

INDUSTRIAL AUTOMATION WITH SCADA

Concepts, Communications and Security



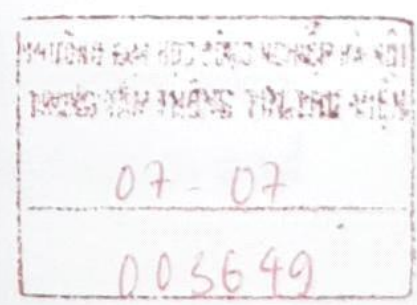
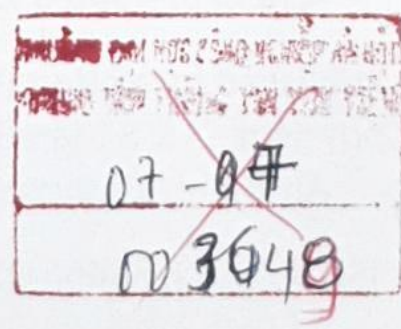
K S MANOJ



Điền

INDUSTRIAL AUTOMATION WITH SCADA

Concepts, Communications and Security



K S MANOJ



notionpress.com

INDIA • SINGAPORE • MALAYSIA

I owe this book to my dear sir... Prof. S. Suryadas, who introduced me to the exciting world of Electronics and Communication.

CONTENTS

<i>Preface</i>	15
<i>Author's Note</i>	15
<i>Intended Audience</i>	17
<i>Organization of the Book</i>	19
<i>About the Author</i>	21
<i>Chapter Wise Description</i>	23
<i>Salient Features</i>	27
<i>Acknowledgements</i>	29
<i>List of Acronyms</i>	31
<i>List of Tables</i>	37
<i>List of Figures</i>	39
CHAPTER 1 INTRODUCTION TO SCADA	41
1.1 Introduction	41
1.2 Data Acquisition Systems (DAS)	41
1.2.1 Objectives and Advantages	42
1.2.2 Single Channel Data Acquisition System	42
1.2.3 Multi-Channel Data Acquisition System	43
1.2.4 Sensors	44
1.2.5 Signal Conditioning	45
1.2.6 Sample and Hold Circuit	46
1.2.7 A to D Converters (ADC)	47

1.2.7.1	Integrating or dual slope ADC	48
1.2.7.2	Successive approximation ADC	49
1.2.7.3	Parallel Comparator (Flash) ADC	50
1.2.7.4	Counting type ADC	50
1.2.7.5	ADC specifications	51
1.2.8	Storage and Display	53
1.2.9	Data Forwarding and Communication	53
1.3	Evolution of SCADA	53
1.3.1	Monolithic SCADA – The First Generation SCADA	53
1.3.2	Distributed SCADA – The Second Generation SCADA	54
1.3.3	SCADA with Standard Protocols – The Third Generation SCADA	54
1.3.4	Internet of Things – The Fourth Generation SCADA	54
1.4	Communication in SCADA	55
1.5	Selection criteria of DAS	55
	<i>Summary</i>	59
CHAPTER 2	SCADA SYSTEM COMPONENTS	61
2.1	Introduction	61
2.2	Remote Terminal Unit (RTU)	61
2.2.1	Evolution of RTUs	62
2.2.2	RTU Architecture	63
2.2.2.1	Central Processing Unit (CPU)	64
2.2.2.2	Analog Input Modules (AI)	64
2.2.2.3	Analog Output Module (AO)	65
2.2.2.4	Digital or status inputs (DI)	65
2.2.2.5	Digital Output Modules (DO)	66
2.2.2.6	Power Supply Module	66
2.2.2.7	Communication interfaces	66

2.2.3	RTU Environmental Enclosures	68
2.2.4	RTU Design Standards	69
2.2.5	Selection Criteria of RTUs	69
2.2.6	Securing Remote Terminal Units	70
2.3	Intelligent Electronic Devices (IEDs)	72
2.3.1	IED Hardware and Software	74
2.3.2	IED Communication Module	75
2.4	Programmable Logic Controller (PLC)	76
2.4.1	Ladder Logic	76
2.5	Data Concentrators and Merging Units	77
2.5.1	Data Concentration Units (DCU)	77
2.5.2	Merging Unit (MU)	79
2.6	Master Control Centres (MCC)	79
2.6.1	System SCADA Software	80
2.6.2	Master Station Hardware	80
2.6.3	Servers in the Master Station	80
2.6.4	SCADA Server	81
2.6.5	Application Server	82
2.6.6	Information Storage and Retrieval (ISR) Server	82
2.6.7	Development Server	82
2.6.8	Network Management Server (NMS)	83
2.6.9	Video Projection System (VPS)	83
2.6.10	Communication Front End (CFE)	83
2.6.11	ICCP Server	84
2.6.12	Dispatch Training Simulator (DTS) Server	84
2.7	Global Positioning Systems (GPS)-Relevance to SCADA	85
2.8	Human Machine interface (HMI)	85
2.9	HMI building blocks	86

