NWC OT Cybersecurity MDCBU L1 Devices Hardening Design

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-MDCBU-HDN-L1
Document Title:	NWC OT Cybersecurity MDCBU L1 Devices Hardening Design
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
0	24 February 2022	AMS	NR	MM	Issue for Approval

GLOSSARY

Acronyms	Meaning
ACL	Access Control Lists
AD	Active Directory
ADC	Additional Domain Controller
ATM	Advance System and Technology
ATP	Adaptive Threat Protection
BOM	Bill of Material
BU	Business Unit
BYOD	Bring Your Own Device
CAP	Client Authorization Policy
CAS	Central Administration Server
CIP	Critical Infrastructure Protection
CMC	Central Management Console (Nozomi)
CSMS	Cyber Security Management System
DCS	Distributed Control System
DLD	Detailed-Level Design
DMZ	Demilitarized Zone
DNS	Domain Name System
DNS	Domain Name System
ECC	Essential Cybersecurity Controls
ePO	ePolicy Orchestrator
EPP	End Point Protection
GPS	Global Positioning System
HCIS	High Commission for Industrial Security
HLD	High Level Design
HMI	Human Machine Interface
HSE	Health, Safety, And Environmental
ICS	Industrial Control System
IDS	Intrusion detection System
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
JCBU	Jeddah Central Business Unit
KSA	Kingdom of Saudi Arabia
MBSS	Minimum Baseline Security Standards
MCBU	Makkah Central Business Unit
MDCBU	Madinah Central Business Unit
MGMT	Management
NCA	National Cybersecurity Authority
NERC	North American Electric Reliability Corporation
NGFW	Next Generation Firewall

Acronyms	Meaning
NIST	U.S. National Institute of Standards and Technology
NTP	Network Time Protocol
NWC	National Water Company
OT	Operational Technology
PDC	Primary Domain Controller
PLC	Programmable Logic Controller
RAP	Resource Authorization Policy
RCBU	Riyadh Central Business Unit
RD	Remote Desktop
RDS	Remote Desktop Services
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Incident & Event Management Solution
SSL	Secure Socket Layer
TCBU	Taif Central Business Unit
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network

REFERENCE DOCUMENTS

S/N	Document No.	Title
1	A01001045-HLD-ARCH.00	NWC OT Cybersecurity HLD Reference Architecture
2	A01001045-HLD	NWC OT Cybersecurity High-Level Design
3	A01001045-INV.00	NWC SCADA/OT Asset Inventory
4	ECC – 1: 2018	KSA NCA Essential Cybersecurity Controls (ECC – 1: 2018)
5	ISA–62443-1-1 (99.01.01)–2007	Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models

Table of Contents

1. DOCUMENT PURPOSE

The purpose of this document is to describe the Hardening Configuration of different L1 Devices in MDCBU.

Following is the list of L1 Devices installed at sites:

- Schneider M238
- Schneider SCADAPack 333E
- Siemens S7-300
- Motorola ACE3600
- T-Box LT2-504-3
- Tainy HMOD-L3-IO
- Moxa EDS-611

2. MDCBU LEVEL 1 DEVICE HARDENING SETTINGS

2.1 SCHNEIDER M238

- Upgrade firmware
- Set password for security lock feature
- Disable HTTP/FTP ethernet services

For Firmware Upgrade refer to the document “Attachment 3-M238 Firmware Upgrade Procedure”.

For IP Configuration refer to the document “Attachment 4-M238 IP Configuration Procedure”.

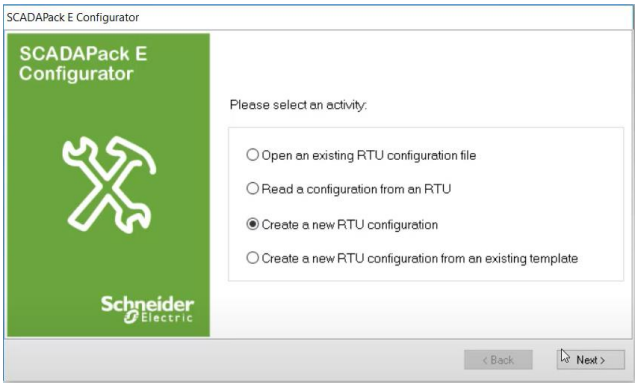
2.2 SCHNEIDER SCADAPACK 333E

- Upgrade Firmware
- Change Default IP Configuration
- Enable Sav2 over DNP3

For IP Configuration:

