NWC OT Cybersecurity SCADA Application Minimum Baseline Security Standard

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-MBSS-SCADA
Document Title:	NWC OT Cybersecurity SCADA Application Security Minimum Baseline Security Standards
Document Version:	0
NWC Contract No.:	101200487
[atm] PO Ref.:	ATMPO2020-034

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

NOTES AND COPYRIGHTS

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

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

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

APPROVALS

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

REVISION HISTORY

Rev No.	Date	Author	Checked By	Approved By	Comments
00	February 17, 2022	MA	SK	MM	Issued For Approval

GLOSSARY

Acronyms	Meaning
ACL	Access Control Lists
AD	Active Directory
ADC	Additional Domain Controller
AST	Advance System and Technology
ATP	Adaptive Threat Protection
BOM	Bill of Material
BU	Business Unit
BYOD	Bring Your Own Device
CAP	Client Authorization Policy
CAS	Central Administration Server
CIP	Critical Infrastructure Protection
CMC	Central Management Console (Nozomi)
CSMS	Cyber Security Management System
DCS	Distributed Control System
DLD	Detailed-Level Design
DMZ	Demilitarized Zone
DNS	Domain Name System
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
MBSS	Minimum Baseline Security Standards
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
OT	Operational Technology
PDC	Primary Domain Controller
PLC	Programmable Logic Controller
RPO	Recovery Point Objective
SCADA	Supervisory Control and Data Acquisition

Acronyms	Meaning
SIEM	Security Incident & Event Management Solution
SSL	Secure Socket Layer
TCBU	Taif Central Business Unit
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network

REFERENCE DOCUMENTS

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

Table of Contents

1. Document Purpose 7

2. General Requirements 7

1. DOCUMENT PURPOSE

The purpose of this document is to describe the minimum baseline security standard for SCADA Application.

2. General Requirements

The following application features shall be configured wherever possible:

- Application(s)/ software that are approved shall be installed in NWC OT environment.
- Application shall be configured to utilize Active Directory based unique user credentials (where applicable) for application launch and configuration.
- Applications that don't support integration with Active Directory, a dedicated local user accounts shall be created (after proper approval and authorization) on application hosted server.
- Enforce password policy wherever applicable within the application, all exceptions shall be documented and implemented after proper approval and authorization.
- Implement user lock-out for failed login attempts in applications wherever applications offer such features.
- Using Principles of Least Privilege Access user accounts shall be created based on role and function of users for all applications.
- Application user identity within OT environment shall never be same as IT environment.
- Implement audit controls such as logging and monitoring of system access and modification.
- Aggregate system logs and conduct frequent review of application and systems events.
- Use of service accounts with least privileges.
- Intra/Inter Application(s) Communication shall be encrypted as per Vendor recommendation.
- Application shall be configured for user inactivity time-out wherever applicable.
- Secure Programming Practices for SCADA Applications shall be followed wherever applicable.
    - *Input Validation:* Ensure that the data enters the system from the trusted sources only. Be suspicious of the most external data sources, validate all client provided data before processing inclusive of the URLs and HTTP content.
    - *Architect and design for security policies:* Enforce security policies within the application/software by designing it appropriately.

- *Adhere to the principle of least privilege:* Execute the processes within the application shall execute with least privileges to complete the job. Elevated permissions shall be provided for defined amount of time if required.
- *Authentication and Authorization:* Code the applications effectively following the principles of authentication and authorization, only authorized persons can access the application for defined rights.
- *Modelling threats*: Use threat modeling wherever needed to anticipate the threats to which the software will be subjected. Threat modeling involves identifying key assets, decomposing the application, identifying and categorizing the threats to each asset or component, rating the threats based on a risk ranking, and then developing threat mitigation strategies that are implemented in designs, and code.
- *Sanitize data sent to other systems:* Sanitize data passed to all complex systems to ensure their safety and security.
- *System Configuration:* Clear your system of any unnecessary components and ensure all working software is updated with latest version and patches.
- *Cryptographic Practices:* Use quality modern cryptographic algorithms with keys stored in key vaults to increase the security of your code.
- *Error Handling and Logging:* Document and log all the failures or errors in the code to minimize their impact and preventing any catastrophic failure.
- *Access Control:* Take a default deny approach for all the sensitive data. Limit privileges and restrict access to secure data to only users who need it.
- *Password Management:* Disable password entry after multiple incorrect login attempts. Passwords for the applications should be of adequate length, complexity and should be changed periodically.
- *Output Encoding:* Outline a standard routine for output encoding, sanitize all output of an untrusted data to queries and operating systems
- *Communication Security:* Implement encryption for transmission of all sensitive data/information. Inclusion of TLS for connection protection

- Database Security
  - All unused or unnecessary services or functions of the database shall be removed or turned off.
  - Unneeded default accounts are removed, or else passwords shall be changed from defaults.
  - Null passwords shall not be used, and temporary files from the install process that may contain passwords shall be removed.
  - Database software shall be patched to include all current security patches. Provisions shall be made to maintain security patch levels in a timely fashion.
  - Strongly typed parametrized queries shall be used.

- Unnecessary default Vendor Content such as sample schemas shall be removed.
- Authentication Modes shall be used for database security.
- Minimum user privileges shall be applied for securing database.

- Security of Proprietary Protocols shall be applied for secure communications.
  - Following is the list of proprietary protocols for SCADA:
    - Proprietary
- Application Protection
  - Development environment/Applications shall be password protected wherever applicable.
  - Authorization and logging controls shall be implemented wherever applicable.
  - Configuration of authentication as per users shall be enabled wherever applicable.
  - Applications shall be periodically patched to avoid vulnerabilities.
- Application Configuration Security
  - Dedicated Service accounts shall be used for the configuration of applications.
  - Access level for users and roles shall be defined for using the application.
  - All unnecessary functionalities and files shall be removed.
- Refer to standards Appendix (A01001045-MBSS-SCADA-APP.00) for Vendor Specific Secure Application Configuration.

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