NWC OT Cybersecurity MCBU L1 Devices Hardening Design

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-MCBU-HDN-L1
Document Title:	NWC OT Cybersecurity MCBU 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

The information contained in this document is confidential, privileged, and only for the intended recipient's information and may not be used, published, or redistributed without the prior written consent of ACET Solutions LLC. This document contains confidential, sensitive information of National Water Company (NWC).

Information contained herein is for the sole use of the customer (NWC) receiving this document. Acceptance of the document by the customer constitutes agreement by the customer & ACET Solutions that either party shall not disclose confidential information to any third party and shall not transmit any documents or copies thereof containing confidential information to any third party except as may by authorized in writing by NWC & ACET Solutions.

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	11-Feb-2021	HSN	NR/SK	MM	Issued 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

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		Sofrel Data Logger and RTU Documentation
5		Schneider SCADAPack Documentation
6	ECC – 1: 2018	KSA NCA Essential Cybersecurity Controls (ECC – 1: 2018)
7	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 MCBU.

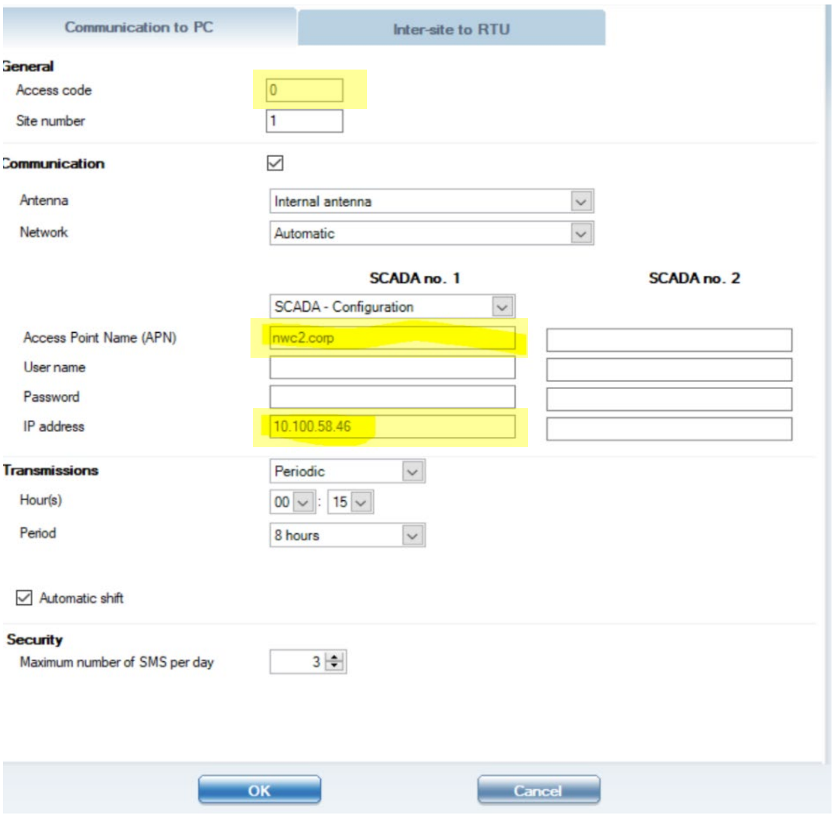
Following are list of L1 Devices:

- Schneider ScadaPack 333E/545E/337E
- Sofrel AS50 RTUs
- Sofrel Data Loggers

2. MCBU LEVEL 1 DEVICE HARDENING SETTINGS

2.1 SOFREL DATA LOGGER HARDENING

- Change Access Point Name (APN) in Data Logger to following:
  - **MakkahOT.M2M**
- Change FR 4000 IP in Data Logger to following:
  - **10.101.13.10**
- Firmware upgrade:
  - Not required.



