

PRACTICAL SCADA

March 2009 SCADA PERSPECTIVE

- Developing Gap Training Capabilities

Ron Southworth

F. Inst. M. Sci., EE.



**Homeland
Security**

CSSP SME



Celebrating 125 Years
of Engineering the Future

Member IEEE

Practical SCADA

Developing Gap Training Capabilities

Copyright Ron Southworth

March 2009

Prepared for use as part of a training package for people seeking a SCADA Perspective

ABSTRACT

The strength, growth and prosperity of our nations are dependant on being sustained by key resources and a functioning and healthy infrastructure. The heart of this infrastructure is kept beating by a variety of industrial control systems. The term SCADA (supervisory control and data acquisition) or industrial control systems can equally refer to process control, distributed control, and any other kindred systems that control, monitor, and manage critical infrastructure.

Critical SCADA infrastructure and key resources are usually considered to consist of electric power generators, transmission systems, transportation systems, dam and water systems, communication systems, chemical and petroleum systems, and other critical systems that cannot tolerate sudden interruptions to service. Simply stated, a control system gathers information and then performs a function based on the established parameters and information it receives.

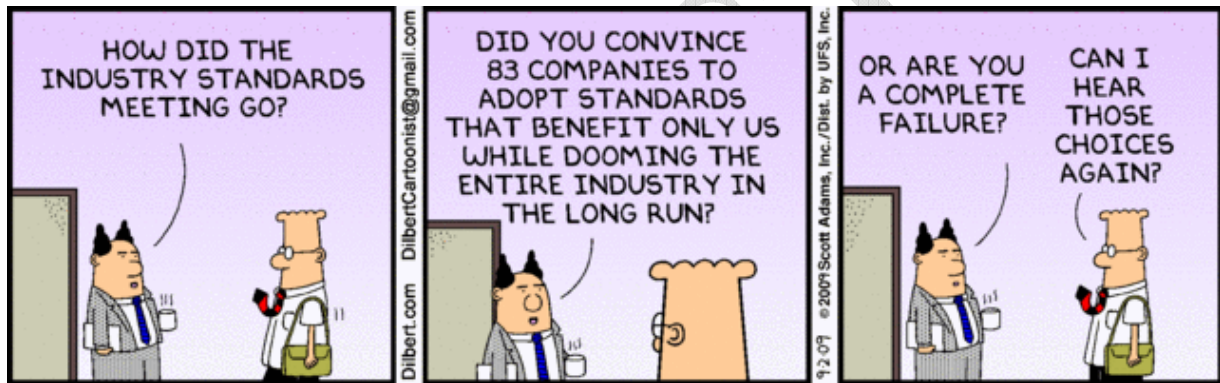
Gaps or shortfalls are appearing in industry generally in terms of knowledge and or experience, especially with respect to the practical aspects of application of design, configuration, maintenance and operation of ICS systems. This problem is relentlessly increasing, every day through the situation of natural attrition of the wealth of talent leaving the industry without any form of effective succession planning being put into place.

The intent of this body of work is to help address and close these gaps by providing practical material so that knowledge and experience can be better imparted or applied.

All future instances where reference is made to SCADA Systems in this text as mentioned in the above collection of control systems variations all can be considered to be inferred or apply generally.

EXECUTIVE SUMMARY

This manual provides practical information for those interested in the design, installation, maintenance and safe & secure operation of industrial control systems within a enterprise, organization or facility. The manual is an attempt to consider the SCADA system in a holistic way or as I like to say "from end to end".



ACKNOWLEDGEMENTS

The Author would like to thank the many contributors from the SCADA Mail list (SCADA@SCADPerspective.com) , the many friends, peers, colleagues, & numerous vendors that have provided practical advice, assistance, moral support, ideas, concepts and original material to turn this manual from a pipe dream into a reality.

