 802.15.4 Frame Control Fields. ....	144
Table 10.2 IEEE 802.15.4 MAC Header. ....	145
Table 10.3 WirelessHART values for IEEE 802.15.4 Fields. ....	149
Table 11.1 Wi-Analys Display Fields. ....	162
Table 13.1 Wi-HTest AP Code Size. ....	184
Table 16.1 Control Performance Difference. ....	220
Table 19.1 Time related parameters. ....	247
Table 19.2 Physical Layer Message Format. ....	248
Table 19.3 Data Link Layer Data Message Format. ....	249
Table 19.4 Data Link Layer Acknowledgement Message Format. ....	249
Table 19.5 Data Link Layer Advertisement Message Format. ....	249
Table 19.6 Data Link Layer Keep Alive Message Format. ....	250
Table 19.7 Data Link Layer Disconnect Message Format. ....	250
Table 19.8 Network Layer Message Format. ....	251
Table 19.9 Application Layer Message Format. ....	251
Table 20.1 Symbols and Abbreviations. ....	253