NWC OT Cybersecurity L0-1 Devices Minimum Baseline Security Standard Appendix

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-MBSS-L1-APP
Document Title:	NWC OT Cybersecurity NWC L0-1 Devices Minimum Baseline Security Standard Appendix
Document Version:	0
NWC Contract No.:	101200487
[atm] PO Ref.:	ATMPO2020-034

1400 Broadfield Blvd Suite 200 Houston TX, 77084
Tel: +1 832 386 5593 | Fax: +1 832 201 0337
Email: sales@acetsolutions.com |
URL: www.acetsolutions.com

NOTES AND COPYRIGHTS

NWC has contracted this project to [atm] under contract number 101200487. ACET Solutions is the technical consultant of [atm] responsible for planning and execution of this project. All references to ACET Solutions in this document should be construed as [atm]/ACET Solutions for contractual purpose. Acceptance of this deliverable by NWC shall meet the requirements of the respective deliverable under NWC contract number 101200487.

Questions or comment regarding this deliverable should be directed to the ACET Solutions Project Director.

ACET Solutions LLC
1400 Broadfield Blvd Suite 200
Houston TX, 77084
Email: sales@acetsolutions.com | URL: www.acetsolutions.com

APPROVALS

Name	Company	Signature	Date
Mubarik Mustafa (Project Director)	ACET Solutions		
Abdulhadi G. Alshammari (Project Manager)	NWC		
Ahmed I. Almutairi (Project Sponsor)	NWC		

REVISION HISTORY

Rev No.	Date	Author	Checked By	Approved By	Comments
00	January 28, 2022	MA	SK	MM	Issued For Approval

REFERENCE DOCUMENTS

S/N	Vendor	Document No.	Title
1	Schneider Electric	SEVD-2019-316-02	M340 Firmware History
2	Schneider Electric	EIO0000000057.02	Modicon M340 Firmware
3	Schneider Electric	140CPU65xx0	140CPU65xx0 firmware history
4	Schneider Electric	EIO000000006403	Quantum Operating System
5	Schneider Electric		How can I update the firmware of a Twido PLC with the TwidoSoft software
6	Schneider Electric		Modicon M580 CPU firmware history SV2.90
7	Schneider Electric		Modicon M580 Firmware Upgrade
8	Schneider Electric		BMENOC firmware upgrade procedure
9	Schneider Electric		TSXETY4103 Firmware History
10	Schneider Electric	SEVD-2018-233-01	Security Notification – Modicon M221
11	Schneider Electric		Modicon M221 Firmware Upgrade
12	Schneider Electric	EIO0000001999.08	Modicon Controllers Cyber Security
13	Schneider Electric	31007131.18	Modicon M340 for Ethernet - Communications Modules and Processors
14	Schneider Electric		Configuring Password Protection
15	Schneider Electric	33002479.20	Quantum using EcoStruxure™ Control Expert - Ethernet Network Modules
16	Schneider Electric	EIO0000001578 09/2020	Modicon M580 Configuration
17	Schneider Electric	35006192 10/2019	Premium and Atrium Ethernet Network Modules
18	Schneider Electric		
19	Schneider Electric		
20	Schneider Electric		
21	Schneider Electric		
22	Schneider Electric		
23	Rockwell Automation		ControlLogix 5570 Family

S/N	Vendor	Document No.	Title
24	Rockwell Automation	UM022D-EN-P	GuardLogix 5570 Controllers
25	Rockwell Automation	2080-RN004C-EN-E	Micro800 Programmable Controllers
26	Rockwell Automation	2080-UM004D-EN-E	Micro800 Plug-in Modules
27	Rockwell Automation	2080-RN004C-EN-E	Micro800 Programmable Controllers
28	Rockwell Automation	2080-UM002L-EN-E	Micro830, Micro850, and Micro870 Programmable Controllers
29	Rockwell Automation	1747-IN007C-EN-P	SLC 5/03™ and SLC 5/04™ Processors Firmware/Operating System Upgrade
30	Rockwell Automation	1768-RN016J-EN-E	CompactLogix Controllers, Firmware Revision 16
31	Rockwell Automation		ControlLogix 5560 Family
32	Rockwell Automation	1756-RN016G-EN-E	ControlLogix Controllers, Revision 16
33	Rockwell Automation	1768-RN016J-EN-E	CompactLogix Controllers, Firmware Revision 16
34	Rockwell Automation		
35	Rockwell Automation		
36	Rockwell Automation		
37	Rockwell Automation		
38	Rockwell Automation		
39	Mitsubishi	Delta DVP 20-EX	
40	Mitsubishi		
41	Mitsubishi		
42	Mitsubishi		
43	Mitsubishi		
44	Mitsubishi		
45	Mitsubishi		
46	Siemens		Firmwareversion V4.4 released for S7-1200
47	Siemens	A5E44115569-AH	S7-1200 Firmware update V4.5.1
48	Siemens		Firmware update for CPU 1214C

