



# Design and Application of SCADA Systems in the Electric Power Industry

(Software and Hardware of ABB Company)

By:

Ali Parizad

Publication: Science Center Publication

Main Entry: Parizad, Ali, 1983

Title and author: Design and Application of SCADA Systems in the Electric Power Industry (Software and Hardware of ABB Company), Ali Parizad; Scientific Editor: Majid Ghadimi

Publication Specifications: Tehran, Science Center Publication, 2017

Appearance Specifications: 2 V., Illustrated, Table, Graph

ISBN: Volume: 978-964-327-188-6; Volume: 978-964-327-187-9; Volume1; 978-964-327-189-3

Listing status: FIPA

Note: Glossary

Subject: SCADA systems

Subject: Supervisory control Systems

Subject: Power - Systems - Software

Subject: Electric power Systems -- Software

Subject: Automatic data collection Systems

Congressional Classification: TJ222/P4T4 2017

Dewey Decimal Classification: 629/8

National Bibliographic Number: 4951727

.....  
Book Title: Design and Application of SCADA Systems in the Electric Power Industry (Software and Hardware of ABB Company)

Publication: Science Center Publication

Author: Ali Parizad

Scientific Editor: Majid Ghadimi

Page Designer: Fatemeh AdigoozalPour Ardabili

Cover Designer: Ali Parizad

First Publication: 2017 Autumn

Circulation: 1000

Printing and binding: Science Center Publication

2 Volumes Series with DVD Cost: 110000 T

First Volume ISBN: 9789643271879

Series ISBN: 9789643271893

Reproduction or re-production of all or part of this book, including printing, photocopying, any kind of dissemination in Internet and websites, the provision of CDs and DVDs, is prohibited. This work is covered by the Law on the Protection of the Rights of Writers and Writers of Iran, and the offenders are prosecuted under this law.
---

Distribution Centers:

Science Distribution: Enghelab Street, FakhR Razi St., East Azarbaijan St., No. 65, Unit 1, Telephone: (021)-66961568-66494911

<b>1- Chapter 1: SCADA Systems and RTU</b>	<b>23</b>
1-1. Need and role of control systems.....	23
1-1-1. Introduction .....	23
1-1-2. Necessity to Use Control Systems in the Power Grid .....	23
1-1-3. Introduction to Various Control Systems .....	24
1-1-3-1. Local Control.....	24
1-1-3-2. Centralized Control .....	24
1-1-3-3. Programmable Logic Controllers (PLCs) .....	25
1-1-3-4. Distributed Control System.....	26
1-1-3-5. New Control Systems after PLC and DCS .....	28
1-1-3-6. SCADA and Telemetry Systems.....	28
1-2. SCADA Configuration.....	33
1-2-2. Types of SCADA Systems .....	35
1-2-2-1. Local System .....	35
1-2-2-2. Communication System .....	37
1-2-2-3. Central System or Control Center.....	39
1-2-3. SCADA Systems Groups .....	39
1-2-3-1. Group 1 .....	39
1-2-3-2. Group 2 .....	40
1-2-3-3. Group 3 .....	42
1-2-4. Evaluation Parameters in SCADA Systems.....	42
1-2-4-1. Availability.....	42
1-2-4-2. Time Response.....	43
1-2-4-3. Expandability .....	43
1-2-4-4. Flexibility.....	43
1-2-4-5. Reliability .....	44
1-2-4-6. Security .....	44
1-3. Required Criteria for Data Selection.....	44
1-3-1. Introduction to Interface Concept .....	45
1-3-2. Role of Interface and its Importance in Communication between Power System and..	46
1-3-2-1. Data Transferring from Substation to Supervisory and Control Center .....	46
1-3-2-2. Sending Command from Center to Substation.....	46
1-3-3. Classification of Required Data for Substation.....	46
1-3-3-1. Digital Inputs «DI».....	47
1-3-3-2. Analog Inputs «AI» .....	50
1-3-3-3. Digital Outputs «DO».....	50
1-3-3-4. Samples of Digital and Analog Output Commands .....	51
1-4. SCADA and Role of Terminal Units.....	51
1-4-1. The Roles of Remote Terminal Units .....	52
1-4-1-1. Data Acquisition & Control «DAC» .....	52
1-4-1-2. Data Transferring to Upper Control Levels.....	52

