NWC OT Cybersecurity Detailed-Level Design

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-DLD
Document Title:	NWC OT Cybersecurity Detailed-Level Design
Document Version:	7
NWC Contract No.:	101200487
[atm] PO Ref.:	ATMPO2020-034

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.

No part of this document may be used, translated into another language, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written approval from ACET Solutions.

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	07-Jan-2021	RAS	NR/SK	MM	Issued For Approval
1	11-Aug-2021	AR	NR/SK	MM	Issued For Approval
2	18-Oct-2021	HMA/UK	NR/SK	MM	Issued For Approval
3	15-Nov-2021	HMA/UK	NR/SK	MM	Issued For Approval
4	23-Dec-2021	HMA/AR	NR/SK	MM	Issued For Approval
5	31-Jan-2022	HMA	NR/SK	MM	Issued For Approval
6	3-Feb-2022	HMA	NR/SK	MM	Issued For Approval
7	17-Feb-2022	AR	NR	MM	Issued For Approval

GLOSSARY

Acronyms	Meaning
ACL	Access Control Lists
AD	Active Directory
ADC	Additional Domain Controller
AK	Alkhumra
AOS	Automation Object Server
APN	Access Point Name
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
DAS	Data Acquisition Server
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
FO	Fiber Optics
GPRS	General Packet Radio Service
GPS	Global Positioning System
GR	Galaxy Repository
GSM	Global System for Mobile
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
IO	Input/Output
IP	Internet Protocol
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
LS	Lifting Station
MBSS	Minimum Baseline Security Standards
MCBU	Makkah Central Business Unit
MCC	Motor Control Center
MDCBU	Madinah Central Business Unit
MGMT	Management
MTU	Master Telemetry Unit
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
OCC	Operation Control Center
OT	Operational Technology
PDC	Primary Domain Controller
PLC	Programmable Logic Controller
PSB	Prince Sultan Building
RAP	Resource Authorization Policy
RCBU	Riyadh Central Business Unit
RD	Remote Desktop
RDS	Remote Desktop Services
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RTU	Remote Telemetry Unit
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Incident & Event Management Solution
SIM	Subscriber Identification Module
SS	Sea Station
SSL	Secure Socket Layer
STP	Sewerage treatment plant
SW	Switch
TCBU	Taif Central Business Unit
TCP	Transmission Control Protocol
USB	Al Usbah WTP
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network
WTP	Water Treatment Plant
WWTP	Wastewater Treatment Plant

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-DLD	Detailed Design Summary
4	A01001045-DLD-PM	Patch management Detailed Design
5	A01001045-DLD-BM	Backup management Detailed Design
6	A01001045-DLD-EP	Endpoint Protection Management Detailed Design
7	A01001045-DLD-AD	Active Directory Detailed Design
8	A01001045-DLD-RA	Remote Access Management Detailed Design
9	A01001045-DLD-IPSCH	IP Schema
10	A01001045-HQ-DLD-NA	Network Architecture
11	A01001045-INV	SCADA Assets Inventory
12	A01001045-MCBU-EXA	Existing Network Architecture
13	A01001045-MCBU-HDN-L1	Level-1 Devices Hardening Design
14	A01001045-MCBU-DLD-SA	System Architecture
15	A01001045-DLD-FWD	Firewalls Zones Design
16	ECC – 1: 2018	KSA NCA Essential Cybersecurity Controls (ECC – 1: 2018)
17	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

List of Figures

1. DOCUMENT PURPOSE

The purpose of this document is to describe the Detailed-Level Design (DLD) for SCADA/OT Cybersecurity implementation project at NWC. The detailed design comprises of:

- This document
- Detailed design documents for different sections
- Appendices

Note that the terms OT, ICS, SCADA are used interchangeably within this document, and all refer to the NWC SCADA system.

This DLD will be valid even after implementation is complete. Therefore, the design description uses present tense to describe the design as it will be once the implementation is done. For example:

- “There are three security zones in the HQ.”
- “A Central WSUS Server is deployed on management server in OT-DMZ.”

This does not imply that this is the current state in NWC SCADA. It describes how it will be after the implementation.

2. DESIGN BASIS

This section describes the key elements that were considered for development of the HLD for NWC SCADA/OT Cybersecurity implementation project.

The HLD follows the requirements of the following standards:

- KSA NCA Essential Cybersecurity Controls (ECC – 1: 2018)
- ISA–62443-1-1 (99.01.01)–2007

Following are some of the key requirements from the above standards as well as other guiding principles considered during the development of the HLD.

2.1 NCA ECC SEGMENTATION REQUIREMENT

While all applicable NCA ECC requirements will be implemented, the following specific requirement is considered for High-Level Architecture design.

- Strict physical and virtual segmentation to be implemented when connecting industrial production networks (SCADA) to other networks within the organization (e.g., corporate network) as well as with external networks (e.g., Internet, wireless, remote access). (Ref. ECC: 5-1-3)

Note that while NCA ECC requires segregation of SCADA network from corporate and external networks, it does not explicitly require zoning and segmentation within the SCADA network.

2.2 ISA-99 SCADA REFERENCE MODEL

ISA-62443-1-1 clause 6.2 describes the concept of Reference Model as:

> "*A reference model describes a generic view of an integrated manufacturing or production system, expressed as a series of logical levels.*"

The SCADA Reference Model used by the ISA99 series of standards is shown below.

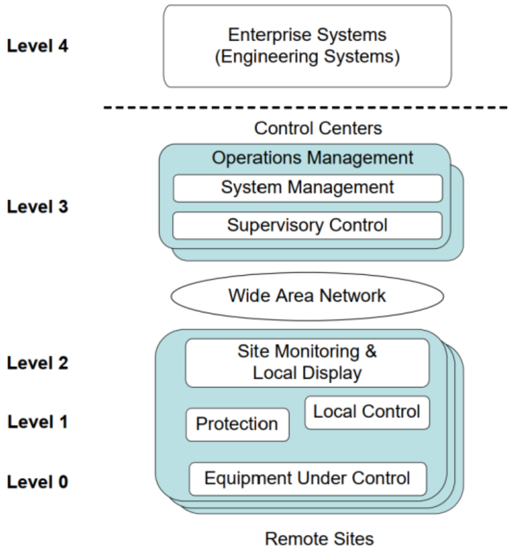


Figure 1 ISA-99 SCADA Reference Model (ISA–62443-1-1 –2007)

The model consists of the same basic levels, each representing a particular class of functionality.

- Level-0 includes the actual physical process, sensors and actuators directly connected to the process and process equipment.
- Level-1 includes the functions involved in sensing and manipulating the physical process. PLCs, RTUs, Data Loggers, MTUs, Data Concentrators are considered as Level-1 devices.
- Level-2 includes the functions involved in monitoring and controlling the physical process. Operator Workstations, HMIs, SCADA servers, Historians are considered Level-2 devices.
- Level-3 includes the functions involved in managing production and operations. A central control room would be an example of Level-3 function.
- Level-4 includes enterprise/corporate network and functions. IT (Information Technology) is a Level-4 function.

While not explicitly listed as an ISA-99 Level, the standard recommends a DMZ (Level-3.5) between Level-3 and Level-4. This DMZ provides the interface between IT and OT/SCADA environment.

Note that the levels presented in the Reference Model are logical levels. The same levels may exist in multiple segregated physical locations (e.g., remote sites, main sites, branch office etc.)

2.3 ISA-99 SCADA REFERENCE ARCHITECTURE

ISA-62443-1-1 clause 6.4 describes the requirement for a Reference Architecture as:

> "*Each organization creates one or more reference architectures depending on the business functions performed, as well as the functions under review. It would be common for an organization to have a single reference architecture for the corporation that has been generalized to cover all operating facilities. Each facility or type of facility may also have a more detailed reference network architecture diagram that expands on the enterprise model.*"

A Reference Architecture helps develop the Zones and Segments for the SCADA system.

This HLD includes the Reference Architecture developed for NWC

2.4 SECURITY ZONES

Security zones, as defined by ISA-62443-1-1, are "*grouping of logical or physical assets that share common security requirements*".

Grouping SCADA assets into security zones helps define, implement, and enforce security requirements based on shared characteristics. These characteristics include:

- Security Policies
- Asset Inventory
- Access Requirements and Controls
- Threats and Vulnerabilities
- Consequences of a Security Breach
- Authorized Technology
- Change Management Process

Assets that share the same characteristics may be grouped into one zone. Assets that have different requirements for these characteristics are grouped into separate zones.

Additional considerations regarding security zoning and segmentation requirements of ISA-62443-1-1:

- It is not mandatory to create separate zone for each Level of the SCADA reference model. Assets at different Levels (PLC, RTU, SCADA servers, Workstations etc.) may be grouped in the same zone if these share the same characteristics.
- It is not mandatory that geographically segregated sites be grouped into separate zones. Multiple sites may be grouped into the same zone if these share the same characteristics.
- One site may have multiple zones.
- One zone may include multiple sites.
- The whole SCADA system may be grouped into one zone if all assets share the same characteristics.

- It is not mandatory to install a firewall between different zones. Any suitable barrier (routers, layer-3 switches) may be installed based on security requirements.

2.5 IT/OT SEGREGATION

Requirements for physical and logical segregation between IT and OT network is well covered in the sections above. Equally important is the functional and operational segregation between IT and OT.

Functional segregation requires the OT environment to have the following segregated from IT:

- Domain
- Access Management
- Patch Management
- End-Point protection
- Backup Management
- System & Network Administration
- System & Network Monitoring, Log collection
- Systems and Applications Backup Management
- SCADA applications (e.g., Historian)

If any of these functions has dependency on IT (e.g., for virus definitions update, patches etc.), or requires integration with IT (e.g., SIEM, SOC), a well-defined secure interface is to be provided with strict security controls and procedures to minimize the risk.

Operational segregation requires separate roles for OT network and systems administration. These include Domain admins, network admins, system admins, backup admins, etc. Any interfaces with enterprise operational teams (e.g., Information security, SOC, IT administration) requires well defined interface personnel and operating procedures.

2.6 NWC SCADA ASSETS AND ORGANIZATION

The physical location of assets, existing architecture, as well as the business organization is also a key consideration for the HLD.

NWC SCADA assets are geographically dispersed across KSA. In addition, the business operation and organization are also distributed based on geographical locations.

The company headquarter (HQ) is in Riyadh. Currently, the company has operations in five cities. Each of these cities is organized as a Business Unit (BU). These five BUs are:

- Riyadh Business Unit (RCBU)
- Jeddah Business Unit (JCBU)
- Makkah Business Unit (MCBU)
- Taif Business Unit (TCBU)
- Madinah Business Unit (MDCBU)

Additional cities may be added to NWC organization in future.

Each of the BUs consists of:

- One BU-Main-Office
- Multiple Branch Offices
- Multiple Field Sites

SCADA assets are installed at all these locations and communicate to assets within as well as across offices/sites. Different mediums are utilized for this communication including Copper, Fiber Optics, MPLS, GSM/GPRS, Radio. NWC relies on a private secure cloud provided by telecom companies for communication between different offices/sites within the BUs as well as with the HQ.

Each BU operates independently from other BUs and from the HQ. For example, MCBU SCADA operates independently from JCBU SCADA.

Sites within each BU operate independently from other sites. For example, SCADA at Mina site in MCBU operates independently from PS-5 site.

Currently, there is no segregation between IT and OT within NWC and the SCADA assets share the infrastructure, services, and resources with the IT.

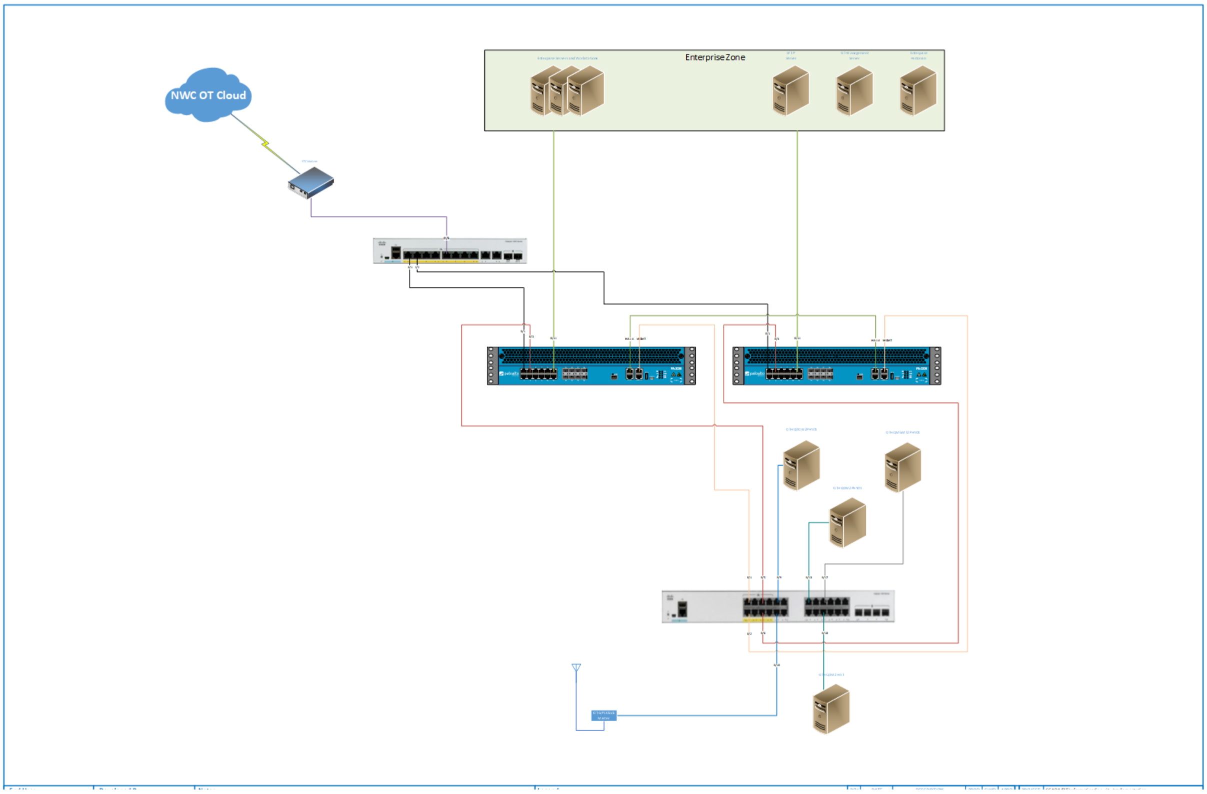
Management and operation of the SCADA involves multiple stakeholder organization within NWC including:

- Infrastructure team: Manages the SCADA servers, workstations, operating systems, and O/S related functions.
- Network team: Manages the SCADA network setup and devices, including interface with the telecom companies for the private cloud. Manages NWC SOC.
- Smart Operations: Operate the SCADA system as well as manage the field devices.
- O&M SCADA Application team: Manages the SCADA software and application.
- Information Security: Responsible for cybersecurity of SCADA systems.
- Enterprise Architecture Team: Responsible for integration of business systems with SCADA.

3. HEAD QUARTER DESIGN

3.1 HQ ARCHITECTURE

Following is the detailed architecture of NWC SCADA/OT environment at the NWC Headquarter.



A high-resolution version of the architecture is provided as an attachment (A01001045-HQ-DLD-NA).

Following is a description of the network setup for OT Cybersecurity in HQ:

- The SCADA/OT environment is fully segregated from IT including servers, workstations, network infrastructure, WAN. The only interface point is the IT/OT interface firewall in HQ. No physical or logical connections between IT and OT are allowed except through this interface firewall. In addition, direct connection from IT is only allowed to the OT-DMZ. No direct connection from IT to any other OT zone is allowed.
- There are three security zones in the HQ.
  - OT-Domain-Zone: Consisting of
    - One host server with two VMs
    - Primary Domain Controller (VM) for the OT Domain
    - Remote Desktop Gateway (VM)
    - GPS Clock Master

- OT-DMZ: Consisting of
    - One host server for OT Cybersecurity, with two VMs
    - McAfee ePO server
    - Microsoft WSUS server
    - Veritas BackupExec Central Administration Server
    - SFTP Server
    - One host server for Historian (existing)
- OT-Management-Zone: Consisting of
    - One host server with two VMs
    - Palo Alto Panorama software
    - Nozomi Networks Central Management Console (CMC)

- The zoning is achieved using VLANs, ACL, and routing configured in the firewall.
- The OT-DMZ contains all functions and services that require interface with IT. These include Antivirus, Patch Management, Backup Management, and Historian.
- The OT-DMZ may communicate with the assets in BU Main-Office or Branch-Offices as required. Refer to individual sections for each function for details.
- The OT Domain Controller is installed in a separate OT-Domain-Zone. The OT Domain controller communicates with the OT assets only; there is no direct communication with IT. Refer to domain design section for details.
- An RD Gateway is installed in the OT-Domain-Zone to manage remote desktop access within the OT environment (from o
- ne OT computer to another). Note that this gateway does not provide remote access from IT. Refer to Remote Access design section for details.
- An GPS Clock Master is installed in the OT-Domain-Zone to provide accurate time source for the OT assets. Refer to relevant design section for details.
- The OT-Management-Zone contains the Firewall management software (Panorama), Nozomi Central Management Console, and Log collection server. Refer to relevant design sections for details.
- An OT cloud circuit provides connectivity from the HQ SCADA assets to the BUs.
- The NextGen OT firewall installed in the HQ is used to segment the HQ networks into zones as described above, and to interface with IT.

3.2 HARDWARE/SOFTWARE COMPONENTS

3.2.1 SERVERS IN OT DOMAIN ZONE

3.2.1.1 PHYSICAL SERVER SPECIFICATION

Component	Configurations
Model	HPE ProLiant DL380 Gen10
Processor	Intel® Xeon® Gold 5218 22M Cache, 2.30 GHz
Memory	32 GB
HDD-1 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-2 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-3 (Raid1-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-4 (Raid1-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
Power Supply	HPE 800W FS Plat Ht Plg LH Pwr Sply Kit x 2

3.2.1.2 HOST CONFIGURATION

Component	Configurations
Host name	HQOTDOMPHY01
O/S	Microsoft Windows Server 2016 DC
C Drive (For Host O/S)	300 GB
D Drive (For VMs)	1.2 TB
Memory available for Host O/S	12 GB

3.2.1.3 VM1 CONFIGURATION

Component	Configurations
VM Name	HQOTADM01
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	100 GB
Memory	12 GB
Software Installed	Active Directory Services

3.2.1.4 VM2 CONFIGURATION

Component	Configurations
VM Name	HQOTADM02
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	100 GB
Memory	12 GB
Software Installed	Remote Desktop Gateway Services

3.2.2 SERVERS IN OT DMZ

3.2.2.1 PHYSICAL SERVER SPECIFICATION

Component	Configurations
Model	HPE ProLiant DL380 Gen10
Processor	Intel® Xeon® Gold 5218 22M Cache, 2.30 GHz
Memory	32 GB
HDD-1 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-2 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-3 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-4 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-5 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-6 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-7 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
Power Supply	HPE 800W FS Plat Ht Plg LH Pwr Sply Kit x 2

3.2.2.2 HOST CONFIGURATION

Component	Configurations
Host name	HQOTDMZPHY01
O/S	Microsoft Windows Server 2016 DC
C Drive (For Host O/S)	300 GB
D Drive (For VMs)	4.8 TB
Memory available for Host O/S	12 GB

3.2.2.3 VM1 CONFIGURATION

Component	Configurations
VM Name	HQOTADM11
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	800 GB
Memory	12 GB
Software Installed	WSUS, ePO

3.2.2.4 VM2 CONFIGURATION

Component	Configurations
VM Name	HQOTADM12
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	3 TB
Memory	12 GB
Software Installed	BackupExec-CAS, SFTP, Qradar SF

3.2.3 SERVERS IN OT MGMT ZONE

3.2.3.1 PHYSICAL SERVER SPECIFICATION

Component	Configurations
Model	HPE ProLiant DL380 Gen10
Processor	Intel® Xeon® Gold 5218 22M Cache, 2.30 GHz
Memory	32 GB
HDD-1 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-2 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-3 (Raid1-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-4 (Raid1-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
Power Supply	HPE 800W FS Plat Ht Plg LH Pwr Sply Kit x 2

3.2.3.2 HOST CONFIGURATION

Component	Configurations
Host name	HQOTMGMPHY01
O/S	Microsoft Windows Server 2016 DC
C Drive (For Host O/S)	300 GB
D Drive (For VMs)	1.2 TB
Memory available for Host O/S	12 GB

3.2.3.3 VM1 CONFIGURATION

Component	Configurations
VM Name	Panorama
CPU Cores	6
O/S	PAN OS
Disk	500 GB
Memory	12 GB

3.2.3.4 VM2 CONFIGURATION

Component	Configurations
VM Name	Nozomi-CMC
CPU Cores	6
O/S	N2OS
Disk	500 GB
Memory	12 GB

3.2.4 FIREWALLS

Following is the Firewall for HQ:

Component	Configurations
Model	Palo Alto Networks PA-3220 (High Availability)

Component	Configurations
Interfaces	12 x Ethernet 1000 - RJ-45 ¦ 4 x Ethernet 1000 - SFP (mini-GBIC) ¦ 3 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 4 x 10Gb Ethernet - SFP+ ¦ 1 x 10GBase-T (management) - SFP+ ¦ 1 x management (USB)
Subscriptions	Threat prevention subscription 2 year prepaid for device in an HA pair, PA-3220 WildFire subscription 2 year prepaid for device in an HA pair, PA-3220

3.2.5 NETWORK SWITCH

Following is the switch to be installed between OT Cloud MODEM and the Firewall in HQ.

Component	Configurations
Model	Cisco Catalyst 1000-8T-2G-L Switch
Interface	8x 10/100/1000 Ethernet ports, 2x 1G SFP

Following is the switch to be installed for OT zones in HQ.

Component	Configurations
Model	Cisco Catalyst 1000-24T-4G-L Switch
Interface	24x 10/100/1000 Ethernet ports, 4x 1G SFP

3.3 IT/OT SEGREGATION

As required by the relevant standards, the OT environment is segregated from IT and only controlled interface/communication is allowed. The segregation includes physical, logical, management, and roles & responsibilities. Here are the key features of this segregation:

- Complete segregation of physical network interface between IT and OT, except for the OT interface firewall in HQ. This means no shared network devices, servers (including hosts for VMs), WAN/Cloud connections, SIMs, etc.
- No physical or logical connectivity is allowed between OT and IT at BU level.
- Logical segregation of IT and OT networks including separation of IP subnets, VLANs, etc.
- Separate Active Directory domain for OT environment; no connection with IT domain.
- Separate network & systems management tools, support functions & services (Antivirus, Patch Management, Backup Management, Clock Master, Vulnerability Management System). Controlled interface of these tool and services with IT where needed.
- Segregation of duties. OT environment to be managed by OT Domain Admin, OT Network Admin, OT System Admin etc. (Roles may be assigned to shared IT resources who log-in directly to OT network from OT devices using OT credentials to perform the required functions).

- All communication between IT & OT passes through the DMZ. No direct communication between IT and any other OT zone.