2.9.1	Operator Console	86
2.9.2	Operator Dialogue	87
2.9.3	Mimic Diagram	87
2.9.4	Peripheral Devices	87
2.9.5	HMI Software Functionalities	87
2.9.6	Situational Awareness and Alarm Handling	88
2.9.7	Intelligent Alarm Filtering	90
2.9.8	Necessities and Requirements of Operators	90

<i>Summary</i>	92
----------------	----

CHAPTER 3 SCADA ARCHITECTURE 93

3.1	Introduction	93
3.2	Communication Architecture	93
3.2.1	Point-to-Point between Two Stations	94
3.2.2	Multipoint or Multiple Stations	94
3.2.3	Talk Through Repeaters	96
3.3	Communication philosophies	97
3.3.1	Polled or Master Slave	97
3.3.2	CSMA/CD System (Peer-to-Peer)	99
3.3.2.1	RTU to RTU communication	99
3.3.2.2	Exception reporting (or event reporting)	100
3.3.2.3	Polling plus CSMA/CD with exception reporting	101
3.4	System reliability and availability	102
3.4.1	Fail Safe System	102
3.4.2	Fault Tolerant System	103
3.4.3	Graceful Degradation Systems	104
3.4.4	Design Considerations for Fault Tolerant System	104
3.4.5	High Availability	105

3.4.6	Critical Functions	105
3.4.7	System Redundancy	109
3.4.8	Channel Redundancy	110
3.5	Design and Configuration Considerations of MCC	111
	<i>Summary</i>	<i>111</i>
CHAPTER 4	SCADA APPLICATIONS	113
4.1	Introduction	113
4.2	Power Sector	113
4.2.1	Energy Management Systems (EMS)	114
4.2.2	Distribution Management System (DMS)	116
4.2.2.1	Distribution Network (DN) Model or Dynamic Mimic Diagram	117
4.2.2.2	Network Connectivity Analysis (NCA) or Topology Analyzer (TA)	118
4.2.2.3	State Estimation (SE)	118
4.2.2.4	Volt -VAR Control (VVC)	119
4.2.2.5	Load Flow Application (LFA)	119
4.2.2.6	Load Shed Application (LSA)	120
4.2.2.7	Fault Management and System Restoration (FMSR) Application	120
4.2.2.8	Loss Minimization via Feeder Reconfiguration (LMFR)	121
4.2.2.9	Load Balancing via Feeder Reconfiguration (LBFR)	121
4.2.2.10	Distribution Load Forecast (DLF)	122
4.2.2.11	Outage Management System (OMS)	122
4.3	Oil and Gas Industry	123
4.4	Automobile Industry	124
4.5	Water Distribution Sector	125

4.5.1	Water Pumping Stations	125
4.5.2	Distribution Pipeline Pressure Monitoring and Control	126
4.5.3	Water Recycling Plant Monitoring and Control	126
	<i>Summary</i>	127
CHAPTER 5 ADVANCED SCADA COMMUNICATIONS		129
5.1	Introduction	129
5.2	Types of Transmission	130
5.2.1	Analog and Digital	130
5.2.2	Synchronous and Asynchronous	131
5.2.3	Broadcast, Multicast, and Unicast	132
5.2.4	Simplex, Half Duplex, and Full Duplex Communication Channels	133
5.2.5	Baseband and Broadband	134
5.3	Guided media	136
5.3.1	Twisted Pair	136
5.3.2	Co-axial	138
5.3.3	Fiber Optical Cables	140
5.3.4	Cabling Considerations	142
5.3.4.1	Noise	142
5.3.4.2	Cabling Connection Types	142
5.3.4.3	Attenuation	143
5.3.4.4	Crosstalk	143
5.3.4.5	Fire-rated and Flame-retardant Cables	143
5.4	Unguided Media	144
5.4.1	Microwaves Communication	145
5.4.2	Terrestrial Communication	145
5.4.3	Satellite Communication	146
5.4.4	Mobile Communication	147

