NWC OT Cybersecurity Backup and Restore Plan

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-PLN-BM
Document Title:	NWC OT Cybersecurity Backup and Restore Plan
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	24-02-2022	SM	SK	MM	Issued for Approval

GLOSSARY

Acronyms	Meaning
CAS	Central Administration Server
LAN	Local Area Network
MBES	Managed Backup Exec Server
OT WAN	Operational Technology Wide Area Network
SCADA	Supervisory Control and Data Acquisition

REFERENCE DOCUMENTS

S/N	Document No.	Title
1	A01001045-HLD.00	NWC OT Cybersecurity High-Level Design
2	A01001045-INV.00	NWC SCADA Asset Inventory
3	A01001045-DLD-BM.00	NWC OT Cybersecurity Backup Management Detailed Design
4	A01001045-DLD-BM-APP1.00	Backup Plan
5	ECC – 1: 2018	KSA NCA Essential Cybersecurity Controls (ECC – 1: 2018)
6	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

Table of Figures

1. DOCUMENT PURPOSE

This document serves as a backup and restore for the NWC SCADA. It lists all the installations and configurations required to implement the Backup solution using the Veritas BackupExec software solution in a tiered structure.

2. OBJECTIVES

- Serves as a guide for NWC OT data backup teams
- References and points to the location(s) of backed-up data, systems, applications and other mission-critical data resources
- Provides procedures and resources needed to back up data, systems and other resources
- Minimizes operational disruptions by documenting, testing and reviewing data backup procedures
- Identifies alternate sources for data backup activities
- Documents data storage, backups and retrieval procedures for vital records and other relevant data

3. BACKUP POLICY

1. A formal procedure of backup and recovery shall be identified, documented, and implemented within all NWC.
2. The formal backup plan shall ensure that backup and restoration requirements of each system determine:
    a. The type of backups to be performed,
    b. The periodicity or schedule of the backup,
    c. The protection to be provided to backup media based on the criticality of the information backed up.
3. All OT applications and operating systems software, data (including databases), user configuration information, system logs and hardware configuration information (where applicable) shall be backed up and restored in accordance with the Backup and Restoration Procedure.
4. A formal time period for backup shall be documented and defined.
5. The backup media shall be replaced immediately after encountering an error or at predefined time intervals whichever is earlier.
6. The backup media shall be appropriately labeled and numbered automatically by the backup system or manually by the administrator taking the backup.
7. Backup Storage shall meet the following requirement:

a. On-site: On-site data backup shall be maintained in safe custody, preferably outside the server room and in a fireproof cabinet.

b. Off-site: Off-site whenever, the backup media is moved to and from an off-site location, it shall be carried in a sealed and tamper-proof bag.

8. Backups shall be stored securely on-premises and off-premises. Recovery of OT Asset shall be tested using Backup at frequent intervals.
9. Backup that contains sensitive information shall be encrypted (where applicable).
10. Access to Backups shall be controlled and only after proper management approval and authorization backup access shall be granted.
11. L0-1 Device Backups (i.e., Configuration & Application) shall be collected using vendor recommended procedures.
12. Network Device Backups (i.e., Configuration) shall be collected using vendor recommended procedures.
13. Recovery Procedures of an OT Asset shall prepare based on vendor recommendations.
14. Testing of OT Asset Recovery shall be performed after proper management approval and authorization.
15. Recovery Test Log shall be maintained and audited periodically.
16. Recovery of an OT Asset shall be performed after proper management approval and authorization as part of Incident Response.

4. BACKUP SOLUTION DEPLOYMENT PLAN

Veritas BackupExec Gold edition is being installed and configured in the NWC-SCADA. A01001045-DLD-BM.01, contains all the pre-requisites for the servers and machines for backup solution.

Two main designs are proposed in the following section. Both are based upon the licensing. The backup and restore strategy is attached in *Appendix A.*

4.1 PLAN A (MBES IN MAIN BU ONLY)

The Veritas BackupExec CAS and MBES is installed in HQ. Another MBES is installed in each BU and the agents will be installed on each site. These agents push the backup job to their respective MBES and store the backed-up fil in the attached storage.

Since the requirement is 130MBps of Veritas BackupExec and OT WAN bandwidth is limited to 10Mbps, an increased bandwidth of OT WAN is required for successful execution of the backup jobs.