S/N	Vendor	Document No.	Title
49	Siemens		Firmware update for CPU 1214C, DC/DC/DC, 14DI/10DO/2AI - ID: 107539750 - Industry Support Siemens
50	Siemens	C79000-G8976-C175-17	Version history / current downloads for S7 CPs Industrial Ethernet
51	Siemens		Operating System Updates for CPU 315-2DP
52	Siemens		Firmware Update for ET 200SP IM 155-6 PN HF
53	Siemens	A5E00103686-08	ET 200S Distributed I/O System
54	Siemens		Firmware updates for IM151-8F PN/DP CPU (6ES7151-8FB01-0AB0) - ID: 47354354 - Industry Support Siemens
55	Siemens		Firmware updates for IM151-8 PN/DP CPU
56	Siemens		S7-200 SMART CPU firmware
57	Siemens	C79000-G8976-C356-08	Operating Instructions
58	Siemens	C79000-G8976-C175-17	Version history / current downloads for S7 CPs Industrial Ethernet
59	Siemens	A5E00267695-13	Fault-tolerant systems S7-400H
60	Siemens	77431846, V2.0, 03/2016	Security with Simatic Controller
61	Siemens		
62	Siemens		
63	Siemens		
64	Siemens		
65	ABB	AC500/AC500-eCo	AC500AC500-eCo FW update description V2.1.5
66	ABB	AC500/AC500-eCo	AC500AC500-eCo FW update description V2.1.5
67	ABB	AC500/AC500-eCo	AC500AC500-eCo FW update description V2.1.5
68	ABB		Release Notes AC500 V2 Firmware Version 2.8.5
69	ABB	AC500/AC500-eCo	AC500AC500-eCo FW update description V2.1.5

S/N	Vendor	Document No.	Title
70	ABB	AC500-eCo	AC500-eCo FW update description V2.2.0
71	ABB		
72	ABB		
73	ABB		
74	ABB		
75	ABB		
76	Sofrel		Firmware Upgrade Version 024
77	Sofrel		
78	Sofrel		
79	Sofrel		
80	Sofrel		
81	Sofrel		

Table 1: Reference Documents

ACRONYMS

Acronyms	Meaning
ACL	Access Control Lists
AD	Active Directory acronyms
ADC	Additional Domain Controller
CSMS	Cyber Security Management System
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DLD	Detailed-Level Design
DNS	Domain Name Server
DTM	Device Type Manager
EIP	Ethernet/IP Protocol
FDT	Field Device Tool
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
KSA	Kingdom of Saudi Arabia
MBSS	Minimum Baseline Security Standards
NTP	Network Time Protocol
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SNMP	Simple Network Management Protocol
S/N	Serial Number
TFTP	Trivial File Transfer Protocol
VM	Virtual Machine
VPN	Virtual Private Network

Table of Contents

1. DOCUMENT PURPOSE

This document is an appendix for Minimum Baseline Security Standards for L0-1 Devices.

Following list of devices are covered in this document:

S.No.	Vendor	Part Number/Model Number/Article Number
1	Schneider Electric	Modicon M340
2	Schneider Electric	Modicon Quantum
3	Schneider Electric	Twido
4	Schneider Electric	Modicon M580
5	Schneider Electric	Modicon TSX Premium
6	Schneider Electric	Modicon M221
7	Schneider Electric	*Place holder for future L0-1 devices*
8	Schneider Electric	*Place holder for future L0-1 devices*
9	Schneider Electric	*Place holder for future L0-1 devices*
10	Rockwell Automation	Logix 5571
11	Rockwell Automation	Micro-850 (2080-LC20-24QBB)
12	Rockwell Automation	Micro-850 (2080-LC50-24QBB)
13	Rockwell Automation	AB 1734-ACNR
14	Rockwell Automation	SLC 5/04
15	Rockwell Automation	CompactLogix L45
16	Rockwell Automation	CompactLogix 5561
17	Rockwell Automation	Allen Bradley
18	Rockwell Automation	*Place holder for future L0-1 devices*
19	Rockwell Automation	*Place holder for future L0-1 devices*
20	Mitsubishi Electric	Delta DVP-20EX
21	Mitsubishi Electric	*Place holder for future L0-1 devices*
22	Mitsubishi Electric	*Place holder for future L0-1 devices*
23	Siemens	S7-1200
24	Siemens	1214 AC/DC/RLY
25	Siemens	S7-300
26	Siemens	ET 200
27	Siemens	IM151-8 PN/DP
28	Siemens	S7-200
29	Siemens	Logo 24RC
30	Siemens	S7-400
31	Siemens	*Place holder for future L0-1 devices*
32	Siemens	*Place holder for future L0-1 devices*
33	ABB	PM591
34	ABB	PM573
35	ABB	PM564
36	ABB	CI590
37	ABB	*Place holder for future L0-1 devices*
38	ABB	*Place holder for future L0-1 devices*
39	Sofrel	S550
40	Sofrel	*Place holder for future L0-1 devices*
41	Sofrel	*Place holder for future L0-1 devices*
42	GE	MDS – SD4 (GE Radio)
43	GE	*Place holder for future L0-1 devices*