General

Access code: 0

Site number: 1

Communication ☑

Antenna: Internal antenna

Network: Automatic

	SCADA no. 1	SCADA no. 2
	SCADA - Configuration	
Access Point Name (APN)	nwc2.corp	
User name		
Password		
IP address	10.100.58.46	

Transmissions: Periodic

Hour(s): 00 : 15

Period: 8 hours

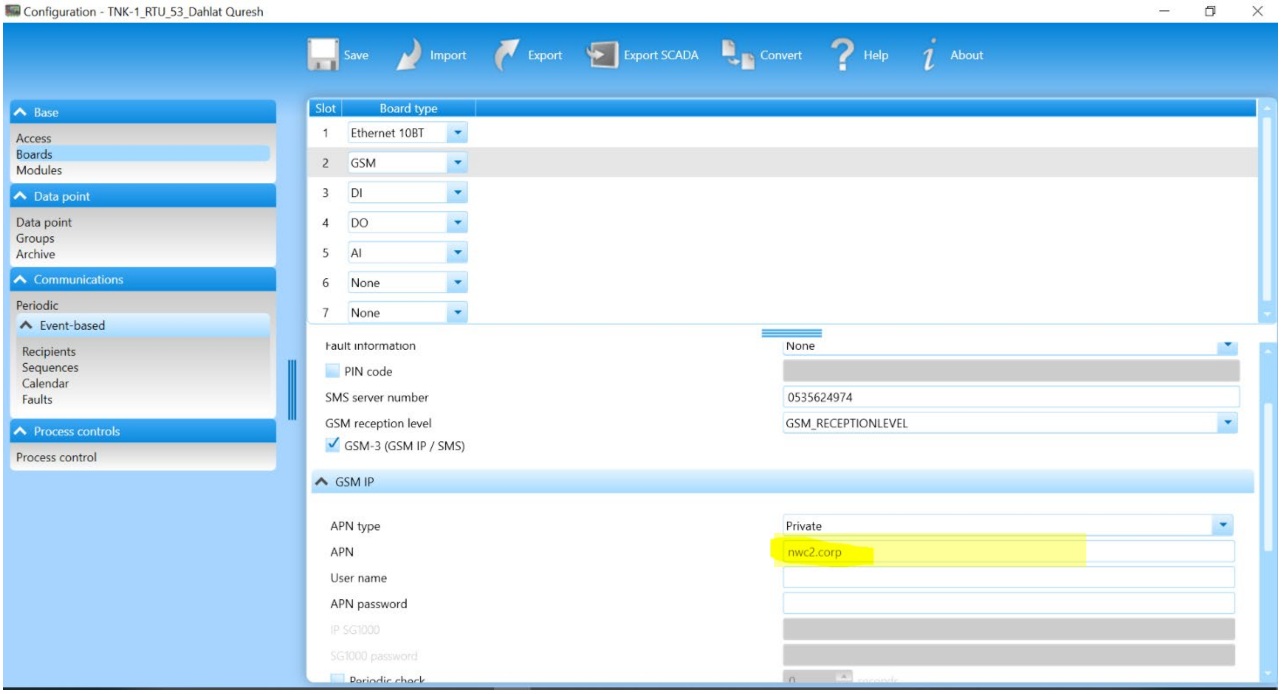
☑ Automatic shift

Security

Maximum number of SMS per day: 3

2.2 SOFEREL RTU HARDENING

- Change APN in Sofrel RTU to following:
  - **MakkahOT.M2M**
- Firmware upgrade:
  - Not required.
- Change Administrator/Operator Password:
  - Password to be changed from DEFAULT to minimum 8-character length password.