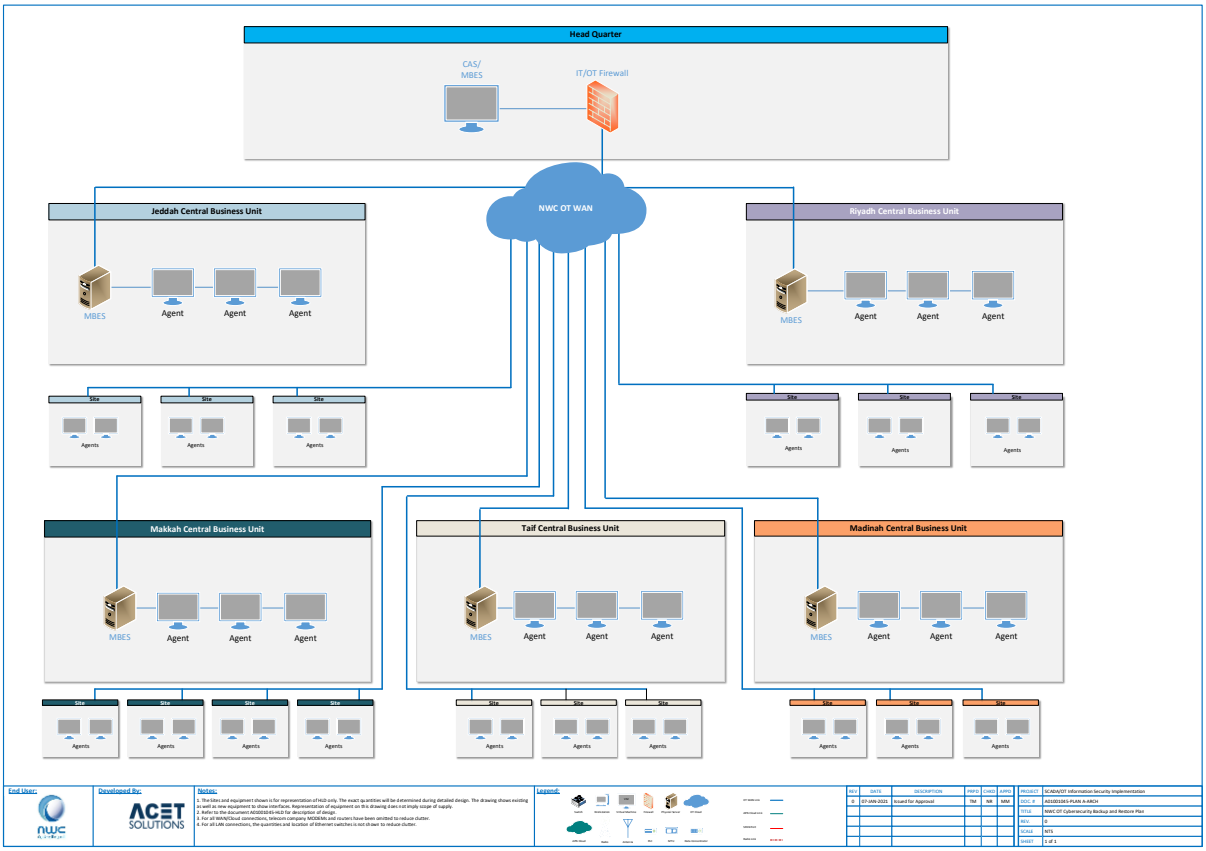

Figure 1 Plan A for Backup and Recovery

4.2 PLAN B (MBES IN ALL MAIN SITES)

To cater OT WAN bandwidth limitation in Plan A, the Veritas BackupExec CAS and MBES server is installed in HQ NWC. A dedicated VM is installed at each site requiring additional infrastructure. Agents are installed on each machine on site to be backed up. Since the machines and MBES are on the same LAN, backup jobs can be executed successfully and stored in the pointed location.

