



*Technology Training that Works*

---

# Setting Up, Understanding and Troubleshooting of Industrial Ethernet and Automation Networks

---

## Contents

---

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Network types	1
1.2	The Open Systems Interconnection (OSI) Model	2
1.3	The Client/Server paradigm	9
1.4	Where the different technologies fit in	10
1.5	Current trends	10
<b>2</b>	<b>Industrial Ethernet</b>	<b>13</b>
2.1	10 Mbps CSMA/CD Ethernet	13
2.2	Medium Access Control (Collisions)	18
2.3	Frame transmission	20
2.4	Frame reception	20
2.5	Frame format	21
2.6	Reducing collisions	23
2.7	Half-duplex Ethernet design rules	23
2.8	100 Mbps Ethernet	25
2.9	Gigabit Ethernet	26
2.10	Switching technology	26
2.11	Industrial Ethernet	30
2.12	Real Time operation	39
<b>3</b>	<b>Industrial Wireless</b>	<b>45</b>
3.1	Wireless LANs (IEEE 802.11)	45
3.2	Wireless Mesh Networks	71
3.3	Wireless Sensor Networks: IEEE 1451.5	84



*Technology Training that Works*

<b>4</b>	<b>TCP/IP</b>	<b>89</b>
4.1	The TCP/IP Protocol suite	89
4.2	IPv4	92
4.3	IPv6	95
4.4	ICMP	101
4.5	Routing	103
4.6	TCP	108
4.7	UDP	110
<b>5</b>	<b>OPC</b>	<b>113</b>
5.1	What is OPC?	113
5.2	The problems addressed by OPC	114
5.3	The OPC logical object model	117
5.4	OPC Specifications	119
5.5	COM/DCOM	120
5.6	OPC Data Access specification	127
5.7	Group attributes	134
5.8	Item properties	137
5.9	Exchange of information between Server and Client	138
5.10	Implementation issues	143
5.11	Tunneling	149
<b>6</b>	<b>Automation Network Developments</b>	<b>151</b>
6.1	Background	151
6.2	Plant automation hierarchies	153
6.3	Ethernet in field buses	154
6.4	HART	155
6.5	DeviceNet	166
6.6	Ethernet/IP	174
6.7	ProfiBus	179
6.8	PROFINet	189
6.9	FOUNDATION Fieldbus	199
6.10	High-Speed Ethernet (HSE)	207
6.11	EtherCAT	208
6.12	Ethernet Powerlink	211



*Technology Training that Works*

---

<b>7</b>	<b>Network Security</b>	<b>213</b>
7.1	Introduction	213
7.2	Security goal	214
7.3	Threats and underlying causes	215
7.4	Motivation for threats	216
7.5	Vulnerabilities	217
7.6	Network attacks	218
7.7	Common Criteria approach for analysis of threats and vulnerabilities	221
7.8	Overview of IP network security	222
7.9	Security policies	223
7.10	Weaknesses in the TCP/IP protocol	224
7.11	Attack mechanisms	224
7.12	Preparing for an attack	225
7.13	Attack through unauthorized access	225
7.14	Attacking the data (data diddling)	226
7.15	Attack the service through Denial of Service (DoS)	228
7.16	Vulnerabilities of OSI layers	229
7.17	Network security at the Transport layer	231
7.18	Network layer security	233
7.19	Data Link layer security	233
7.20	Implementation of security measures for industrial WLANs	234
7.21	Some general guidelines	239