Slot	Board type
1	Ethernet 10BT
2	GSM
3	DI
4	DO
5	AI
6	None
7	None

Fault information: None

□ PIN code

SMS server number: 0535624974

GSM reception level: GSM_RECEPTIONLEVEL

☑ GSM-3 (GSM IP / SMS)

GSM IP

APN type: Private

APN: nwc2.corp

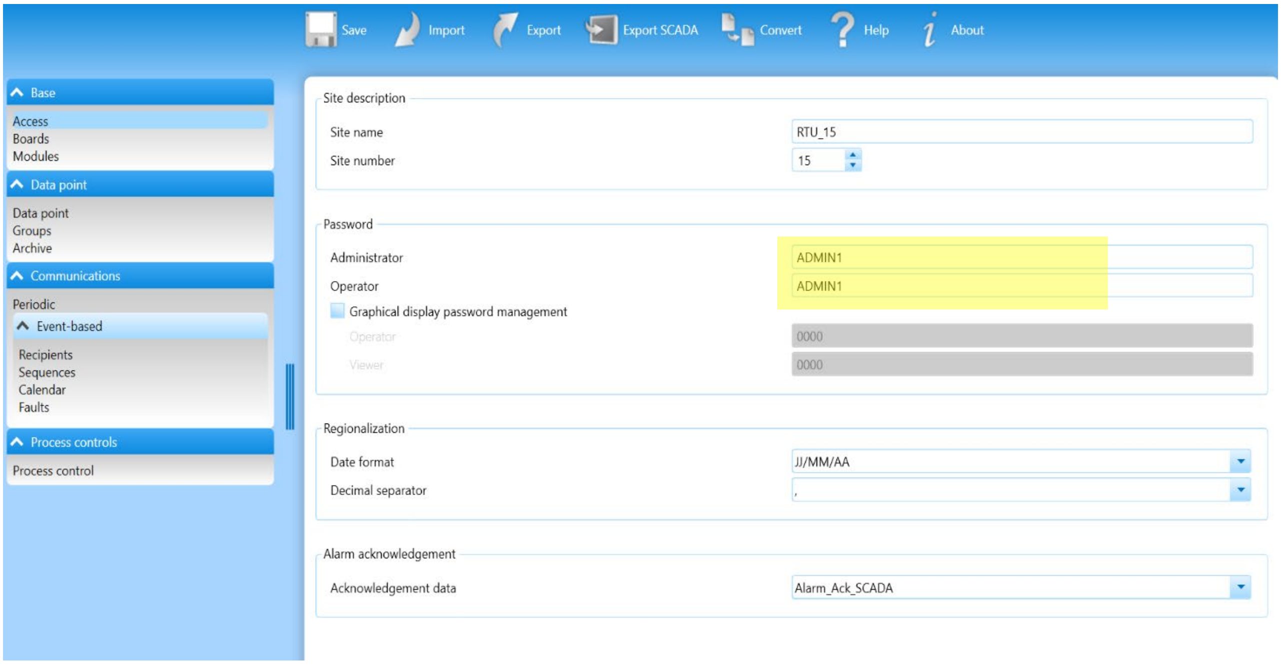
User name:

APN password:

IP SG1000

SG1000 password

□ Periodic check 0 seconds



Site description

Site name: RTU_15

Site number: 15

Password

Administrator: ADMIN1

Operator: ADMIN1

□ Graphical display password management

Operator: 0000

Viewer: 0000

Regionalization

Date format: JJ/MM/AA

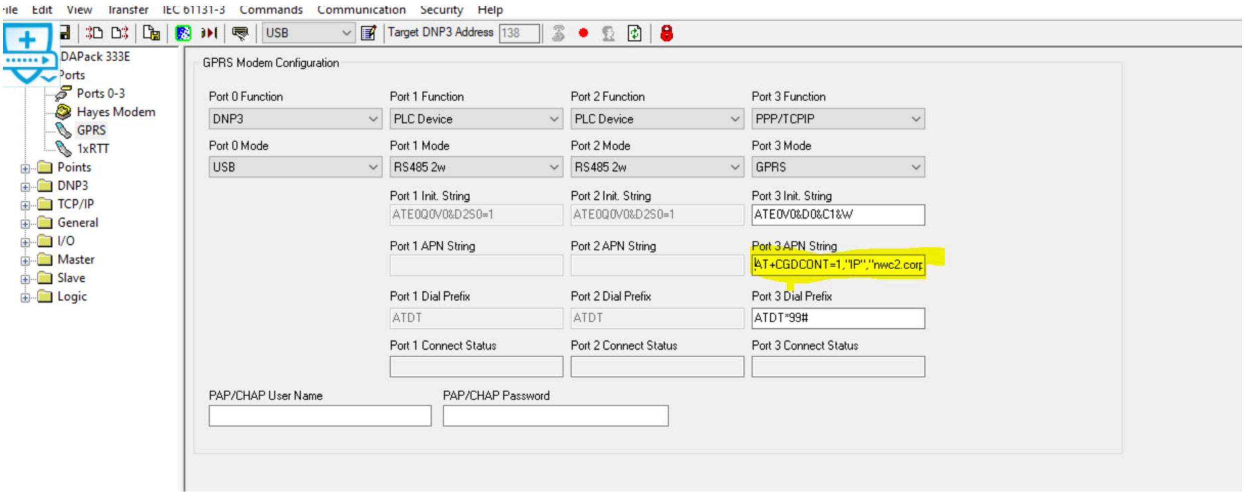
Decimal separator: ,

Alarm acknowledgement

Acknowledgement data: Alarm_Ack_SCADA

2.3 SCADAPACK RTU HARDENING

- Replace “nwc2.corp” in Port3 APN String in RTU with following:
  - **MakkahOT.M2M**



Target DNP3 Address 138

GPRS Modem Configuration

Port 0 Function: DNP3
Port 1 Function: PLC Device
Port 2 Function: PLC Device
Port 3 Function: PPP/TCPIP

Port 0 Mode: USB
Port 1 Mode: RS485 2w
Port 2 Mode: RS485 2w
Port 3 Mode: GPRS

Port 1 Init. String: ATE0Q0V0&D2S0=1
Port 2 Init. String: ATE0Q0V0&D2S0=1
Port 3 Init. String: ATE0V0&D0&C1&W

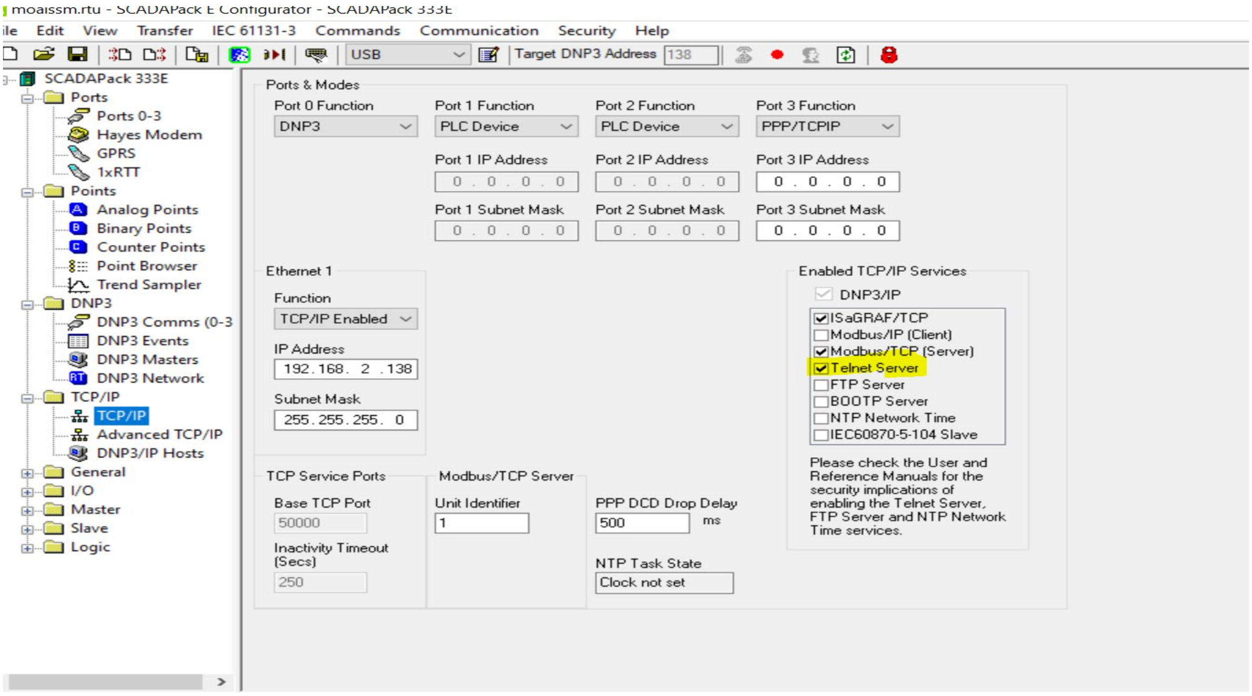
Port 1 APN String
Port 2 APN String
Port 3 APN String: AT+CGDCONT=1,"IP","nwc2.corp