2. APPENDIX I - SCHNEIDER ELECTRIC

2.1 MODICON M340

1. Upgrade the firmware

   Refer to **Error! Reference source not found.Error! Reference source not found.** S/N 2 Page 6-19

2. Upgrade Communication Module Firmware

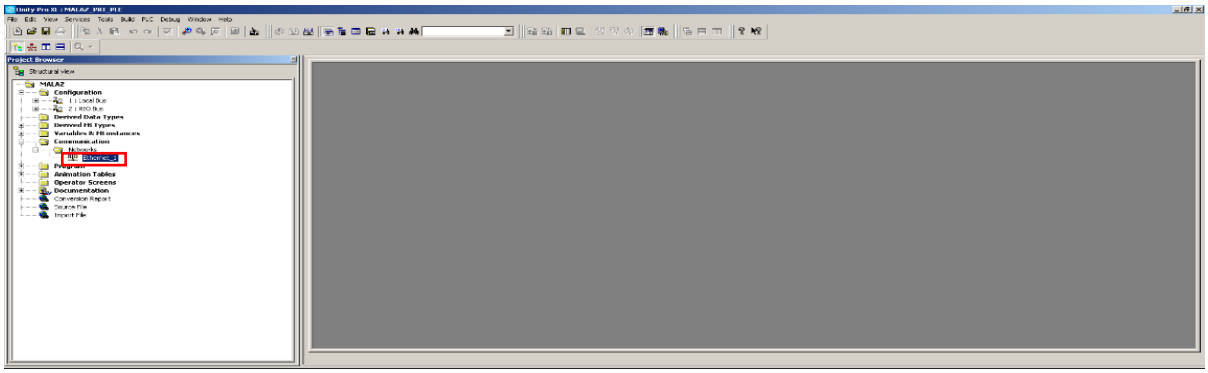
   Refer to **Error! Reference source not found.Error! Reference source not found.** S/N 2 Page 6-16.

3. Disable unused ethernet services such as HTTP/FTP.

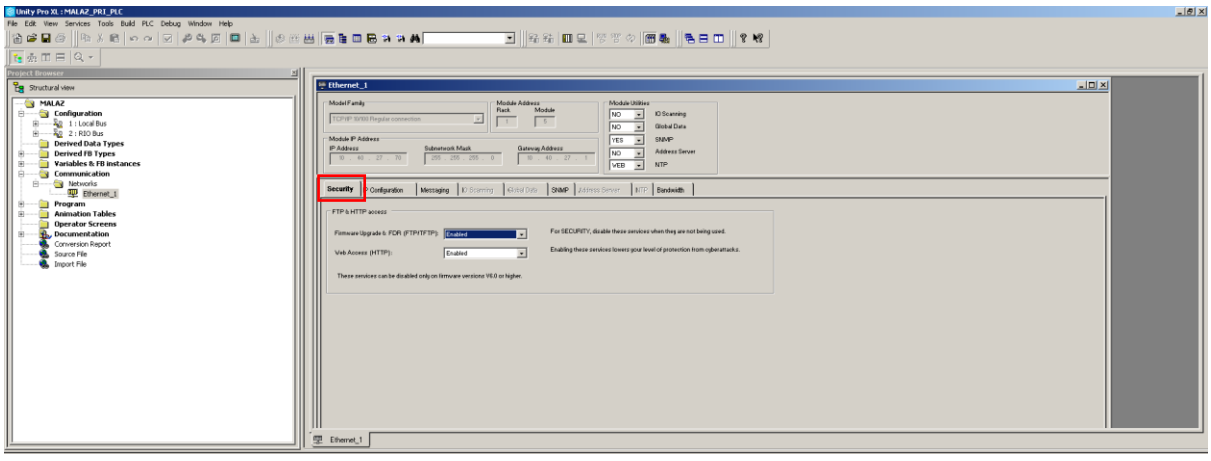
   Refer to Refer to **Error! Reference source not found.Error! Reference source not found.** S/N **Error! Reference source not found.** Page 139-140.