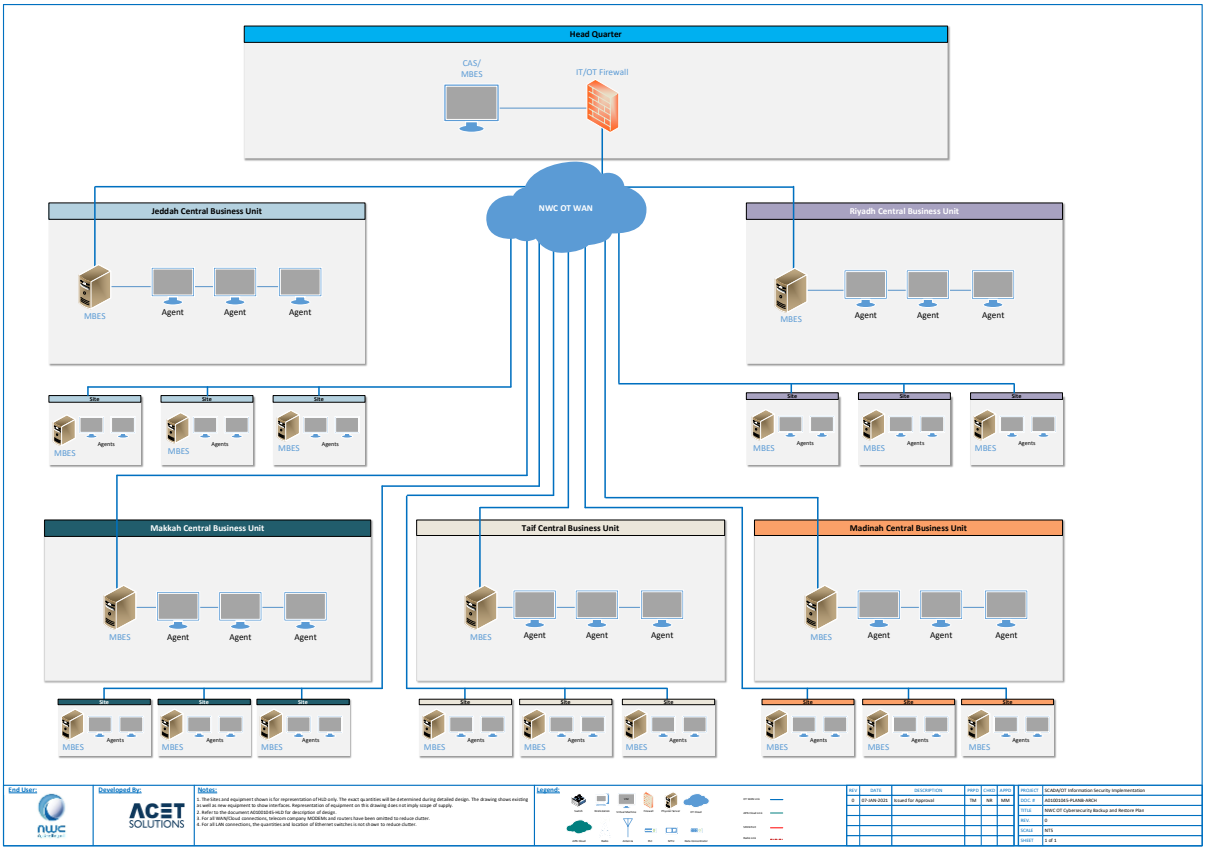

Figure 2 Plan B for Backup and Recovery

5. BACKUP OF SCADA SYSTEMS

For all systems, files backed up, shall be removed after taking backup with automatically for storage availability for the new file.

5.1 BACKUP OF WONDERWARE GALAXY REPOSITORY

Backup Source: GR Server (either VM/Physical Server)

- *"D:\SCDAppBKUP\<SCADA_GR_Name_date>.cab"*

Recovery Point Objective: 1 week

Backup Source Configuration:

Wonderware is configured to generate Galaxy Repository backup file (".cab") automatically weekly at following location:

D:\SCDAppBKUP\<SCADA_GR_Name_date>.cab

MBES Job Configuration:

MBES job is created with following attributes:

Backup Job: Full & Automatic

Backup Folder: "D:\SCDAppBKUP\"

Backup Frequency: Weekly

Backup Storage: MBES Storage

Special Conditions:

a. *MBES Jobs must be scheduled after completion of Wonderware GR ".cab" file generation.*

b. *Post-Backup Actions: Delete ".cab" files after successful backup*

5.2 BACKUP OF WONDERWARE HISTORIAN

Backup Source: Historian Server (either VM/Physical Server)

a. SQL Runtime Database
    a. *"C:\Program Files\Microsoft SQL Server\MSSQLn.MSSQLSERVER\MSSQL\Backup\"*
b. Historian Circular DATA folder
    a. C:\Historian\Data

Recovery Point Objective: 1 week

Backup Source Configuration:

Using SQL Management Studio, a SQL job is created to periodically and automatically backup Historian SQL Runtime Database to default backup location.