1-4-2. Hardware Components of Remote Terminal Units.....	53
1-4-2-2. Digital Input Module «DI».....	53
1-4-2-3. Analog Input Module «AI».....	54
1-4-2-4. Analog Output Module «AO».....	55
1-4-2-5. Digital Output Module «DO».....	55
1-4-2-6. Communication Interface Unit «CIU».....	56
1-4-2-7. Main Module.....	56
1-4-2-8. Pulse Counter Input Module.....	56
1-4-2-9. LTE Module.....	56
1-4-2-10. Automatic Generation Controller Module.....	56
1-4-2-11. Modem.....	56
1-4-2-12. Power Supply.....	57
1-4-2-13. Using “Process Connection List” Table for RTU Installation.....	57
1-4-2-14. RTU Test Relay.....	60
1-4-3. Software Components of Remote Terminal Units.....	61
1-4-3-1. Data Acquisition & Control Module.....	61
1-4-3-2. TSL Module.....	62
1-4-3-3. SPV Module.....	62
1-4-3-4. SUC Module.....	62
1-4-3-5. Data Base Tables Module (DBT).....	62
1-4-3-6. Watchdog Module.....	62
1-4-3-7. Real Time Multi-Tasking Kernel.....	63
1-4-3-8. Diagnostics Module.....	63
1-4-3-9. Software Manager, SMNG Task.....	63
1-4-3-10. CMS, CMM Modules.....	63
1-4-3-11. Data Engineering at RTU.....	63
1-5. Data-Sending/Receiving Tanique.....	63
1-5-1. Communication Configuration.....	63
1-5-1-1. Point to Point.....	64
1-5-1-2. Party-Line.....	65
1-5-2. Communication Systems and Data-Sending Procedure.....	66
1-5-2-1. Public Telephone.....	67
1-5-2-2. Radio Communication.....	67
1-5-2-3. Fiber Optics.....	68
1-5-2-4. Power Line Carrier (PLC).....	68
1-5-2-5. Microwave.....	69
1-5-2-6. Satellite.....	70
1-5-3. Data Transferring Methods from RTU to Control Center.....	70
1-5-3-1. Polling Method and Sending Entire Data.....	71
1-5-3-2. Polling Method and Sending Changed Data.....	71
1-5-3-3. Interrupt Method.....	71
1-5-4. Communication Protocols.....	71
1-5-4-1. Protocol Description.....	72

1-5-4-2. Data Exchange Method.....	73
1-5-4-3. The Characteristics of Precise Data .....	74
1-5-4-4. Hamming Distance.....	74
1-5-4-5. Efficiency .....	75
1-5-4-6. Structure of Standard Frames .....	75
1-5-4-7. Comparison of two Protocols.....	76
1-5-5. Design of SCADA center .....	78
1-5-5-1. Installation of Required Equipment in Substation.....	78
1-5-5-2. Communication Link between Control Center and RTU .....	78
1-5-5-3. Capacity and Limitation of Data Points .....	78
1-5-6. Control and Data Acquisition Software .....	82
1-5-6-1. Data Acquisition and Control .....	82
1-5-6-2. Data Management .....	83
1-5-6-3. Control of Center Equipment.....	83
1-5-6-4. Control Center Software.....	84
1-5-6-5. Increasing System Security .....	85
1-5-6-6. Economic Dispatch Calculation .....	86
1-5-6-7. Scheduling (Load Forecasting, Unit Commitment, Hydro Optimization).....	86
1-5-6-8. Training Simulator.....	86
1-5-6-9. Operating System .....	87
1-6. Hardware Configuration of Control Center.....	87
1-6-1. Computer and Printer .....	87
1-6-2. Communication Equipment.....	88
1-6-3. UPS .....	88
1-6-4. Distributed Computer Architecture.....	88
1-6-5. Control Center Software. ....	88
1-6-5.1. Control Center Software Specifications.....	88
1-6-5.2. Data Base.....	89
1-6-5.3. SCADA Functions .....	90
1-6-5.4. Cursor Control .....	90
1-6-5.5. Point Selection .....	90
1-6-5.6. Alarm and Event Processing.....	91
1-6-5.7. Control .....	92
1-6-5.8. Attribute and Data Entry .....	92
1-6-6. Displays.....	92
1-6-7. Graphics Editor .....	94
1-6-8. Events and Operations Logging.....	94
1-6-9. SCADA Application Programs .....	95
1-6-9-1. Calculations .....	95
1-6-9-2. Archiving Historical Data .....	95
1-6-9-3. Report Generation .....	95
1-6-9-4. Programmer Support Facilities.....	95
1-6-9-5. System Maintenance and Diagnostic Programs.....	96

1-6-9-6. Maintainability and Availability .....	96
1-6-9-7. Human-Machine Interface .....	96
1-7. ABB SCADA Systems .....	96
1-7-1. History of RTU in ABB Company .....	97
1-7-2. RTU and its Communication with Control Center and Other Equipment.....	97

<b>2- Chapter 2: SCADA Hardware</b> .....	<b>101</b>
2-1. Introduction .....	101
2-2. ABB Hardware.....	101
2-3. Application of Hardware in SCADA Systems.....	102
2-4. RTU Hardware Design.....	103
2-5. General Concept of RTU .....	104
2-6. Rack Mounted Systems.....	105
2-6-1. Swing Frame Rack .....	105
2-6-1-1. Swing Frame Mounting 560SFR02 .....	105
2-6-1-2. 23ET23 Rack .....	109
2-6-1-3. 23ET24 Rack .....	113
2-6-1-4. 23TP21 Rack .....	115
2-6-1-5. 23TP22 Rack .....	118
2-6-1-6. 560CSR01 Rack.....	122
2-6-2. Mounting Plate Rack.....	124
2-6-2-1. 560MPR01 Rack .....	124
2-6-2-2. 560MPR03 Rack .....	131
2-6-3. CMU Types in Rack Mounted Systems.....	132
2-6-3-1. 560CMU02 .....	133
2-6-3-2. 560CMU04 .....	138
2-6-3-3. 560CMU05 .....	144
2-6-3-4. 560SLI01.....	151
2-6-3-5. 560SLI02.....	156
2-6-3-6. 560ETH01 .....	157
2-6-3-7. 560ETH02 .....	162
2-6-4. Serial Peripheral Bus .....	166
2-6-5. Different Types of Power Supply.....	168
2-6-5-1. 560PSR00.....	169
2-6-5-2. 560PSU01 (R0001/R0002).....	170
2-6-5-3. 560PSU02.....	173
2-6-6. Bus Communication Unit .....	176
2-6-6-1. Bus Connection Unit 560BCU01 .....	177
2-6-6-2. Bus Connection Unit 560BCU02 .....	181
2-6-6-3. Bus Connection Unit 560BCU03 .....	184
2-6-6-4. Bus Connection Unit 560BCU04 .....	187
2-6-6-5. Bus Connection Unit 560BCU05 .....	190
2-6-7. I/O, Modem Cards .....	192