3.4 OT CLOUD

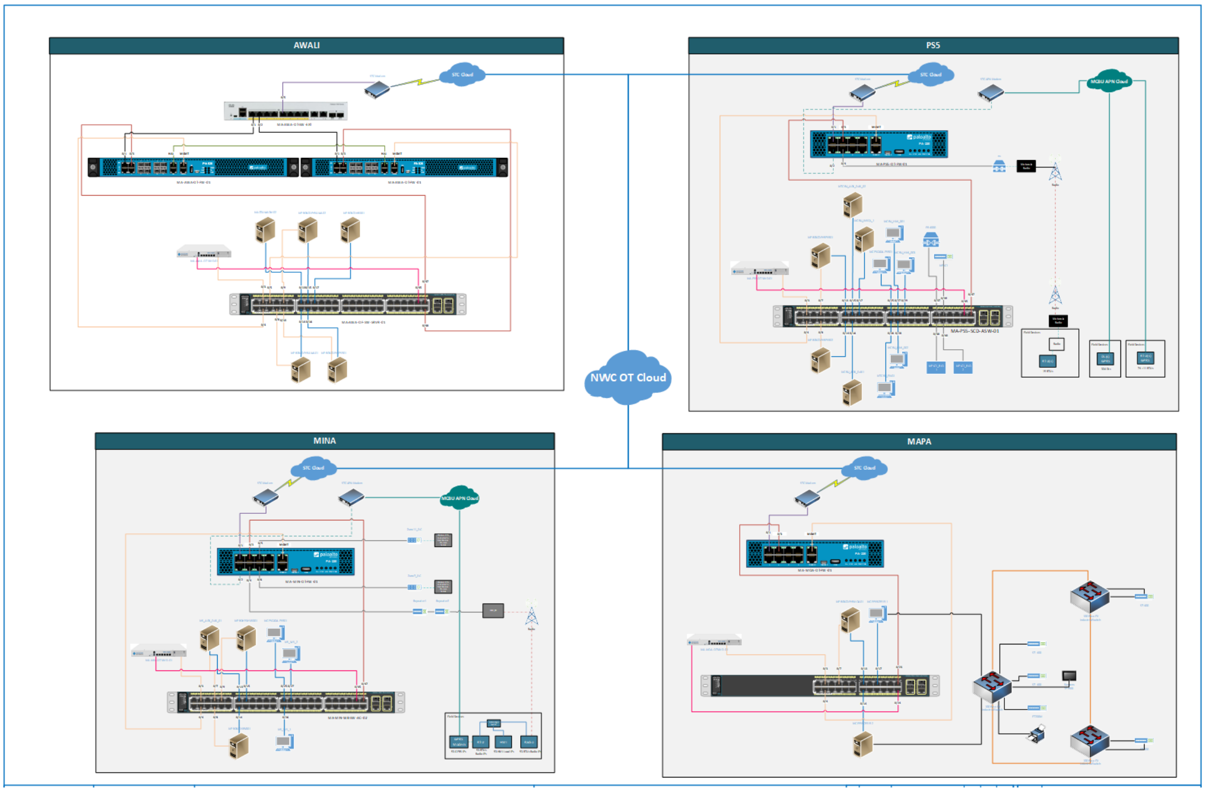
A dedicated, secure, private OT cloud provided and managed by the telecom company provides connectivity between HQ and BU offices. Each office location has one circuit that connects to the OT cloud. An OT firewall installed at each location provides the security barrier between the OT cloud and the assets at the location.

Appropriate bandwidth is to be provided at each location to prevent any communication delays or interruption, as per detailed design.

4. MCBU DESIGN

4.1 MCBU ARCHITECTURE

Following is the detailed architecture of NWC SCADA/OT environment at the MCBU.



A high-resolution version of the architecture is provided as an attachment (A01001045-MCBU-DLD-NA).

Following is a description of the network setup for OT Cybersecurity in MCBU:

- Awali is the BU Main-office. It has the following zones:
  - SCADA-Zone contains Domain Controller, Historian, Management Server as well as additional SCADA servers as needed.
  - MGMT-Zone contains the vulnerability management device (Nozomi Guardian). This zone also provides connectivity to the management port for all network devices.
- PS5, MINA, and MAPA are the branch offices. These have the following zones:
  - SCADA-Zone contains all required servers and workstations for the SCADA system. This includes AOS, DAS, Historian, OWS, EWS.
  - Level-1 Zone contains any Level-1 devices installed in the office (e.g., MTU, Data Concentrators, etc.)
  - MGMT-Zone contains the vulnerability management device (Nozomi Guardian). This zone also provides connectivity to the management port for all network devices.

- The Management server installed in the BU Main-Office contains the required management software including Antivirus, Patch Management, Backup Management.
- Each BU Main-Office and Branch-Office has an OT cloud circuit to provide connectivity to the OT cloud.
- PS5 and Mina offices have an APN cloud circuit to provide connectivity to the GSM/GPRS devices.
- A NextGen OT firewall installed at each BU office provides security barrier for all external interfaces to that office. Following external interfaces connect to the BU office through this firewall:
    - OT cloud
    - APN cloud
    - Radio (TCP/IP only)

4.2 HARDWARE/SOFTWARE COMPONENTS

4.2.1 AWALI OFFICE

4.2.1.1 PHYSICAL SERVER SPECIFICATION

Component	Configurations
Model	HPE ProLiant DL380 Gen10
Processor	Intel® Xeon® Gold 5218 22M Cache, 2.30 GHz
Memory	32 GB
HDD-1 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-2 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-3 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-4 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-5 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
Power Supply	HPE 800W FS Plat Ht Plg LH Pwr Sply Kit x 2

4.2.1.2 HOST CONFIGURATION

Component	Configurations
Host name	MAOTAWAPHY01
O/S	Microsoft Windows Server 2016 DC
C Drive (For Host O/S)	300 GB
D Drive (For VMs)	2.18 TB
Memory available for Host O/S	12 GB

4.2.1.3 VM1 CONFIGURATION

Component	Configurations
VM Name	MAOTAWADM01

Component	Configurations
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	100 GB
Memory	12 GB
Software Installed	Additional Domain Controller

4.2.1.4 VM2 CONFIGURATION

Component	Configurations
VM Name	MAOTAWADM02
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	1.9 TB
Memory	12 GB
Software Installed	WSUS, BackupExec-MG, Super-Agent (McAfee)

4.2.1.5 FIREWALL

Following is the specification for Firewall for Awali.

Component	Configurations
Model	Palo Alto Networks PA-820 (High Availability)
Interfaces	4 x 1000Base-T - RJ-45 ¦ 8 x - SFP (mini-GBIC) ¦ 1 x micro-USB ¦ 3 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB
Subscriptions	Threat prevention subscription 2 year prepaid for devices in HA pair, PA-820

4.2.1.6 NETWORK SWITCH

Following is the switch to be installed between OT Cloud MODEM and the Firewall in Awali.

Component	Configurations
Model	Cisco Catalyst 1000-8T-2G-L Switch
Interface	8x 10/100/1000 Ethernet ports, 2x 1G SFP and RJ-45 combo uplinks

4.2.1.7 VULNERABILITY MONITORING SYSTEM

Following is the specification for VMS for Awali.

Component	Configurations
Model	Nozomi Networks Guardian Appliance - NSG-L-100
Interfaces	4 x 1000Base-T - RJ-45 ¦ 8 x - SFP (mini-GBIC) ¦ 1 x micro-USB ¦ 3 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB

Component	Configurations
Subscriptions	Threat Intelligence - Guardian Appliance - NSG-L-100 (1 year)

4.2.2 PS5 BRANCH OFFICE

Following is the specification for Firewall for PS5 branch office.

Component	Configurations
Model	Palo Alto Networks PA-220
Interfaces	8 x 1000Base-T - RJ-45 ¦ 1 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB ¦ 1 x console
Subscriptions	Threat prevention subscription 2 year prepaid for device in an HA pair, PA-220

4.2.3 MINA BRANCH OFFICE

Following is the specification for Firewall for Mina branch office.

Component	Configurations
Model	Palo Alto Networks PA-220
Interfaces	8 x 1000Base-T - RJ-45 ¦ 1 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB ¦ 1 x console
Subscriptions	Threat prevention subscription 2 year prepaid for device in an HA pair, PA-220

4.2.4 MAPA BRANCH OFFICE

Following is the specification for Firewall for MAPA branch office.

Component	Configurations
Model	Palo Alto Networks PA-220
Interfaces	8 x 1000Base-T - RJ-45 ¦ 1 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB ¦ 1 x console
Subscriptions	Threat prevention subscription 2 year prepaid for device in an HA pair, PA-220

4.3 APN CLOUD

A dedicated, secure, private OT APN cloud provided and managed by the telecom company provides GSM/GPRS connectivity from BU offices to field sites/equipment.

In MCBU, PS5 and Mina branch offices each has one circuit that connects to the OT APN cloud. The OT firewall installed at these location provides the security barrier between the OT APN cloud and the assets at the location.

The APN cloud for MCBU is dedicated to provide connectivity to all SIM-based devices in MCBU with a separate APN profile for all SIMs in the BU.

The APN profile for MCBU APN Cloud is “MakkahOT.M2M”

4.4 LEVEL-1 DEVICES HARDENING AND CHANGES

Refer to the document “A01001045-MCBU-HDN-L1” for details of changes to be made on Level-1 devices in MCBU.

5. RCBU DESIGN

5.1 RCBU ARCHITECTURE

Following is the detailed architecture of NWC SCADA/OT environment at the RCBU.

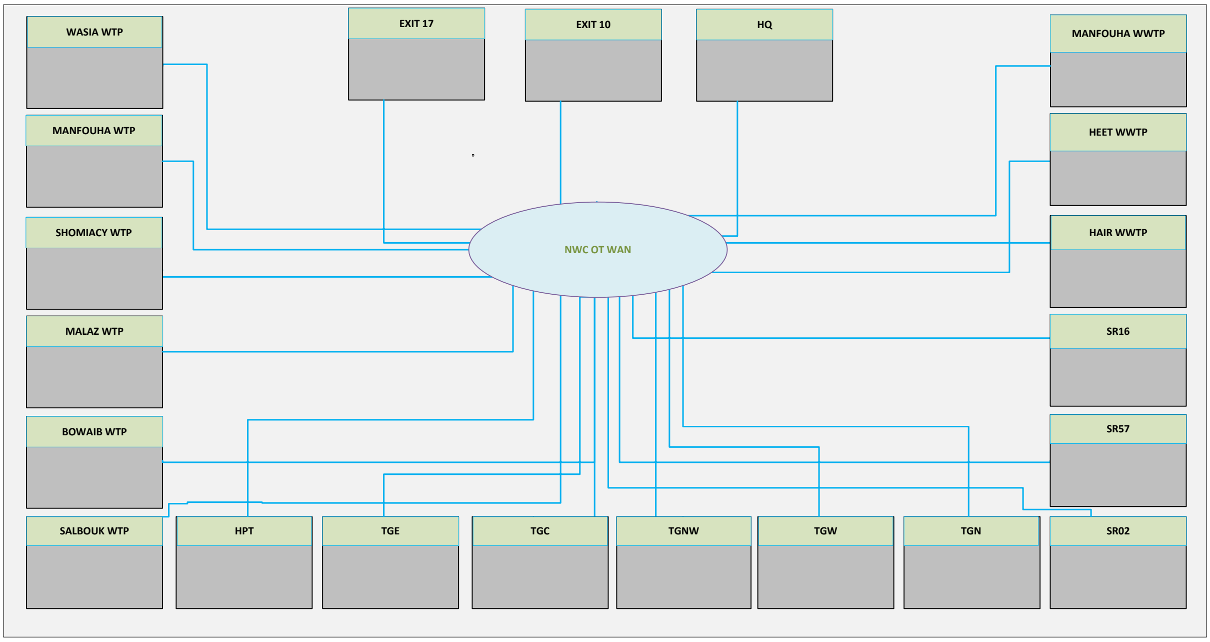


Figure 2 : RCBU Architecture

A high-resolution version of the architecture is provided as an attachment (A01001045-RCBU-DLD-NA).

Following is a description of the network setup for OT Cybersecurity in RCBU:

- Exit-10 is the BU Main-office. It has the following zones:
  - SCADA-Zone contains Domain Controller, Historian, Management Server as well as additional SCADA servers as needed.
  - Level-1 Zone contains any Level-1 devices installed in the office (e.g. Data Concentrators, etc.)
  - MGMT-Zone contains the vulnerability management device (Nozomi Guardian). This zone also provides connectivity to the management port for all network devices.

- Exit-17, Bowaib WTP, Manfouha WTP, Malaz WTP, Hayer WTP, Shomaisy WTP, Salbukh WTP, Wasi WTP, Manfouha WWTP, Heet WWTP, Hayer WWTP, TGW, TGC, TGNW, HPT, TGN and SR02 are the branch offices. These have the following zones:
  - SCADA-Zone contains all required servers and workstations for the SCADA system. This includes AOS, DAS, Historian, OWS and EWS.
  - Level-1 Zone contains any Level-1 devices installed (e.g., MTU, Data Concentrators, etc.)
  - MGMT-Zone contains the vulnerability management device (Nozomi Guardian). This zone also provides connectivity to the management port for all network devices.
- The Management server installed in the Exit-10 (BU Main-Office) contains the required management software including Antivirus, Patch Management, Backup Management.
- BU Main-Office and each Branch-Office has an OT WAN circuit to provide connectivity to the OT WAN.
- BU Main office (Exit-10) has an OT APN circuit to provide connectivity to the GSM/GPRS devices.
- A NextGen OT firewall installed at each BU office provides security barrier for all external interfaces to that office. Following external interfaces connect to the BU office through this firewall:
  - OT WAN
  - OT APN
  - Radio (TCP/IP only)

5.2 RCBU INTER SITE COMMUNICATION

VPN Tunnelling

- All RCBU sites will be connected via VPN Tunnel to Exit-10 (RCBU Main office) and HQ.
- Sites which are interconnected are following
  - There is a VPN Tunnel to communicate DAS in Manfouha WWTP to some of the PLCs in Hayer WWTP.
  - There is a VPN Tunnel to communicate DAS in Manfouha WWTP to some of the PLCs in Heet WWTP.
  - There is a VPN Tunnel to communicate DAS in Heet WWTP to Lifting station PLCs in Hayer WWTP.

5.3 BILL OF MATERIALS

Below Table shows the quantities of OT equipment which is installed in each RCBU site.

Sr. no.	RCBU Site Name	MGMT Server	OT Ethernet Switch	Firewall	Nozomi
1	Exit-10	1	1	2	1
2	Malaz WTP	-	2	1	1
3	Shomacy	-	2	1	1
4	Manfouha WTP	-	3	1	1
5	Exit-17	-	1	1	1
6	Hayer WTP	-	1	1	1
7	Wasi WTP	-	2	1	1
8	Salbukh WTP	-	2	1	1
9	Bowaib WTP	-	2	1	1
10	Manfouha WWTP	-	1	1	1
11	HEET WWTP	-	1	1	1
12	HAYER WWTP	-	1	1	1
13	TGW	-	1	1	1
14	TGNW	-	1	1	1
15	TGC	-	1	1	1
16	HPT	-	-	1	-
17	SR02	-	-	1	-

5.3.1 MANAGEMENT SERVER SPECIFICATION

Management server is installed in Exit-10 BU main office, and it has following specification.

Component	Configurations
Model	HPE ProLiant DL380 Gen10
Processor	Intel® Xeon® Gold 5218 22M Cache, 2.30 GHz
Memory	32 GB
HDD-1 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-2 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-3 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-4 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-5 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
Power Supply	HPE 800W FS Plat Ht Plg LH Pwr Sply Kit x 2

5.3.1.1 HOST CONFIGURATION

Component	Configurations
Host name	RDOTE10PHY01
O/S	Microsoft Windows Server 2016 DC
C Drive (For Host O/S)	300 GB
D Drive (For VMs)	2.18 TB
Memory available for Host O/S	12 GB

5.3.1.2 VM 1 CONFIGURATION

Component	Configurations
VM Name	RDOTE10ADM01
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	100 GB
Memory	12 GB
Software Installed	Additional Domain Controller

5.3.1.3 VM 2 CONFIGURATION

Component	Configurations
VM Name	RDOTE10ADM02
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	1.9 TB
Memory	12 GB
Software Installed	WSUS, BackupExec-MG, Super-Agent (McAfee)

5.3.2 FIREWALL

Following is the specification for Firewall installed in Exit-10 BU main office.

Component	Configuration
Model	Palo Alto Networks PA-820 (High Availability)
Interfaces	4 x 1000Base-T - RJ-45 ¦ 8 x - SFP (mini-GBIC) ¦ 1 x micro-USB ¦ 3 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB
Subscriptions	Threat prevention subscription 2 year prepaid for devices in HA pair, PA-820

Following is the specification for Firewall for each RCBU branch office.

Component	Configurations
Model	Palo Alto Networks PA-220
Interfaces	8 x 1000Base-T - RJ-45 ¦ 1 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB ¦ 1 x console
Subscriptions	Threat prevention subscription 2 year prepaid for device in an HA pair, PA-220

5.3.3 OT ETHERNET SWITCH

Following is the specification for OT Switch for RCBU.

Component	Configurations
Model	Cisco Catalyst 1000-24T-4G-L - Switch
Interfaces	24 X 10/100/1000 + 4 x Gigabit SFP Uplinks

5.3.4 VULNERABILITY MONITORING SYSTEM

Following is the specification for VMS (NOZOMI) for RCBU.

Component	Configurations
Model	Nozomi Networks Guardian Appliance - NSG-L-100
Interfaces	4 x 1000Base-T - RJ-45 ¦ 8 x - SFP (mini-GBIC) ¦ 1 x micro-USB ¦ 3 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB
Subscriptions	Threat Intelligence - Guardian Appliance - NSG-L-100 (1 year)

5.3.5 EXIT-10 DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at Exit-10.

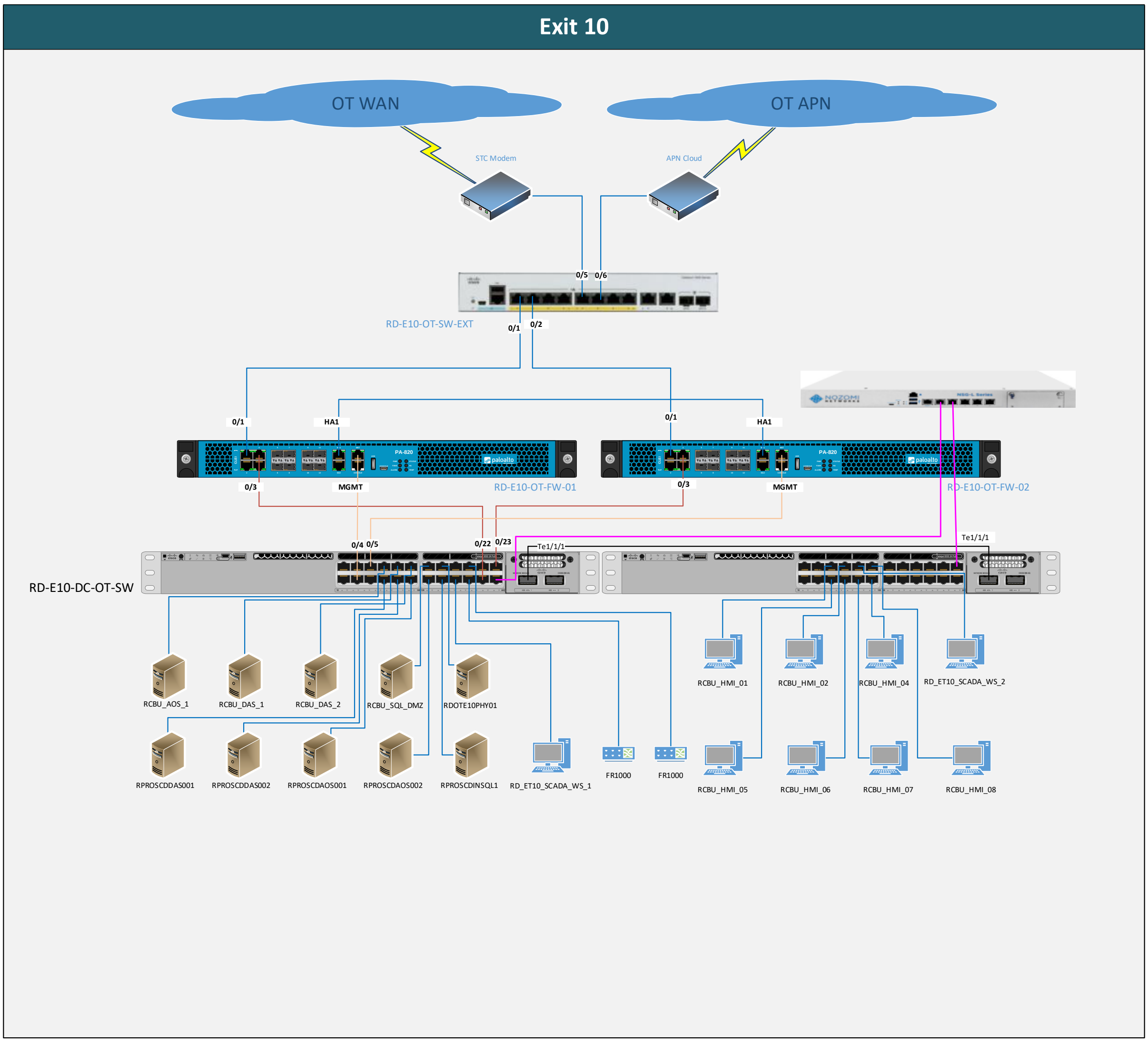


Figure 3 : Exit-10 Architecture

5.3.5.1 DESIGN DESCRIPTION

- Exit-10 Main building Ground Floor Datacenter Room OT cabinet has OT Ethernet switch, Nozomi and Firewall.

  - All the network cables from OT devices in control room is connected to OT Ethernet switch.

- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.6 EXIT-17 DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at Exit-17.

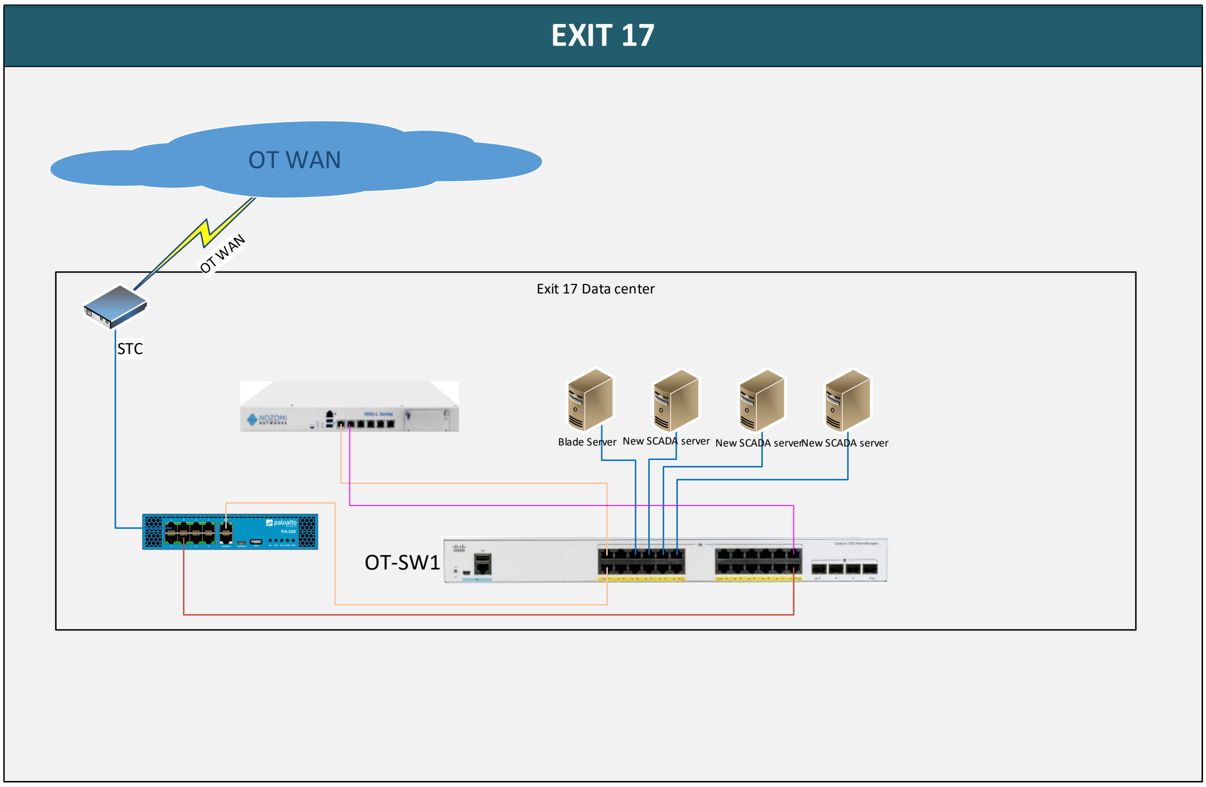


Figure 4 : Exit-17 Architecture

5.3.6.1 DESIGN DESCRIPTION

- Exit-17 Main building Datacenter Room Network cabinet has OT Ethernet switch, Nozomi and Firewall.
  - All the network cables from OT devices in Datacenter is connected to OT Ethernet switch.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.7 TGC DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at TGC.