CONTENTS

1.	DEVELOPING GAP TRAINING CAPABILITIES	21
1.1	Introduction.....	21
1.2	Background.....	21
1.3	Audience and Scope	21
1.4	A High level definition of a SCADA system	22
1.5	What is a SCADA system comprised of	23
2.	THE PRINCIPALS OF MEASUREMENT	25
2.1	Why Measure.....	25
2.2	Why have standards	25
2.3	THE METRIC SYSTEM OF MEASUREMENT.....	26
2.3.1	STANDARDS INTERNATIONAL (SI) UNITS.....	26
2.4	THE ENGLISH SYSTEM OF MEASUREMENT.....	32
2.5	US CUSTOMARY STANDARD OF MEASUREMENT	33
2.5.1	Units of length	34
2.5.2	Units of capacity	35
2.5.3	Fluid volume.....	35
2.5.4	Units of mass	36
2.5.5	Units of temperature	37
2.5.6	Other units	37
2.6	MEASURING INSTRUMENTS	38
2.7	MEASUREMENT STANDARDS.....	38
2.8	MEASUREMENT PERFORMANCE TERMS AND SPECIFICATIONS.....	39
2.8.1	Accuracy	40
2.8.2	Hysteresis.....	40
2.8.3	Linearity.....	41
2.8.4	Drift.....	41
2.8.5	Repeatability	42
2.8.6	Response.....	44
2.9	INSTRUMENTATION CALIBRATION	45
2.9.1	Compliant Calibration	45
2.9.2	Calibration Certificates	45
2.9.3	Calibration Certificate Facts.....	46
2.10	PRESSURE MEASUREMENT	47
2.10.1	Units used to measure pressure.....	47
2.10.2	Absolute, Gauge and Differential Pressure (DP).....	47
2.10.3	Pressure sources.....	48
2.11	MECHANICAL PRESSURE TRANSDUCERS AND ELEMENTS.....	51
2.11.1	C-Bourdon tube	51
2.11.2	Helix and spiral tubes.....	52
2.11.3	Spring and bellows	54
2.11.4	Pressure Diaphragm.....	56

2.11.5	Manometers	57
2.11.6	Single and double inverted bell	58
2.12	PRESSURE TRANSDUCERS AND ELEMENTS – ELECTRICAL/ELECTRONIC.....	59
2.12.1	Strain Gauge	59
2.12.2	Vibrating Wire	61
2.12.3	Piezoelectric	61
2.12.4	Capacitance.....	62
2.12.5	Linear variable differential transformer (LVDT)	64
2.12.6	Optical	64
2.12.7	Installation Considerations.....	65
2.13	LEVEL MEASUREMENT.....	69
2.13.1	Continuous measurement.....	70
2.13.2	Point Detection	70
2.13.3	Gauging Rod Method.....	71
2.13.4	Buoyancy Tape Systems	72
2.13.5	Float and Tape Systems.....	72
2.13.6	Wire Guided Float Detectors.....	72
2.13.7	Hydrostatic Pressure	74
2.13.8	Capacitive Level Measurement.....	83
2.13.9	Using DP for measuring process filter performance.....	87
2.13.10	Atmospheric Vessels	87
2.13.11	Pressurised Vessels.....	88
2.13.12	Weighing Method	88
2.14	Ultrasonic Measurement.....	89
2.14.1	Principle of Operation.....	89
2.15	Radar Measurement.....	93
2.16	Volume Measurement For Different Vessel Shapes	94
2.17	Vibration Switches.....	94
2.18	Radiation Measurement.....	95
2.18.1	The Source	95
2.18.2	The Strip Detector	96
2.18.3	Point Level Measurement.....	97
2.18.4	Continuous Level Measurement	97
2.19	LT Impact on process control loop performance	100
2.20	Density Measurement.....	100
2.20.1	Hydrostatic pressure method	100
2.20.2	Radiation	100
2.20.3	Vibration	101
2.20.4	Differential Pressure.....	101
2.20.5	Temperature Effects.....	101
2.21	TEMPERATURE MEASUREMENT	102
2.21.1	Contact	102
2.21.2	Liquid-In-Glass, Filled, Bimetallic	102
2.21.3	Bimetallic	106
2.21.4	Non Contact Pyrometers.....	107
2.21.5	Resistance Temperature Detectors (RTD's)	109