2-6-7-1. Digital Input Card (23BE23).....	192
2-6-7-2. Digital Output Card (23BA20) .....	198
2-6-7-3. Analog Input Card (23AE23).....	203
2-6-7-4. Analog Output Card (23AA20) .....	210
2-6-7-5. Modem (23WT25) .....	216
2-6-7-6. Time Clock Card (560RTC03).....	233
2-6-8. Rack Types .....	239
2-6-9. Communication Racks .....	239
2-6-9-1. Input / Output Racks.....	240
2-6-9-2. Composite Racks.....	241
2-6-10. Hardware Redundancy.....	241
2-6-10-1. Power Supply Redundancy in Composite Racks .....	241
2-6-10-2. CMU Redundancy.....	242
2-6-11. System Limitations.....	243
2-6-12. System Licenses .....	244
2-6-13. Examples for Different Configurations .....	244
2-6-13-1. Small Systems with 560MPR01 .....	244
2-6-13-2. Small Systems with 560CMU02 .....	245
2-6-13-3. Standard Systems with I/O Extension.....	245
2-6-13-4. Sample Systems with Redundancy .....	246
2-6-13-5. Systems with Protocol Converter Gateway.....	247
2-7. DIN RAIL Mountable Modules .....	247
2-7-1. Types of DIN Rail Modules .....	247
2-7-2. I/O Bus .....	248
2-7-3. Communication Modules for DIN Rail Systems .....	249
2-7-3-1. 560CMU01 .....	250
2-7-3-2. 560CMG10.....	251
2-7-3-3. 560CIG10.....	257
2-7-3-4. 560CMD11 .....	274
2-7-4. Power Supply for DIN Rail Systems .....	285
2-7-4-1. 560PSU40, 560PSU41.....	286
2-7-4-2. 560PSU10.....	287
2-7-4-3. Adaptor 23VG23 .....	288
2-7-4-4. Adaptor 23VG24 .....	289
2-7-4-2. 23PU63.....	290
2-7-5. Interface Adaptor .....	291
2-7-5-1. 23AD62.....	292
2-7-5-2. 23AD63.....	292
2-7-5-3. 23AD64 (Interface Adaptor 23AD64).....	292
2-7-5-4. 23SC60 (Interface Adaptor 23SC60).....	293
2-7-5-5. Interface Adaptor 211ADD52.....	295
2-7-6. System Limitations .....	295
2-7-6-1. Stand Alone Modules .....	296

2-7-6-2. Scalable Housings Modules .....	297
2-7-6-3. Fixed Length Housing Modules .....	297
2-7-7. Examples of Different Configurations .....	297
2-7-7-1. Configuration with 560CMU01 .....	297
2-7-7-2. Configuration with 560CMG10 ,560CMD11.....	298
2-7-7-3. Configuration with 560CIG10 .....	298
2-7-7-4. Connection of Independent I/O Modules.....	299
2-7-7-5. Connection of Scaled I/O in DIN Rail to RTU560 Racks.....	299
2-8. Cabinet.....	300
2-8-1. Rack Mount Cabinet, Swing Frame 23SR20 .....	300
2-8-1.1. Cabinet Design. ....	300
2-8-2. Mounting Assembly 23SC20 Cabinet.....	307
2-8-3. Wall Housing 23WG22 Cabinet .....	308
2-8-4. Types of Configuration for Racks and Cabinets in Projects .....	310
2-8-4-1. RTU560A Standard.....	310
2-8-4-2. RTU560C Compact.....	312
2-8-4-3. RTU560 D New Solution .....	316
2-8-5. Cabinet Inspection.....	318
2-8-6. Battery Charger Cabinet .....	319

### **3- Chapter 3: SCADA Monitoring and Command Signals (Specification and Adjustment)325**

3-1. Introduction .....	325
3-2. Indication Processing.....	325
3-2-2. Function Distribution.....	326
3-2-3. Binary Input Functions.....	327
3-2-3-1. Digital Filter.....	327
3-2-3-2. Oscillation Suppression .....	328
3-2-3-3. Intermediate and Indeterminate Positions Handling for DPI .....	329
3-2-3-4. Signal Inversion.....	330
3-3. Analog Measured Information Processing.....	331
3-3-1. Analog Measured Information (AMI) Types .....	332
3-3-2. Function Distribution for AMI.....	332
3-3-3. Analog Input Board Functions.....	333
3-3-4. Zero Value Supervision and Switching Detection.....	333
3-3-5. Smoothing.....	335
3-3-6. Threshold Supervision on Integrator Algorithm.....	336
3-3-7. PDP Functions of the CMU .....	337
3-3-7-1. Bipolar, Unipolar and Live Zero conversion .....	337
3-3-7-2. Conversion Factor.....	340
3-3-7.3. Threshold Supervision on Absolute Threshold Value .....	341
3-4. Digital Measured Value Processing.....	342
3-4-1. Binary Input Board Functions (DMI) .....	344
3-4-1-1. Digital Filter.....	344