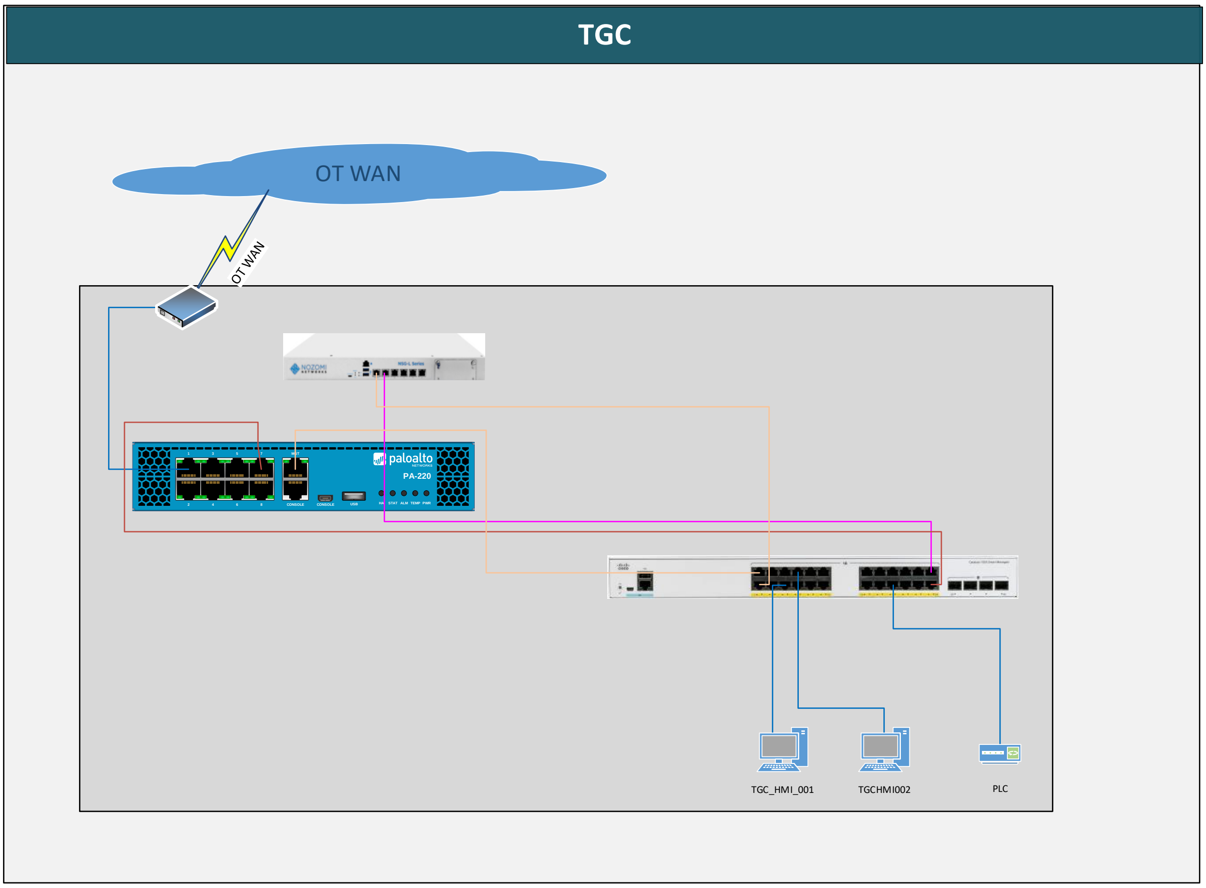


Figure: TGC Architecture

5.3.7.1 DESIGN DESCRIPTION

- Workshop building supervisor room network cabinet has OT Ethernet switch, Firewall, Nozomi.
  - All the network cables from OT devices in control room and supervisor room is connected to OT Ethernet switch.
- Operator Stations communicate to DAS/AOS in Exit-10 on OT WAN.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.8 TGN DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at TGN.

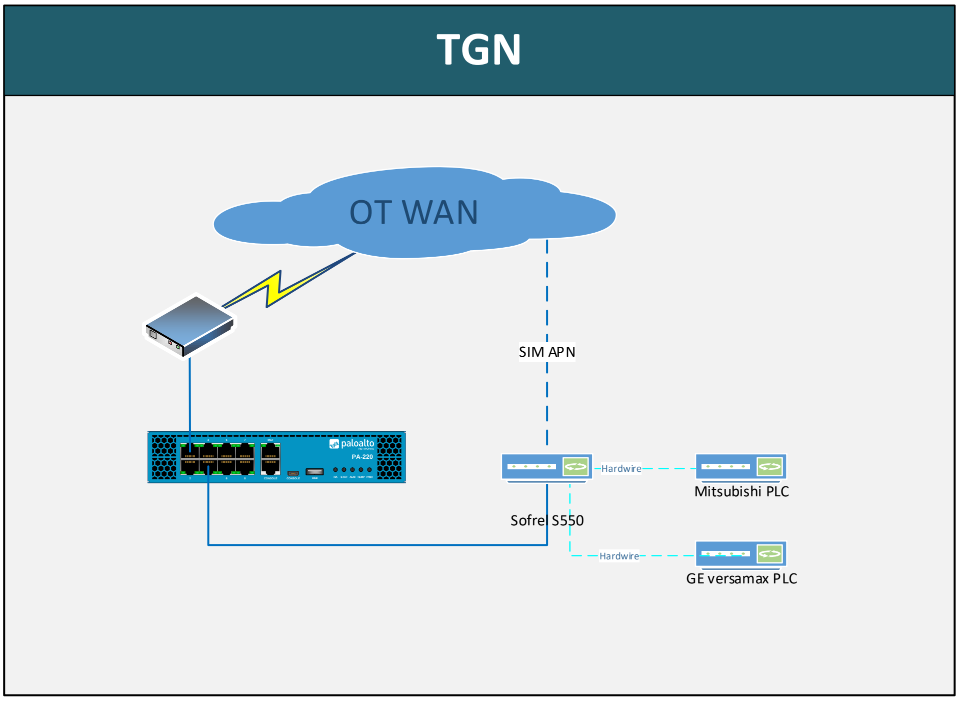


Figure 5 : TGN Architecture

5.3.8.1 DESIGN DESCRIPTION

- Pump building 1st floor control room network cabinet has Firewall.
  - All the network cables from OT devices in control room is connected to OT Ethernet switch.
- Due to weak GSM signal strength this site communicates over OT WAN to Exit-10.
- All OT assets are reconfigured with new IP addresses as per IP schema

5.3.9 HPT DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at HPT.

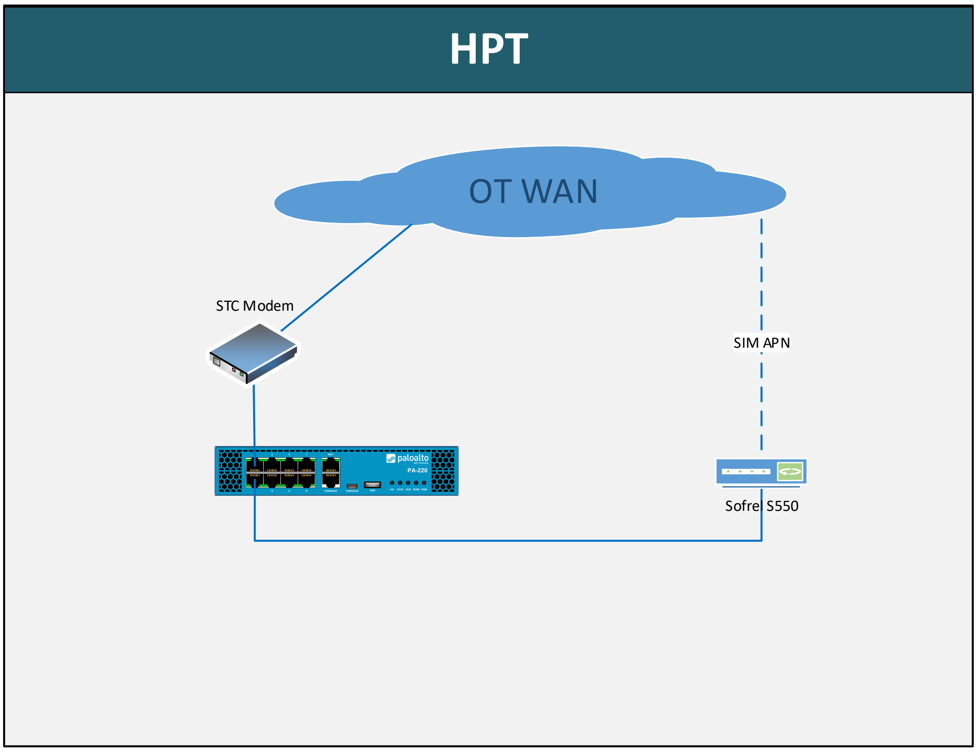


Figure 6 : HPT Architecture

5.3.9.1 DESIGN DESCRIPTION

- SWCC Main building control room RTU Panel has Firewall.
  - All the network cables from OT devices in control room and supervisor room is connected to Firewall.
- Due to weak GSM signal strength this site communicates over OT WAN to Exit-10.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.10 TGW DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at TGW.

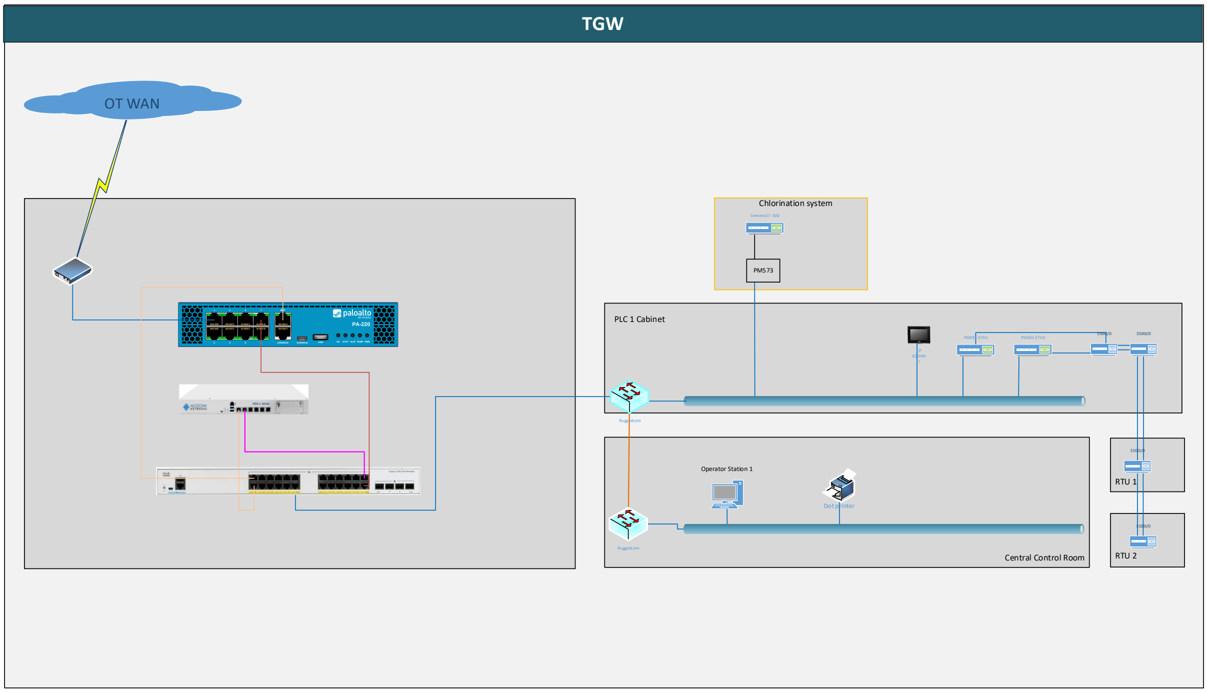


Figure 7 : TGW Architecture

5.3.10.1 DESIGN DESCRIPTION

- Pumping station building 1st floor control room network cabinet has OT Ethernet switch, Firewall and Nozomi.
  - All the network cables from OT devices in the control room are connected to OT Ethernet switch.
- This site has standalone ABB SCADA System and independent of Exit-10.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.11 TGNW DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at TGNW.

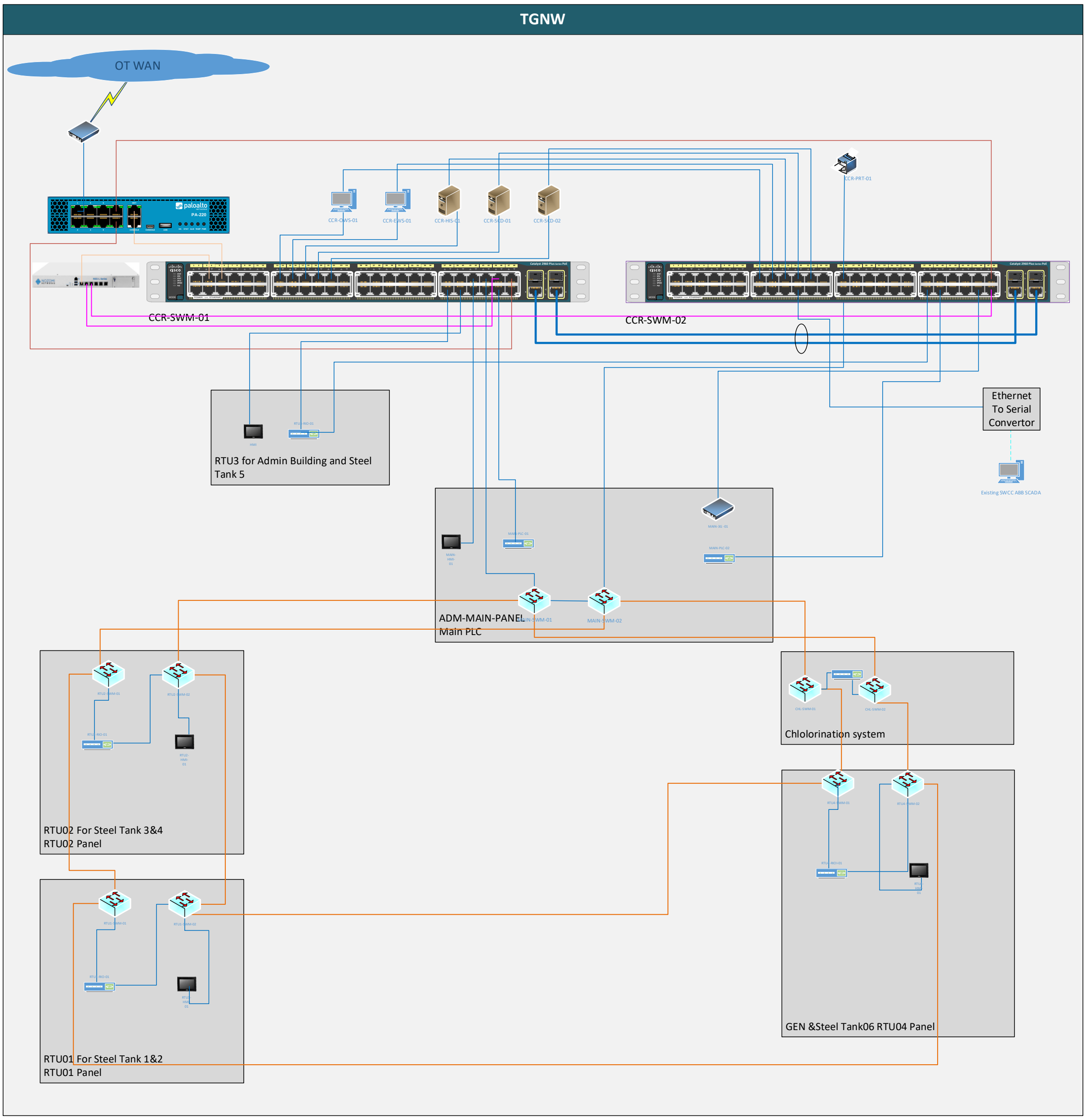


Figure : TGNW Architecture

5.3.11.1 DESIGN DESCRIPTION

- Admin building control room network cabinet has OT Ethernet switch, Firewall and Nozomi.
    - All the network cables from OT devices in control room and main PLC room are connected to OT Ethernet switch.
- This site has on premises DAS, AOS, Historian and OWS.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.12 MANFOUHA WTP DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at Manfouha WTP.

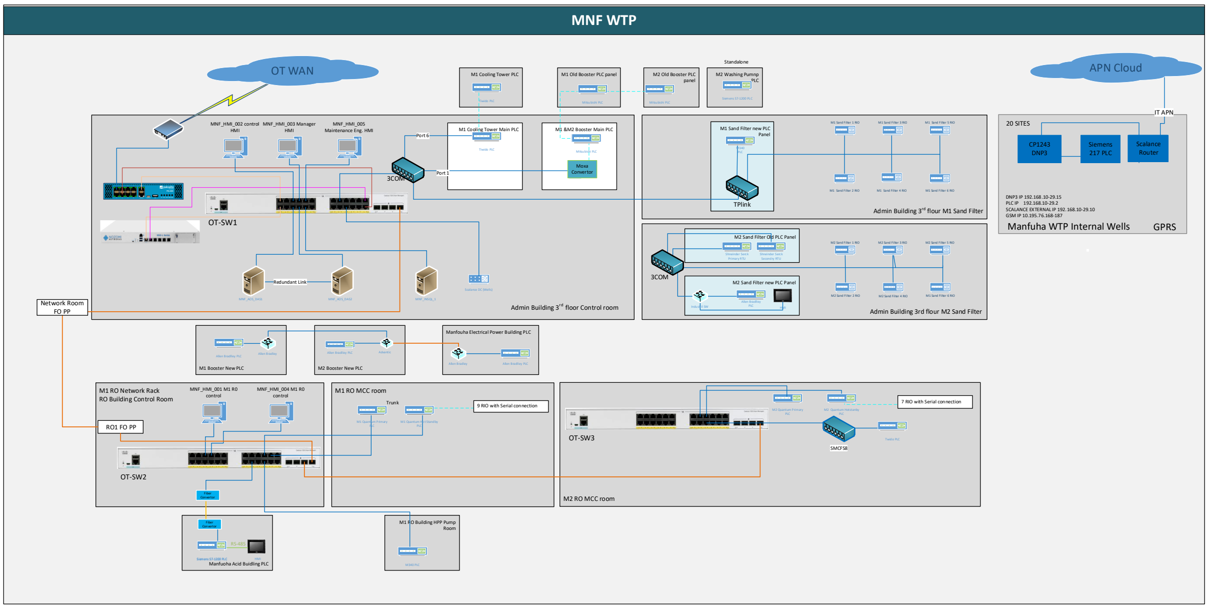


Figure 8 : Manfouha WTP Architecture

5.3.12.1 DESIGN DESCRIPTION

- Admin Building 3rd floor Control Room Server Cabinet has OT Ethernet switch, Firewall, Nozomi, SCADA Servers and Scalance.
    - All the network cables from OT devices in control room, manager, maintenance engineer room and Sand Filter area is connected to OT Ethernet switch.
    - FO cable from RO1 building is also connected to OT ethernet switch via FO patch panel in network room.
- RO-1 Building-Control Room-Network Cabinet has OT Ethernet switch
    - FO cable from Admin building, RO2 and acid building is also connected to OT ethernet switch via FO patch panel in network cabinet.
- This site has on premises DAS, AOS, GR, Historian and OWS. Data from wells is being acquired via GSM/GPRS and Radio.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.13 MALAZ WTP DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at Malaz WTP.

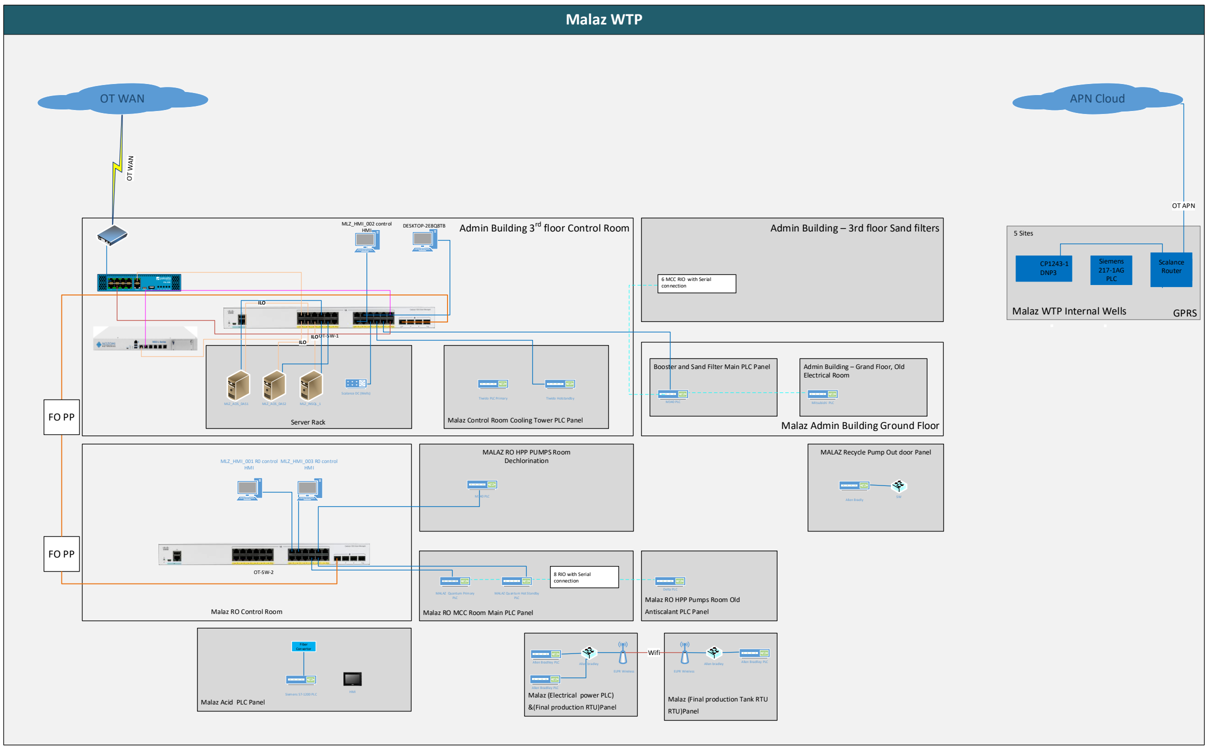

Malaz WTP
OT WAN
OT WAN
APN Cloud
OT APN
Admin Building 3rd floor Control Room
MLZ_HMI_002 control HMI
DESKTOP-2E8Q8TB
ILO
ILO
ILO
OT-SW-1
MLZ_AOS_DAS1
MLZ_AOS_DAS2
MLZ_INSQL_1
Scalance DC (Wells)
Server Rack
Tiwido PLC Primary
Tiwido Hotstandby
Malaz Control Room Cooling Tower PLC Panel
Admin Building – 3rd floor Sand filters
6 MCC RIO with Serial connection
Booster and Sand Filter Main PLC Panel
M340 PLC
Admin Building – Grand Floor, Old Electrical Room
Mitsubishi PLC
Malaz Admin Building Ground Floor
5 Sites
CP1243-1 DNP3
Siemens 217-1AG PLC
Scalance Router
Malaz WTP Internal Wells
GPRS
FO PP
FO PP
MLZ_HMI_001 R0 control HMI
MLZ_HMI_003 R0 control HMI
OT-SW-2
Malaz RO Control Room
MALAZ RO HPP PUMPS Room Dechlorination
M340 PLC
MALAZ Recycle Pump Out door Panel
Allen Bradly
SW
MALAZ Quantum Primary PLC
MALAZ Quantum Hot Standby PLC
8 RIO with Serial connection
Malaz RO MCC Room Main PLC Panel
Delta PLC
Malaz RO HPP Pumps Room Old Antiscalant PLC Panel
Fiber Convertor
Siemens S7-1200 PLC
HMI
Malaz Acid PLC Panel
Allen Bradley PLC
Allen bradley
ELPR Wireless
Allen Bradley PLC
Malaz (Electrical power PLC) &(Final production RTU)Panel
Wifi
ELPR Wireless
Allen bradley
Allen Bradley PLC
Malaz (Final production Tank RTU RTU)Panel

Figure 9 : Malaz Architecture

5.3.13.1 DESIGN DESCRIPTION

- Admin Building 3rd floor Control Room Server Cabinet has OT Ethernet switch, Firewall, Nozomi, SCADA Servers and Scalance.
    - All the network cables from OT devices in control room, maintenance engineer room and Sand Filter area is connected to OT Ethernet switch.
    - FO cable from RO building is also connected to OT ethernet switch via FO patch panel in network room.
- RO Building-Control Room-Network Cabinet has OT Ethernet switch
    - FO cable from Admin building and acid building is also connected to OT ethernet switch via FO patch panel in network cabinet.
- This site has on premises DAS, AOS, Historian and OWS. Data from wells is being acquired via GSM/GPRS.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.14 SHOMACY WTP DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at Shomacy WTP.

