NWC OT Cybersecurity High-Level Design

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-HLD
Document Title:	NWC OT Cybersecurity High-Level Design
Document Version:	0
NWC Contract No.:	101200487
[atm] PO Ref.:	ATMPO2020-034

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

NOTES AND COPYRIGHTS

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

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

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

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

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

APPROVALS

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

REVISION HISTORY

Rev No.	Date	Author	Checked By	Approved By	Comments
0	07-Jan-2021	RAS	NR/SK	MM	IFA

GLOSSARY

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

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

REFERENCE DOCUMENTS

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

Table of Contents

1. DOCUMENT PURPOSE

The purpose of this document is to describe the High-Level Design (HLD) for SCADA/OT Cybersecurity implementation project at NWC. The document is divided into the following sections.

- Section-2 describes the key design principles and considerations taken into account for the HLD
- Section-3 describes the High-Level design.
- Section-4 summarizes the preliminary list of hardware, software, and network infrastructure required to implement the project.

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

This HLD 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. KEY DESIGN PRINCIPLES AND CONSIDERATIONS

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.

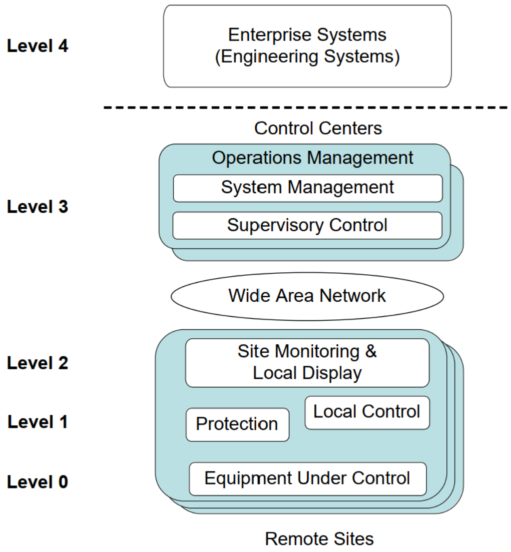


Figure 1 ISA-99 SCADA Reference Model (ISA–62443-1-1 –2007)

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 considered to be 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:

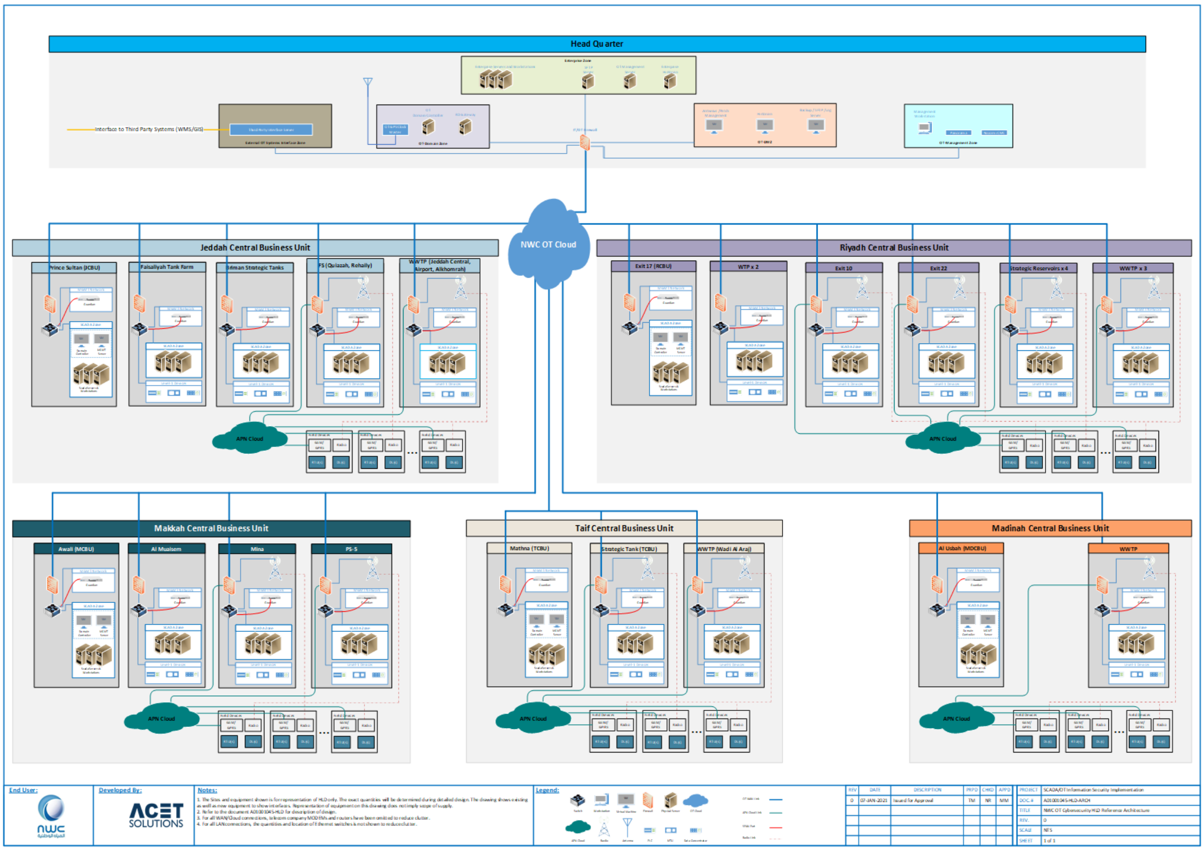
- Infrastructure team: Manages the SCADA servers, workstations, operating systems, and O/S related functions.
- Network team: Manages the SCADA network setup and devices, including interface with the telecom companies for the private cloud. Manages NWC SOC.
- Smart Operations: Operate the SCADA system 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. HIGH-LEVEL DESIGN (HLD)

