شركة المياه الوطنية
National Water Company

ACET SOLUTIONS

# NWC OT Cybersecurity L0-1 Devices Minimum Baseline Security Standard

## National Water Company (NWC), KSA

## SCADA/OT Information Security Implementation Project

| | |
|---|---|
| Document Number: | A01001045-MBSS-L1 |
| Document Title: | NWC OT Cybersecurity L0-1 Devices Minimum Baseline Security Standard |
| 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<br>(Project Director) | ACET Solutions | | |
| Abdulhadi G. Alshammari<br>(Project Manager) | NWC | | |
| Ahmed I. Almutairi<br>(Project Sponsor) | NWC | | |

# REVISION HISTORY

| Rev No. | Date | Author | Checked By | Approved By | Comments |
|---|---|---|---|---|---|
| 00 | January 28, 2022 | MA | SK | MM | Issued For Approval |
| | | | | | |
| | | | | | |
| | | | | | |

# GLOSSARY

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

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

# REFERENCE DOCUMENTS

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

# Table of Contents

# 1. DOCUMENT PURPOSE

The purpose of this document is to describe the minimum baseline security standard for L0-1 Devices in NWC.

# 2. GENERAL SECURITY REQUIREMENTS

Following are the features that shall be configured on L0-1 devices as per their applicability:

- L0-1 Device firmware shall be upgraded upon discovery of vulnerability as per vendor recommendation.
- L0-1 device firmware shall be upgraded to the latest version on periodic basis.
- L0-1 device shall be configured as per vendor-recommended secure configurations.
- L0-1 device default configurations shall be changed as per vendor recommendation.
- L0-1 device shall have the following access control features implemented wherever applicable:
    - Password protection
    - Application security
    - Physical security
        - Panel lock requirements
        - Panel location requirements
- L0-1 device shall only be programmed with vendor recommended and certified Programming Software/Tool.
- L0-1 device shall be programmed utilizing following secure coding practices, where applicable.
    - *Modularize Code:* Split L0-1 Device code into modules, using different function blocks (sub-routine), Test modules independently
    - *Track Operating Modes:* Keep the L0-1 Device in RUN mode. If device is not in RUN mode, there should be alarm to the Operators.
    - *Leave Operational Logic in the L0-1 Device wherever feasible:* Leave as much operational logic e.g., totalizing or integrating, as possible directly in the L0-1 device. The HMI doesn’t get enough update to do this well.
    - *Use L0-1 Device Flags as Integrity Checks:* Put counters on L0-1 device flags (wherever applicable) to capture any math problems
    - *Use Cryptographic and/or Checksum Integrity Checks for L0-1 device Code:* Use cryptographic hashes and/or checksums (wherever applicable). If cryptographic hashes are unavailable, to check L0-1 device code integrity and raise an alarm when they change.
    - *Validate and Alert Paired Inputs/Outputs:* If Inputs and Outputs in L0-1 Device are paired, then ensure that both signals are not asserted together. Alarm the

operator when Inputs and Outputs states occur that are physically not feasible. It is recommended to make Inputs and Outputs independent or add delay timers or other function, to remedy toggling Outputs due to toggling Inputs which could damage Actuators.

- *Validate HMI Input Variables at L0-1 Device Level, not only at HMI:* HMI access to L0-1 Device variables can (and should) be restricted to a valid operational value range at the HMI, but further cross-checks in L0-1 device should be added to prevent, or alert on, values outside the acceptable ranges which are programmed into the HMI.
- *Validate Indirections:* Validate indirections by poisoning array ends to catch fence-post errors.
- *Assign Designated Register Blocks by Function (Read/Write/Validate):* Assign designated register blocks for specific functions in order to validate data, avoid buffer overflows and block unauthorized external writes to protect controller data.
- *Instrument for Plausibility Checks:* Instrument the process in a way that allows for plausibility checks by cross-checking different measurements.
- *Validate Inputs based on Physical Plausibility:* Ensure operators can only input what's practical or physically feasible in the process. Set a timer for an operation to the duration it should physically take. Consider alerting when there are deviations. Also alert when there is unexpected inactivity.
- *Disable unneeded/unused Communication ports and protocols:* L0-1 devices network interface modules generally support multiple communication protocols that are enabled by default. Disable ports and protocols that aren't required for the application.
- *Restrict Third-party Interfaces:* Restrict the type of connections and available data for 3rd Party interfaces. The connections and/or data interfaces should be well defined and restricted to only allow read/write capabilities for the required data transfer.
- *Define a Safe Process State in case of L0-1 Device Restart/Failure:* Define safe states for the process in case of L0-1 Device restarts (e.g. energize contacts, de-energize, keep previous state & etc.)
- *Summarize L0-1 Device Cycle Times and Trend them on HMI:* Summarize the L0-1 Device Cycle Time every 2-3 seconds (if applicable) and report to HMI for visualization on a graph.
- *Log L0-1 Device Uptime and Trend it on the HMI:* Log L0-1 Device uptime to know when it's been restarted. Trend and log uptime on the HMI diagnostics.
- *Monitor L0-1 Device Hard Stops and Trend them on HMI:* Store L0-1 Device Hard Stop events from faults or shutdowns for retrieval by HMI alarm systems to consult before L0-1 Device restarts.

  - *Perform Time Sync of L0-1 Device:* For accurate logging of L0-1 Device events and ensure time sync is properly implemented.
  - *Monitor L0-1 Device Memory Usage and Trend it on HMI:* Measure and provide a baseline of memory usage for every L0-1 Device deployed in the production environment and trend it on HMI.
  - *Trap false negatives and false positives for critical alerts:* Identify critical alerts and program a trap for those alerts. Set the trap to monitor the trigger conditions and alert state for any deviation.

- L0-1 device shall not be connected with any type of portable storage where applicable.
- L0-1 device shall not be connected to internet by any means.
- L0-1 device changes such as code change, configuration, & etc., shall be following NWC OT Change Management procedures.
- L0-1 device unused ports shall be disabled (wherever applicable).
- L0-1 device unused ports shall be locked using mechanical port lockers.
- L0-1 device unused network services (wherever applicable) shall be deactivated i.e., ftp, http, etc.
- L0-1 devices on remote networks shall be connected to on-premises L0-1 network using Firewall/Layer-3 Switches/Routers with ACL capability.
- L0-1 devices shall be in Active Product Lifecycle Phase, so that any vulnerabilities discovered are patched by device vendors and relevant patches are installed.
- Refer to standards Appendix (A01001045-MBSS-L1-APP.00) for Vendor Specific Device 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