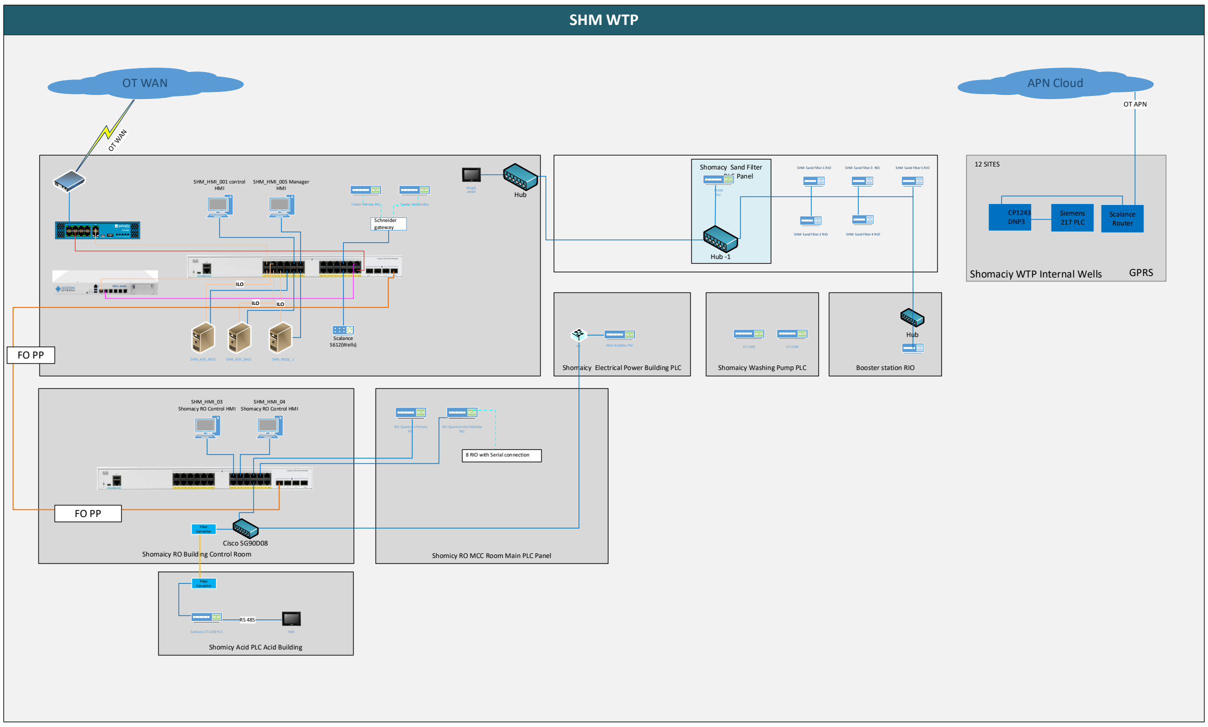


Figure 10 : Shomacy Architecture

5.3.14.1 DESIGN DESCRIPTION

- Admin Building 3rd floor Control Room Server Cabinet has OT Ethernet switch, Firewall, Nozomi, SCADA Servers and Scalance.
  - All the network cables from OT devices in control room, manager room and Sand Filter area is connected to OT Ethernet switch.
  - FO cable from RO building is also connected to OT ethernet switch via FO patch panel in network room.
- RO Building-Control Room-Network Cabinet has OT Ethernet switch
  - FO cable from Admin building and acid building is also connected to OT ethernet switch via FO patch panel in network cabinet.
- This site has on premises DAS, AOS, Historian and OWS. Data from wells is being acquired via GSM/GPRS and Radio.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.15 HAYER WTP DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at Hayer WTP.

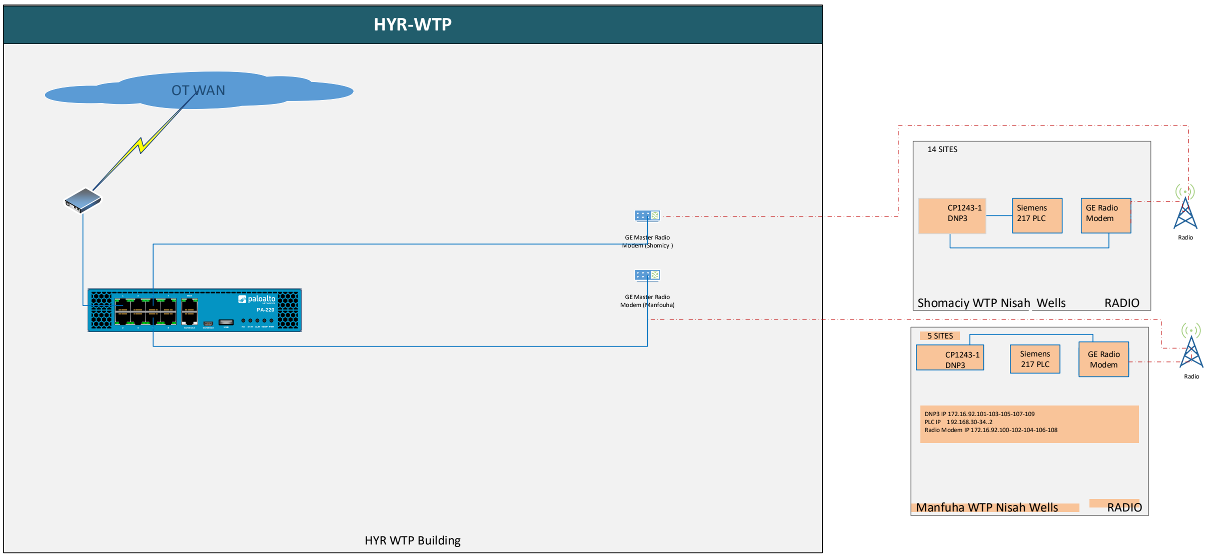


Figure 11: HAYER WTP Architecture

5.3.15.1 DESIGN DESCRIPTION

- Network room network cabinet has Firewall.
    - Network cables from both Master radios in are connected to OT Ethernet switch.
- This site hosts Master Radios for wells of Manfouha and Shomacy.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.16 BOWAIB WTP DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at Bowaib WTP.

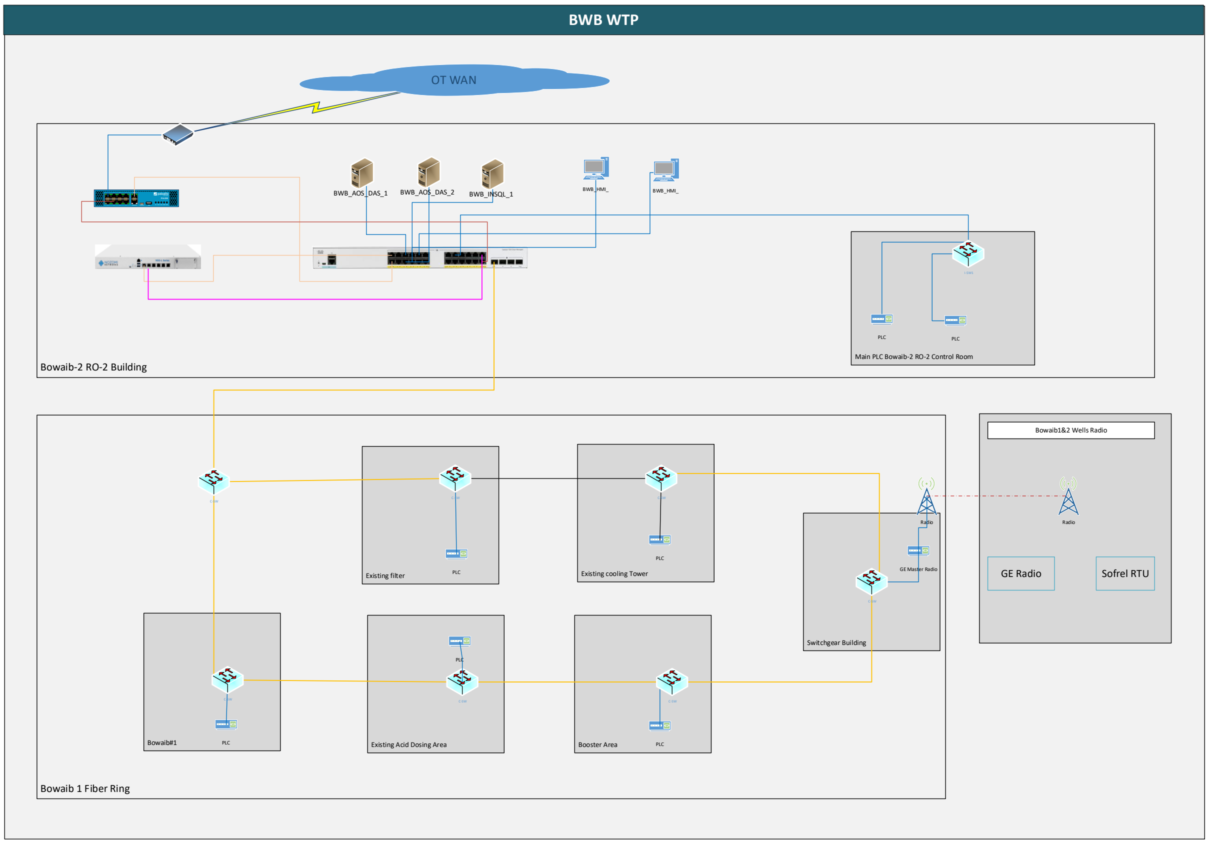


Figure 12 : Bowaib Architecture

5.3.16.1 DESIGN DESCRIPTION

- Bowaib 2 RO Building MCC Room Server cabinet has OT Ethernet switch, Nozomi and Firewall.
  - Network cables from all OT assets in MCC Room are connected to OT Ethernet switch.
- This site has on premises DAS, AOS, Historian and OWS for Bowaib 1 and 2. Data from wells is being acquired via Radio.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.17 SALBUKH WTP DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at Salbukh WTP.

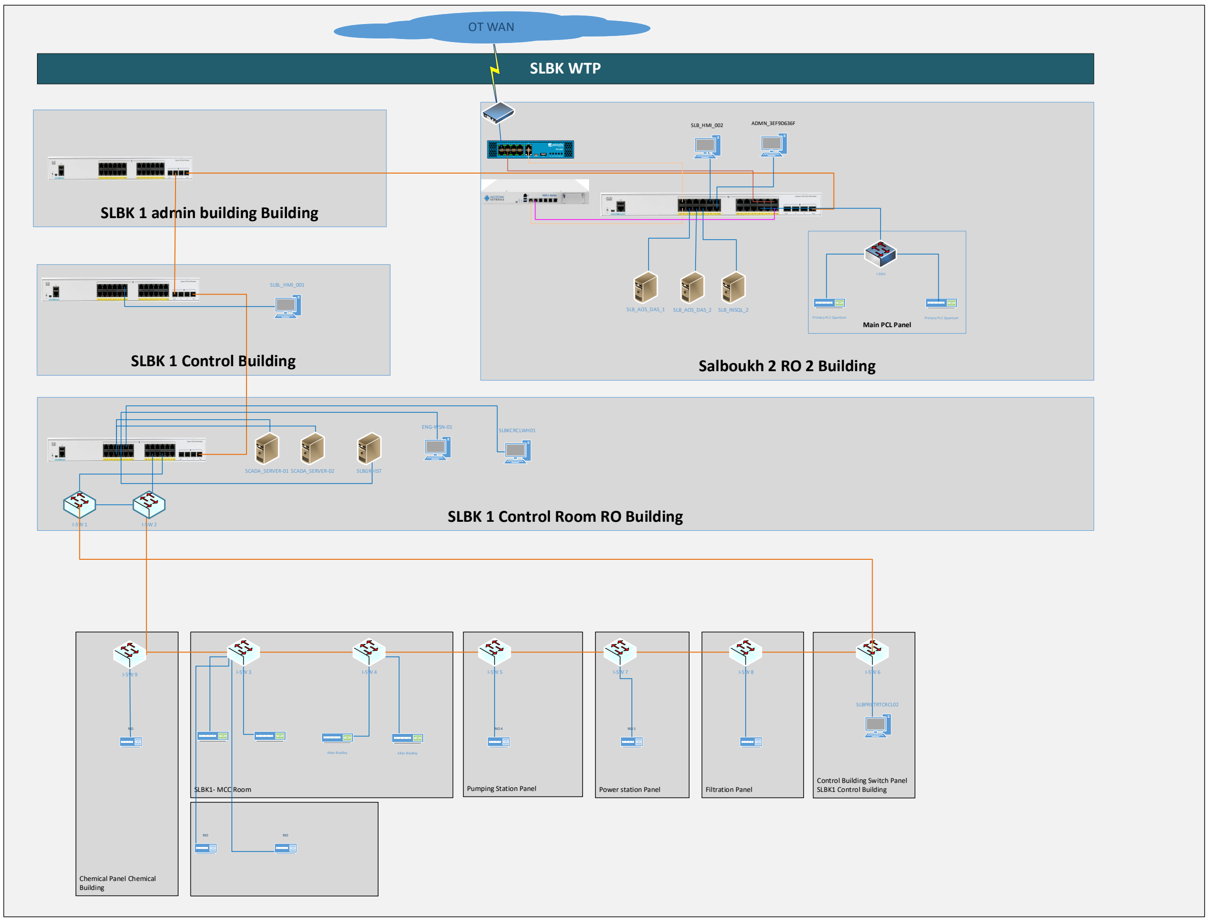


Figure: Salbukh WTP Architecture

5.3.17.1 DESIGN DESCRIPTION

- Salbukh 2 RO Building MCC Room Server cabinet has OT Ethernet switch, Nozomi and Firewall.
  - Network cables from all OT assets in Salbukh 2 RO building MCC Room are connected to OT Ethernet switch.
- This site has on premises DAS, AOS, Historian and OWS for Salbukh 1 and 2.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.18 WASI WTP DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at Wasi WTP.

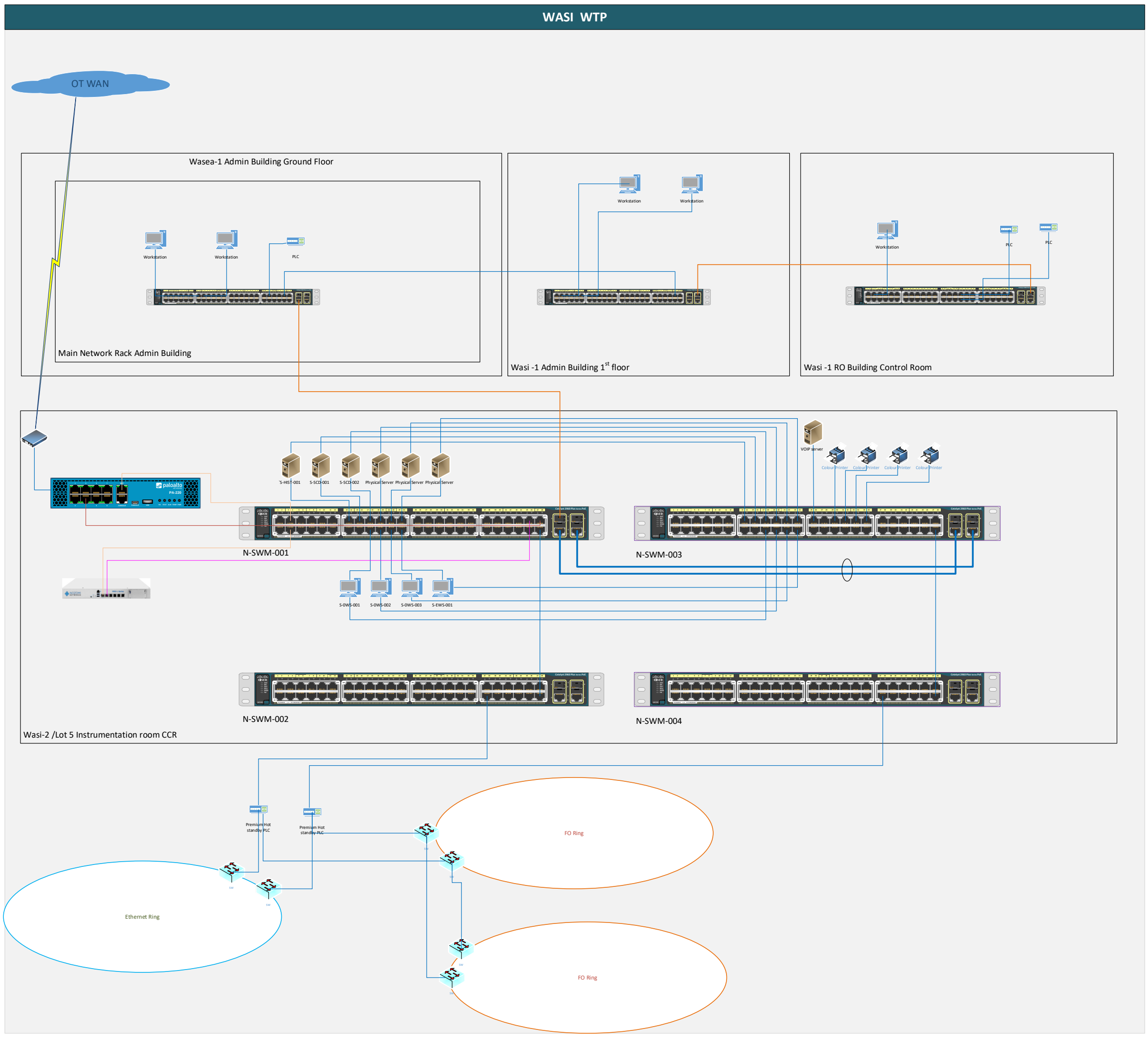


Figure 13 : Wasi WTP Architecture

5.3.18.1 DESIGN DESCRIPTION

- LOT-5 Admin Building 1st floor Instrumentation Room Network cabinet has OT Ethernet switch, Nozomi and Firewall.
    - Network cables from all OT assets in Instrumentation Room are connected to OT Ethernet switch.
- This site has on premises DAS, AOS, Historian and OWS for Wasi 1 and LOT-5(Wasi 2).
- Data from Wasi 1 wells is being acquired via GSM/GPRS.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.19 MANFOUHA WWTP DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at Manfouha WWTP.

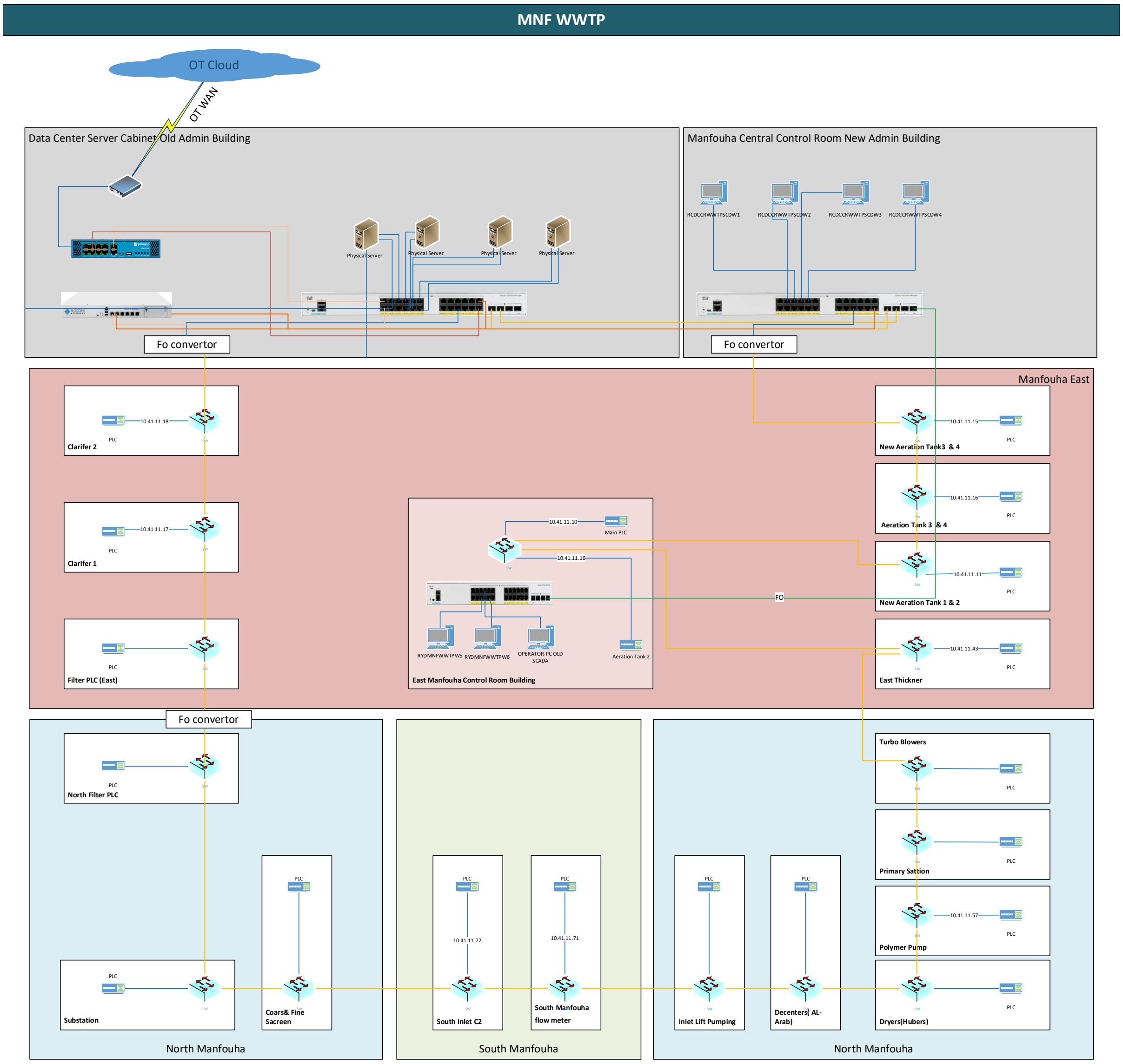


Figure 14 : Manfouha WWTP Architecture

5.3.19.1 DESIGN DESCRIPTION

- New Admin building ground floor Datacenter room Cab01 (OT Cabinet) has OT Ethernet switch, Firewall, Nozomi and SCADA Servers.
- DAS in Manfouha WWTP is reading data from some of PLCs in Hayer and Heet.
- Lifting station data is being monitored via APN.
- SCADA VLAN for Operator Workstations in Manfouha East is extended by using spare FO cores. A managed switch is installed in Manfouha East Control room which is part of SCADA VLAN.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.20 HEET WWTP DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at HEET WWTP.