This section describes the High-Level Design for NWC SCADA/OT Cybersecurity implementation project.

3.1 NWC SCADA REFERENCE ARCHITECTURE

Following is the reference architecture developed for NWC SCADA/OT environment.



A high-resolution version of the architecture is provided as an attachment (A01001045-HLD-ARCH).

Following description will help understand the key features of this SCADA reference architecture.

3.1.1 HEADQUARTER

- 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-DMZ

  - OT-Domain-Zone
  - OT-Management-Zone
- The zoning is achieved using VLANs, ACL, and routing.
- 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 one 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.

3.1.2 BU’S

- Each BU Main-office and its branch offices are part of one Security Zone.
- Each branch office is a sub-zone within the BU zone.
- The BU Main-office and each branch office will have multiple zones:
  - SCADA-Zone contains all required servers and workstations for the SCADA system (as applicable for each office). This includes Domain Controller, GR, AOS, DAS, Historian, OWS, EWS, Management Server.
  - 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 may be installed in the BU Main-Office and one or more Branch-Offices. It will contain 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.
- Each BU office may have an APN cloud circuit to provide connectivity to the GSM/GPRS devices. Refer to APN cloud section for details.
- 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 (if applicable)
  - Radio (TCP/IP only)

3.2 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.

3.3 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.

3.4 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. Each office location that requires GSM/GPRS communication with field equipment has one circuit that connects to the OT APN cloud. The OT firewall installed at each location provides the security barrier between the OT APN cloud and the assets at the location.

For example, in MCBU, only two offices need connection to GPRS/GSM devices, PS-5 and Mina. An APN circuit is therefore required for PS-5 and Mina. No APN circuit is needed at Awali and Moaisim locations.

The APN cloud is a common NWC-wide cloud that provides connectivity to all SIM-based devices in NWC. The cloud is shared by all NWC BUs. Separate APN profile for each BU provide the required communication segregation across BUs. In addition, the SIMs for each BU have IP addresses on separate subnets to provide logical segregation. The OT firewall at each office location is configured to allow communication from/to only the devices that belong to the same office.

3.5 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.

3.5.1 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.

3.6 END-POINT PROTECTION

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
- Additional ePO Servers 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.
- The EPP policies are configured on ePO Server in OT-DMZ and synchronized to the ePO Servers in BUs.
- At a predefined interval as defined by policies, new virus definitions are downloaded into ePO Server at Enterprise Level.
- Then the definitions are transferred to the ePO Server in OT-DMZ.
- The definitions are validated by the EPP administrator in ePO Server in OT-DMZ according to the procedure (e.g., approvals from SCADA vendors etc.).
- Once approved, the virus definitions are transferred to each BU's Management Server. The BU management Server updates the nodes within the BU with the new definitions.

- ePO on BU Management Server keeps a track of definition updates, virus scans and virus detection on each node in the BU level and provide the status to the Central ePO Server in OT-DMZ.
- The ePO Server in Enterprise Level is managed by OT administrators.

Following features are installed on each SCADA node:

- McAfee Endpoint Security Platform
- McAfee Adaptive Threat Protection
- McAfee Threat Prevention
- McAfee Device Control

3.7 PATCH MANAGEMENT

Below are the highlights of Patch Management design:

- Patch Management for NWC SCADA system is performed using Microsoft Window Server Update Services (WSUS).
- A dedicated WSUS Server is deployed at Enterprise Level on the OT Management server.
- 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.
- At a predefined interval as defined by policies, new patches and updates are downloaded into WSUS Server at Enterprise Level.
- The patches are then transferred to the WSUS Server in OT-DMZ.
- The patches are validated by the administrator in WSUS Server in OT-DMZ according to the procedure (e.g., approvals from SCADA vendors etc.).
- Once approved, the patches are transferred to each BU's Management Server. The BU management Server updates the nodes within the BU with the new patches. Manual intervention is required to plan/coordinate the installation and any system reboots.
- WSUS on BU Management Server keeps a track of updates on each node in the BU level and provide the status to the Central WSUS Server in OT-DMZ.
- The WSUS Server in Enterprise Level is managed by OT administrators.

