



Technology Training that Works

Practical Industrial Wireless for Engineers and Technicians

Contents

1	Introduction	1
1.1	Introduction	1
1.2	WINA and ISA-SP100	2
1.3	The OSI concept	3
1.4	Ethernet	10
1.5	TCP/IP	11
2	Wireless Fundamentals	13
2.1	Introduction	13
2.2	Electromagnetic waves	13
2.3	Radio/microwave frequency allocation	16
2.4	Single- and dual-frequency systems	18
2.5	Gain and loss	20
2.6	Power levels	21
2.7	Attenuation	23
2.8	Modulation/demodulation	24
2.9	Spread Spectrum techniques	35
2.10	Orthogonal Frequency Division Multiplexing	41
2.11	Complementary Code Keying	42
2.12	Ultra Wide Band	43
3	Terrestrial Wireless Systems	45
3.1	Terrestrial microwave	45
3.2	Wireless modems	52
4	Wireless LANs	59
4.1	Introduction	59
4.2	Architecture	62
4.3	Specifications	67
4.4	Medium Access Control	74
4.5	Frame structure	82
4.6	Industrial WLAN	89
5	Wireless Mesh Networks	95
5.1	Mesh basics	95
5.2	IEEE 802.11 WMNs	97
5.3	IEEE 802.15.4	100



Technology Training that Works

5.4	Stack implementation	102
5.5	Method of operation	103
5.6	WirelessHART	109
6	Wireless Sensor Networks	115
6.1	IEEE 1451.5	115
7	Auxiliary Wireless Technologies	119
7.1	Bluetooth	119
7.2	Low Power Radio	126
7.3	WiMAX	127
7.4	Cellular (mobile) systems	131
7.5	VSAT	138
8	Wireless Network Security	119
8.1	Bluetooth	119
8.2	Security goal	119
8.3	Threats and underlying causes	148
8.4	Motivation for threats	148
8.5	Vulnerabilities	148
8.6	Network attacks	150
8.7	Common criteria approach for analysis of threats and vulnerabilities	152
8.8	Overview of IP network security	153
8.9	Security policies	154
8.10	Weaknesses in the TCP/IP protocol	155
8.11	Attack mechanisms	156
8.12	Preparing for an attack	156
8.13	Attack through unauthorized access	157
8.14	Attacking the data (data diddling)	157
8.15	Denial of Services (DoS)	159
8.16	Vulnerabilities of OSI layers	161
8.17	Network security at the transport layer	163
8.18	Network security layer	165
8.19	Data Link layer security	165
8.20	Implementation of security measures for industrial WLANs	166
8.21	Some general guidelines	172
	Appendix: Ethernet and TCP/IP Networking	173
A.1	Introduction	173
A.2	TCP/IP	179
A.3	Transmission Control Protocol (TCP)	190
A.4	User Datagram Protocol (UDP)	198