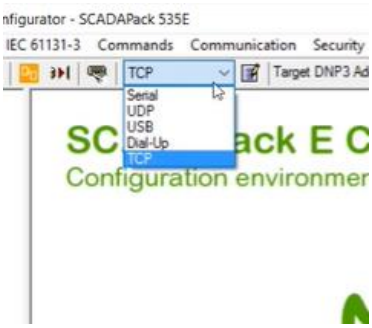
Step 1: Open SCADAPack E Configurator

Step 2: Select “Create a new RTU configuration” and click “Next”



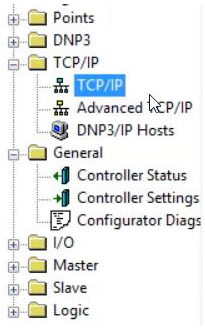
Step 4: Set the type of RTU to “SCADAPack 300E Series”, set the model to “SCADAPack 333E” and click “Finish”

Step 5: Select USB from drop down communications menu.



Step 6: Go to File > Read RTU Configuration.

Step 7: Once the configuration has been read, drill down into the TCP/IP folder and double click TCP/IP.



Step 8: Enter the desired IP Address and Subnet Mask in the relevant Ethernet Port available

For Firmware Upgrade refer to the document “Attachment 5-SCADAPack Firmware Upgrade Procedure”.

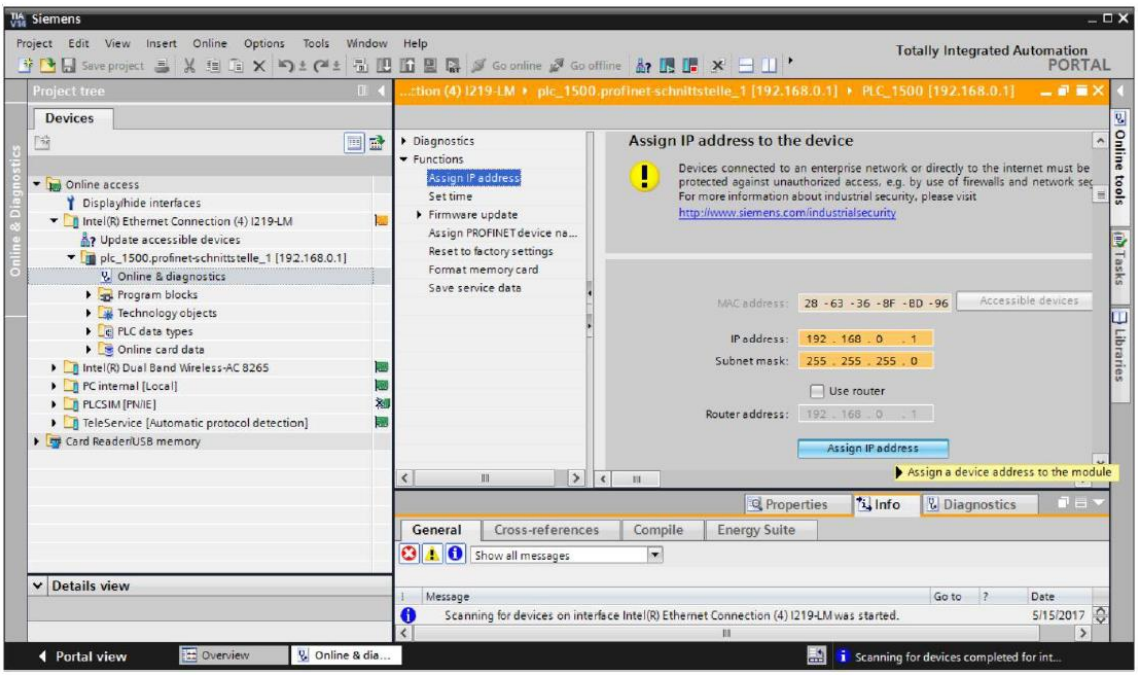
2.3 SIEMENS S7-300

- Upgrade firmware
- Set password for security lock feature
- Disable HTTP/FTP ethernet services

For IP Setting:

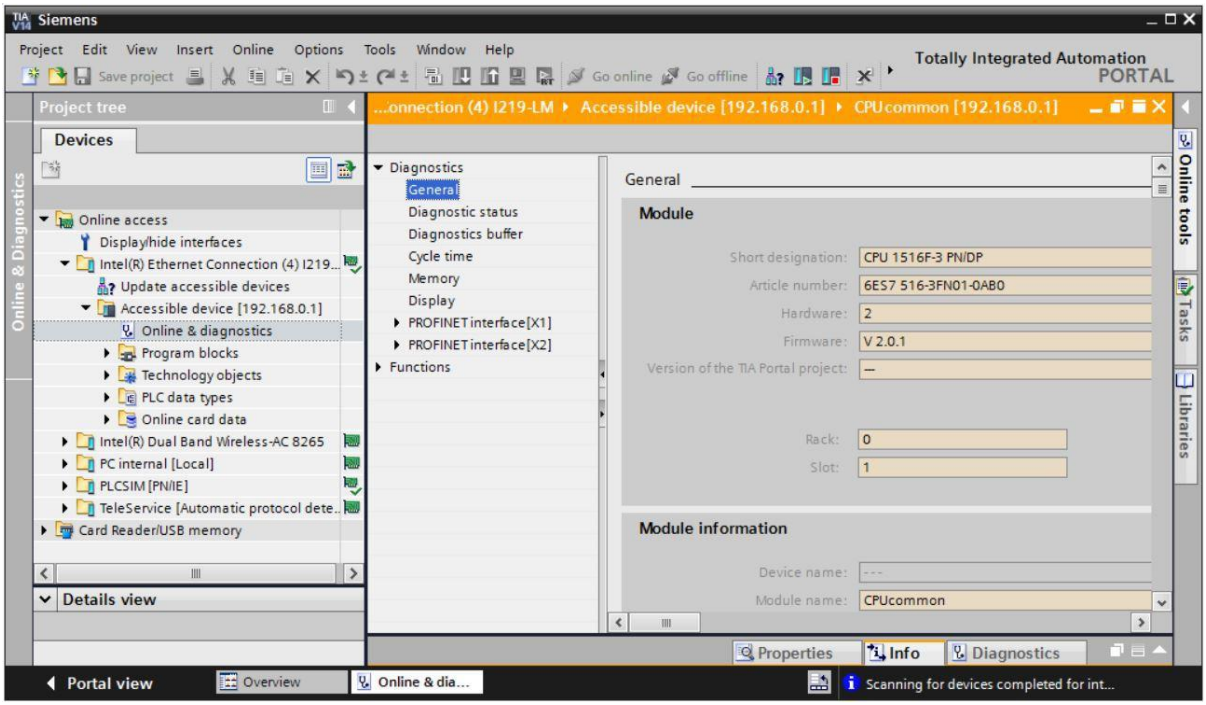
Step 1: Go to “Online & Diagnostics”

Step 2: Under "Functions", you now find the "Assign IP address" item. Enter the following IP address here (example): IP address: 192.168.0.1 Subnet mask 255.255.255.0. Next, click "Assign IP address" and this new address will be assigned.