   Following are the steps followed for disabling HTTP/FTP services:

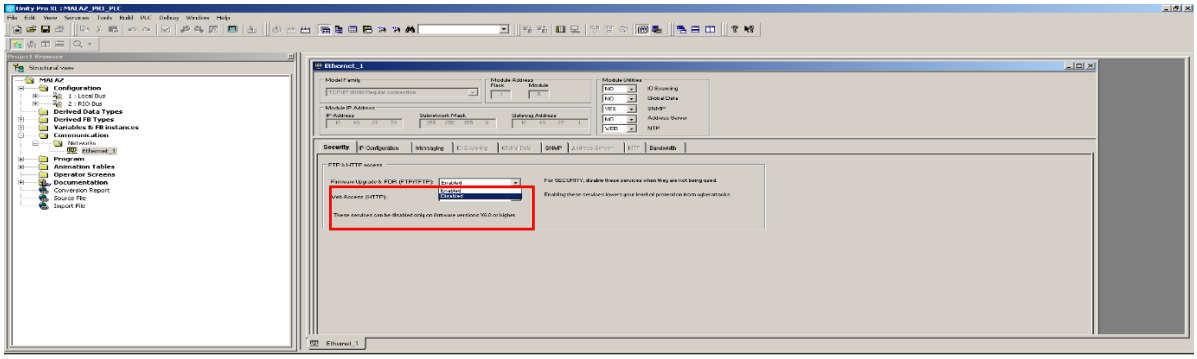
   Step 1: Select Communication >> Networks >> Ethernet_1



   Step 2: Select Security tab in Ethernet_1 window



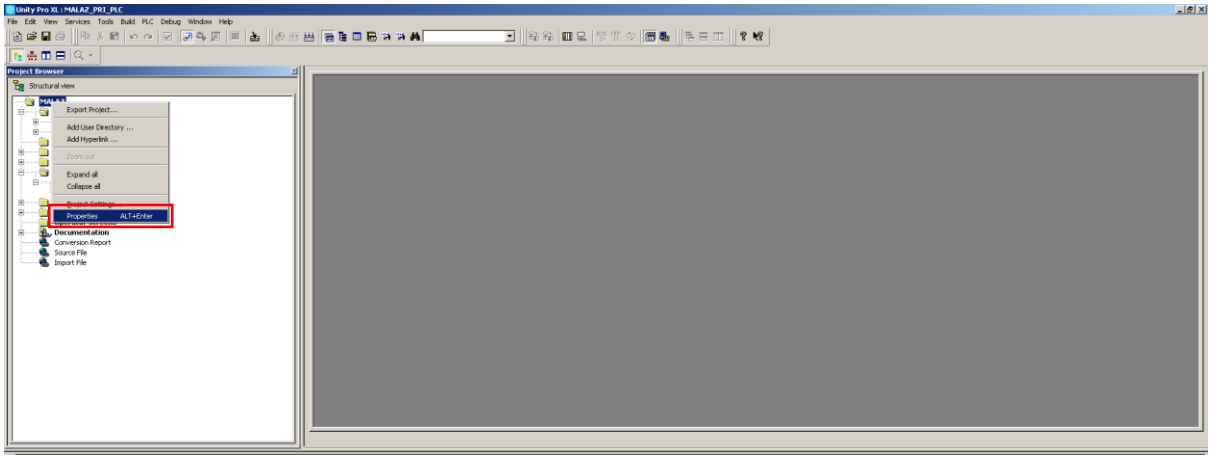
   Step 3: In security tab, disable HTTP/FTP services