2.21.6	Thermistors	113
2.21.7	Thermocouples	115
2.21.8	The Reference Junction	116
2.21.9	The Peltier and Seebeck Effect.....	117
2.21.10	Acoustic Pyrometers	122
2.21.11	Installation Considerations	122
2.21.12	Location and Cabling	122
2.21.13	Thermowells	123
2.21.14	Effects of Self Heating	123
2.21.15	Noise	123
2.21.16	Thermal Lag effect on control loop response.....	124
2.22	HUMIDITY.....	124
2.22.1	Relative Humidity.....	124
2.22.2	Absolute Humidity	124
2.22.3	Capacitive Humidity Measurement.....	125
2.23	FLOW MEASUREMENT	127
2.23.1	Types of Flow.....	127
2.23.2	Basic Terms and Concepts.....	127
2.23.3	Vena Contracta	131
2.23.4	Range-ability	131
2.23.5	Flow Measurements.....	131
2.23.6	Differential Pressure Flow meters	133
2.23.7	Formulae for flow rate with respect to pressure change	134
2.23.8	Primary Element	134
2.23.9	Orifice Plate.....	134
2.23.10	Orifice Type	135
2.23.11	Tap Locations	137
2.23.12	Selection and Sizing	138
2.23.13	Venturi Tube.....	138
2.23.14	Flow Nozzles.....	139
2.23.15	Flow Tube	139
2.23.16	Application Limitations.....	139
2.23.17	Pitot Tube	139
2.23.18	Multiport Pitot Averaging (Annubar).....	140
2.23.19	Elbow.....	141
2.23.20	Primary element.....	142
2.23.21	Open Channel Flow Measurement.....	143
2.23.22	Weirs	143
2.23.23	Flumes.....	144
2.23.24	Flow Installation and Selection Considerations	145
2.23.25	Primary Element.....	145
2.23.26	Secondary Element	145
2.23.27	Variable area flowmeters.....	146
2.23.28	Oscillatory Flow Measurement	147
2.23.29	Turbine.....	152
2.23.30	Magnetic Flowmeters.....	153
2.23.31	Advantages of a Magmeter	154

2.23.32	Positive Displacement.....	156
2.23.33	Ultrasonic Flow Measurement.....	158
2.23.34	Mass Flow Meters.....	160
2.23.35	The Coriolis Meter.....	160
2.23.36	Thermal Mass Flowmeters.....	162
2.24	MEASURING MASS (WEIGHTOMETERS).....	166
2.24.1	Introduction.....	166
2.24.2	Load cell.....	166
2.24.3	Types of Load cells.....	167
2.24.4	Weighing with Load cells.....	168
2.24.5	Installation of belt Weightometers.....	171
2.25	CONTROL VALVES.....	177
2.25.1	Functional Application.....	177
2.25.2	Operating Conditions.....	177
2.25.3	Construction.....	177
2.25.4	Sizing.....	178
2.25.5	Sliding Stem Valves.....	178
2.25.6	Globe Valves.....	178
2.25.7	Cage Valves.....	179
2.25.8	Split Body Valves.....	179
2.25.9	Angle Valves.....	179
2.25.10	Y-Style Valves.....	180
2.25.11	Three-Way Valves.....	180
2.25.12	Single Seated.....	181
2.25.13	Double Seated.....	181
2.25.14	Rotary Valves.....	184
2.25.15	Ball Valves.....	185
2.25.16	Control Valve Selection and Sizing.....	186
2.25.17	Control Valve Characteristics/Trim.....	189
2.25.18	Control Valve Noise and Cavitation.....	192
2.25.19	Cavitation and Flashing.....	193
2.25.20	Actuator and Positioner Operation.....	194
2.25.21	Valve Benchset and Stroking.....	197
2.25.22	Overall process control performance.....	197
3.	THE COMMUNICATIONS PROCESS.....	199
3.1	ISO 7 LAYER MODEL.....	201
3.1.1	The open systems interconnection model.....	204
3.1.2	Application layer.....	205
3.1.3	Presentation layer.....	205
3.1.4	Session layer.....	205
3.1.5	Transport layer.....	206
3.1.6	Network layer.....	207
3.1.7	Data link layer.....	207
3.1.8	Physical layer.....	208
3.1.9	Local Area Networks, Introducing Ethernet and TCP/IP.....	208
4.	STRUCTURED CABLING SYSTEMS.....	212