3-4-1-2. Consistency Check .....	344
3-4-1-3. Signal Inversion.....	344
3-4-2. Integrated Total Values Signal.....	345
3-5. Object Command Output (Digital Output Command).....	347
3-5-1. Single Object Command Output (SCO).....	347
3-5-2. Process Commands Circuit for SCO (1-pole) .....	348
3-5-3. Process Commands Circuit for SCO (2-pole) .....	349
3-5-4. Double Object Command Output (DCO) .....	350
3-5-5. Process Commands Circuit for DCO (1-pole).....	351
3-5-6. Process Commands Circuit for DCO (2-pole).....	352
3-5-7. Related Parameters for DCO in PDP tab .....	353
3-5-7-1. Termination of Command Output by Response Indication .....	353
3-5-7-2. Termination of Command Output by Select Before Operate Only (Two Steps).....	354
3-6. Command Output without Supervision .....	354
3-7. Command Output with Supervision .....	355
3-8. Object command output limitations .....	359
3-8-1. Related Parameters for RCO (Regulation Step Command Output) in PDP tab .....	360
3-8-3. Related Parameters for ASO (Analogue Set Point Command Output) in PDP tab...	360

<b>4- Chapter 4: Communication with RTU via Web Server</b> .....	<b>363</b>
4-1. Introduction .....	363
4-2. Webserver Description.....	363
4-3. System Diagnosis Page .....	366
4-4. Network Tree Page.....	367
4-5. Hardware Tree Page.....	368
4-6. Archive Information Page.....	374
4-6-1. Process Archives.....	375
4-6-2. File Archives.....	376
4-6-3. Security Event Archive .....	377
4-7. HMI (Integrated HMI) .....	377
4-8. Configuration Files Page .....	378
4-9. Firmware Files Page .....	380
4-10. Administration Page.....	381
4-10-1. Edit User Accounts Page.....	382
4-10-1-1. Security Policies .....	382
4-10-1-2. User Accounts.....	383
4-10-1-3. User Roles.....	384
4-10-2. Download / Upload Password Files Page .....	386
4-10-3. Activation of Debugging Options Page.....	386
4-11. Help Page .....	387
4-12. Others Page .....	388
4-13. PPP Installation.....	389

## Contents of SCADA Systems for Electric Power Industry, Volume II

## Volume II

<b>5- Chapter 5: Implementation and Monitoring of Network by HMI Editor</b>	<b>401</b>
5-1. Introduction .....	401
5-2. HMI Editor Installation.....	402
5-3. Starting by HMI Editor.....	405
5-4. Page Menu.....	407
5-5. Insert Menu .....	407
5-6. Project Menu .....	407
5-6-1. Setting Page.....	407
5-6-1-1. Application.....	407
5-6-1-2. Colors .....	408
5-6-1-3. Process Archive List.....	408
5-6-1-4. Alarm List .....	409
5-6-2. Import Image in HMI Editor.....	410
5-6-3. Import Sound file in HMI Editor .....	410
5-6-4. Communication between HMI and RTU file (Configuration file and consistency check) ...	411
5-7. Option Menu.....	414
5-7-1. Grid and Graphical Tab.....	414
5-7-2. Language Tab .....	414
5-8. About.....	414
5-9. Basic Functions for HMI Editor .....	415
5-9-1. Drawing Function.....	415
5-9-2. Changing Position and Size .....	415
5-9-3. Text Font and Text Size.....	415
5-9-4. Line Style Chooser (Drawing Network Lines) .....	416
5-10. Components .....	416
5-10-1. Static Components .....	417
5-10-1-1. Line Component.....	417
5-10-1-2. Rectangle Component.....	417
5-10-1-3. Ellipse Component.....	418
5-10-1-4. Polygon Component.....	418
5-10-1-5. Label Component .....	419
5-10-1-6. Image Component .....	419
5-10-2. Dynamic Components.....	419
5-10-2-1. Byte Value Component .....	419

5-10-2-2. Integrated Total Component .....	420
5-10-2-3. Text Field Component .....	420
5-10-2-4. System Time Component.....	421
5-10-2-5. System Event Component.....	422
5-10-2-6. System-Event Line-Component.....	423
5-10-3. Dynamic Components with Control .....	423
5-10-3-1. Symbol Component.....	425
5-10-3-2. Tap Position Component.....	425
5-10-3-3. Normalized Value Component .....	426
5-10-3-4. Bit String Component .....	427
5-10-3-5. Floating Point Component.....	427
5-10-4. Link Components .....	428
5-10-4-1. Link Label Component.....	428
5-10-4-2. Link Button Component .....	428
5-10-5. Table Components .....	429
5-10-5-1. History Table Component.....	429
5-10-5-2. Process Archive List Component.....	429
5-10-5-3. Alarm List Component .....	432
5-10-6. HMI Control Components.....	434
5-10-6-1. Control Authority Component.....	434
5-10-6-2. Acknowledge Audible Alarm Component.....	437
5-10-7. Chart Components.....	437
5-11. HMI Component View and Editor Mode .....	438
5-11-1. HMI Editor Mode .....	438
5-11-2. Component View Editor.....	439
5-11-2-1. Create New Component.....	439
5-12. How to Upload HMI file on Flash.....	441