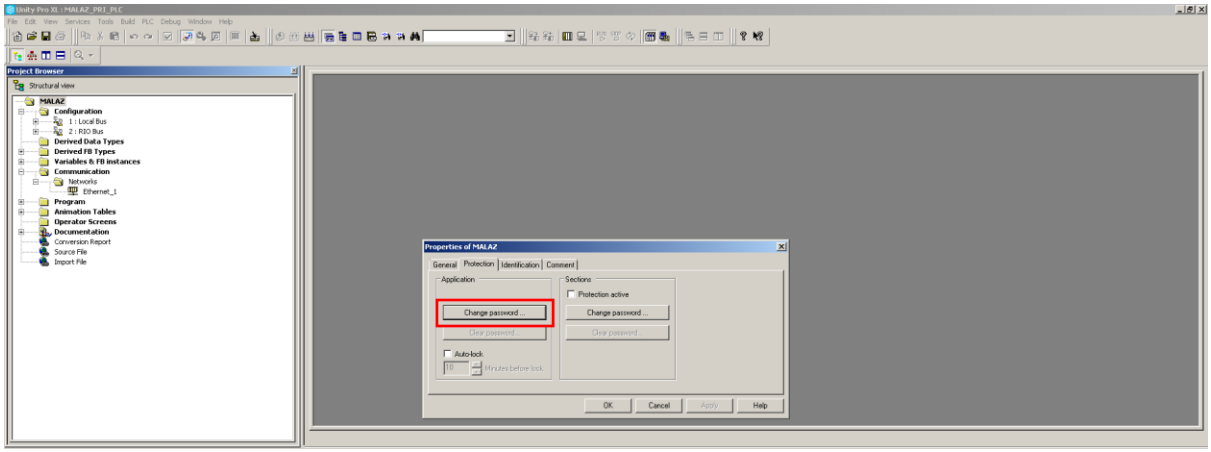
4. Set Password for ensuring security lock features.

Following are the steps performed for password protecting the application:

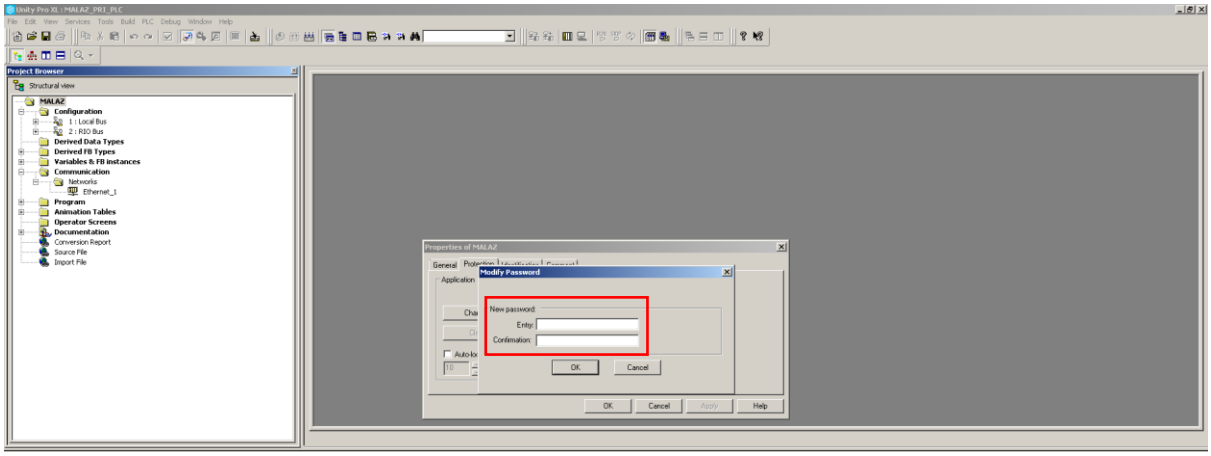
Step 1: Select the project and right click to select the properties



Step 2: Select “Protection” tab in properties, select change password



Step 3: Enter the new password and confirm it.



5. Configuration of Access Control List based on IP address

   Refer to **Error! Reference source not found.Error! Reference source not found.** S/N **Error! Reference source not found.** Page 20-21, S/N **Error! Reference source not found.** Page 147-149

2.2 MODICON QUANTUM

1. Upgrade the firmware

   Refer to **Error! Reference source not found.** S/N 4 Page 7-51

2. Upgrade Communication Module Firmware

   Refer to **Error! Reference source not found.** S/N 4 Page 52-59

3. Set password for security lock feature.

   Refer to **Error! Reference source not found.** S/N **Error! Reference source not found.**

4. Disable unused ethernet services like FTP/HTTP

   Refer to **Error! Reference source not found.** S/N **Error! Reference source not found.** Page 107

2.3 TWIDO

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 5

2. Set password for security lock feature

   Refer to **Error! Reference source not found.** S/N **Error! Reference source not found.**

3. Disable HTTP/FTP ethernet services

   Refer to “ ”

2.4 MODICON M580

1. Upgrade the firmware.

   Refer to **Error! Reference source not found.** S/N 7

2. Upgrade Communication Module Firmware

   Refer to **Error! Reference source not found.** S/N 8

3. Disable unused services such as HTTP, FTP, SNMP, DHCP, EIP, NTP, TFTP

   Refer to **Error! Reference source not found.** S/N **Error! Reference source not found.** Page 126-127

4. Log DTM and Module Events to the Syslog Server or Control Expert Logging Screen

   Refer to **Error! Reference source not found.** S/N **Error! Reference source not found.** Page 168-169

5. Control Identification and Authentication by managing accounts, User Account Controls, Passwords, and various services such as HTTP/SNMP.