3.8 BACKUP DESIGN

This section is 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.
- Additionally, these backups may be pushed to enterprise backup systems as required per the backup policy.

3.9 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.

3.10 TIME SYNCHRONIZATION

Accurate time synchronization is critical for the SCADA system operation and management. Historians use timestamps to store time-series data. System and network monitoring alerts require accurate timestamps to ensure logs can be correlated correctly.

Here is how time synchronization is achieved within the SCADA environment.

- A dedicated OT GPS Clock Master is installed at the OT-Domain Zone at the HQ.
- The OT Primary Domain Controller (PDC) synchronizes its time with the OT GPS Clock Master.

- The PDC acts as the NTP time server for Additional Domain Controllers (ADC) at the BUs.
- The ADC at each BU acts as the NTP time server for all devices within the BU.
- The devices in OT-DMZ synchronize the time with the OT GPS Clock Master.

3.11 LOG AND ALERTS MANAGEMENT

Logs and alerts from SCADA need to be communicated to the SIEM Solution at Enterprise Level. Below are the highlights of how this will be achieved.

- A logs collection software is installed on management server in every BU main office.
- The log collection software in BU Main Office collect logs from devices on all the local sites and forwards these logs to the SIEM Solution at Enterprise Level through OT-DMZ.
- Logs from all Palo Alto NGFWs are collected by Panorama in OT Management Zone and communicated to the SIEM Solution at Enterprise Level.
- Logs from Nozomi Guardian Appliances are collected by Virtual CMC in OT-Management Zone and communicated to the SIEM Solution at Enterprise Level.

3.12 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.

3.13 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.

3.14 STANDALONE DEVICE MANAGEMENT

Below is the design to integrated/manage standalone OT computers and laptops into the OT domain.

- All standalone, preauthorized OT computers (laptops etc.) are to be configured to join the OT domain, even if these are not permanently connected to the network.
- Appropriate policies are configured in the domain for such computers will apply.
- These computers must regularly join the OT domain in a predefined interval to monitor and enforce policies.
- Only pre-authorized computers are allowed to join the OT domain. BYOD or non-OT systems are not allowed.

3.15 EXTERNAL OT SYSTEMS INTERFACE

An External OT Systems Interface Zone in HQ allows for any external OT systems to connect to NWC SCADA network. The exact communication method and interface design will depend on the type of system connected. Examples of such systems include:

- GIS
- WMS

4. HARDWARE/SOFTWARE/NETWORK REQUIREMENTS

Following is a summary of hardware, software, and network infrastructure required for implementing SCADA Cybersecurity based on the High-Level Design. Note that this is a preliminary list which may change based on the detailed design.

S/N	Description	Quantity
HQ		
1	IT/OT interface firewall (redundant)	2
2	Total Hosts	3
3	*Host for OT Domain Zone*	*1*
4	*Host for DMZ*	*1*
5	*Host for Management Zone*	*1*
6	Total VMs	6
7	*VM for Antivirus and Patch Management*	*1*
8	*VM for Backup solution and SFTP Server*	*1*
9	*VM for Panorama*	*1*
10	*VM for Virtual CMC*	*1*
11	*VM for Domain controller*	*1*
12	*VM for RD gateway*	*1*
MCBU		
13	BU interface firewalls (one for each site)	4
14	Host for ADC and MGMT VM	1
15	VM for MGMT Server	1
16	Nozomi Guardian Appliances	4
RCBU		
17	BU interface firewalls (one for each site)	12
18	Host for ADC and MGMT VM	1
19	VM for MGMT Server	1
20	Nozomi Guardian Appliances	12
TCBU		
21	BU interface firewalls (one for each site)	3
22	Host for ADC and MGMT VM	1
23	VM for MGMT Server	1
24	Nozomi Guardian Appliances	3
JCBU		
25	BU interface firewalls (one for each site)	9
26	Host for ADC and MGMT VM	1
27	VM for MGMT Server	1
28	Nozomi Guardian Appliances	9
MDCBU		
29	BU interface firewalls (one for each site)	2
30	Host for ADC and MGMT VM	1

S/N	Description	Quantity
31	VM for MGMT Server	1
32	Nozomi Guardian Appliances	2
Software		
33	McAfee EPP licenses for all SCADA nodes	As Required
34	Veritas BackupExec agent licenses for all SCADA nodes	As Required
35	Veritas BackupExec Servers licenses for BUs	5
36	Veritas BackupExec Central Administration Server	1
37	Remote Desktop CALs	As Required
38	Nozomi CMC	1
39	Palo Alto Panorama software	1
40	Log collection software	As Required
41	Windows Operating System licenses	As Required
42	SFTP Server license	2
Network Requirements		
43	OT Cloud circuits	1 at each office
44	APN Cloud circuits (at each office which needs access to SIM-based devices	As Required

Notes:

- Quantities marked “As Required” will be finalized during detailed design.
- The list and quantities are provided here to summarize the requirements and does not constitute commitment to supply by any party.

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