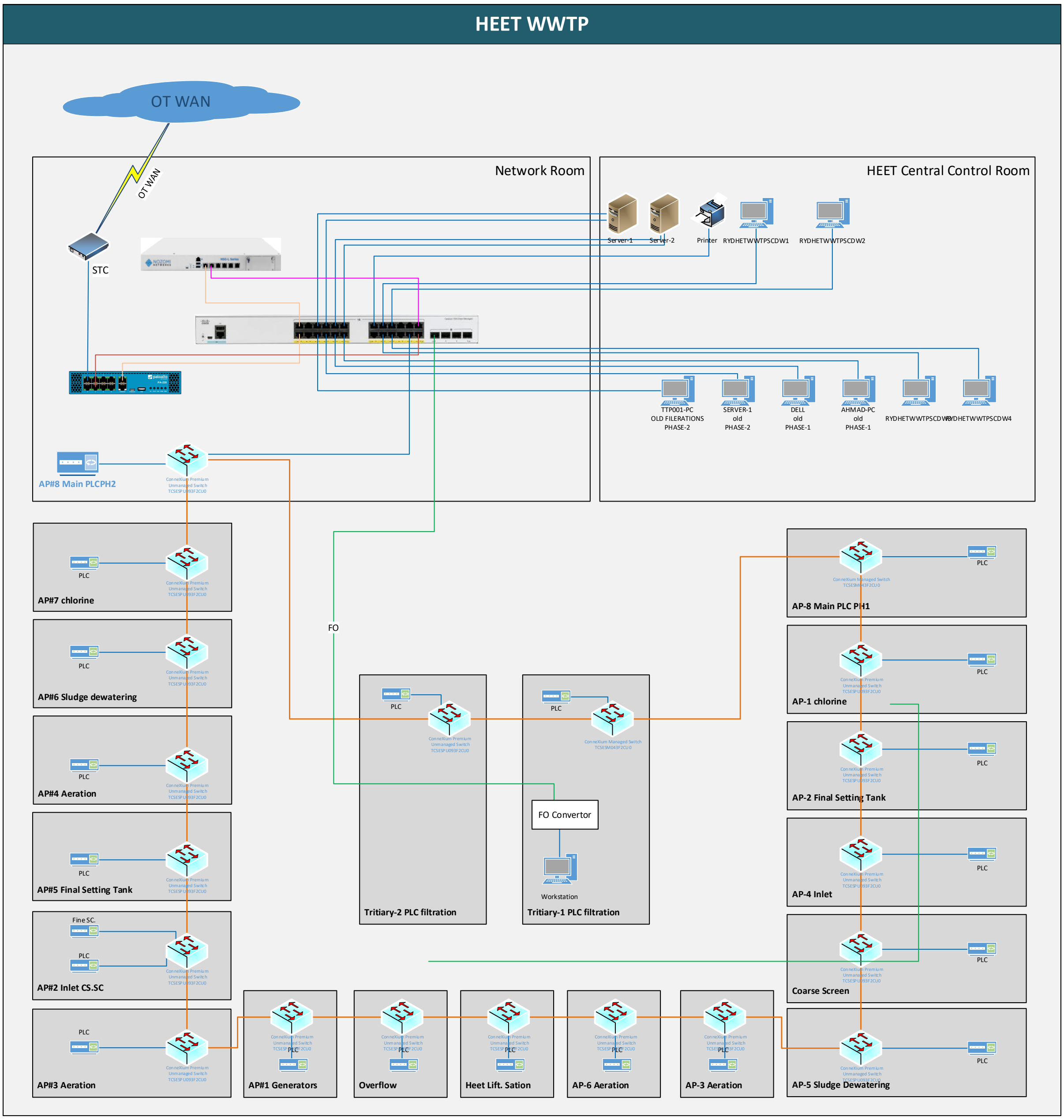


Figure 15 : HEET WWTP Architecture

5.3.20.1 DESIGN DESCRIPTION

- New Admin building 1st floor Rack room OT Cabinet has OT Ethernet switch, Firewall, Nozomi and SCADA Servers.
- SCADA VLAN for Operator Workstations in Filtration-1 Control Room is extended by using spare FO cores. A managed switch is installed in Filtration-1 Control Room which is part of SCADA VLAN.
- This site has on premises DAS, AOS, Historian, GR and OWS.
- Heet Lifting station outlet flow data is being monitored in Hayer.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.21 HAYER WWTP DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at HAYER WWTP.

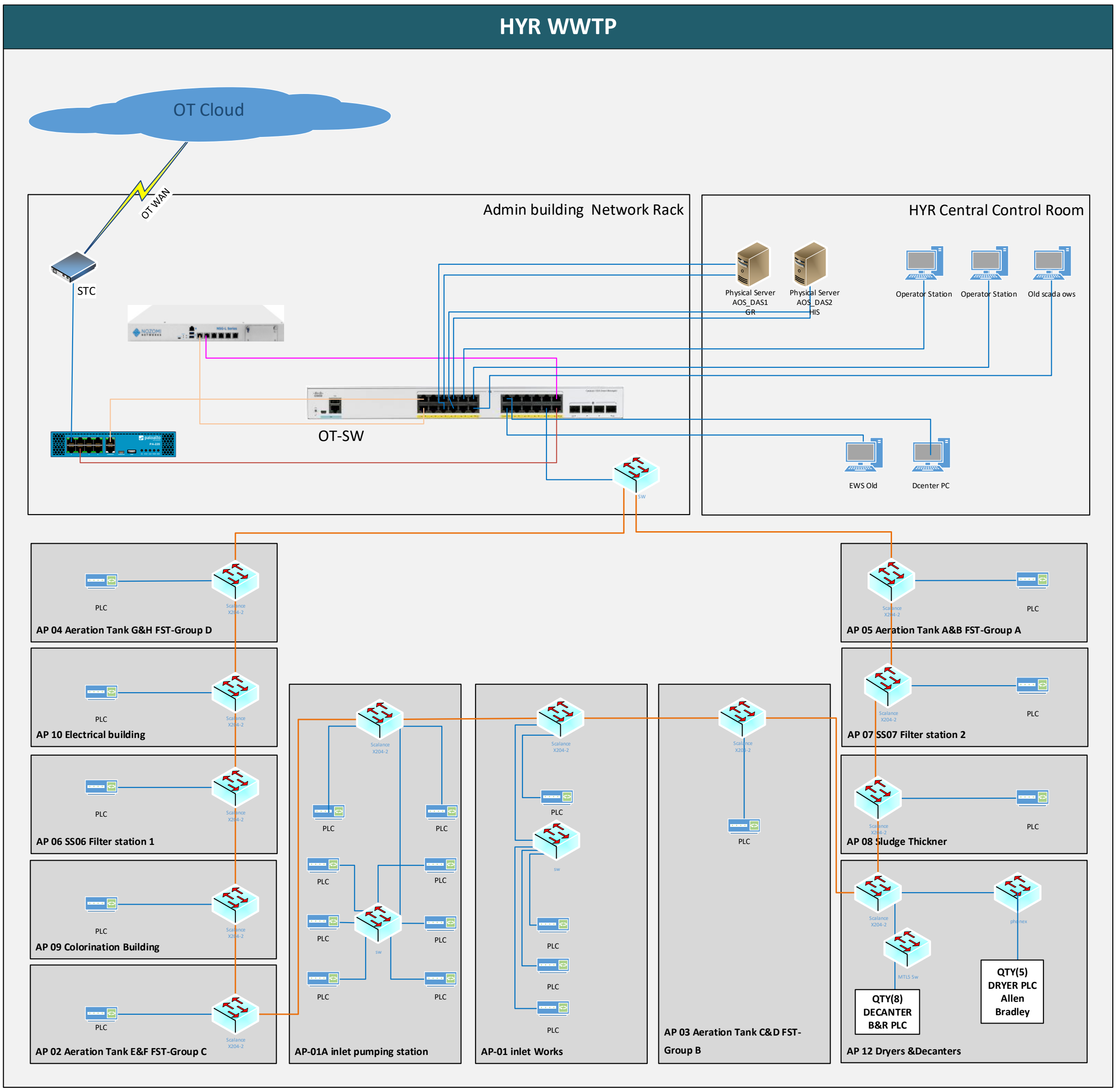

HYR WWTP
OT Cloud
OT WAN
STC
Admin building Network Rack
HYR Central Control Room
Physical Server AOS_DAS1 GR
Physical Server AOS_DAS2 HIS
Operator Station
Operator Station
Old scada ows
OT-SW
EWS Old
Dcenter PC
SW
PLC
Scalance X204-2
AP 04 Aeration Tank G&H FST-Group D
AP 05 Aeration Tank A&B FST-Group A
AP 10 Electrical building
AP 07 SS07 Filter station 2
AP 06 SS06 Filter station 1
AP 08 Sludge Thickner
AP 09 Colorination Building
AP 02 Aeration Tank E&F FST-Group C
AP-01A inlet pumping station
AP-01 inlet Works
AP 03 Aeration Tank C&D FST-Group B
AP 12 Dryers &Decanters
sw
phoenex
MTLS Sw
QTY(8) DECANTER B&R PLC
QTY(5) DRYER PLC Allen Bradley

Figure 16 : HAYER-WWTP Architecture

5.3.21.1 DESIGN DESCRIPTION

- Admin building 2nd floor Control Room Network Rack Room OT Cabinet has OT Ethernet switch, Firewall, Nozomi and SCADA Servers.
- This site has on premises DAS, AOS, Historian, GR and OWS.
- DAS in Hayer is reading outlet flow of HEET lifting station from PLC in HEET on Modbus TCP/IP.
- All OT assets are reconfigured with new IP addresses as per IP schema.

5.3.22 SR02 DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at SR02.

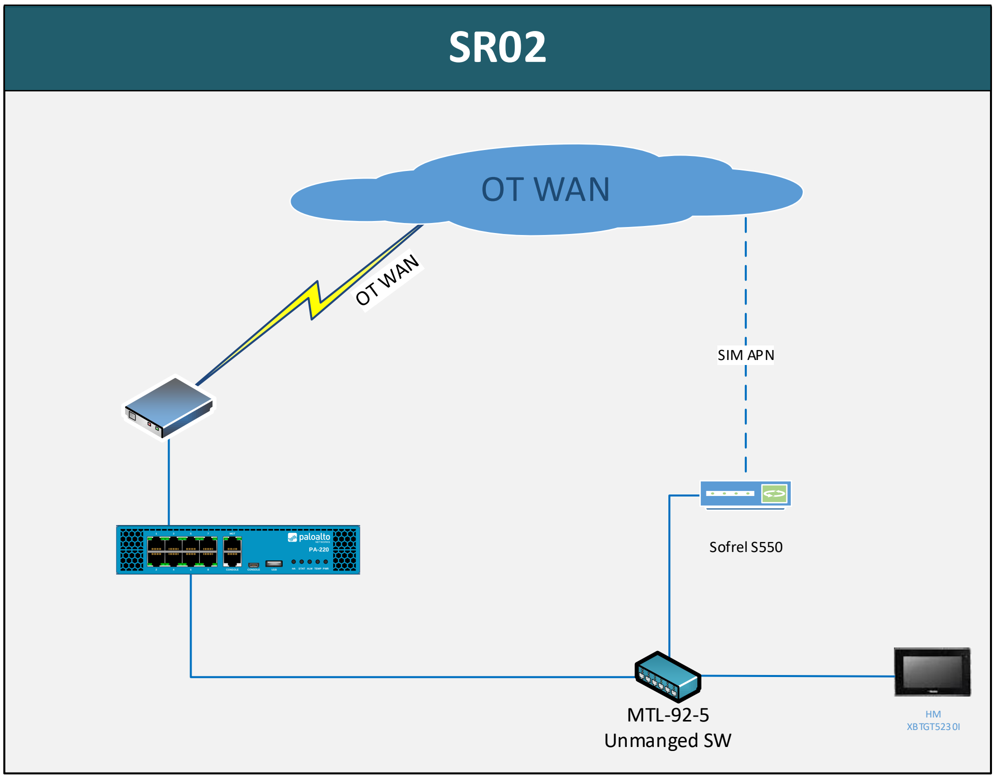


Figure 17 : SR02 Architecture

5.3.22.1 DESIGN DESCRIPTION

- Admin building network cabinet has Firewall.
    - All the network cables from OT devices in this room is connected to firewall.
- Due to weak GSM signal strength this site communicates over OT WAN to Exit-10.
- All OT assets are reconfigured with new IP addresses as per IP schema.

6. OT APN

A dedicated, secure, private OT APN is provided and managed by the telecom company provides GSM/GPRS connectivity from BU offices to field sites/equipment.

6.1 MCBU OT APN DESIGN

In MCBU, PS5 and Mina branch offices each has one circuit that connects to the OT APN. The OT firewalls installed at these locations provides the security barrier between the OT APN and the assets at the location.

The OT APN for MCBU is dedicated to provide connectivity to all SIM-based devices in MCBU with a separate APN profile for all SIMs in the BU.

The APN profile for MCBU APN Cloud is “MakkahOT.M2M”

6.2 RCBU OT APN DESIGN

In RCBU, Exit-10 has one circuit that connects to the OT APN. The OT firewalls installed at all other locations provides the security barrier between the OT APN and the assets at those locations.

The OT APN for RCBU is dedicated to provide connectivity to all SIM-based devices in RCBU with a separate APN profile for all SIMs in the BU.

The APN profile for RCBU APN Cloud is “RCBUOT.M2M”

7. JCBU DESIGN

7.1 JCBU ARCHITECTURE

Following is the data flow of NWC SCADA/OT environment at the JCBU.

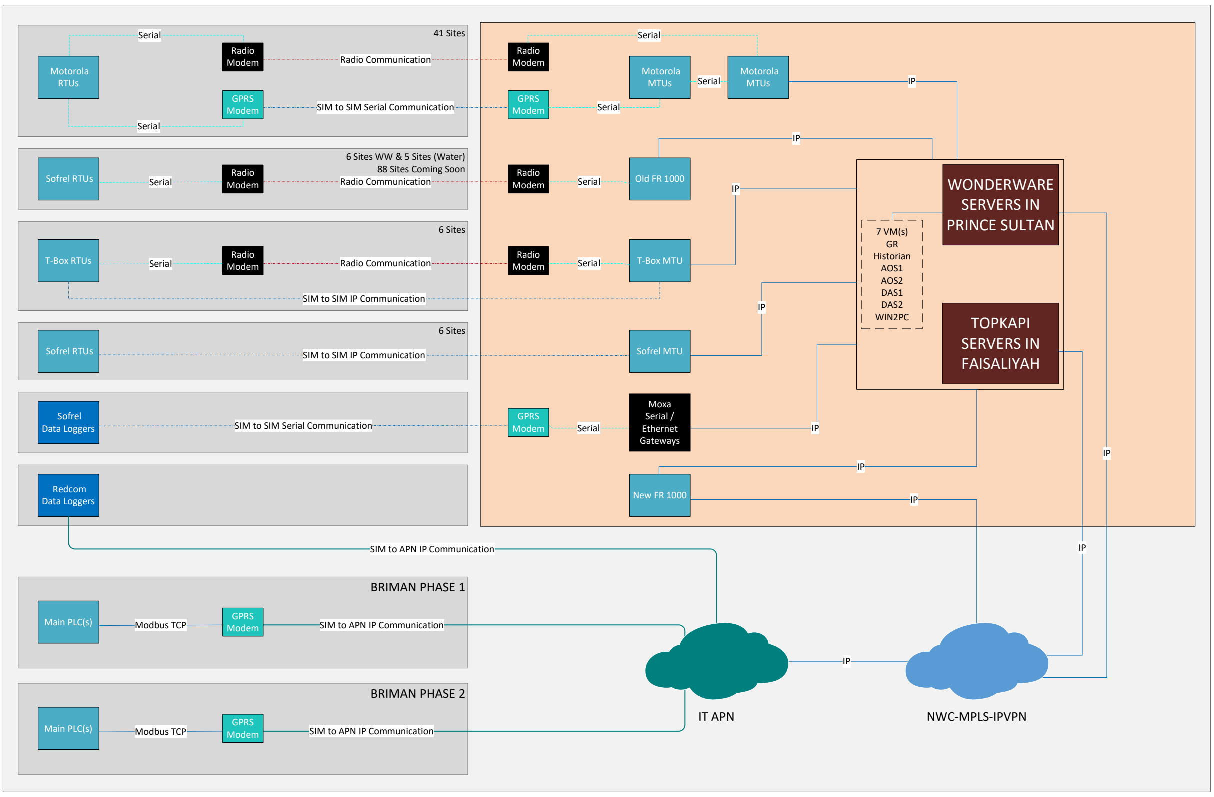


Figure 1: JCBU Data Flow

A high-resolution version of the data flow is provided as an attachment (A01001045-JCBU-DF).

Following is a description of the network setup for OT Cybersecurity in JCBU:

- Faisaliyah is the BU Main-office. It has the following zones:
  - SCADA-Zone contains Management Server, Wonderware SCADA Host Servers (Contains VMs of DAS_01, DAS_02, AOS_01, AOS_02, GR, Historian and PCWin2).
  - MGMT-Zone contains the vulnerability management device (Nozomi Guardian). This zone also provides connectivity to the management port for all network devices.
  - Level-1 Zone contains Level-1 devices installed (e.g., MTU, Data Concentrators, etc.)
- Faisalyah, Briman Phase-1, Briman Phase-2, AK-3 WWTP, AK-4 WWTP, AK-5 LS, AK-6 WWTP, SJSS, Airport-1 WWTP, Airport-1 LS and Rehaily are the branch offices.
- PSB has the following zones:

  - MGMT-Zone contains the vulnerability management device (Nozomi Guardian). This zone also provides connectivity to the management port for all network devices.
- Briman Phase-1 and Briman Phase-2 has the following zones:
  - SCADA-Zone contains all required servers and workstations for the SCADA system.
  - Level-1 Zone contains any Level-1 devices installed (e.g., MTU, Data Concentrators, etc.)
  - MGMT-Zone contains the vulnerability management device (Nozomi Guardian). This zone also provides connectivity to the management port for all network devices.
- The Management server installed in the Faisaliyah (BU Main-Office) contains the required management software including Antivirus, Patch Management, Backup Management.
- PSB, Faisalyah, Briman Phase-1, Briman Phase-2, AK-3 and Airport-1 LS has an OT WAN circuit to provide connectivity to the OT WAN.
- PSB and Faisaliyah has an OT APN circuit to provide connectivity to the GSM/GPRS devices.
- A NextGen OT firewall installed at PSB, Faisalyah, Briman Phase-1 and Briman Phase-2, AK-3 and Airport-1 LS provides security barrier for all external interfaces to that office. Following external interfaces connect to the BU office through this firewall:
  - OT WAN
  - OT APN

7.2 BILL OF MATERIALS

Below Table shows the quantities of OT equipment which will be installed in each JCBU site.

Sr. no.	JCBU Site Name	MGMT Server	OT Ethernet Switch	Firewall	Nozomi
1	PSB	-	5	1	1
2	Faisalyah	1	2	2	1
3	Briman Phase-1	-	1	1	1
4	Briman Phase-2	-	1	1	1
5	AK-3	-	1	1	1
6	AK-4	-	-	-	-
7	AK-5	-	-	-	-
8	AK-6	-	-	-	-
9	SJSS	-	-	-	-
10	Airport-1 WWTP	-	-	-	-
11	Airport-1 LS	-	3	1	1
12	Rehaily	-	-	-	-

7.2.1 MANAGEMENT SERVER SPECIFICATION

Management server is installed in Faisaliyah BU main office, and it has following specification.

Component	Configurations
Model	HPE ProLiant DL380 Gen10
Processor	Intel® Xeon® Gold 5218 22M Cache, 2.30 GHz
Memory	32 GB
HDD-1 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-2 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-3 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-4 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-5 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
Power Supply	HPE 800W FS Plat Ht Plg LH Pwr Sply Kit x 2

7.2.1.1 HOST CONFIGURATION

Component	Configurations
Host name	JDOTFASPHY01
O/S	Microsoft Windows Server 2016 DC
C Drive (For Host O/S)	300 GB
D Drive (For VMs)	2.18 TB
Memory available for Host O/S	12 GB

7.2.1.2 VM 1 CONFIGURATION

Component	Configurations
VM Name	JDOTFASADM01
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	100 GB
Memory	12 GB
Software Installed	Additional Domain Controller

7.2.1.3 VM 2 CONFIGURATION

Component	Configurations
VM Name	JDOTFASADM02
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	1.9 TB
Memory	12 GB
Software Installed	WSUS, BackupExec-MG, Super-Agent (McAfee)

7.2.2 FIREWALL

Following is the specification for Firewall installed in Faisaliyah BU main office.

Component	Configuration
Model	Palo Alto Networks PA-820 (High Availability)
Interfaces	4 x 1000Base-T - RJ-45 ¦ 8 x - SFP (mini-GBIC) ¦ 1 x micro-USB ¦ 3 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB
Subscriptions	Threat prevention subscription 2 year prepaid for devices in HA pair, PA-820

Following is the specification for Firewall for each JCBU branch office.

Component	Configurations
Model	Palo Alto Networks PA-220
Interfaces	8 x 1000Base-T - RJ-45 ¦ 1 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB ¦ 1 x console
Subscriptions	Threat prevention subscription 2 year prepaid for device in an HA pair, PA-220

7.2.3 OT ETHERNET SWITCH

Following is the specification for OT Switch for JCBU.

Component	Configurations
Model	Cisco Catalyst 1000-24T-4G-L - Switch
Interfaces	24 X 10/100/1000 + 4 x Gigabit SFP Uplinks

7.2.4 VULNERABILITY MONITORING SYSTEM

Following is the specification for VMS (NOZOMI) for JCBU.

Component	Configurations
Model	Nozomi Networks Guardian Appliance - NSG-L-100
Interfaces	4 x 1000Base-T - RJ-45 ¦ 8 x - SFP (mini-GBIC) ¦ 1 x micro-USB ¦ 3 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB
Subscriptions	Threat Intelligence - Guardian Appliance - NSG-L-100 (1 year)

7.2.5 ABOUT PSB

PSB BU site of JCBU is connected with Faisalyah site over IT-WAN.

7.2.5.1 CURRENT STATUS

Currently PSB has two Blade servers and two Engineering Stations installed at PSB 2nd Floor Datacenter and PSB 1st Floor respectively. PSB 3rd Floor contains two Topkapi Clients and two Video Servers. PSB Ground Floor also contains Two Wonderware Clients (One for Makkah and one for Taif) and one Topkapi Client for Faisalyah, connected over IT-WAN but are not communicating. These Blade servers contain Wonderware SCADA VMs and IT applications as well. Blade servers are connected with Access switch which is shared with IT assets. This access switch is connected with core switch (shared with IT assets) and finally to IT-WAN router.

Data from MTUs and Data Concentrators is directly received by Wonderware SCADA Server over IT-WAN in PSB. SCADA Servers also connect with Briman Phase-1 and Briman Phase-2 over IT-WAN.

Engineering Stations at 1st Floor are connected with Access switch which is shared with IT assets. This access switch is connected with core switch (shared with IT assets) over FO to make a communication between Blade servers and Engineering Stations.

Topkapi Clients and Video Servers at 1st Floor are connected with Access switch which is shared with IT assets. This access switch is connected with core switch (shared with IT assets) over FO.

Wonderware Clients and Topkapi Client at 1st Floor are connected with Access switch which is shared with IT assets. This access switch is connected with core switch (shared with IT assets) over FO.

7.2.5.2 PROPOSED DESIGN DESCRIPTION

Following is the detailed architecture of NWC SCADA/OT environment at PSB.

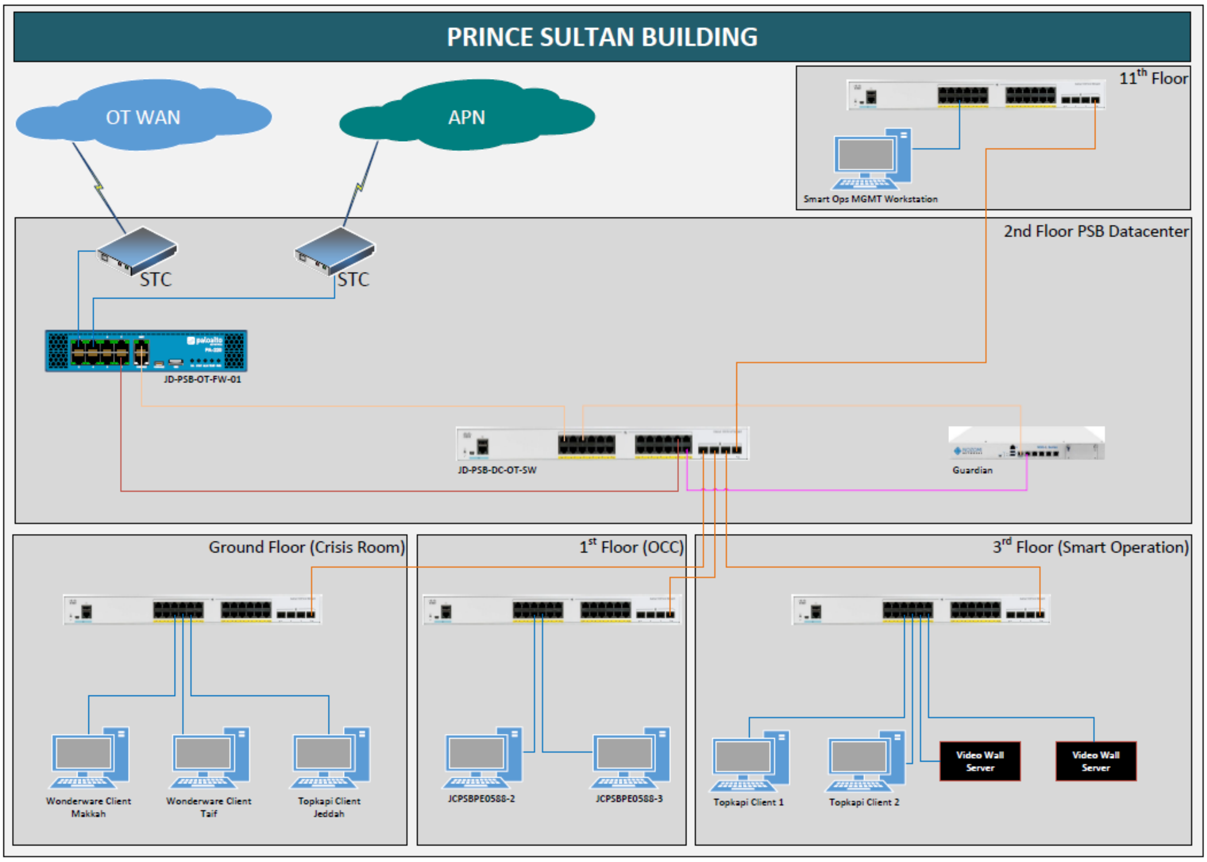


Figure 2: PSB Architecture

- PSB 2nd Floor Datacenter Room OT cabinet has OT Ethernet switch, Nozomi and Firewall.
  - All the network cables from OT devices in 2nd Floor Datacenter Room are connected to OT Ethernet switch.