   Refer to **Error! Reference source not found.** S/N **Error! Reference source not found.** Page 126-129

6. Enable Integrity checks feature in Control Expert to help prevent files and software from being changed or affected via a virus/malware.

   Refer to **Error! Reference source not found.Error! Reference source not found.** S/N **Error! Reference source not found.** Page 51

7. Set Password for ensuring security lock features.

   Refer to **Error! Reference source not found.** S/N **Error! Reference source not found.**

2.5 MODICON TSX PREMIUM

1. Upgrade the firmware

   Refer to “ ”

2. Disable unused services ethernet services such as FTP/HTTP

   Refer to **Error! Reference source not found.** S/N **Error! Reference source not found.**

3. Set Password for ensuring security lock features

   Refer to **Error! Reference source not found.** S/N **Error! Reference source not found.**

2.6 M221

1. Upgrade the firmware

   Refer to **Error! Reference source not found.** S/N 11

2. Disable all unused protocols such as HTTP, FTP, SNMP.

   Refer to **Error! Reference source not found.** S/N 10

3. Set up a password for ensuring security lock features.

   Refer to **Error! Reference source not found.** S/N **Error! Reference source not found.**

3. APPENDIX II - ROCKWELL

3.1 ROCKWELL LOGIX 5571

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 24 Page 33-39

2. Set password for security lock feature

   Refer to “ ”

3. Disable HTTP/FTP ethernet services.

   Refer to “ ”

3.2 ROCKWELL MICRO-850 (2080-LC20-24QBB)

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 28

2. Upgrade Communication Module Firmware

   Refer to **Error! Reference source not found.** S/N 26 Page 88-92

3. Set password for security lock feature

   Refer to “ ”

3.3 ROCKWELL MICRO-850 (2080-LC50-24QBB)

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 28 Page 217-219

2. Upgrade Communication Module Firmware

   Refer to **Error! Reference source not found.** S/N 26 Page 88-92

3. Set password for security lock feature

   Refer to “ ”

3.4 ROCKWELL AB 1734-ACNR

1. Upgrade firmware

   Refer to “ ”

3.5 ROCKWELL SLC 5/04

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 29

3.6 ROCKWELL COMPACTLOGIX L45

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 30

2. Set password for security lock feature

   Refer to “ ”

3. Disable unused ethernet services such as HTTP/FTP etc.

3.7 ROCKWELL COMPACTLOGIX 5561

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 32

2. Set password for security lock feature

   Refer to “ ”

3. Disable unused ethernet services such as HTTP/FTP etc.

   Refer to Rockwell Automation

3.8 ROCKWELL ALLAN BRADLEY

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 33

2. Disable unused ethernet services such as HTTP/FTP etc.

   Refer to Rockwell Automation

4. APPENDIX III - MITSUBISHI

4.1 DELTA DVP-20EX

1. Upgrade firmware
2. Set password for security lock feature
3. Disable unused HTTP/FTP ethernet services
4. Previous Firmware Logs

Document Number	Document Title	Publication Date	Link

5. Upgrade to latest firmware

Document Number	Document Title	Publication Date	Link	Section	Page Number
Awaiting Vendor Input					