"C:\Program Files\Microsoft SQL Server\MSSQLn.MSSQLSERVER\MSSQL\Backup\"

Where n= number of server instance

MBES Backup Jobs Configuration:

1st MBES job is created with following attributes:

Backup Job: Full & Automatic

Backup Folder: "C:\Program Files\Microsoft SQL Server\MSSQLn.MSSQLSERVER\MSSQL\Backup\"

Backup Frequency: Weekly

Backup Storage: MBES Storage

Backup Retention: 2 weeks

Special Conditions:

a. *MBES Jobs must be scheduled after completion of SQL Backup Job.*

b. *Pre-Backup Actions: Backup Only latest database file*

c. *Post-Backup Actions: Delete database files on successful backup*

2nd MBES job is created with following attributes:

Backup Job: Full

Backup Folders: "C:\InSQL\Data\" for wonderware ver < 9.0

Or "C:\Historian\Data" for Wonderware ver => 10.0

Backup Frequency: Weekly

Backup Storage: MBES Storage

Backup Retention: 2 weeks

5.3 BACKUP OF WONDERWARE DAS

Backup Source: DAS Server (either VM/Physical Server)

" *C:\ProgramData\Wonderware\OI-Server\$Operations Integration Supervisory Servers$"*

For DAS, Backup Source folder will be copied using script in schedule manner using Windows Task Scheduler to Galaxy Repository Server:

- "D:\eSCDAppBKUP\<DASHostName>\"

Refer to "A01001045-PLN-BM-APP2.00" for automatic secure copy details.

Recovery Point Objective: 6 months

Backup Source Configuration:

Upon configuration of DAServer, SMC auto creates running ".aaCFG". It is recommended to create manually create "Archive Configuration Set" periodically. It'll create duplicate copy of running ".aaCFG" file and store at same location.

Steps to create "Archive Configuration Set"

a. Open SMC

b. Expand DAServer Manager

c. Expand Default Group

d. Expand local

e. Right Click on Archestra.[DA Server Manager Name].[x] and Click on Archive Configuration Set

MBES Backup Job Configuration:

Since all files are moved to "D:\eSCDAppBKUP"*

Thus, additional job shall be created on GR to Backup DAS folders.

Backup Job: Full & Automatic

Backup Folder: " D:\eSCDAppBKUP\<DASHostname> \"

Backup Frequency: 6 Months

Backup Storage: MBES Storage

Backup Retention: 1 year

Special Conditions:

a. *MBES Jobs must be scheduled after completion of Basic Task executed by Windows Task Scheduler.*

b. *Post-Backup Actions: Delete files on successful backup*

6. RECOVERY OF SCADA SYSTEMS

6.1 RECOVERY OF WONDERWARE GALAXY REPOSITORY

Recovery Location: GR Server (either VM/Physical Server)

- *"D:\SCDAppBKUP\<SCADA_GR_Name_date>.cab"*

Recovery Time Objective: 1 week

MBES Recovery Job Configuration:

MBES recovery job is created with following attributes:

Recovery Job: Manual

Recovery Folder: "D:\SCDAppBKUP\"

Recovery Frequency: NA

Recovery from Backup Storage: MBES Storage

6.2 RECOVERY OF WONDERWARE HISTORIAN

Recovery Location: Historian Server (either VM/Physical Server)

a. SQL Runtime Database

    a. *C:\Program Files\Microsoft SQL Server\MSSQLn.MSSQLSERVER\MSSQL\Backup*

b. Historian Circular DATA folder

    a. "C:\InSQL\Data" for wonderware ver < 9.0

    b. "C:\Historian\Data" for Wonderware ver => 10.0

Recovery Time Objective: 1 week

MBES Recovery Jobs Configuration:

1st MBES Recovery job is created with following attributes:

Recovery Job: Manual

Recovery Folder: "C:\Program Files\Microsoft SQL Server\MSSQLn.MSSQLSERVER\MSSQL\Backup\"

Recovery Frequency: NA

Recovery from Backup Storage: MBES Storage

2nd MBES recovery job is created with following attributes:

Recovery Job: Manual

Recovery Folders:

"C:\InSQL\Data" for wonderware ver < 9.0

Or "C:\Historian\Data" for Wonderware ver => 10.0

Recovery Frequency: NA

Recovery from Backup Storage: MBES Storage

6.3 RECOVERY OF WONDERWARE DAS

Recovery Location: DAS Server (either VM/Physical Server)

- "*D:\eSCDAppBKUP\<DASHostname>*"

Recovery Time Objective: 4 hrs

MBES Recovery Job Configuration:

Recovery Job: Manual

Recovery Folder: "D:\eSCDAppBKUP\<DASHostName>\"

Recovery Frequency: NA

Recovery from Backup Storage: MBES Storage

Post restore of DAS folder, DAS folder can be moved to DAS Server either via SFTP or Manually.

APPENDIX A

A01001045-PLN-BM-APP1.00 contains the backup and restore strategy based upon RTOs and RPOs.

APPENDIX B

A01001045-PLN-BM-APP2.00 contains the procedure for configuring SSH to move DAS file to GR for backup.

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