4.1	Copper Cabling.....	212
4.1.1	Factors affecting copper cable performance.....	212
4.1.2	Twisted pair cable.....	213
4.1.3	Components of twisted pair cable.....	214
4.1.4	Shielded twisted pair (STP) cable.....	215
4.1.5	Unshielded twisted pair (UTP) cable.....	215
4.1.6	Performance requirements.....	216
4.1.7	Advantages of twisted pair cable.....	217
4.1.8	Disadvantages of twisted pair cable.....	218
4.1.9	Sources of interference and noise on cables.....	218
4.2	Distribution frames – The Krone System.....	220
4.2.1	The main distribution frame (MDF).....	221
4.2.2	Intermediate distribution frames (IDF).....	222
4.2.3	Final distribution frames (FDF).....	222
4.3	INSTRUMENTATION CABLING SYSTEMS.....	222
4.3.1	Field wiring system.....	222
4.3.2	Noise and interference on loop signals.....	223
4.3.3	How do we reducing signal interference.....	224
4.3.4	Grounding.....	227
5.	RS232 RS422 RS485.....	230
5.1	RS-232 Interface Standard.....	230
5.1.1	Asynchronous Operation RS-232.....	234
5.1.2	Synchronous Communications.....	235
5.1.3	Disadvantages of the RS-232 standard.....	236
5.1.4	The RS-422 Interface Standard for Serial Data Communications.....	236
5.1.5	The RS-485 Interface Standard.....	237
5.1.6	RS-485 Interface.....	238
6.	LIGHTNING PROTECTION.....	244
6.1.1	Typical earthing plan.....	245
6.1.2	Levels of lightning protection.....	246
6.1.3	Separating equipment and lightning.....	247
6.1.4	Dissipating the lightning.....	248
6.1.5	Dissipation of high voltages or currents.....	249
6.1.6	High current protection.....	249
6.1.7	High voltage protection.....	249
7.	FIBER OPTIC CABLING SYSTEMS.....	251
7.2	Fiber Optic Fundamentals.....	253
7.2.1	Reflection, refraction and diffraction.....	253
7.2.2	Construction of an optical fiber.....	255
7.2.3	Fresnel reflection.....	257
7.2.4	The light transmission nature of glass.....	257
7.2.5	Modal propagation in fibers.....	259
7.2.6	Number of modes.....	260
7.2.7	Modal Leakage.....	261