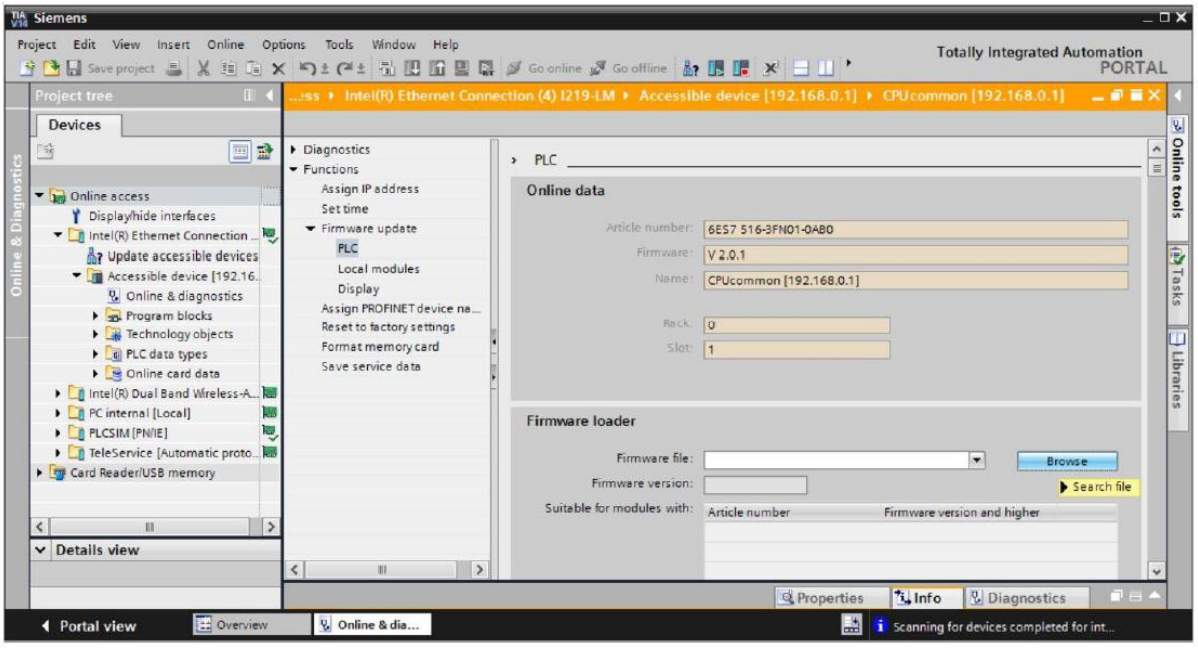


For firmware upgrade:

Step 1:

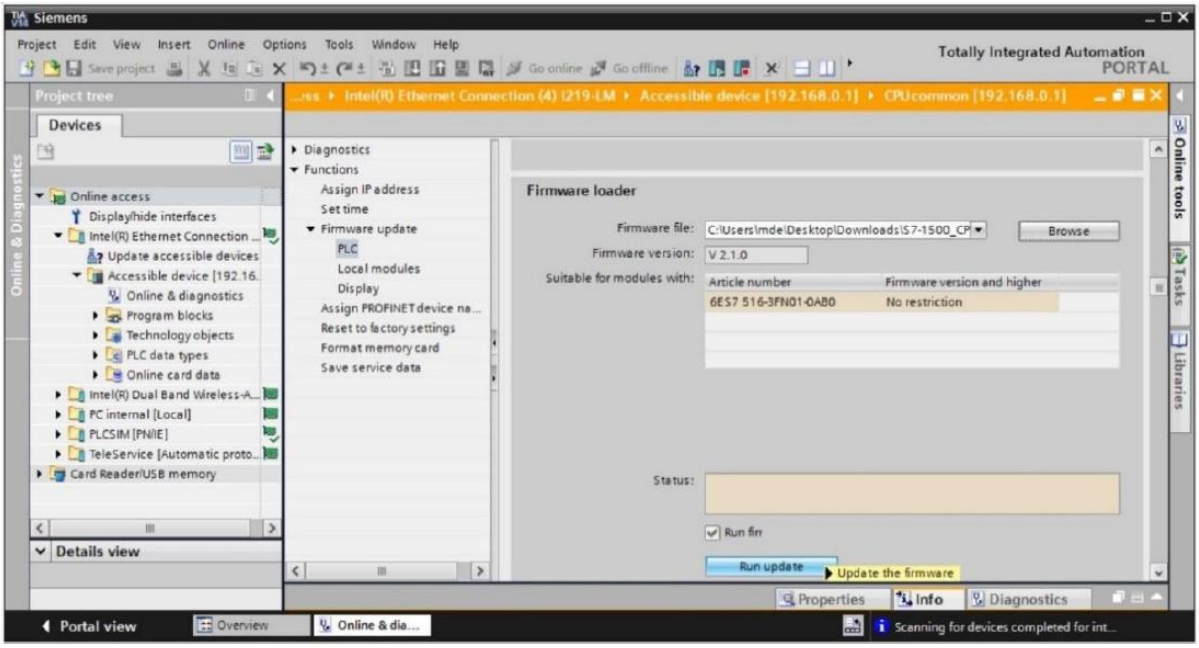


Step 2: In the "Functions" menu, change to "Firmware update" > "PLC". In the "Firmware loader" sub-item, click "Browse".