5. APPENDIX IV - SIEMENS

5.1 SIEMENS S7-1200

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 46

2. Deactivation of the time synchronization via NTP server if not needed.

   Refer to **Error! Reference source not found.** S/N 46

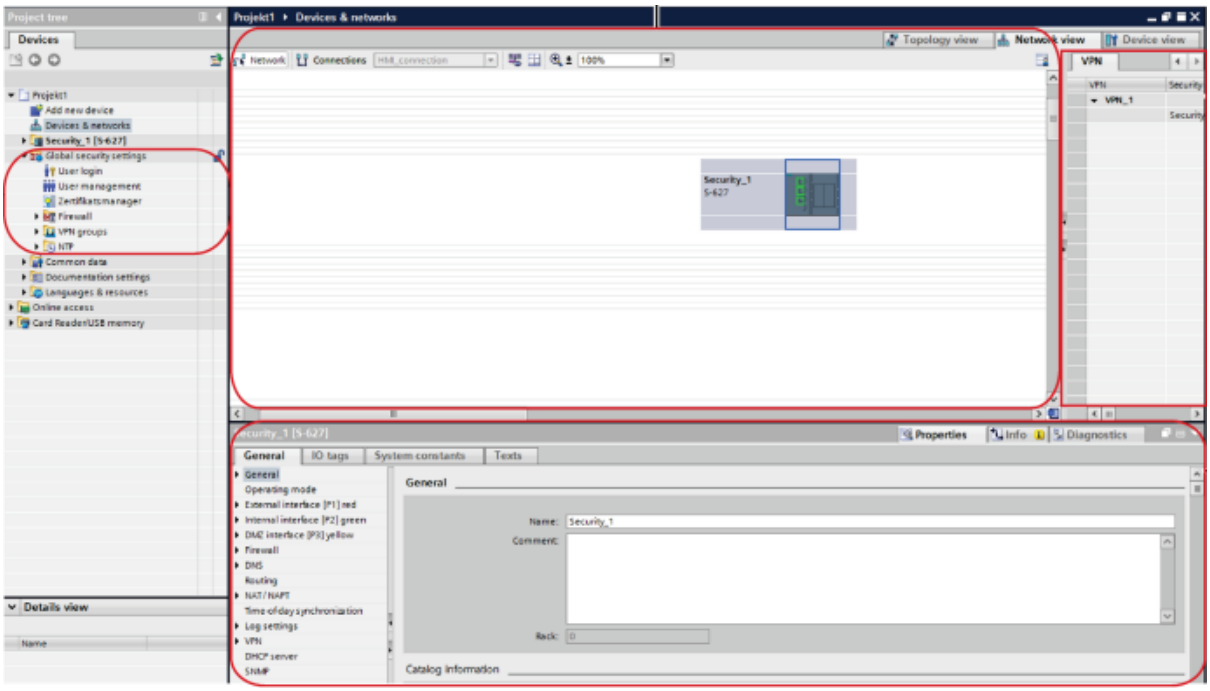
3. Deactivation of PUT/GET communications

   Refer to **Error! Reference source not found.** S/N 60, Page 8-12

4. Configuration of the user and functions rights via the user list
   a. Creating User
   b. Defining Execution Rights
   c. Assigning Passwords

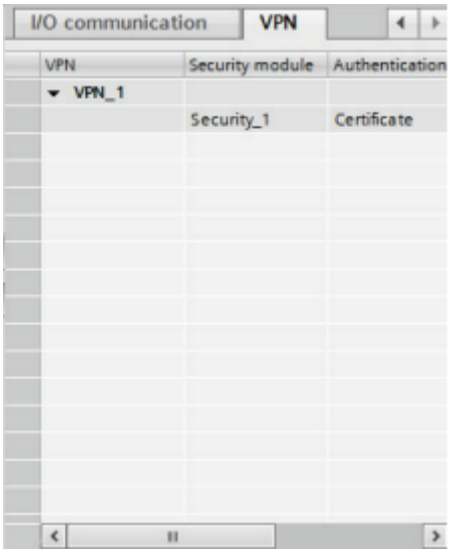
   Refer to **Error! Reference source not found.** S/N 60, Page 15

5. Know-how block protection for the protection of blocks against unauthorized persons.
   a. Select Devices>> General Security Settings

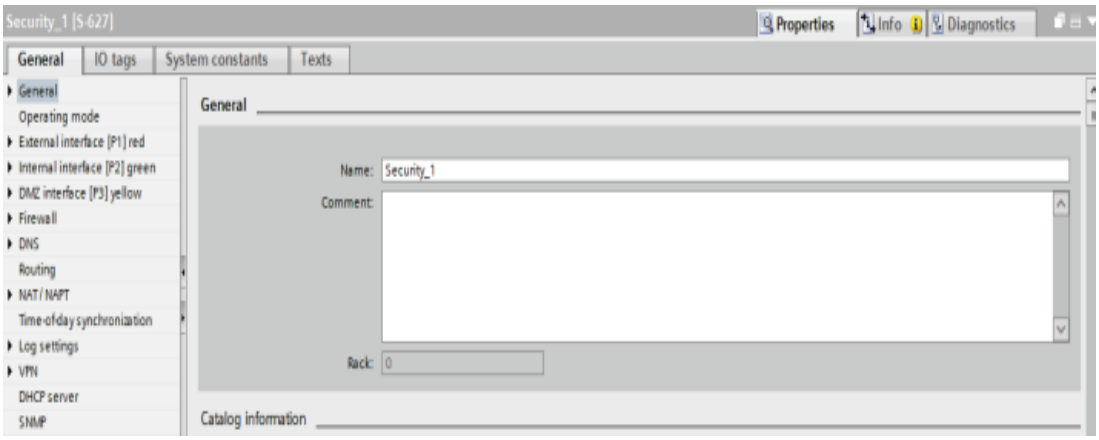


b. After selection of security module, the security settings are configured in Properties>> General