7.2.8	Profiling Refractive index	261
7.2.9	Multimode Step and Graded Index Fibers	261
7.2.10	Standards	265
7.2.11	Wave division multiplexing (WDM /DWDM)	268
7.2.12	Signal Quality Effects on optical signal transmission.....	268
7.2.13	Other types of fibers	273
7.2.14	Fiber System Installation objectives	275
7.2.15	Classes of Fiber optic cables.....	280
7.3	Splicing & Connecting Fibers.....	285
7.3.1	Splicing Fibers.....	289
7.3.2	Optical couplers	296
7.3.3	Laser diodes.....	300
7.3.4	Pin photodiodes.....	303
7.3.5	Avalanche photodiodes	305
7.4	Optical receiver modules	306
7.5	Installing Fiber Optic Cables	308
7.5.2	Fiber optic problems.....	327
8.	ETHERNET	329
8.1	Ethernet Systems	329
8.1.1	DIX and IEEE 802.3 frames.....	329
8.1.2	Ethernet MAC addresses.....	330
8.1.3	Use of type field for protocol identification	331
8.1.4	Media access control (MAC) for half-duplex LANs (CSMA/CD).....	333
8.1.5	MAC (CSMA-CD) for gigabit half-duplex networks.....	337
8.1.6	Full-duplex transmissions.....	338
8.1.7	Ethernet flow control.....	339
8.1.8	Auto Negotiation.....	340
8.1.9	Deterministic Ethernet.....	341
8.1.10	Industrial Ethernet Equipment	342
8.1.11	Noise.....	346
8.1.12	UTP problems.....	346
9.	DATA COMMUNICATION PROTOCOLS.....	357
9.1	Communications Protocols	357
9.2	The TCP/IP protocol suite	358
9.2.1	The network interface layer.....	358
9.2.2	The Internet layer	358
9.2.3	Host-to-host layer.....	359
9.2.4	The application layer	359
9.2.5	Transmission Control Protocol (TCP).....	359
9.2.6	Ports	360
9.2.7	Sockets.....	361
9.2.8	Sequence numbers.....	361
9.2.9	Acknowledgement numbers	361
9.2.10	The TCP frame.....	362
9.2.11	Internet Protocol (IP).....	363

9.2.12	The purpose of the IP address.....	364
9.2.13	IPv4 address notation.....	364
9.2.14	Network ID and host ID.....	365
9.2.15	Subnet masks.....	365
9.2.16	Private vs. Internet-unique IP addresses.....	366
9.2.17	IPv4 header structure.....	367
9.2.18	Address Resolution Protocol (ARP).....	369
9.2.19	General Overview of Routing/Routers.....	369
9.2.20	Direct or indirect delivery method.....	370
9.2.21	Static versus dynamic routing.....	370
9.3	User Datagram Protocol (UDP).....	371
9.3.1	Basic functions.....	371
9.3.2	UDP frame format.....	372
9.3.3	Domains (Autonomous systems).....	373
9.3.4	Interior, exterior and gateway-to-gateway protocols.....	373
9.4	MODBUS.....	374
9.4.1	MODBUS Protocol.....	374
9.4.2	Principals of MODBUS.....	374
9.4.3	MODBUS functions.....	375
9.4.4	Protocol characteristics.....	375
9.4.5	Message format.....	375
9.4.6	Synchronization.....	376
9.4.7	Memory notation.....	377
9.4.8	MODBUS TCP/IP.....	384
9.5	Distributed Network Protocol 3.0 (DNP3).....	386
9.5.1	Application layer.....	386
9.5.2	Application message formats.....	387
9.5.3	Application control field.....	388
9.5.4	Application function codes.....	389
9.5.5	Internal indications.....	391
9.5.6	The object header.....	392
9.5.7	DNP Objects.....	393
9.5.8	The qualifier and range fields.....	394
9.5.9	The transport layer.....	395
9.5.10	The data link layer.....	396
9.5.11	The physical layer.....	399
9.5.12	DNP3 over a network.....	400
9.5.13	DNP3 subset definitions.....	401
9.5.14	Polling and communications options.....	404
9.5.15	Time synchronization.....	406
9.5.16	DNP3 over TCP/IP and UDP/IP.....	408
9.5.17	DNP3 LAN/WAN Functionality.....	410
9.5.18	DNP3 device Interoperability.....	413
9.5.19	Data classes and events.....	415
9.6	IEC16850.....	428
9.6.1	Version 2 options.....	429
9.6.2	UCA Security.....	436

