



Technology Training that Works

Practical DNP3, 60870.5 & Modern SCADA Communication Systems

Contents

Preface

1	Introduction	1
1.1	Overview	1
1.2	SCADA systems	1
1.3	OSI reference model	4
1.4	IEC 60870.5 and DNP 3.0	8
1.5	Local Area Networks, Ethernet and TCP / IP	9
1.6	UCA and IEC 61850 protocols	11
2	Fundamentals of SCADA communications	13
2.1	SCADA systems	13
2.2	Remote terminal units	20
2.3	PLCs used as RTUs	25
2.4	The master station	25
2.5	Communication architectures	28
2.6	Communication philosophies	30
2.7	Interface standards: RS- 232 and RS- 485	34
2.8	MODBUS protocols	42
3	Open SCADA Protocols DNP3 and IEC 60870-5	53
3.1	Interoperability and open standards	53
3.2	Development of standards	54
4	Preview of DNP3	57
4.1	What is DNP3?	57
4.2	Interoperability and open standard	57
4.3	Benefits of DNP3	59
4.4	Features of DNP3	59



Technology Training that Works

4.5	System topology	60
4.6	Background and development	61
4.7	Why use DNP3?	61
5	Fundamentals of Distributed Network Protocol	63
5.1	Fundamental concepts	63
5.2	Understanding DNP3 message structure	68
5.3	Physical layer	70
5.4	Datalink layer	72
5.5	Transport layer (Pseudo- transport)	84
5.6	Application layer message handling	86
5.7	Application layer message functions	96
5.8	Data object library	110
6	Advanced considerations of DNP	127
6.1	DNP3 subset definitions	127
6.2	Interoperability between DNP3 devices	137
6.3	Implementation rules and recommendations	138
6.4	Conformance testing	142
6.5	DNP3 polling and communications options	145
6.6	Time synchronization	146
6.7	Secure authentication	147
7	Configuration of DNP3 over serial links	153
7.1	General description	153
7.2	System overview	153
7.3	Description of control system	154
7.4	RTUs	155
7.5	DNP3 configuration aspects	157
7.6	Data mapping in RTUs	158
7.7	DNP3 configuration	159
7.8	Summary	167
8	Review of Ethernet and TCP/IP Protocols	169
8.1	IEEE 802.3 CSMA/CD ('Ethernet')	169
8.2	Physical layers	170
8.3	Media access control	175
8.4	Ethernet frame format	177
8.5	Fast ethernet	178



Technology Training that Works

8.6	Gigabit ethernet	179
8.7	Switched ethernet	180
8.8	TCP/IP model overview	181
8.9	Internet protocol	183
8.10	ICMP	188
8.11	TCP	191
8.12	UDP	192
9	DNP3 operation over LAN and WAN networks	195
9.1	Routers	195
9.2	Types of routers	196
9.3	Routing protocols	197
9.4	Wide area networks	200
9.5	Digital transmission hierarchies	201
9.6	WAN protocol overview	203
9.7	DNP3 over TCP/IP and UDP/IP	210
9.8	Link layer confirmations	212
9.9	Time synchronization over LAN	213
10	Overview of IEC 60870-5 protocols	215
10.1	Introduction	215
10.2	The IEC 60870-5 standards	215
10.3	System topology	220
10.4	Data link layer	220
10.5	Addressing	224
10.6	Message Transport	224
10.7	Application layer	225
10.8	Interoperability	233
10.9	IEC 60870-5-104 (T104) Architecture	235
11	Differences between DNP3 and IEC 60870	241
11.1	Comparing DNP3 and IEC 60870	241
11.2	Which one will win?	244
12	Intelligent Electronic Devices (IEDS)	245
12.1	Definition	245
12.2	Functions	245
12.3	Example of GE power automation IEDS	247



Technology Training that Works

13	IEC 61850 Overview	253
13.1	Introduction	253
13.2	Basic features of IEC 61850	255
13.3	Data Modelling	255
13.4	Abstract communication service interface	258
13.5	Information (data) exchange model	266
13.6	Communication model	269
13.7	Substation configuration language	274
13.8	Conformance testing	275
13.9	Benefits of IEC 61850	276
14	Fieldbus and SCADA communications systems	279
14.1	Introduction	279
14.2	Profibus	279
14.3	Foundation fieldbus	284
15	Future Developments	291
Appendix A: Glossary		293
Appendix B: Implementers of DNP3		307
Appendix C: Device Profile Document		311
Appendix D: Practical Exercises		323