---

**6- Chapter 6: SCADA Systems Protocols 447**

6-1. Introduction of SCADA Protocols .....	447
6-1-1. Physical Layer .....	447
6-1-2. Data Link.....	448
6-1-3. Network Layer.....	448
6-1-4. Transport Layer.....	449
6-1-5. Session Layer .....	449
6-1-6. Presentation Layer .....	449
6-1-7. Application Layer.....	449
6-2. IEC 101 Protocol .....	450
6-2-1. IEC 101 Standards .....	450
6-2-2. IEC 101 Structure.....	451
6-2-2-1. Physical Layer.....	451
6-2-2-2. Data Link Layer .....	451
6-2-2-3. Network Layer.....	452

6-2-3. Data Transferring in IEC 101 Protocol.....	452
6-2-3-1. Transmission Formats .....	452
6-2-3-2. Application Data Structure.....	462
6-2-4. IEC101 Settings in RTUtil560 .....	470
6-2-4-1. Type Identification.....	478
6-2-4-2. Qualifier, Cause of Transmission.....	480
6-2-4-3. Structured Address Scheme .....	485
6-3. IEC104 Protocol.....	490
6-4. IEC101 and IEC 104 Settings in RTUtil560 .....	494
6-4-1. Implementation of IEC 60870-5-101/104 in RTU560.....	494
6-4-2. Analog Signal Page (AMI) In IEC101 Protocol-SUB.....	498
6-4-3. Analog Signal Page (AMI) In IEC101 Protocol-HOST.....	500
6-4-4. Digital Signal Page (DPI) In IEC101 Protocol-SUB .....	502
6-4-5. Digital Signal Page (DPI) In IEC101 Protocol-Host .....	502
6-4-6. IEC101 Protocol Page (HOST) .....	504
6-4-6-1. IEC101 Protocol Page (Slave).....	505
6-4-7. IEC104 Protocol Page.....	506
6-5. DNP3 Protocol.....	507
6-5-1. History of DNP3 Protocol .....	507
6-5-2. DNP3 Specifications .....	508
6-5-2-1. DNP3 Features .....	508
6-5-2-2. DNP3 Architecture .....	508
6-5-3. DNP3 Layers .....	511
6-5-3-1. Physical Layer in DNP3 Protocol.....	511
6-5-3-2. Data Link Layer in DNP3 Protocol .....	513
6-5-3-3. Pseudo-Transport Layer in DNP3 Protocol .....	516
6-5-3-4. Application Layer in DNP3 Protocol .....	517
6-6. DNP3 Protocol Page in RTUtil560.....	524
6-7. INDACTIC Protocol.....	526
6-7-1. INDACTIC Protocol History .....	526
6-7-2. INDACTIC Protocol Specification .....	526
6-7-3. INDACTIC Protocol Layers .....	527
6-7-4. Telegram Structure in INDACTIC Protocol.....	529
6-7-4-1. B-Word Block.....	530
6-7-4-2. G-Word Block.....	531
6-7-4-3. D-Word Block.....	533
6-7-4-4. C-Word Block.....	536
6-7-5. Hamming.....	539
6-7-6. Cyclic Redundancy Checks.....	540
6-7-7. INDACTIC Protocol Settings in RTUtil560 .....	542
6-7-7-1. Single Point Information Page for INDACTIC Protocol in RTUtil560 .....	542
6-7-7-2. Double Point Information Page for INDACTIC Protocol in RTUtil560 .....	544
6-7-7-3. Analog Measured Information Page for INDACTIC Protocol in RTUtil560 .....	545