10.	SMART INSTRUMENTATION BUS TECHNOLOGY SYSTEMS.....	439
10.1	Highway Addressable Remote Transducer Protocol (HART).....	440
10.1.1	Application Layer	441
10.1.2	Universal commands	441
10.2	FOUNDATION FIELDBUS.....	441
10.2.1	Field Bus.....	442
10.2.2	Fieldbus Signaling 31.25 kbit/s.....	443
10.2.3	The data link layer.....	447
10.2.4	The application layer.....	448
10.2.5	The user layer.....	448
10.2.6	High speed Ethernet.....	450
10.2.7	The physical layer and wiring rules.....	451
10.2.8	Noise and Earthing Considerations	453
10.2.9	Capacitive Coupling	454
10.3	Profibus.....	464
10.3.1	The physical layer.....	465
10.3.2	The data link layer.....	466
10.4	Controller Area Network (CAN) Protocol.....	470
10.5	DF1.....	470
10.6	DeviceNet.....	470
10.7	ControlNet.....	470
10.8	OLE for Process Control (OPC)	470
11.	RADIO FREQUENCY COMMUNICATIONS.....	471
11.1	A BRIEF HISTORY OF RADIO.....	472
11.2	ELECTROMAGNETIC WAVES.....	472
11.2.1	CW The first information transmissions.....	474
11.2.2	The Oscillator.....	475
11.3	RADIO FREQUENCY ALLOCATION ITU (LICENSING).....	475
11.3.2	Simplex (single frequency allocation).....	478
11.3.3	Duplex (Two-frequency allocation).....	479
11.3.4	The Amplifier.....	479
11.4	Filters	479
11.4.1	Type of filters.....	480
11.4.2	Mechanical filters.....	481
11.4.3	Crystal filters.....	482
11.4.4	Cavity filters (Bottles).....	483
11.5	Modulation and demodulation.....	483
11.5.1	Amplitude modulation	484
11.5.2	Frequency modulation (FM).....	485
11.5.3	Phase modulation (PM).....	487
11.6	Transmitters	487
11.6.1	AM transmitters	487
11.6.2	PM and FM transmitters.....	488
11.6.3	Modulation schemes.....	489

11.6.4	Sidebands and bandwidth.....	490
11.7	Receivers	490
11.7.1	AM receiver	491
11.7.2	Pre-emphasis and de-emphasis	491
11.7.3	Signal to noise ratio and SINAD	492
11.8	SPREAD SPECTRUM.....	493
11.8.1	Orthogonal frequency division multiplexing (OFDM).....	495
11.8.2	Types of spread spectrum	498
11.8.3	Transmission limitations.....	499
11.9	Components of a radio link	500
11.10	Radio Frequency Feeder Systems.....	501
11.11	Multi coupler and cavity filters.....	506
11.11.1	Duplexer.....	506
11.11.2	Splitters.....	508
11.11.3	Receiver pre-amplifiers.....	508
11.11.4	Circulators and isolators	508
11.12	ANTENNAE.....	509
11.12.1	So how do they work.....	510
11.12.2	Types of antennas.....	512
11.12.3	Antenna installation	513
11.12.4	Stacked arrays.....	513
11.12.5	Antenna diversity	514
11.12.6	VSWR and return loss.....	515
11.12.7	Microwave antennas (Dishes)	517
11.12.8	Interference.....	519
11.12.9	Propagation	521
11.12.10	Ionospheric reflection and scatter	521
11.12.11	Line of sight.....	522
11.12.12	Transmitter power/receiver sensitivity	527
11.13	Implementing a radio link	527
11.13.1	Gain and loss.....	528
11.13.2	Level.....	528
11.13.3	Attenuation.....	529
11.13.4	Free space attenuation	530
11.13.5	RF path loss calculations	530
11.14	Path profile	530
11.14.1	Calculating Fade Margin	532
11.15	IEEE 802.11BASED Technologies	537
11.15.1	Which Standard should be deployed?	537
11.15.2	802.11 Specifications.....	538
11.15.3	802.11 OSI Layer Implementation	538
11.15.4	IR PHY.....	539
11.15.5	802.11 PHY layers.....	539
11.15.6	802.11 FH PHY	540
11.15.7	ISM emission rules and maximum throughput.....	541
11.15.8	802.11 DS PHY	541