  - OT devices at Ground Floor are connected to OT Access switch, That Access switch is connected to OT Access Switch at 2nd Floor Datacenter over FO.
  - OT devices at 1st Floor are connected to OT Access Switch, That Access switch is connected to OT Access Switch at 2nd Floor Datacenter over FO.
  - OT devices at 3rd Floor are connected to OT Access Switch, That Access switch is connected to OT Access Switch at 2nd Floor Datacenter over FO.
  - OT devices at 11th Floor are connected to OT Access Switch, That Access switch is connected to OT Access Switch at 2nd Floor Datacenter over FO.
- OT-WAN router is connected with firewall.
- APN-WN circuit is connected with firewall.
- All OT assets are reconfigured with new IP addresses as per IP schema.

7.2.6 ABOUT FAISALYAH

Faisalyah is the main BU which is connected with PSB over IT-WAN. It also connects with Briman Phase-1 and Briman Phase-2 sites.

7.2.6.1 CURRENT STATUS

Currently Faisalyah has two Topkapi SCADA servers connected with two OT-switches.

T-Box MTU, Motorolla MTU, Sofrel MTU, Old FR-1000 and MOXA Serial-to-Ethernet Gateways (which are connected with Gener data concentrators) are connected with 48-port OT-switch installed at the top of rack and this switch is connected with IT core switch over FO and core switch is connected with IT-WAN router.

Topkapi Servers and New FR-1000 are connected with 24-port OT-switch which is connected with core switch over ethernet.

7.2.6.2 PROPOSED DESIGN DESCRIPTION

Following is the detailed architecture of NWC SCADA/OT environment at Faisalyah.

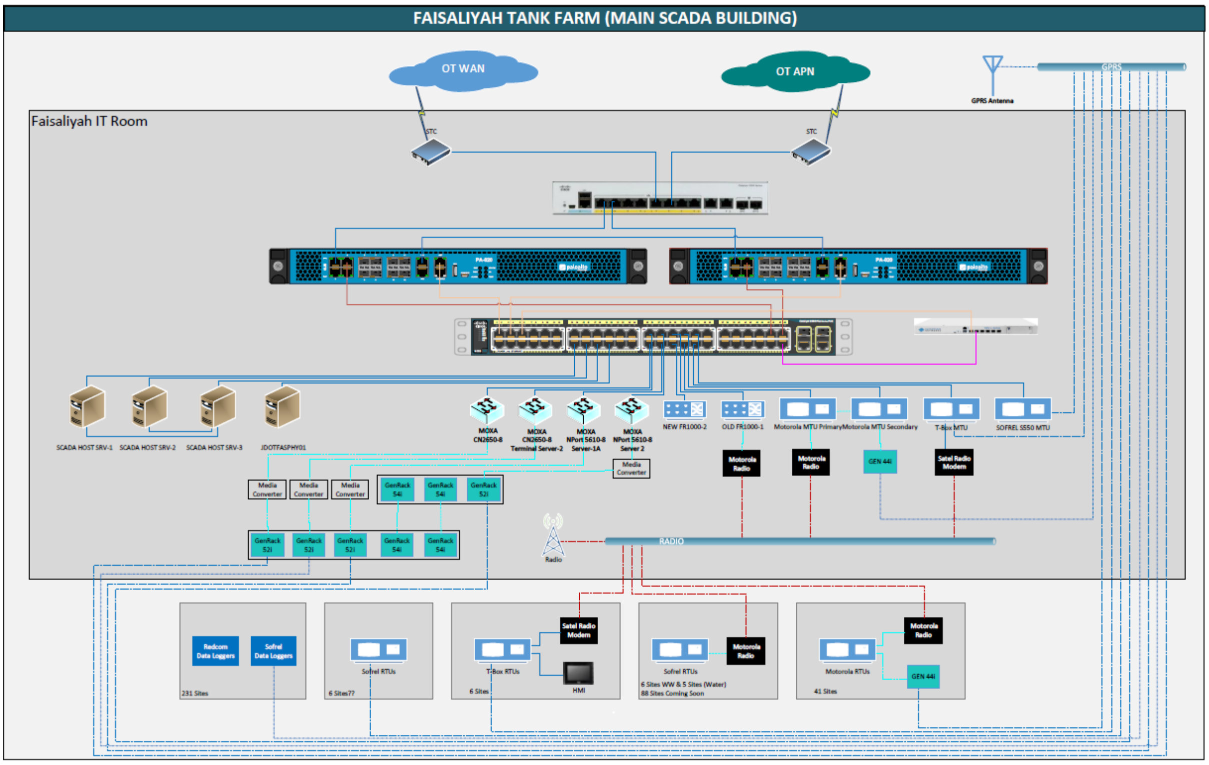


Figure 3: Faisaliyah Architecture

7.2.6.3 DESIGN DESCRIPTION

- Faisalyah Main Building IT Room SCADA cabinet has OT Ethernet switches, Nozomi and Redundant Firewall.
  - All the network cables from OT devices in IT Room is connected to OT Ethernet switches.
- OT-WAN router is connected with redundant firewall.

- OTAPN router is connected with redundant firewall.
- Data from multiple sites is being acquired via Radio and GSM/GPRS in Faisalyah MTU and Data Concentrators.
- All OT assets are reconfigured with new IP addresses as per IP schema.

7.2.7 ABOUT BRIMAN PHASE-1

Briman Phase-1 of JCBU is connected with PSB and Faisalyah over IT-WAN.

7.2.7.1 BRIMAN PHASE-1 CURRENT STATUS

Briman Phase-1 SCADA Server and two Operator Workstations located in SCADA Control Room are connected with Redundant Master PLCs via Redundant OT-Switches over ethernet. These master PLC are connected with three field PLCs over FO ring.

Master PLCs are also connected with local HMI and M340 PLC over ethernet.

Redundant Arctic GSM Gateways connected with Redundant OT-Switches over ethernet, are used to transfer data from master PLCs to PSB Wonderware SCADA Servers and Faisalyah Topkapi Servers over APN-WAN and then from APN-WAN to IT-WAN.

7.2.7.2 DESIGN DESCRIPTION

Following is the detailed architecture of NWC SCADA/OT environment at Briman Phase-1.

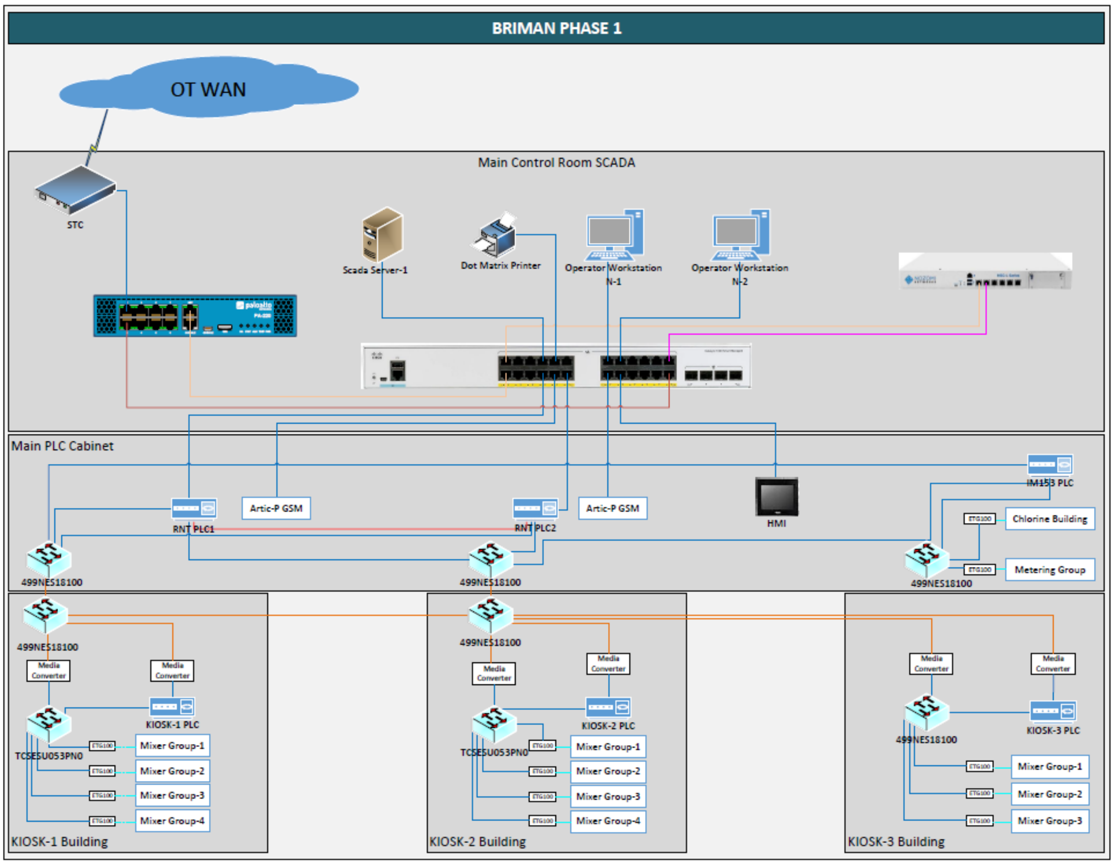


Figure 4: Briman Phase-1 Architecture

- SCADA Cabinet Room has OT Ethernet switch, Firewall and Nozomi.
  - All the network cables from OT devices in SCADA Room and SCADA Cabinet Room is connected to OT Ethernet switch.
- This site has on premises SCADA Server and Workstations.
- OT-WAN router is connected with firewall.
- All OT assets are reconfigured with new IP addresses as per IP schema.

7.2.8 ABOUT BRIMAN PHASE-2

Briman Phase-1 of JCBU is connected with PSB and Faisalyah over IT-WAN.

7.2.8.1 BRIMAN PHASE-2 CURRENT STATUS

Briman Phase-2 SCADA Server and Operator Workstation located in SCADA Control Room are connected with Redundant Master PLCs via OT-Switch over ethernet. These master PLC are connected with three field PLCs over FO ring.

Master PLCs are also connected with local HMI and IM153 PLC over ethernet.

Redundant Dr.Neuhaus GSM Gateways connected with OT-Switch, are used to transfer data from master PLCs to PSB Wonderware SCADA Servers and Faisalyah Topkapi Servers over APN-WAN and then from APN-WAN to IT-WAN.

7.2.8.2 DESIGN DESCRIPTION

Following is the detailed architecture of NWC SCADA/OT environment at Briman Phase-2.

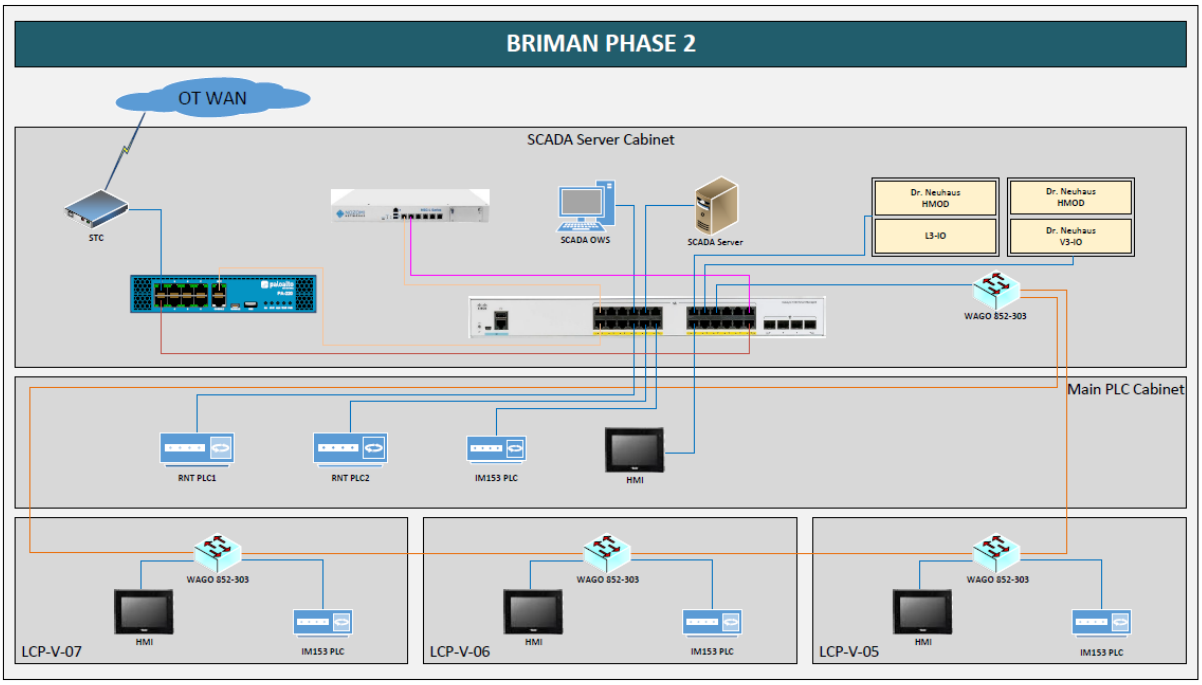


Figure 5: Briman Phase-2 Architecture

- SCADA Cabinet has OT Ethernet switch, Firewall and Nozomi.

    - All the network cables from OT devices in SCADA Room is connected to OT Ethernet switch.

- This site has on premises SCADA Server and Workstation.
- OT-WAN router is connected with firewall.
- All OT assets are reconfigured with new IP addresses as per IP schema.

7.2.9 AK-3 WWTP CURRENT STATUS

AK-3 is WWTP located in South Zone of JCBU. It has standalone SCADA system.

Two SCADA Servers and two Operator Workstations located in SCADA Control Room are connected with OT-Switch. OT-Switch is connected to Industrial WAGO switch which is connected to seven field PLCs (Disk Filter, Sludge Dewatering, RAS Pumping Station, Aeration Tank, Kiosk 4, Blower, Motor Control Center and Kiosk 5) over FO ring.

RAS Pumping Station PLC is also connected with six Final Settling Tank PLCs over Radio.

7.2.10 AK-4 WWTP CURRENT STATUS

AK-4 is WWTP located in South Zone of JCBU. It has standalone SCADA system.

Two SCADA Servers are located in Ground floor and 1st floor of Main SCADA Building, respectively. SCADA Server at Ground Floor is connected with Industrial Switch over ethernet. This Industrial Switch is connected with nine field PLCs (Aeration Blower, Aeration Mixer, RAS/WAS A, RAS/WAS B, Final Effluent, Sand Filter, Sludge Dewatering, Main Switchgear and Inlet) over FO and finally to 1st Floor SCADA Server over ethernet connected over Industrial Switch.

7.2.11 SOUTH JEDDAH LS CURRENT STATUS

South Jeddah LS located in South Zone of JCBU. It has standalone SCADA system.

South Jeddah LS Two SCADA Servers, Database Server, Asset Management Server and Two Operator Workstations located in Main SCADA Control Room are connected with Redundant OT-Switch over ethernet. Nine field PLCs (Odor Control, Pumping Shaft, Hydraulic Part-2 Hydraulic Part-2, Screen Shaft, Pumping Shaft, MCC-1, MCC-2, MCC-3, Generator, ventilation and Auxiliary) over FO to Industrial Switch and this industrial switch is finally connected to SCADA network over ethernet.

7.2.12 AK-SS WWTP CURRENT STATUS

AK-SS is Sea Station located in South Zone of JCBU. It has standalone SCADA system.

AK-SS has Two SCADA Servers located in Main SCADA Control Room are connected with Industrial Switch over ethernet. Two Master PLCs connected with four RIOs and Local Panel HMI over ethernet are also connected with SCADA Servers over same SCADA Industrial Switch.

7.2.13 AIRPORT-1 WWTP CURRENT STATUS

Airport-1 WWTP is located in North Zone of JCBU. It has standalone SCADA system.

One SCADA Server and Three Client Stations are located in Main SCADA Control Room are connected with Industrial Switch over ethernet. This Insdutrial Switch is connected with another Industrial Switch which connects with twelve field PLCs (Generator, BIO-P-Tank, New Inlet, New Air Blower, Aeration Tank, Secondary Clarifier, New RAS, UV Processing Unit, Filtration, Chlorination System and New Decenter) over FO.

7.2.14 AIRPORT-1 LS CURRENT STATUS

Airport-1 LS is located in North Zone of JCBU. It has standalone SCADA system.

Airport-1 LS has Two SCADA Servers, Historian, Three Operator Workstations, GPS NTP Time Server, Viper IP Radio Receiver located in Main SCADA Control Room are connected with OT-Switch over ethernet. MCC-1 and MCC-2 Master PLCs and Field PLCs are connected over Redundant FO ring.

MCC-1 and MCC-2 Admin Client 1 &2 are connected with OT-Switch which is connected with Redundant Industrial Switches linked with FO rings.

Shaft S1, Shaft S3 and Shaft 5B PLCs are connected with Viper IP Radios which transfer data to Viper IP Radio receiver over Radio on SCADA network.

MCC-1 Industrial switch-1 is connected with Airport-1 WWTP SW-1 installed at Ventilation Building over FO.

8. TCBU DESIGN

8.1 TCBU ARCHITECTURE

Following is the detailed architecture of NWC SCADA/OT environment at the TCBU.

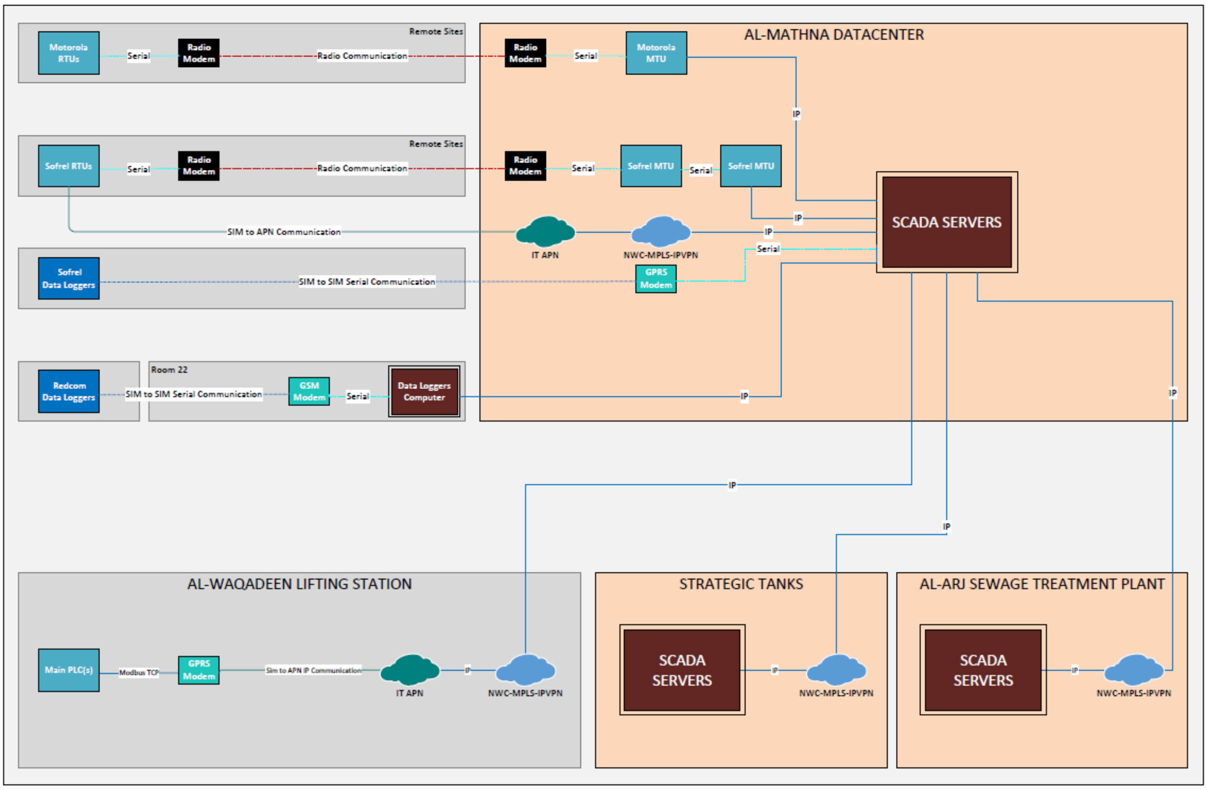


Figure 1: TCBU Data Flow

A high-resolution version of the architecture is provided as an attachment (A01001045-TCBU-DLD-NA).

Following is a description of the network setup for OT Cybersecurity in TCBU:

- Al-Mathna is the BU Main-office. It has the following zones:
  - SCADA-Zone contains AOS, DAS, GR, Historian, Workstations and Management Server.
  - Level-1 Zone contains Level-1 devices installed in the office (e.g., MTU, Data Concentrators, etc).
  - MGMT-Zone contains the vulnerability management device (Nozomi Guardian). This zone also provides connectivity to the management port for all network devices.
- Al-Arj WWTP, Strategic Tanks and Al-Waqadeen LS are the branch offices.
- Al-Arj WWTP, Strategic Tanks and Al-Waqadeen LS have the following zones:

  - SCADA-Zone contains all required servers and workstations for the SCADA system.
  - Level-1 Zone contains any Level-1 devices installed (e.g., MTU, Data Concentrators, etc.)
  - MGMT-Zone contains the vulnerability management device (Nozomi Guardian). This zone also provides connectivity to the management port for all network devices.

- The Management server installed in the Al-Mathna (BU Main-Office) contains the required management software including Antivirus, Patch Management, Backup Management.
- Al-Mathna, Al-Arj WWTP, Strategic Tanks and Al-Waqadeen LS has an OT WAN circuit to provide connectivity to the OT WAN.
- Al-Mathna has an OT APN circuit to provide connectivity to the GSM/GPRS devices.
- A NextGen OT firewall installed at each BU office provides security barrier for all external interfaces to that office. Following external interfaces connect to the BU office through this firewall:
  - OT WAN
  - OT APN

8.2 BILL OF MATERIALS

Below Table shows the quantities of OT equipment which is installed in each TCBU site.

Sr. no.	RCBU Site Name	MGMT Server	OT Ethernet Switch	Firewall	Nozomi
1	Al-Mathna	1	3	2	1
2	Al-Arj WWTP	-	1	1	1
3	Strategic Tanks	-	1	1	1
4	Al-Waqadeen LS	-	1	1	1

8.2.1 MANAGEMENT SERVER SPECIFICATION

Management server is installed in Al-Mathna BU main office, and it has following specification.

Component	Configurations
Model	HPE ProLiant DL380 Gen10
Processor	Intel® Xeon® Gold 5218 22M Cache, 2.30 GHz
Memory	32 GB
HDD-1 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-2 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-3 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-4 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-5 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
Power Supply	HPE 800W FS Plat Ht Plg LH Pwr Sply Kit x 2

8.2.1.1 HOST CONFIGURATION

Component	Configurations
Host name	TFOTMATPHY01
O/S	Microsoft Windows Server 2016 DC
C Drive (For Host O/S)	300 GB
D Drive (For VMs)	2.18 TB
Memory available for Host O/S	12 GB

8.2.1.2 VM 1 CONFIGURATION

Component	Configurations
VM Name	TFOTMATADM01
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	100 GB
Memory	12 GB
Software Installed	Additional Domain Controller

8.2.1.3 VM 2 CONFIGURATION

Component	Configurations
VM Name	TFOTMATADM02
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	1.9 TB
Memory	12 GB
Software Installed	WSUS, BackupExec-MG, Super-Agent (McAfee)

8.2.2 FIREWALL

Following is the specification for Firewall installed in Al-Mathna BU main office.