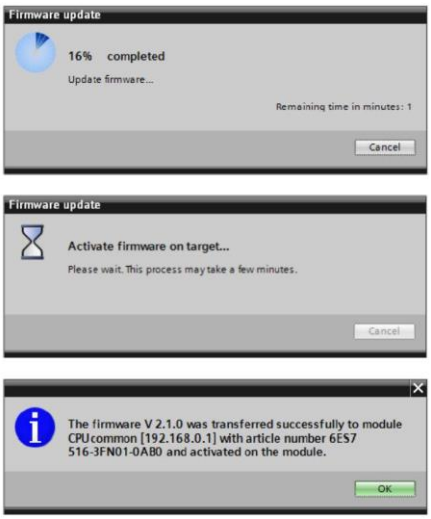


Step 3: Select the downloaded and extracted firmware file.

Step 4: The following dialog indicates whether your firmware file is compatible with your CPU. Now start the update. ("Run update")



Step 5: The progress of the update and its successful completion are indicated with the following dialogs. Click "OK" to confirm.



2.4 MOTOROLA ACE3600

- Upgrade firmware
- Set password for security lock feature
- Disable HTTP/FTP ethernet services

For IP Change refer to the “Attachment 1-Motorola ACE3600 IP Config”.

For Firmware Upgrade refer to “Attachment 2-Motorola ACE3600 Firmware Upgrade”.

2.5 T-BOX LT2-504-3

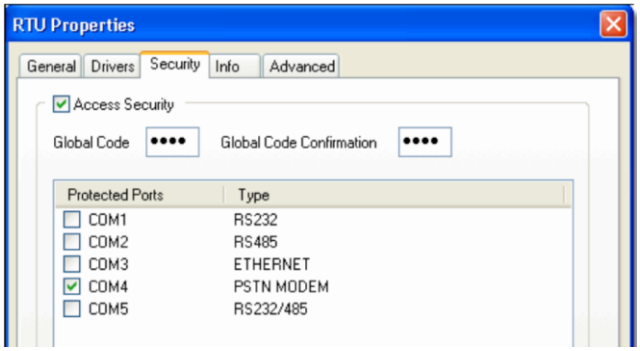
- Upgrade firmware
- Set password for security lock feature
- Disable HTTP/FTP ethernet services

For setting access security:

Step 1: From RTU Properties > tab “Security”, check the “Access security”.

Step 2: Enter the “Global Code” and confirm it.

Step 3: Check the port you want to protect.



Setting Password for Access Security:

Step 1: Open “PASSWORD”, which can be accessed from “Start” button > “Techno Trade” > “Accessories”.

Step 2: Enter the “Global Code” (as set above) and confirm it. Enter desired Username and set the Access Level. The password is generated based on the Global Code, unique Username and Access Level.

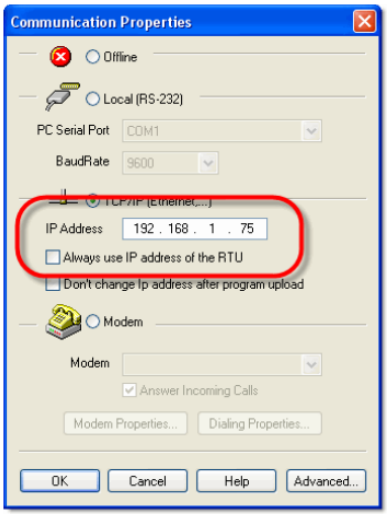
Step 3: Click Get Password, this will generate a User ID and Password to be used to login.

For IP Configuration:

Step 1: Uncheck the “Always use IP address of the RTU” option

Step 2: Uncheck the “Don’t Change IP address after program upload” option

Step 3: Enter the desired IP address



Step 4: Click “OK” and upload the program

2.6 TAINY HMOD-L3-IO

- Upgrade Firmware
- Set password for security lock feature
- Disable HTTP/FTP ethernet services

For Firmware Upgrade procedure refer to the document “Attachment 6-Tainy HMOD-L3-IO Firmware Upgrade Procedure”.

For IP Configuration procedure refer to the document “Attachment 7-Tainy HMOD-L3-IO IP Configuration Procedure”.

For cybersecurity features configuration refer to the document “Attachment 8-Tainy HMOD-L3-IO Cybersecurity Features”.

2.7 MOXA EDS-611

- Set password for security lock feature
- Limit the number of Ips which can access the switch
- Configure SNMP

For IP configuration procedure and security features implementation procedure refer to the document “Attachment 9-Moxa EDS-611 Use Manual”.

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