6-8. Hitachi Protocol.....	550
6-8-1. Hitachi Protocol Setting Page in RTUtil560.....	550
6-8-1-1. Single Point Information Page for Hitachi Protocol in RTUtil560 .....	551
6-8-1-2. Double Point Information Page for Hitachi Protocol in RTUtil560 .....	552
6-8-1-3. Analog Measured Information Page for Hitachi Protocol in RTUtil560.....	553
6-9. Protocol Test Analyzer.....	556
6-9-1. Installation of Protocol Test Harness .....	558
6-9-2. Analyzing and Testing of IEC101 Master by Protocol Test Harness .....	560
6-9-2-1. Import Configuration from CSV file (Excel) .....	576
6-9-3. Analyzing and Testing of IEC104 Master by Protocol Test Harness .....	577
6-9-4. Analyzing and Testing of DNP3 Master by Protocol Test Harness .....	578
6-9-4. Analyzing and Testing of DNP3 Slave by Protocol Test Harness .....	581
6-10. Serial Port .....	582
6-10-1. Introduction.....	582
6-10-2. Reason for Employing RS-232 Standard.....	583
6-10-2-1. Types of Communication Network for Equipment .....	583
6-10-3. RS-232 Hardware Description .....	584
6-10-3-1. RS-232 Voltage Levels .....	584
6-10-3-2. Types of Cable and Connectors .....	584
6-10-3-3. RS-232 Employed Pins.....	585
6-10-3-4. Description of RS-232 PINs.....	590
6-10-3-5. Null-Modem Cables in RS-232 .....	590
6-10-3-6. Cable Length and Noise Security in RS-232.....	592
6-10-4. RS-232 Software Description .....	592
6-10-4-1. Parallel and Serial Communication.....	592
6-10-4-2. Parallel Communication .....	593
6-10-4-3. Serial Communication.....	594
6-10-4-4. Direction of Data Transferring.....	595
6-10-4-5. Transmitter and Receiver Operational Status .....	596
6-10-4-6. Baud Rate .....	597
6-10-4-7. Serial Data Format.....	597
6-10-4-8. Serial Data Format in UART .....	598
6-10-4-9. UART Communication Considering Handshaking.....	599
6-10-5. RS-232 Disadvantages.....	602
6-10-6. RS-423 Standard.....	602
6-10-7. RS-422 Standard.....	602
6-10-8. RS485 Standard.....	605

<b>7- Chapter 7: RTUtil560 and its Applications</b> .....	<b>607</b>
7-1. Introduction .....	607
7-2. RTUtil560 Installation.....	607
7-3. Data Structure in RTUtil560.....	614
7-3-1. Network Tree .....	614

7-3-2. Signal Tree.....	614
7-3-3. Hardware Tree.....	615
7-4. Implementation of a Practical Project in RTUtil560.....	618
7-4-1. Network Tree Implementation.....	620
7-4-1-1. Network Tree Engineering.....	620
7-4-2. Signal Tree Implementation .....	623
7-4-2-1. Signal Tree Engineering.....	623
7-4-3. Hardware Tree Implementation.....	627
7-4-3-1. Hardware Tree Engineering.....	627
7-5. Consistency Check.....	635
7-5-1. Object Name Equal, Solution for Error .....	636
7-5-2. IP-address on Ethernet Interface is not configured, Solution for Error .....	636
7-5-3. Node Slave from IEDs not Linked to Hardware Tree, Solution for Error.....	638
7-5-4. Equal host Number “1” in Master to BSCC and Master to SCC, Solution for Error.....	638
7-5-5. No Comboard configured as time administration master, Solution for Error.....	639
7-5-6. No time master configured, Solution for Error .....	640
7-5-7. I/O Bus, Solution for Error.....	641
7-5-8. Protocol Address of ..... equal to..., Solution for Error .....	642
7-6. Analog Card Settings.....	651
7-7. Analog Card Settings.....	652
7-8. Communication Protocol Settings .....	653
7-9. Building RTU Configuration File.....	656
7-9-1. Extract RTU- Configuration Files.....	658
7-9-2. Exporting Data by Excel .....	658
7-10. Data Import from Excel to RTUtil560 .....	663
7-10-1. General Description for Data Import from Excel.....	663
7-10-2. Required Excel Page and Related Spreadsheets .....	664
7-10-2-1. Configuration with CS - RTU - Sub-RTU.....	665
7-10-2-2. Configuration with CS - RTU - IED.....	665
7-10-2-3. Configuration with CS1 - CS2 - RTU - Sub-RTU - IED's .....	666
7-10-3. Different Sheets in Excel File .....	667
7-10-4. General Notes Related to Rows and Columns in Excel .....	667
7-10-5. Functions in the Exported Excel Sheets.....	668
7-10-5-1. Drop-Down Menu for Predefined Values.....	668
7-10-5-2. Range Supervision.....	668
7-10-5-3. Online Help in Excel.....	668
7-10-6. Excel Sheets Structure .....	670
7-10-6-1. General Blocks of Excel Sheets .....	670
7-10-6-2. Signals Block .....	670
7-10-6-3. Process Object Identification Block .....	671
7-10-6-4. RTU Hardware Address Block .....	671
7-10-6-5. Line Address and Host Parameters Block.....	672
7-10-6-6. Block of Parameters of Data Point.....	672

7-10-7. Data Importing from Excel to RTUtil560.....	673
7-10-7-1. Adding Signals in Excel.....	673
7-10-7-2. Errors Table in Excel.....	687
7-11. Employing RTU for Converting IEC101 to INDACTIC.....	691
7-12. Employing RTU for Converting IEC101 to Hitachi.....	701
7-13. Employing RTU for Converting IEC101 to DNP3.....	707
7-14. RTU Configuration with one Modem.....	714
7-15. RTU Configuration with two Modems.....	719
7-16. Signal Monitoring in HMI and Webserver.....	724
7-16-1. Execution of Substation Program in Webserver.....	725
7-16-2. Building a Configuration File for Control Center.....	730
7-16-3. Executing Control Center Program in HMI Editor.....	735