Component	Configuration
Model	Palo Alto Networks PA-820 (High Availability)
Interfaces	4 x 1000Base-T - RJ-45 ¦ 8 x - SFP (mini-GBIC) ¦ 1 x micro-USB ¦ 3 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB
Subscriptions	Threat prevention subscription 2 year prepaid for devices in HA pair, PA-820

Following is the specification for Firewall for each TCBU branch office.

Component	Configurations
Model	Palo Alto Networks PA-220
Interfaces	8 x 1000Base-T - RJ-45 ¦ 1 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB ¦ 1 x console

Component	Configurations
Subscriptions	Threat prevention subscription 2 year prepaid for device in an HA pair, PA-220

8.2.3 OT ETHERNET SWITCH

Following is the specification for OT Switch for TCBU.

Component	Configurations
Model	Cisco Catalyst 1000-24T-4G-L - Switch
Interfaces	24 X 10/100/1000 + 4 x Gigabit SFP Uplinks

8.2.4 VULNERABILITY MONITORING SYSTEM

Following is the specification for VMS (NOZOMI) for TCBU.

Component	Configurations
Model	Nozomi Networks Guardian Appliance - NSG-L-100
Interfaces	4 x 1000Base-T - RJ-45 ¦ 8 x - SFP (mini-GBIC) ¦ 1 x micro-USB ¦ 3 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB
Subscriptions	Threat Intelligence - Guardian Appliance - NSG-L-100 (1 year)

8.2.5 ABOUT AL-MATHNA

Al-Mathna is the main BU site of TCBU which is connected with Al-Arj WWTP, Stretigic Tank and Al-Waqadeen LS over IT-WAN.

8.2.5.1 CURRENT STATUS

Al-Mathna SCADA Servers (GR, Historian, DAS1+AOS1, DAS2+AOS2) Sofrel Redundant MTUs and Motorolla MTU installed in Al-Mathna Datacenter. Operator Workstation 1, 2, 3, 4, Engineering Station installed in Al-Mathna OCC are connected with Datacenter over FO. Redcom Data Logger Server in Room 22 are connected with OT-Switch installed in Al-Mathna Datacenter over ethernet. OT-Switch is connected with IT-Core Switch which is connected with IT-WAN router. Two New SCADA hosts Servers are installed for New SCADA System.

Motorola RTUs are communicating over Radio with Motorolla MTU which is connected with SCADA over Modbus TCP/IP. Sofrel RTUs data is received by DAS directly over Modbus using IT APN. Sofrel Data Loggers data is received by Wavecom modem which is serially connected with GR through Telemetry Trace Sofrel OPC Server over Modbus.

Redcom Dataloggers are communicating with GSM modem by SMS technology and that GSM modem is connected with Redcom Datalogger computer serially. That computer is connected with SCADA server over ethernet to transfer Redcom Dataloggers data to SCADA Server.

8.2.5.2 DESIGN DESCRIPTION

Following is the detailed architecture of NWC SCADA/OT environment at Al-Mathna.

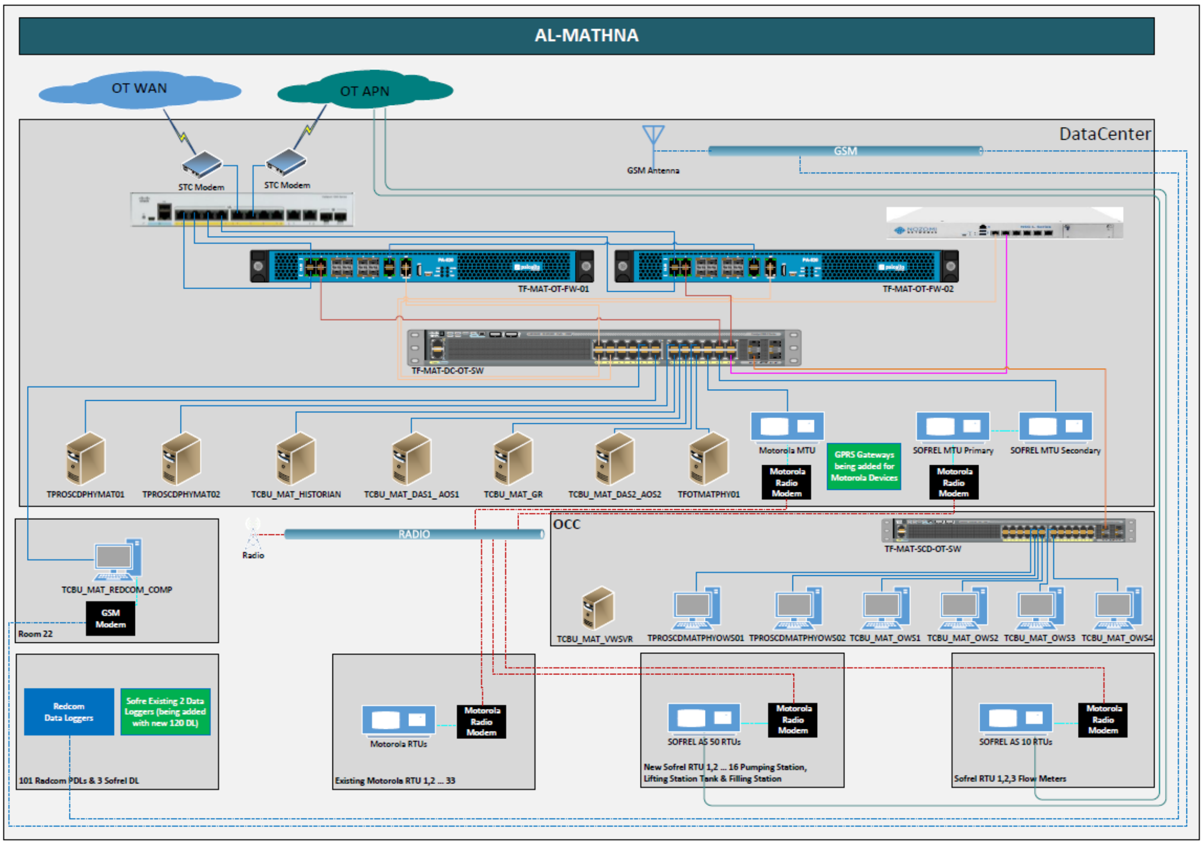


Figure 2: Al-Mathna Architecture

- Al-Mathna Datacenter Room OT cabinet has OT Ethernet switch, Nozomi and Firewall.
    - All the network cables from OT devices in Datacenter Room, OCC and Room 22 is connected to OT Ethernet switch.
- This site has on premises SCADA AOS-DAS, GR, Historian, Operator Workstations and Video Wall Server.
- Data from field devices is acquired over radio and GSM/GPRS.
- All OT assets are reconfigured with new IP addresses as per IP schema.

8.2.6 ABOUT AL-ARJ WWTP

Al-Arj is WWTP of TCBU which is connected with Al-Mathna Central SCADA over IT-WAN.

8.2.6.1 CURRENT STATUS

Al-Arj WWTP existing SCADA Servers (GR+AOS1, Historian, DAS, AOS2), Operator Workstation 1,2,3 and Video Wall Server are connected with OT-Switch installed in Al-Arj Datacenter over ethernet. OT-Switch is connected with IT-Core Switch which is connected with IT-WAN router. AP-7 Main PLC is connected with OT-Switch over ethernet through Scalance Industrial switch. Field PLC (AP6 Inlet Screen, AP6-1 Grease Removal, AP4 Thickner & Selector Tank, Master PLC, AP6 Belt Press, Master PLC, AP2 Aeration, AP2-1 FST, AP3 Transformer, AP1 Filteration, AP1-1 Filteration, Master PLC, AP1-2 Filteration Disk, AP1-3 Filteration Disk and UV) are connected with AP-7 Main PLC over FO ring.

Chlorination PLC (22), Carbon PLC (26), Furnaces PLC, Computer RP2 (99), Main Pumps PLC (21), Standby Power PLC (27), Computer STP (97), Screen PLC (11), Aeration PLC (13), Clarifier PLC (12), Computer RP1 (98), Multimedia PLC (16), Chemical PLC (17), Retention PLC (26), Flotation PLC (15) and Workstation are connected with IO Server over Profibus ring.

Two New SCADA hosts Servers are installed for New SCADA System.

8.2.6.2 DESIGN DESCRIPTION

Following is the detailed architecture of NWC SCADA/OT environment at Al-Arj WWTP.

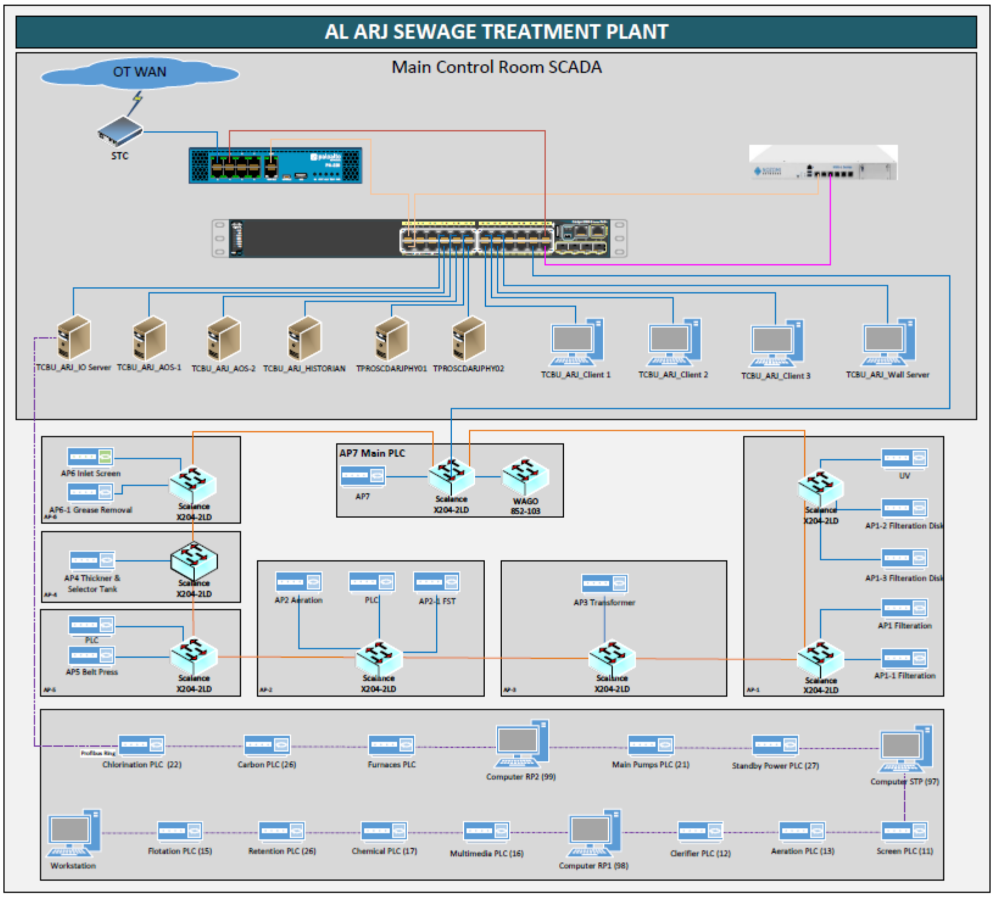


Figure 18: Al-Arj WWTP Architecture

- Al-Arj WWTP Main Building SCADA cabinet has OT Ethernet switch, Nozomi and Firewall.
  - All the network cables from OT devices in Datacenter is connected to OT Ethernet switch.
- This site has on premises Old and New SCADA AOS, GR, Historian, Workstations and IO Server.
- All OT assets are reconfigured with new IP addresses as per IP schema.

8.2.7 ABOUT STRATEGIC TANKS

Strategic Tanks of TCBU is connected with Al-Mathna Central SCADA over IT-WAN.

8.2.7.1 CURRENT STATUS

Strategic Tanks SCADA Server and Operator Workstation located in Main Building SCADA Room are connected with OT-Switch located in SCADA Cabinet Room. OT-switch is connected with IT-Core switch and it is connected with IT-WAN Router. Five field RTUs are connected with MC100CM switches over FO and MC100CM are connected with SCADA through OT-switch over ethernet. Five remote RTUs are connected with SCADA over radio by a radio receiver connected with SCADA through OT-switch over ethernet.

One New SCADA host Server is installed for New SCADA System.

8.2.7.2 DESIGN DESCRIPTION

Following is the detailed architecture of NWC SCADA/OT environment at Strategic Tanks.

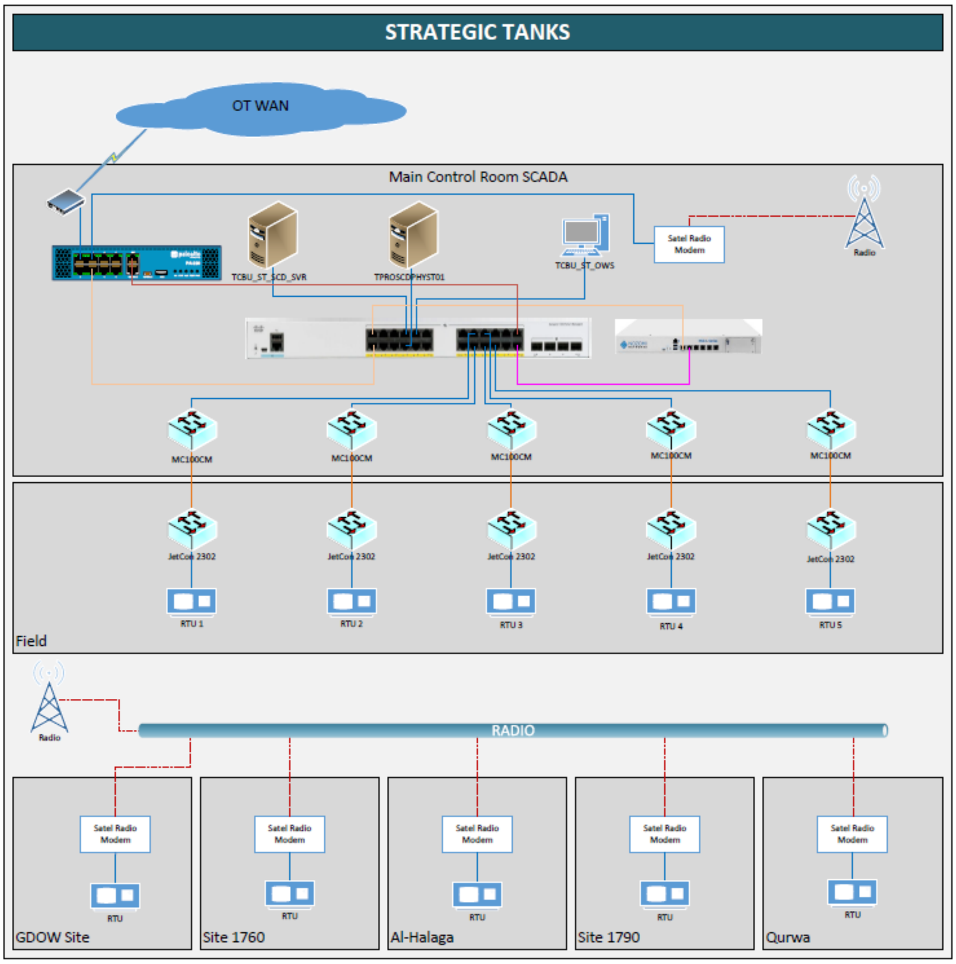


Figure 4: Strategic Tanks Architecture

- SCADA Cabinet Room has OT Ethernet switch, Firewall and Nozomi.
  - All the network cables from OT devices in SCADA Room and SCADA Cabinet Room is connected to OT Ethernet switch.

- This site has on premises Old and New SCADA Server and Workstation.
- Data from RTUs in field and remote locations is acquired over radio and FO.
- All OT assets are reconfigured with new IP addresses as per IP schema.

8.2.8 ABOUT AL-WAQADEEN LS

Al-Waqadeen LS of TCBU is connected with Al-Mathna Central SCADA over IT-WAN.

8.2.8.1 AL-WAQADEEN LS CURRENT STATUS

Al-Waqadeen LS has a SCADA Server and Operator Workstation located in SCADA Control Room are connected with Redundant Master PLCs with OT-Switch over ethernet.

Ewon Flexy GPRS Gateways connected with OT-Switch, are used to transfer data from master PLCs to Al-Mathna SCADA Server over APN-WAN and then from APN-WAN to IT-WAN.

8.2.8.2 DESIGN DESCRIPTION

Following is the detailed architecture of NWC SCADA/OT environment at Al-Waqadeen LS.

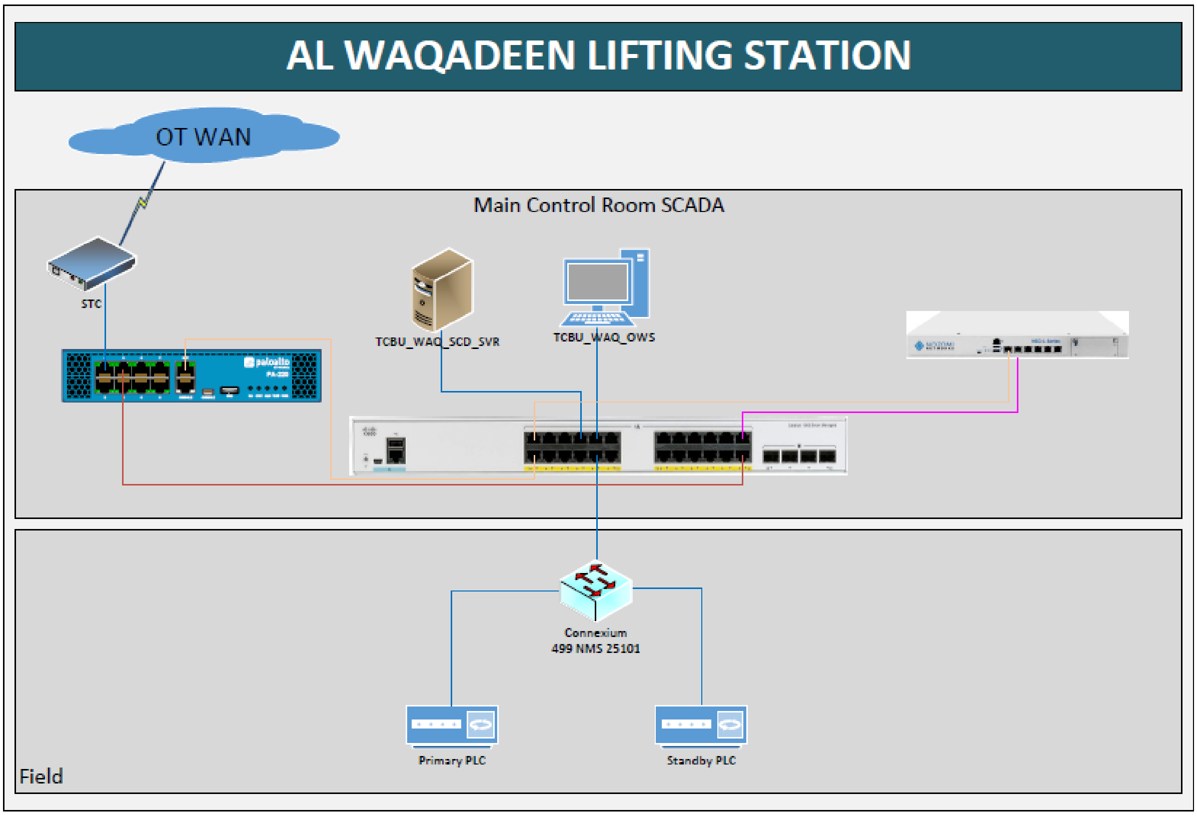


Figure 5: Al-Waqadeen LS Architecture

- SCADA Room has OT Ethernet switch, Firewall and Nozomi.
  - All the network cables from OT devices in SCADA Room and PLC Cabinet Room is connected to OT Ethernet switch.
- This site has on premises SCADA Server and Workstation.

- All OT assets are reconfigured with new IP addresses as per IP schema.

9. MDCBU DESIGN

9.1 MDCBU ARCHITECTURE

Following is the overview architecture of NWC SCADA/OT environment at the MdCBU.

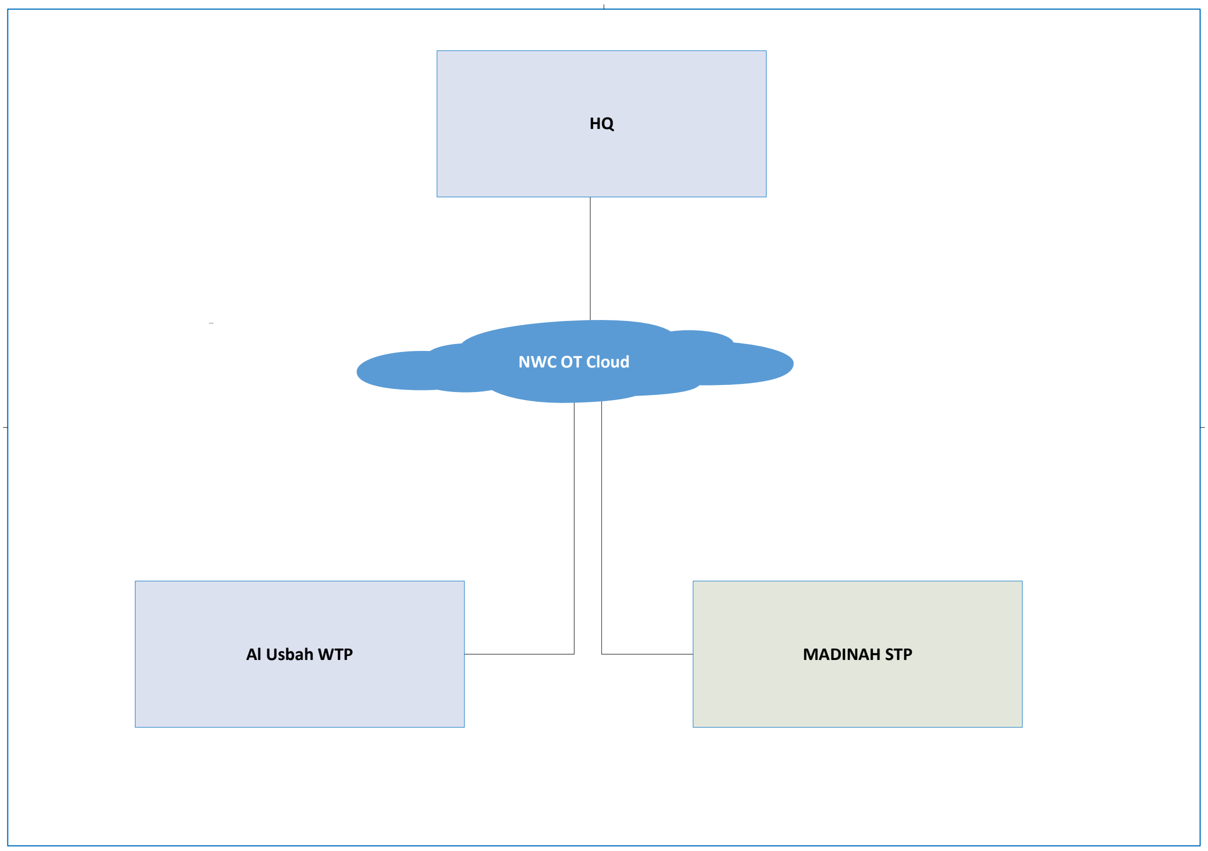


Figure 19 : MDCBU Architecture

Following is a description of the network setup for OT Cybersecurity in MDCBU:

- Al Usbah WTP is the BU Main-office. It has the following zones:
  - SCADA-Zone contains Domain Controller, Historians, Management Server as well as additional SCADA servers as needed.
  - Level-1 Zone contains any Level-1 devices installed in the office (e.g., Data Concentrators, etc.)
  - MGMT-Zone contains the vulnerability management device (Nozomi Guardian). This zone also provides connectivity to the management port for all network devices.
- Madinah STP is the branch office. It has the following zones:
  - SCADA-Zone contains all required servers and workstations for the SCADA system. This includes AOS, DAS, Historian, OWS and EWS.