5.5	SCADA Communication Technologies	152
5.5.1	Wired or Guided Media Technologies	152
5.5.1.1	Copper UTP	152
5.5.1.2	Optical Fiber	152
5.5.1.3	Fiber to the home (FTTH)	152
5.5.1.4	Hybrid Fiber Coax (HFC)	153
5.5.1.5	Power Line Carrier Communication (PLCC)	153
5.5.1.6	Broadband over Power Line (BPL)	154
5.5.1.7	HomePlug	154
5.5.2	Wireless or Unguided Media Technologies	155
5.5.2.1	IEEE and Wireless Standards	156
5.5.2.2	Frequency Hopping Spread Spectrum (FHSS)	156
5.5.2.3	3G Cellular	158
5.5.2.4	Wi-Fi	159
5.5.2.5	WiMax	160
5.5.2.6	ZigBee	161
5.5.2.7	ZWave	162
5.5.2.8	VSAT	164
5.6	Security in Wireless Communications	164
5.6.1	Endpoint Threat Detection and Response (ETDR)	165
5.6.2	Transparency	165
5.6.3	Redundancy in SCADA and Smart Grid	166
	<i>Summary</i>	167
CHAPTER 6	SCADA AND DCS PROTOCOLS	169
6.1	Introduction	169
6.2	Evolution of SCADA Communication Protocols	169

6.3	SCADA Communication Protocols	170
6.3.1	Distributed Network Protocol (DNP) 3.0	171
6.3.1.1	Protocol Architecture of DNP3	171
6.3.2	Modbus	172
6.3.2.1	Modbus Limitations	176
6.3.2.2	Attacks on the DNP3 and Modbus	177
6.3.3	Profibus	177
6.3.3.1	Profibus Process Automation (PA)	178
6.3.3.2	Profibus Factory Automation (Decentralized Peripherals-DP)	179
6.3.3.3	Profibus Fieldbus Message Specification (FMS)	179
6.3.3.4	Communication Architecture of Profibus	180
6.3.4	IEC 60870-5-101/103/104	181
6.3.5	IEC 60870-5-101 [T-101]	181
6.3.6	IEC 60870-5-103 [T-103]	182
6.3.7	IEC 60870-5-104 [T-104]	183
6.3.7.1	Protocol Architecture of IEC 60870-5	184
6.3.7.2	Attacks on IEC 60870-5	185
6.3.8	IEC 61850	185
6.3.8.1	Comparison of DNP3 vs. IEC- 61850 GOOSE	187
6.3.8.2	Attacks on IEC 61850 Protocol	188
6.3.9	ICCP TASE .2 (IEC 60870-6)	188
6.3.9.1	ICCP Functionalities	189
6.3.9.2	Protocol Architecture of ICCP TASE 2	189
6.3.9.3	Implementation Issues and Interoperability	190
6.3.9.4	ICCP-Product Differentiation	191
6.3.9.5	ICCP- Product Configurations	191

6.4	Other Relevant Standards	192
6.4.1	IEEE C37.118.1 Synchrophasor Standard	192
6.4.2	IEC 61968 Standard	193
6.4.3	IEC 61970 Standard	193
6.4.4	IEC 62325 Standard	193
6.4.5	IEC 61508 Standard	194
6.4.6	IEC 62351 Security Standard	195
6.4.7	IEC 62056 Electricity Metering Data Exchange Standard	196
6.4.8	IEC 62056-21	197
6.5	Secure Communication (sCOMMUNICATION)	197
6.6	Selecting the Right Protocol for SCADA	197
	<i>Summary</i>	199

CHAPTER 7 SECURING INDUSTRIAL CONTROL SYSTEMS 201

7.1	Introduction	201
7.2	IT Security and SCADA Security	202
7.3	Security Definitions	203
7.4	Managing Risk	205
7.5	SCADA Threat Sources	206
7.6	SCADA and Smart Grid Vulnerabilities, Threats and Attacks	206
7.7	Alarming SCADA and Smart Grid Threats	209
7.7.1	Zero Day Vulnerabilities	209
7.7.2	Non-prioritization of Tasks	210
7.7.3	Database Injection	210
7.7.4	Communication Protocol Issues	210
7.7.5	Stealthy Integrity Attacks	211
7.7.6	Replay Attack	211

7.7.7	False Data Injection Attack	211
7.7.8	Zero-Dynamics Attack	212
7.7.9	Covert Attack	212
7.7.10	Surge Attack, Bias Attack, and Geometric Attack	212
7.8	Dreadful SCADA Malwares	213
7.9	Privilege Targets of Hackers	213
7.9.1	Attack Vector Through HMI	214
7.9.2	Security Concerns of SCADA Control Centre	215
7.9.3	Flash Drive Usage and End Node Security (ENS)	217
7.9.4	BadUSB	217
7.10	SCADA Intrusion Detection SYSTEMS (IDS)	218
7.11	Defence-in-Depth Architecture	220
7.12	Firewall deployment and Firewall Policies	222
7.13	Proposed Security Solutions	225
7.13.1	Securing the AMI	226
7.13.2	Making the Smart Grid Smarter than Cyber-Attacks	227
7.13.3	Zone Based Architecture	231
7.13.4	Follow Standards and Guidelines	232
	<i>Summary</i>	233
	<i>Index</i>	235