   For example: the selected module is VPN Group, the related information in this case will be displayed in VPN tab



c. Local Security settings are configured for the selected module in the inspector window under Properties>> General



d. Before the configuration of Security settings for CPs the following must be enabled under Activate security feature>>Properties>>General Tab>> Security

i. CP x43-1 Adv.:
    1. SNMP
    2. FTP configuration
    3. Time-of-day synchronization
    4. Web server
    5. Entries of IP access lists

ii. CP 1543-1:
    1. SNMP
    2. FTP configuration
    3. Time-of-day synchronization

iii. CP 1243-1:
    1. SNMP
    2. Time-of-day synchronization

Security Module	Navigation in the hardware Catalog
CP 343-1 Advanced	"Controller" >"SIMATIC S7-300" > "Communications modules" > "PROFINET/Ethernet" > "CP 343-1 Advanced-IT"
CP 443- Advanced	"Controller" >"SIMATIC S7-400" > "Communications modules" > "PROFINET/Ethernet" > "CP 443-1 Advanced-IT"
CP 1243-1	"Controller" > "SIMATIC S7-1200" > "Communications modules" > "Industrial Remote Control" > "CP 1243-1"
CP 1543-1	"Controller" > "SIMATIC S7-1500" > "Communications modules" > "PROFINET/Ethernet" > "CP 1543-1"

5.2 SIEMENS 1214 AC/DC/RLY

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 48

2. Set password for security lock feature

   Refer to “ “

3. Disable unused ethernet services.

   Refer to “ “

5.3 SIEMENS S7-300

1. Upgrade firmware

Refer to **Error! Reference source not found.** S/N **Error! Reference source not found.**

2. S7-Block Privacy and Know-how block protection for the protection of blocks against unauthorized persons.

   Refer to **Error! Reference source not found.** S/N 60, Page 8-12

3. Configuration of the user and functions rights via the user list
   a. Creating User
   b. Defining Execution Rights
   c. Assigning Passwords

   Refer to **Error! Reference source not found.** S/N 60, Page 15

5.4 SIEMENS ET 200

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 7

2. Set password for security lock feature

   Refer to “ “

3. Disable unused ethernet services.

   Refer to “ “

5.5 SIEMENS IM151-8 PN/DP

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 54

2. Set password for security lock feature

   Refer to “ “

3. Disable unused ethernet services

   Refer to “ “

5.6 SIEMENS S7-200

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 55

2. Set password for security lock feature

   Refer to “ “

3. S7-Block Privacy and Know-how block protection for the protection of blocks against unauthorized persons.

   Refer to Security Step7

5.7 SIEMENS LOGO 24RC

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 56

2. Set password for security lock feature

   Refer to “ ”

3. Disable HTTP/FTP ethernet services

   Refer to “ ”

5.8 SIEMENS S7-400

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 58

2. S7-Block Privacy and Know-how block protection for the protection of blocks against unauthorized persons.

   Refer to **Error! Reference source not found.** S/N 60, Page 8-12

3. Configuration of the user and functions rights via the user list
   a. Creating User
   b. Defining Execution Rights
   c. Assigning Passwords

   Refer to C79000-G8976-C379-01

6. APPENDIX V- ABB

6.1 ABB PM591

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 64

2. Set password for security lock feature

   Refer to “ ”

3. Encrypted communications with engineering systems.

   Refer to “ ”

6.2 ABB PM573

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 67

2. Set password for security lock feature

   Refer to “ ”

3. Encrypted communications with engineering systems

   Refer to “ ”

6.3 ABB PM564

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 69

2. Set password for security lock feature

   Refer to “ ”

3. Encrypted communications with engineering systems

   Refer to “ ”

7. APPENDIX VI- SOFREL

7.1 SOFREL S550

1. Upgrade firmware

   Refer to **Error! Reference source not found.** S/N 75

2. Set password for security lock feature

   Refer to “ ”

3. Disable unused ethernet services

   Refer to “ ”

8. APPENDIX VII- GE

8.1 LGE MDS - SD4 (GE RADIO)

1. Upgrade the firmware

   Refer to “ ”

2. Change the SSID/ESSID

   Refer to “ ”

3. Use strong radio encryption method (like WPA2 AES)

   Refer to “ ”

4. Disable unused services

   Refer to “ ”

ACET Solutions LLC
1400 Broadfield Blvd Suite 200 Houston TX, 77084.
United States of America.
Tel: +1 832 386 5593 | Fax: +1 832 201 0337
sales@acetsolutions.com | www.acetsolutions.com