- Level-1 Zone contains any Level-1 devices installed (e.g., MTU, Data Concentrators, etc.)
- MGMT-Zone contains the vulnerability management device (Nozomi Guardian). This zone also provides connectivity to the management port for all network devices.

- The Management server installed in Al Usbah WTP (BU Main-Office) contains the required management software including Antivirus, Patch Management, Backup Management.
- BU Main and Branch-Office have an OT WAN circuit to provide connectivity to the OT WAN.
- BU Main office (Al Usbah WTP) has an OT APN circuit to provide connectivity to the GSM/GPRS devices.
- A NextGen OT firewall installed at each BU office provides security barrier for all external interfaces to that office. Following external interfaces connect to the BU office through this firewall:
    - OT WAN
    - OT APN
    - Radio (TCP/IP only)

9.2 MDCBU INTER SITE COMMUNICATION

VPN Tunnelling

- Madinah STP will be connected via VPN Tunnel to HQ and Al Usbah WTP (MDCBU Main office).
- Al Usbah WTP will be connected to via VPN Tunnel to HQ and Madinah STP.

9.3 BILL OF MATERIALS

Below Table shows the quantities of OT equipment which is installed in each MDCBU site.

Sr. no.	RCBU Site Name	MGMT Server	OT Ethernet Switch	Firewall	Nozomi
1	Al Usbah WTP	1	1	2	1
2	Madinah STP	-	1	1	1

9.3.1 MANAGEMENT SERVER SPECIFICATION

Management server is installed in Al Usbah WTP BU main office, and it has following specification.

Component	Configurations
Model	HPE ProLiant DL380 Gen10
Processor	Intel® Xeon® Gold 5218 22M Cache, 2.30 GHz

Component	Configurations
Memory	32 GB
HDD-1 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-2 (Raid1-VirtualDisk1)	300GB SAS 12G Enterprise 10K SFF (2.5in)
HDD-3 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-4 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
HDD-5 (Raid5-VirtualDisk2)	1.2TB SAS 12G Enterprise 10K SFF (2.5in)
Power Supply	HPE 800W FS Plat Ht Plg LH Pwr Sply Kit x 2

9.3.1.1 HOST CONFIGURATION

Component	Configurations
Host name	MDOTUSBPHY01
O/S	Microsoft Windows Server 2016 DC
C Drive (For Host O/S)	300 GB
D Drive (For VMs)	2.18 TB
Memory available for Host O/S	12 GB

9.3.1.2 VM 1 CONFIGURATION

Component	Configurations
VM Name	MDOTUSBADM01
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	100 GB
Memory	12 GB
Software Installed	Additional Domain Controller

9.3.1.3 VM 2 CONFIGURATION

Component	Configurations
VM Name	MDOTUSBADM02
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	1.9 TB
Memory	12 GB
Software Installed	WSUS, BackupExec-MG, Super-Agent (McAfee)

9.3.2 FIREWALL

Following is the specification for Firewall installed in Al Usbah WTP BU main office.

Component	Configuration
Model	Palo Alto Networks PA-820 (High Availability)
Interfaces	4 x 1000Base-T - RJ-45 ¦ 8 x - SFP (mini-GBIC) ¦ 1 x micro-USB ¦ 3 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB

Component	Configuration
Subscriptions	Threat prevention subscription 2 year prepaid for devices in HA pair, PA-820

Following is the specification for Firewall for Madinah STP MdCBU branch office.

Component	Configurations
Model	Palo Alto Networks PA-220
Interfaces	8 x 1000Base-T - RJ-45 ¦ 1 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB ¦ 1 x console
Subscriptions	Threat prevention subscription 2 year prepaid for device in an HA pair, PA-220

9.3.3 OT ETHERNET SWITCH

Following is the specification for OT Switch for MdCBU.

Component	Configurations
Model	Cisco Catalyst 1000-24T-4G-L - Switch
Interfaces	24 X 10/100/1000 + 4 x Gigabit SFP Uplinks

9.3.4 VULNERABILITY MONITORING SYSTEM

Following is the specification for VMS (NOZOMI) for MdCBU.

Component	Configurations
Model	Nozomi Networks Guardian Appliance - NSG-L-100
Interfaces	4 x 1000Base-T - RJ-45 ¦ 8 x - SFP (mini-GBIC) ¦ 1 x micro-USB ¦ 3 x 1000Base-T (management) - RJ-45 ¦ 1 x console - RJ-45 ¦ 1 x USB
Subscriptions	Threat Intelligence - Guardian Appliance - NSG-L-100 (1 year)

9.3.5 AL USBAH WTP DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at AL Usbah WTP.

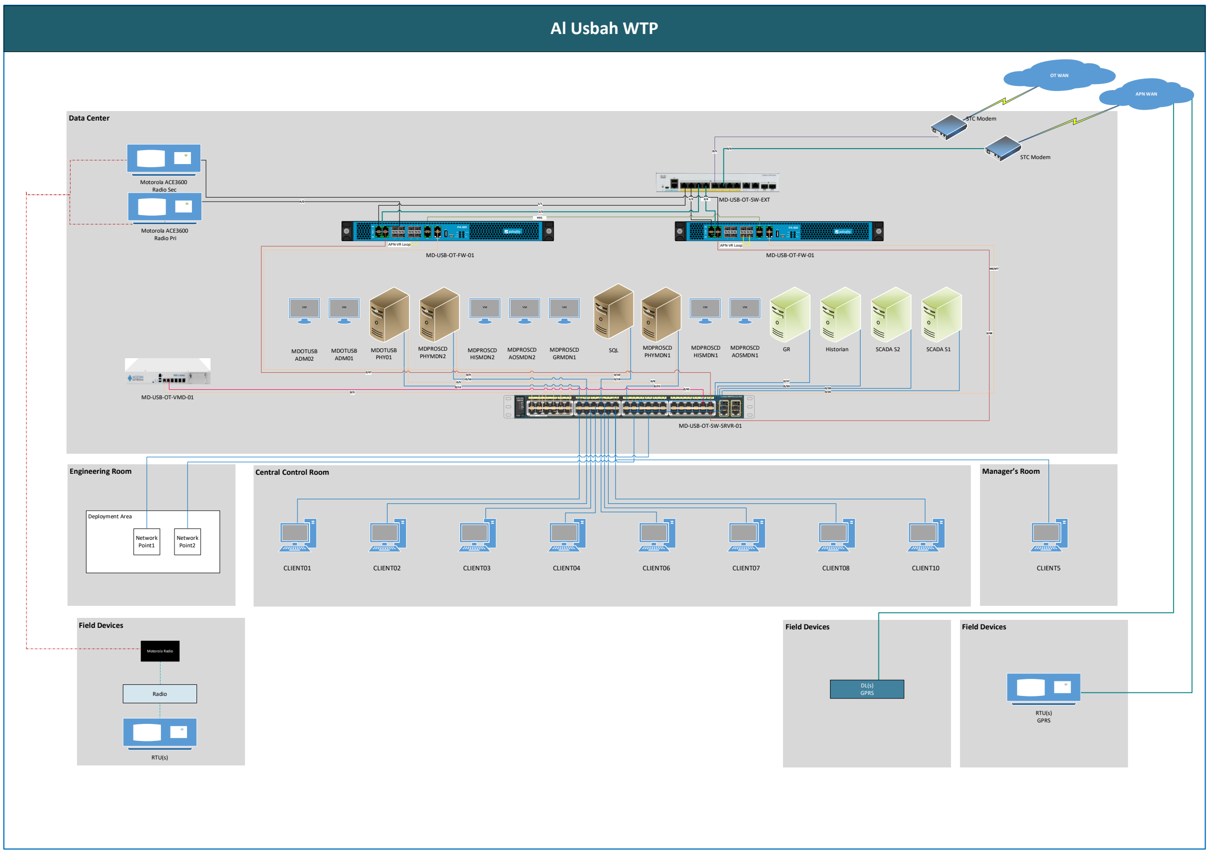


Figure 20 : Al Usbah WTP Architecture

9.3.5.1 DESIGN DESCRIPTION

- Al Usbah WTP Central Control Room (CCR) cabinet has OT Ethernet switch, Nozomi and Firewall.
  - All the network cables from OT devices in control room is connected to OT Ethernet switch.
- All OT assets are reconfigured with new IP addresses as per IP schema.

9.3.6 MADINAH STP DESIGN

Following is the detailed architecture of NWC SCADA/OT environment at Madinah STP.

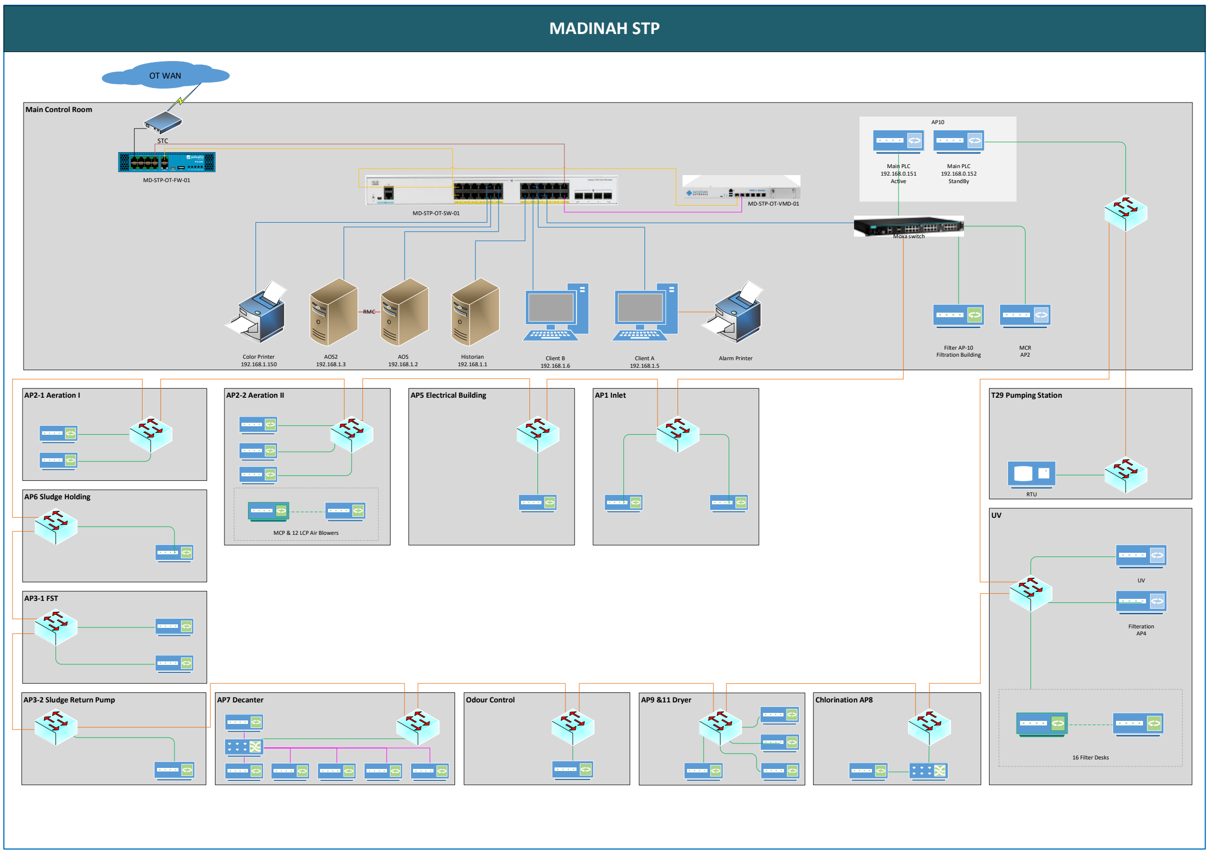


Figure 21 : Madinah STP Architecture

9.3.6.1 DESIGN DESCRIPTION

- Madinah STP Main Control Room cabinet has OT Ethernet switch, Nozomi and Firewall.
  - All the network cables from OT devices in control room is connected to OT Ethernet switch.

All OT assets are reconfigured with new IP addresses as per IP schema

10. OT APN

A dedicated, secure, private OT APN is provided and managed by the telecom company provides GSM/GPRS connectivity from BU offices to field sites/equipment.

10.1 MCBU OT APN DESIGN

In MCBU, PS5 and Mina branch offices each has one circuit that connects to the OT APN. The OT firewalls installed at these locations provides the security barrier between the OT APN and the assets at the location.

The OT APN for MCBU is dedicated to provide connectivity to all SIM-based devices in MCBU with a separate APN profile for all SIMs in the BU.

The APN profile for MCBU APN Cloud is “MakkahOT.M2M”

10.2 RCBU OT APN DESIGN

In RCBU, Exit-10 has one circuit that connects to the OT APN. The OT firewalls installed at all other locations provides the security barrier between the OT APN and the assets at those locations.

The OT APN for RCBU is dedicated to provide connectivity to all SIM-based devices in RCBU with a separate APN profile for all SIMs in the BU.

The APN profile for RCBU APN Cloud is "RCBUOT.M2M"

10.3 JCBU OT APN DESIGN

In JCBU, Faisalyah has one circuit that connects to the OT APN. The OT firewalls installed at all other locations provides the security barrier between the OT APN and the assets at those locations.

The OT APN for JCBU is dedicated to provide connectivity to SIM-based devices in JCBU with a separate APN profile for SIMs in the BU.

The APN profile for JCBU APN Cloud is "MakkahOT.M2M"

10.4 TCBU OT APN DESIGN

In TCBU, Al-Mathna has one circuit that connects to the OT APN. The OT firewalls installed at all other locations provides the security barrier between the OT APN and the assets at those locations.

The OT APN for TCBU is dedicated to provide connectivity to SIM-based devices in TCBU with a separate APN profile for SIMs in the BU.

The APN profile for TCBU APN Cloud is "TCBUOT.M2M"

10.5 MDCBU OT APN DESIGN

In MDCBU, Al Usbah has one circuit that connects to the OT APN. The OT firewalls installed at all other locations provides the security barrier between the OT APN and the assets at those locations.

The OT APN for MDCBU is dedicated to provide connectivity to SIM-based devices in MDCBU with a separate APN profile for SIMs in the BU.

The APN profile for MDCBU APN Cloud is "NWOT.M2M".

11. L0-1 DEVICE'S COMMUNICATION TYPES

Following are the types of communication:

- SIM to SIM TCP/IP Communication (Uses APN)
- APN to SIM TCP/IP Communication (Uses APN)
- SIM to SIM Direct communication (Does Not Use APN)

- Radio to radio direct communication

11.1 L0-1 DEVICE'S COMMUNICATION TYPES AT JCBU

There are four types of communication between L0-1 devices at JCBU:

- SIM to SIM TCP/IP Communication (Uses APN)
    - Data from Sofrel RTUs and T-BOX RTUs is received by Sofrel MTU and T-BOX MTU respectively over GSM/GPRS communication.
- APN to SIM TCP/IP Communication (Uses APN)
    - Data from the Slaves PLC (Modbus TCP) of Briman Phase-1 & 2 is transmitted over GSM/GPRS to PSB and Faisalyah Sites where data is received over APN-WAN by Wonderware SCADA Servers and Topkapi Servers acting as Master (Modbus TCP).
- SIM to SIM Direct communication (Does Not Use APN)
    - Gener, Sofrel MTU and Motorolla MTU SIM devices in Faisalyah are receiving data from Sofrel Data Loggers, Sofrel RTUs and Motorolla RTUs respectively, in one to one communication over GSM/GPRS.
- Radio to radio direct communication
    - T-Box and Motorolla MTUs in Faisalyah are receiving data from T-BOX and Motorolla RTUs from remote locations

11.2 L0-1 DEVICE'S COMMUNICATION TYPES AT TCBU

There are two types of communication between L0-1 devices at TCBU:

- SIM to SIM Direct communication (Does Not Use APN)
- Wavecom SIM device is receiving data from Sofrel Data Loggers in one to one communication over GPRS.
- Radio to radio direct communication
    - Motorolla MTUs in Al-Mathna is receiving data from Motorolla RTUs from remote locations.

12. LEVEL-1 DEVICES HARDENING AND CHANGES

Refer to the document "A01001045-RCBU-HDN-L1" for details of changes to be made on Level-1 devices in RCBU.

13. IP ADDRESS SCHEMA

The new IP Address Schema for NWC OT/SCADA system is provided in the document "A01001045-DLD-IPSCH".

14. ASSET INVENTORY

A comprehensive Asset Inventory database is provided as part of the DLD. Refer to the document "A01001045-INV".

The asset inventory contains all the equipment related to NWC OT/SCADA systems. The detailed information in the database includes:

- List of BUs
- List of Sites and sub-sites in each BU
- Detailed locations
- All Field Devices (IDs, Description, Location, Make, Model, Function, SIM details, IP Addresses, Firmware, Communication interfaces etc.)
- All Computer assets (IDs, Description, Location, Make, Model, Function, Operating System etc.)
- All software installed in computer assets
- All network assets
- Network ports details for all network assets
- Comprehensive IP Addresses list

15. FIREWALL ZONES AND POLICIES

Palo Alto NextGen firewalls are being implemented to provide network segmentation and zoning for the NWC OT infrastructure as per the design below.

- Different zones within HQ, MCBU and RCBU for network segmentation. See the document "A01001045-INV.01 D21" and sheet "FW_Zones" for list of zones.
- All network devices assigned to one of the zones.
- All traffic between zones is controlled through policies.
- All communication through the firewall is blocked by default.
- Specific policies are implemented to allow specific communication between defined zones/groups for defined applications.
- Dedicated access interfaces used for different security zones. VLANs configured to segregate the zones within the same office.
- Firewall management through central Panorama management and monitoring software.
- Refer to the document "A01001045-INV.01" and sheets "FW_Policies" and "FW_Zones" for detailed design of firewall zones and policies.

16. OT DOMAIN DESIGN

This section of the document describes an overall approach to implementing Active Directory services in NWC SCADA system. The primary goal of this design is to provide an Active Directory infrastructure which meet the authentication and administrative needs of the NWC SCADA environment, while keeping the segregation between OT and IT.

The NWC OT Active Directory environment is based on a single forest and a single domain. A single-domain design provides the following benefits:

- Less management overhead
- Single access management and DNS
- Central Domain administration

Here are the highlights of the OT domain design:

- Single domain for complete NWC SCADA environment.
- Primary domain controller in HQ OT-Domain Zone.
- Additional DCs in each BU main office.
- Further additional DCs in branch offices as required.
- The primary domain controller has all the five FSMO roles.
- Organizational units (OU’s) are created for each BU and objects from the BU’s are added to their respective OU’s. Policies are applied to each OU as required. This allows for granular management and control of security for devices and users in each BU.
- The design allows for independent operation of BUs without continuous connection with the HQ, while still allowing the flexibility to manage the domain centrally.

Refer to the document “A01001045-DLD-AD” for Detailed-Level-Design for OT domain in NWC.

17. REMOTE ACCESS

Considering the current requirements from NWC, our design provides remote access only within the OT environment. Remote access from IT or external networks is not provided.

Authorized users within the OT network will be able to connect to OT servers and workstations using remote desktop.

Here are the highlights of remote-access design.

- The Microsoft remote desktop service (RDS) is utilized for remote access solution within NWC SCADA network.
- An RD-Gateway server deployed in OT-Domain Zone provides central management and control of remote-access.
- The RD-Gateway is integrated with primary domain controller to manage remote access for all devices and users within the domain.

- Resource Authorization Policies (RAP) and Client Authorization Polices (RD CAP) implemented in the RD-Gateway provide a structured management and control of remote access.
- Connection to RD hosts is only allowed through RD gateway server.
- RD service is only allowed from computers on SCADA network.

Refer to the document “A01001045-DLD-RA” for Detailed-Level-Design for Remote Access in NWC.

18. END-POINT PROTECTION DESIGN

The End-Point Protection for SCADA Servers and Workstations is provided using McAfee EPP software. Below are the highlights of End-Point Protection design:

- A dedicated ePO Server deployed at Enterprise Level on the OT Management server.
- A Central ePO Server deployed on management server in OT-DMZ
- Super-Agents deployed at each BU’s Main Office to manage endpoint protection for all the nodes on all the sites in that BU.
- Local Agents are installed on each SCADA node.

Refer to the document “A01001045-DLD-EP” for Detailed-Level-Design for OT End-Point Protection in NWC.

19. PATCH MANAGEMENT DESIGN

Below are the highlights of Patch Management design:

- Patch Management for NWC SCADA system is performed using Microsoft Window Server Update Services (WSUS).
- A Central WSUS Server is deployed on management server in OT-DMZ.
- Additional WSUS Servers deployed at each BU’s Main Office to manage endpoint protection for all the nodes on all the sites in that BU.
- All SCADA nodes are configured to connect to the respective Patch Management server (through domain GPO).
- The patch management policies are configured on WSUS Server in OT-DMZ and synchronized to the WSUS Servers in BUs.

Refer to the document “A01001045-DLD-PM” for Detailed-Level-Design for Patch Management in NWC.

20. BACKUP MANAGEMENT DESIGN

This section describes the Backup Design for the OT assets in the NWC SCADA.

- Veritas BackupExec software installed in a three-tiered architecture is utilized for backup and restore services for SCADA system.
- A Central Administration Server (CAS) is installed in OT-DMZ.
- Managed BackupExec Server software is installed on the Management servers in each BU.
- All backup information is centralized on the CAS. Backup and restore plan for all BUs is configured at the CAS. The CAS then delegate the jobs to run on the managed Backup Exec server at the BUs.
- The managed Backup Exec servers at the BU perform the actual processing of backup and restore jobs for all nodes in the BU according to the backup plan.
- Primary backups are stored locally at the BU on storage connected to the Management server.
- Secondary backups are stored at the central backup server in OT-DMZ.

Refer to the document “A01001045-DLD-BM” for Detailed-Level-Design for OT Backup Management in NWC.

21. VULNERABILITY MANAGEMENT SYSTEM

Nozomi Networks Guardian-based solution provides vulnerability management system for SCADA network.

- A Nozomi Guardian Appliance is deployed at every major site to monitor the SCADA system for any vulnerabilities and detect any intrusions. It connects to the SPAN ports on SCADA core switches at each location to capture data and monitor data for any unwanted communications, any intrusions, unusual traffic flow etc.
- Centralized Management Console (CMC) is deployed in OT Management Zone for centralized management and monitoring of Nozomi Guardians installed in SCADA network. It also aggregates all ICS assets, vulnerabilities, and alerts in a single console and forwards the alerts to the SIEM solution at the enterprise.

22. ENTERPRISE HISTORIAN INTERFACE

Time-series historical data from SCADA needs to be provided to the enterprise historian. Following are the highlights of the Historian interface design.

- Tiered historian architecture provides OT historical data to enterprise Historian.
- Tier-1 Historians are installed at each BU, at different locations, to collect and store SCADA data.
- A Tier-2 Historian is installed at HQ OT-DMZ. All Tier-1 Historians synchronize the historical data with this Tier-2 Historian.
- The Tier-2 Historian communicates the historical data from all BUs to the enterprise Historian.

23. FILE TRANSFER FROM SCADA TO ENTERPRISE

Users at the OT/SCADA environment may need to transfer files from SCADA to enterprise network (e.g., reports etc.). Direct file transfer from OT to IT environment using Windows file transfer, shared folders, or through USBs exposes the SCADA system to threat vectors. Following design facilitates the transfer of files from SCADA to enterprise while minimizing the security risks.

SFTP SSH File Transfer Protocol, or Secure File Transfer Protocol, is a protocol packaged with SSH that works over a secure connection. The advantage is the ability to leverage a secure connection to transfer files and traverse the filesystem on both the local and remote system.

- A dedicated OT SFTP Server is installed in the Enterprise Level to receive the OT files. Users at the Enterprise Level have access to files on this server through a file share.
- An SFTP server is installed and configured in the OT-DMZ.
- SFTP Clients are installed on servers and workstations within each BU (as per business needs).
- Based on business requirements specified users are granted access to upload files from SCADA workstations and servers to SFTP Server in the OT-DMZ.
- The SFTP Server in the OT-DMZ uploads the files to the OT SFTP server in the Enterprise.
- SFTP clients at the Enterprise Level are not allowed to connect to the SFTP Server in OT-DMZ.

ACET SOLUTIONS

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