<b>8- Chapter 8: Other Important Functions</b>	<b>743</b>
8-1. Introduction.....	743
8-2. Local Print.....	743
8-2-1. Message Processing and Buffering.....	744
8-2-2. Queue Handling and Maximum Allowable Range.....	745
8-2-3. Messages Format.....	745
8-2-4. Define Local Printer in RTUtil560.....	746
8-4. Process Archive Function.....	751
8-3-1. Archive Data Import to MS Excel.....	751
8-3-2. Process Archive in RTUtil560.....	754
8-4. File Archive Function.....	757
8-4-1. File Archive in RTUtil560.....	758
8-4-2. Logic Function in RTUtil560.....	761
8-5. COMPROTware.....	764

<b>Appendix</b>	<b>767</b>
Appendix A.....	767
Appendix B.....	771
Appendix C.....	822

Last Frame	<b>842</b>
References	<b>844</b>

# SCADA Systems and RTU

## 1-1. Need and Role of Control Systems

### 1-1-1. Introduction

The need for high-reliability electrical energy in today's societies is quite clear and has a very significant role. In general, the main goal of energy supply is to satisfy consumers, and in order to achieve this goal, the electrical system must be monitored and investigated accurate, constantly and thoroughly.

Obviously, the main goal of the establishment of power plants, transmission lines, substations and distribution networks is to provide electrical power demand. The application of electrical energy in today's life is inevitable and, given the scientific innovations of researchers and scientists, is being enlarged every day.

From another perspective, with the increasing population growth and various development plans, with the expansion of electrical networks, should provide the conditions for everyone to use this energy. The point to be taken into account here is to increase the quality and compliance with the permissible limits and the standard of energy demanded by consumers. Features such as continuity and energy supply, stable voltage and uniformity of it are important for consumers. From a competitive point of view, also the manufacturer must provide electrical energy at the lowest cost. To achieve this, various studies have to be done on how to secure the energy supply and to make the necessary controls, based on complex and accurate scientific calculations.

According to description mentioned above, three important points should be considered in power system operation:

- 1) Provide high quality electrical energy
- 2) secure electrical energy
- 3) Minimizing generation, transmission and ... costs.

### 1-1-2. Necessity to Use Control Systems in the Power Grid

In the vicinity of all power networks from the simplest to the most complex ones, there are one or more control centers that have the rule of Governance the network. This control system is called dispatching system. Current dispatching systems use SCADA technology to collect information and apply different



commands. The main purpose of this chapter is to provide a brief explanation of the SCADA system and its role in power networks control. Since the main task of the SCADA system is the collection of information and centralized control for optimal operation, this section first examines the control systems.

In general, control systems have a long way in the advancement process of technology. Among the factors that have led to changes in the control systems in the industry, economic issues, the need to control the quality of generation, increase the demand for more accuracy in measurement, speed in measurement and control, reduce energy losses, consider the behavior and experiences of the system history, preventing various events before occurrence, increasing the reliability of the system etc. have a special important.

In general, the advancement of control systems has always been concurrent with advancement of computer science, and whenever improvements have taken place in the computer industry, control systems have also undergone significant changes. In general, with a review of the history of the use of control systems, in particular PLC, DCS and SCADA show that use of control systems has been growth when the cost of computers is economically efficient. For example, the use of PLC systems at first was not economical due to the high costs of semiconductor chips. But with the development of the world of electronics and the emergence of LSI and VLSI demand for the use of these systems has greatly increased.

### **1-1-3. Introduction to various control systems**

This section provides general information about various control systems for more information.

#### **1-1-3-1. Local Control**

In the first generation of process control systems in the industry, large equipment such as registers, controllers and indicators were in the process location and among all the signs and warnings, only send alarms to another location that users rest (the substation operator) or office shift responsible. Various boards such as relays and so on were in the location. In this case, the operators and engineers in the factory site examined the conditions at certain times note the special information from the indicator(s) or controllers to provide as work report. The problem of this system was low efficiency, low accuracy and lack of information collection.

#### **1-1-3-2. Centralized Control**

The centralized control is based on transmission of signals to one or more centers by cable and connecting them to the receiving equipment on the switchgear. Each control center, usually consisting of a command room and an aid switchgear room. In the command room, the main switchgears are placed with the mimic boards and worktable.

The characteristics of the centralized system with independent circuits are the simplicity, high volume of the equipment, and therefore the busy situation of the control room, the length of the boards, the high energy consumption, the middle efficiency of the users and the impossibility of processing the information in a comprehensible way, and record and maintain it for referencing in future.

This system does not work well in large industrial complexes that consist of multiple units, and for each unit a separate command room should be considered. In some units built in the 1970s, a supervisory system with large computers is intended for data collection.

Centralized systems at pump stations and gas pressure boost stations are sometimes designed for fully automated and non-user operation, but their efficiency has never been high due to the low reliability of the

equipment. Generally, on the control boards of the industries, most of the equipment by different generations are beside together.

### **1-1-3-3. Programmable Logic Controllers (PLCs)**

In the last half century, due to the advancement of solid state technology and the emerging of microprocessors, industrial control systems have undergone dramatic changes, so that it can be said that the components and equipment used in industrial process control circuits have a lot of differences with equipment used in circuits even the past fifteen years, and these differences are mainly due to the use of electronic equipment.