Port 1 Dial Prefix: ATDT
Port 2 Dial Prefix: ATDT
Port 3 Dial Prefix: ATDT*99#

Port 1 Connect Status
Port 2 Connect Status
Port 3 Connect Status

PAP/CHAP User Name
PAP/CHAP Password

- Firmware upgrade to version **8.17.1**:
- Disable Telnet Server
- Security Lock feature
  - In latest firmware 8.17, Option to use Security Lock feature is available to protect RTU Application from Unauthorized changes.
  - It is recommended is to use it with appropriate procedures.
  - Set Username and password for security lock feature.



Target DNP3 Address 138

Ports & Modes

Port 0 Function: DNP3
Port 1 Function: PLC Device
Port 2 Function: PLC Device
Port 3 Function: PPP/TCPIP

Port 1 IP Address: 0 . 0 . 0 . 0
Port 2 IP Address: 0 . 0 . 0 . 0
Port 3 IP Address: 0 . 0 . 0 . 0

Port 1 Subnet Mask: 0 . 0 . 0 . 0
Port 2 Subnet Mask: 0 . 0 . 0 . 0
Port 3 Subnet Mask: 0 . 0 . 0 . 0

Ethernet 1
Function: TCP/IP Enabled
IP Address: 192.168. 2 .138
Subnet Mask: 255.255.255. 0

Enabled TCP/IP Services
☑ DNP3/IP
☑ ISaGRAF/TCP
☐ Modbus/IP (Client)
☑ Modbus/TCP (Server)
☑ Telnet Server
☐ FTP Server
☐ BOOTP Server
☐ NTP Network Time
☐ IEC60870-5-104 Slave