11.15.9	802.11b: HR/DSSS PHY.....	544
11.15.10	Medium Access Control (MAC).....	549
11.15.11	MAC access modes and timing.....	549
11.15.12	Network Allocation Vector (NAV).....	550
11.15.13	802.11 Frame format.....	551
11.15.14	IEEE 802.11 architecture.....	556
11.15.15	Adhoc (Independent) 802.11 networks.....	557
11.15.16	Infrastructure 802.11 networks.....	557
11.15.17	802.11 IP roaming.....	558
11.15.18	802.11 Security issues.....	559
11.15.19	802.11 Cryptographic background to WEP.....	560
11.15.20	802.11 WEP Encryption Conclusions and recommendations.....	562
11.15.21	Authentication Security Issues 802.1x.....	562
11.15.22	The Extensible Authentication Protocol (EAP).....	563
11.15.23	Wireless Ethernet Point to Multipoint Networks.....	564
12.	MICROWAVE SYSTEMS.....	568
12.1	SATELLITE.....	577
12.1.1	Background.....	577
12.1.2	Classes of Services.....	577
12.1.3	Domestic.....	580
12.1.4	Experimental Systems.....	580
12.1.5	Relevant Organizations.....	580
12.1.6	Theory of operation.....	583
12.1.7	Downlinks and Uplinks.....	583
12.1.8	VSat TM.....	587
12.2	Cellular radio concepts.....	589
12.2.1	Common Carrier networks Cellular Signalling.....	590
12.2.2	Cellular Analog Systems.....	591
12.2.3	AMPS.....	592
12.2.4	NAMPS.....	593
12.2.5	Digital Cellular Systems.....	593
12.2.6	TDMA.....	595
12.2.7	CDMA.....	596
12.2.8	GSM.....	597
12.2.9	CTS.....	599
12.2.10	DECT.....	599
12.2.11	Wireless Data Systems.....	601
12.2.12	GPRS.....	603
12.2.13	PCS.....	603
12.2.14	WAP.....	605
12.2.15	3G Systems.....	606
12.3	Trunked Radio Terrestrial (TETRA).....	607
12.3.1	TETRA PMR Standard.....	608
12.3.2	The CALL PROCESS.....	609
13.	PROCESS & INSTRUMENTATION DIAGRAMS (P&ID).....	611

14.	PRINCIPALS OF PROCESS CONTROL.....	622
15.	The SCADA System.....	624
15.1	Features of a SCADA system.....	624
15.1.1	Modern SCADA systems.....	625
15.1.2	Remote terminal units.....	631
15.1.3	Analog output modules.....	634
15.1.4	Digital input modules.....	634
15.1.5	PLCs used as RTUs.....	636
15.1.6	The master station.....	636
15.1.7	Communication philosophies.....	638
15.1.8	Polled (master–outstation).....	638
15.2	Human Machine Interface.....	644
15.2.1	Abnormal Situation Management.....	644
15.2.2	Alarm Management.....	658
16.	SYSTEMS INTERGRATION.....	661
16.1.1	Displays and HMIs.....	661
16.1.2	Calculation of Individual Instruments and Total Error for the System.....	666
17.	Network Architecture.....	668
17.1	Design Considerations.....	668
17.1.1	System Category.....	668
17.2	Communication Architectures.....	669
17.2.1	Point to Point (Two Stations).....	669
17.2.2	Multipoint (or Multiple Stations).....	669
17.2.3	Appropriate radio systems.....	670
17.2.4	Continuous Keyed (Hot Carrier) Repeaters.....	672
17.2.5	Types of Radio Installations.....	673
17.2.6	Antenna support structure.....	675
17.2.7	Typical community radio site configuration.....	675
17.2.8	Miscellaneous considerations.....	675
17.2.9	Duplication.....	679
17.2.10	Standby transmitters.....	679
17.2.11	Fiber Optic System Design.....	684
17.2.12	Transmission parameters.....	685
17.2.13	Testing of Fiber Optic Systems.....	699
18.	Performance Analysis.....	715
18.1	Reliability.....	716
18.1.1	Definition of reliability.....	716
18.1.2	Landlines.....	720
18.1.3	SCADA system reliability (or failure) rates.....	722
18.2	Reliability calculations.....	723
18.2.1	Failure Rate.....	723
18.2.2	Mean time between failure.....	723
18.2.3	Availability.....	723