PLCs have been used in the industry since 1969, and since 1974 using microprocessors as the brain of the system, they removed the contactor relay circuits and used PLC programmable controls (PLC) instead of them.

Today, designers of production lines and machinery and industrial processes do not have much interest to use of contact relays, and the use of contact relay circuits in the larger and complex industrial processes is almost obsolete. Due to these developments, PLC systems have been used in many of our factories and industrial centers in Iran, especially in the centers that have been installed since the 1980s.

Some of the disadvantages of electromechanical command circuits that replaced them with PLC are as follows:

- 1- When the big process and the control needs become more complex, the number of necessary components (relay, timer, counter, etc.) will increase, so the size of the switchgear become bigger and will occupy larger space.
- 2- Final cost of the control and command circuits increases.
- 3- Electromechanical circuits are more expensive than electronic circuits.
- 4- Due to energy losses in electromechanical circuits, appropriate ventilation is required.
- 5- The assembly of a switchgear with a large and complex wiring takes time and requires specialist personnel.
- 6- Electromechanical depreciation is high due to its mechanical parts.
- 7- The probability of mistake in assembly is high, and a specific algorithm and logic cannot be proposed for troubleshooting electromechanical command circuits.
- 8- A command switchgear constructed for a particular process is not usable for controlling another process and has a unique application, and changing the method or changing the control demands requires changing the wiring and adding or removing some parts, which requires a lot of time and money.
- 9- The disadvantages of the relay contact systems and advantages of PLC have led to a gradual change in the programmable logic controllers and replacing them with the contact control relay command circuits.

Figure (1) shows configuration of a system including a PLC.

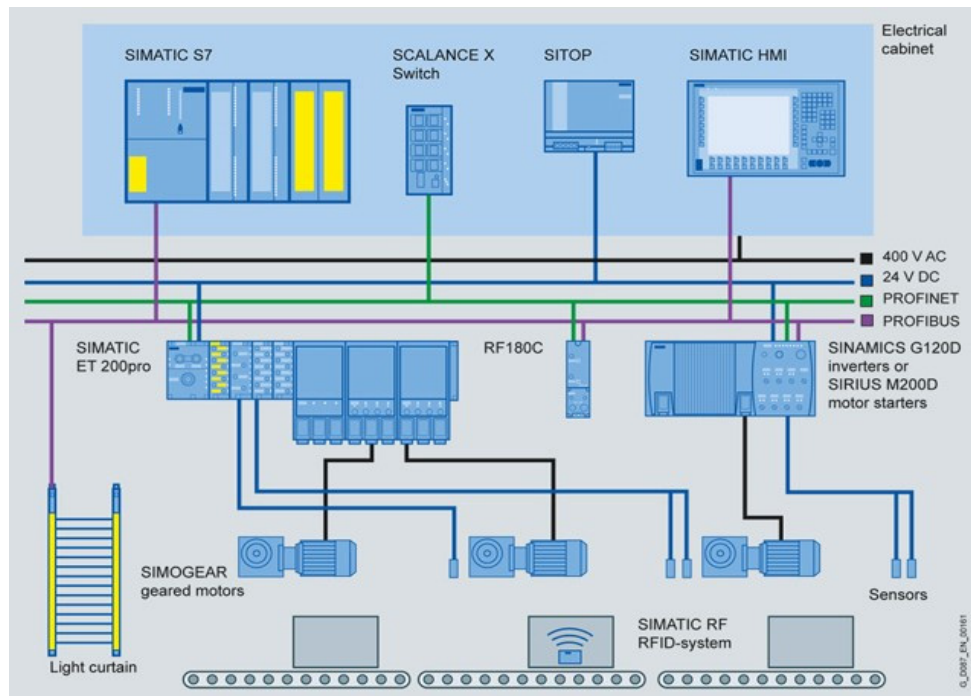


Figure 1- Configuration of a sample system using PLC

#### 1-1-3-4. Distributed Control System

DCS is a distributed control system whose function is distributed rather than concentrated in a single point. A distributed control system consists of a number of microprocessor modules that control and monitor the performance of a system by co-operating with each other. Computers are distributed according to geographic location, which reduces the cost of installation and wiring.

It is a computer network but differs from home or office computer networks. In DCS real-time processing problem is important, unlike what is seen in processes on office or home computers. The difference between the two methods of processing is how they execute their programs. On traditional computers, processing is such that at one time only one single program is executed, so that the program starts with complicated calculations with a fixed set of data and ultimately ends up desirable, and when the process is completed, the program stopped to re-execute with a new data set. In the "real time" processing, process is started with a fixed data series, except that the same program is repeated continuously (several times per second) and updates the data according to the data in the previous step. As an example of a real-time performance, automobile speed control of a car is an example of real-time processing. The control starts with fixed speed data at optimal speed and at each step of the machine speed is sampled and due to its difference with the desired speed, control signals are applied to open or close the gas valve. A DCS controller also continuously monitors hundreds or perhaps thousands of under control systems and replicates computations based on a specific scheme for the respective systems. The data received from the environment can be divided into two groups:

##### a- Analog data

These data are continually changed and analyzed through control loops of software that may include relative controllers, Lead Lag, or PIDs, as needed, and appropriate output signals are send. For example, examples of this data are active and reactive power flowing through the line, the voltage of substation bus and so on.