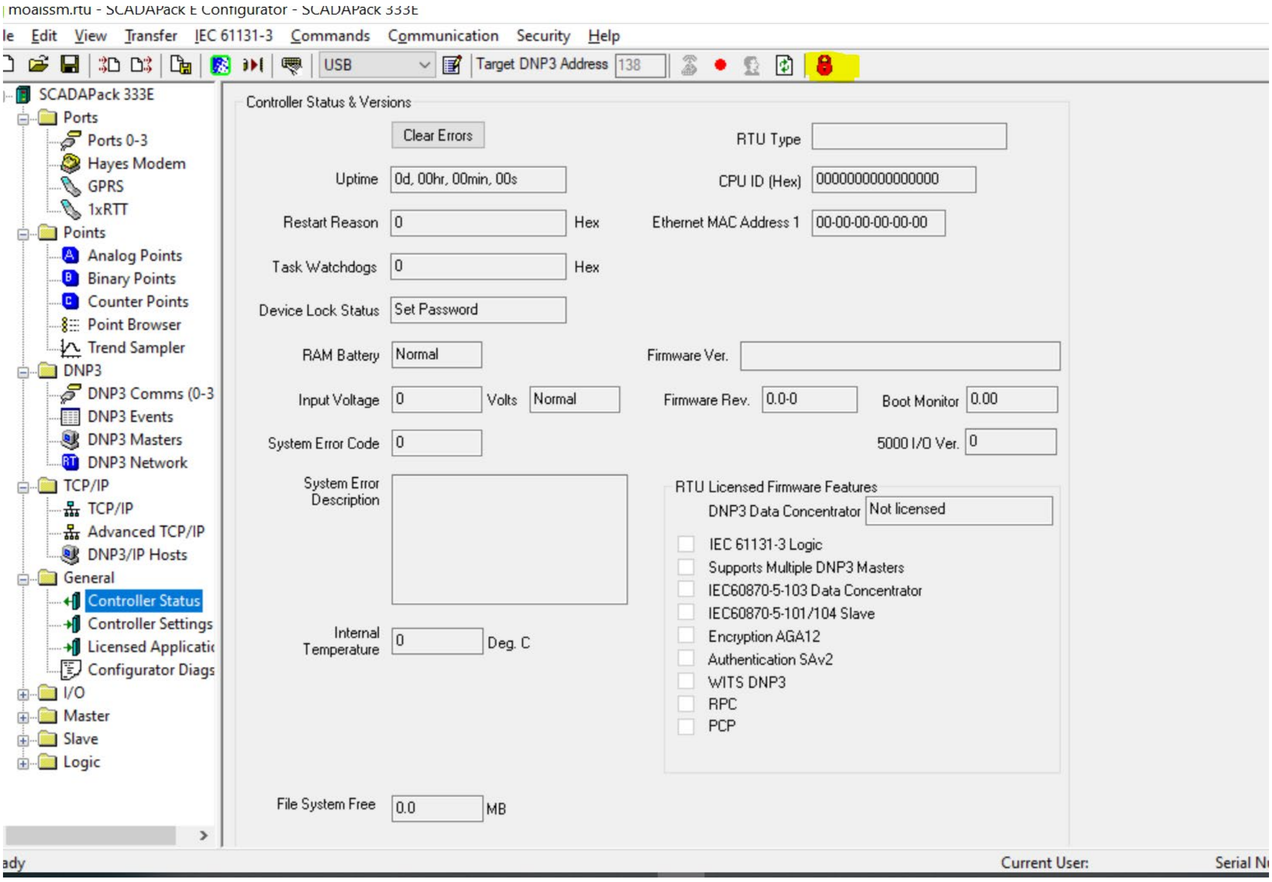
Please check the User and Reference Manuals for the security implications of enabling the Telnet Server, FTP Server and NTP Network Time services.

TCP Service Ports
Base TCP Port: 50000
Inactivity Timeout (Secs): 250

Modbus/TCP Server
Unit Identifier: 1

PPP DCD Drop Delay: 500 ms

NTP Task State: Clock not set



Controller Status & Versions

Uptime	0d, 00hr, 00min, 00s	RTU Type	
Restart Reason	0 Hex	CPU ID (Hex)	0000000000000000
Task Watchdogs	0 Hex	Ethernet MAC Address 1	00-00-00-00-00-00
Device Lock Status	Set Password		
RAM Battery	Normal	Firmware Ver.	
Input Voltage	0 Volts Normal	Firmware Rev.	0.0-0
System Error Code	0	Boot Monitor	0.00
System Error Description		5000 I/O Ver.	0
Internal Temperature	0 Deg. C		
File System Free	0.0 MB		

RTU Licensed Firmware Features

DNP3 Data Concentrator: Not licensed

- □ IEC 61131-3 Logic
- □ Supports Multiple DNP3 Masters
- □ IEC60870-5-103 Data Concentrator
- □ IEC60870-5-101/104 Slave
- □ Encryption AGA12
- □ Authentication SAv2
- □ WITS DNP3
- □ RPC
- □ PCP

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