18.2.4	Qualification of the processes	724
18.3	Equipment shelters (Outstation).....	724
18.3.1	Temperature management.....	724
18.3.2	Other aspects of building design.....	726
18.4	Power supplies	726
18.4.1	Distributed DC supply and batteries	727
18.4.2	Types of storage battery cells	727
18.4.3	Lead acid	727
18.4.4	Installation and operation of battery systems	728
18.4.5	Mains Non-essential, essential and uninterruptible supplies	729
18.4.6	Mains power supplies	729
18.4.7	Standby plant.....	729
18.4.8	Diesel powered installations	729
18.4.9	Mains powered UPS.....	730
18.4.10	Solar power.....	731
18.4.11	Wind generators.....	731
18.4.12	Diesel Fuel Generators.....	732
18.4.13	Filtering dc supplies.....	734
18.4.14	SCADA monitoring of plant and equipment	735
18.4.15	Equipment racks.....	737
19.	Resilience & Risk management good practices	738
19.1	SCADA Resilience Framework.....	739
19.1.1	Framework Objectives.....	739
19.1.2	Strategic Benefits.....	739
19.2	SCADA Risk Management Framework (To AS4360).....	741
19.2.2	Treating Risk.....	746
19.2.3	Generic SCADA Process Model	746
19.2.4	Generic SCADA Enablers.....	747
20.	HAZOP.....	750
20.1.1	The Life Cycle Approach to HAZOP.....	750
20.1.2	Making allowance for quality assurance in hazard studies	751
20.1.3	The Six Level Hazard Study Lifecycle	752
20.1.4	Process hazard study 1	755
20.1.5	Level 2 process hazard study	758
20.1.6	HAZOP Study methods.....	758
20.1.7	Level 2 Hazard study systematic procedure.....	759
20.1.8	Software tools for PHA.....	766
20.1.9	HAZOP Study Methods	766
20.1.10	Overview of HAZOP method	767
20.1.11	The examination phase	767
21.	SAFETY INSTRUMENTED SYSTEMS	774
21.1	An Overview of Safety Instrumented Systems.....	774
21.2	Safety Instrumented Systems (SIS).....	775
21.3	Safety Systems Overview	776

21.3.1	Why do we need Safety systems	776
21.3.2	The architecture structure of an SIS.....	777
21.3.3	Safety integrity	777
21.4	Practical example of an SIS.....	777
21.4.1	Safety Integrity Levels (SIL).....	778
21.4.2	Protection layers.....	779
21.4.3	Diversification	780
21.5	Risk reduction models.....	780
21.5.1	Safety management principles	782
21.5.2	Managing risk.....	783
21.5.3	The process for managing risk.....	784
21.5.4	Risk management for plant safety	787
22.	SCADA Security 101.....	806
22.1.1	Partitioning of the network.....	807
22.1.2	Authentication.....	808
22.1.3	Firewalls	809
22.1.4	Routers.....	815
22.1.5	Encryption	816
22.1.6	Introduction to cryptography.....	816
22.1.7	Use and applicability of encryption in SCADA Systems.....	817
23.	Recommended Reading References.....	821
24.	Websites	823
25.	ACRONYMS.....	824
26.	GLOSSARY	827
27.	INSTRUMENTATION FEATURES AND LIMITATIONS	849
28.	SIS REFERENCES AND SOURCES OF INFORMATION	861
29.	Glossary of terms and abbreviations used in safety-instrumented systems	861
30.	HAZOP Appendix Guideline documents for hazard studies	869
31.	Appendix Summary of parameters used in the reliability analysis of safety systems	895
32.	Appendix Composite safety integrity levels table.....	896
33.	Appendix Hazard studies for computer systems	896