



Memorandum from the Office of the Inspector General

June 17, 2024

Allen A. Clare
Tammy W. Wilson

**REQUEST FOR MANAGEMENT DECISION – AUDIT 2023-17433 – OPERATIONAL
TECHNOLOGY CYBERSECURITY – COMBINED CYCLE PLANT**

Attached is the subject final report for your review and management decision. Your written comments have been incorporated into the report. You are responsible for determining the necessary actions to take in response to our findings. Please advise us of your management decision within 60 days from the date of this report. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance.

If you have any questions or wish to discuss our findings, please contact Andrew J. Jurbergs, Senior Auditor, at (865) 633-7393 or Sarah E. Huffman, Director, Information Technology Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)

AJJ:KDS

Attachment

cc (Attachment):

TVA Board of Directors
Brett A. Atkins
Janda E. Brown
Kenneth C. Carnes II
Sherri R. Collins
Samuel P. Delk
Buddy Eller
David B. Fountain
Greg G. Jackson
T. Daniel Lunsford
Jeffrey J. Lyash

Jill M. Matthews
Todd E. McCarter
Donald A. Moul
Dustin C. Pate
Ronald R. Sanders II
John M. Thomas III
Josh Thomas
Ben R. Wagner
Kay W. Whittenburg
OIG File No. 2023-17433



Office of the Inspector General

Audit Report

To the Senior Vice President,
Power Operations and to the
Vice President and Chief
Information and Digital Officer,
Technology and Innovation

OPERATIONAL TECHNOLOGY CYBERSECURITY – COMBINED CYCLE PLANT

Audit Team

Andrew J. Jurbergs
Jonathan S. Gibson
Frank B. Lord
Scott A. Marler
Megan S. Spitzer

Audit 2023-17433
June 17, 2024

ABBREVIATIONS

IT	Information Technology
NIST	National Institute of Standards and Technology
OT	Operational Technology
SSP	System Security Plan
TVA	Tennessee Valley Authority

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
BACKGROUND.....	1
OBJECTIVE, SCOPE, AND METHODOLOGY	2
FINDINGS	3
CONTINGENCY PLANS NOT DOCUMENTED	3
OT INVENTORY INCOMPLETE	3
SYSTEM BASELINES NOT IN PLACE.....	4
CYBERSECURITY MONITORING INCOMPLETE	4
RISK ASSESSMENT NOT CONDUCTED	4
RECOMMENDATIONS	5

APPENDIX

MEMORANDUM DATED JUNE 13, 2024, FROM ALLEN CLARE AND TAMMY WILSON TO DAVID P. WHEELER



Audit 2023-17433 – Operational Technology Cybersecurity – Combined Cycle Plant

EXECUTIVE SUMMARY

Why the OIG Did This Audit

Power plants rely on operational technology (OT)ⁱ to ensure the plants can run without disruption. OT encompasses a large range of programmable systems that interact with and manage the physical environment. OT cybersecurityⁱⁱ is essential to the reliable operation of modern industrial processes. Implementing logical, physical, and general security controls can reduce the risk of cyber threats to OT systems.

Due to the high risks associated with threat events against OT, we performed an audit of the Tennessee Valley Authority's (TVA) OT cybersecurity at a combined cycle plant. Our objective was to determine if logical, physical, and general security controls were (1) appropriately designed to reduce cybersecurity risk and (2) operating effectively. The scope of this audit was limited to the OT at one combined cycle plant.

What the OIG Found

We reviewed logical, physical, and general security controls and determined the following areas were appropriately designed and operating effectively:

- Logical controls used to manage logical system protection.
- Physical controls used to manage personnel access to areas of the plant with OT systems.
- General controls used to provide awareness and training as well as security authorization.ⁱⁱⁱ

However, we found the following general security control deficiencies that were significant to our audit objective:

- Contingency plans were not documented.
- OT inventory was incomplete.

ⁱ OT systems and devices monitor or control industrial processes or events.

ⁱⁱ OT cybersecurity is the application of cybersecurity controls to OT. OT cybersecurity programs should be part of OT safety and reliability programs at the plant site and within the enterprise cybersecurity program.

ⁱⁱⁱ Security authorizations are official management decisions by senior officials to authorize the operation of system and explicitly accept the risk to organizational operations and assets based on the implementation of security controls.



Audit 2023-17433 – Operational Technology Cybersecurity – Combined Cycle Plant

EXECUTIVE SUMMARY

- System baselines^{iv} were not in place.
- Cybersecurity monitoring was incomplete.

In addition, we determined a risk assessment had not been completed for the site's OT systems.

Specifics of the identified issues were omitted from this report due to their sensitive nature in relation to TVA's cybersecurity but were formally communicated to TVA management in a briefing on March 21, 2024.

What the OIG Recommends

We made five recommendations to TVA management to develop contingency plans, improve inventory for OT equipment, document OT system baselines, implement cybersecurity monitoring, and assess risks.

TVA Management's Comments

In response to our draft audit report, TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

^{iv} System baselines are a set of specifications for a system or its components that has been formally reviewed and can only be changed through a change control process.

BACKGROUND

Power plants rely on operational technology (OT)¹ to ensure the plants can run without disruption. OT encompasses a large range of programmable systems that interact with and manage the physical environment. Examples of OT include industrial control systems, building automation systems, transportation systems, and physical access control systems. Implementing logical, physical, and general security controls can reduce the risk of cyber threats to OT systems. TVA documents these controls in system security plans (SSPs). OT cybersecurity² is essential to the reliable operation of modern industrial processes. As an example, cyber attackers have been able to create malicious code that alters the behavior of OT. By injecting this malicious code into an OT network, cyber attackers can cause machines and equipment to malfunction, even damaging them to the point of catastrophic failure. When working with malfunctioning machines that are spinning at high speeds or burning natural gas at very high temperatures, there is a risk of injury or death for power plant employees and contractors. Additionally, a successful cyberattack against a combined cycle power plant could cause damage to equipment and grid instability/blackouts.

According to the National Institute of Standards and Technology (NIST),³ OT networks previously bore little resemblance to Information Technology (IT) networks due to system isolation, proprietary control protocols, and specialized hardware and software; however, OT is now starting to resemble traditional IT systems. While this brings OT new IT capabilities, it provides “significantly less isolation for OT from the outside world than predecessor systems, creating a greater need to secure OT systems.”

Within the Tennessee Valley Authority (TVA) fleet, there are nine combustion turbine and eight combined cycle plants that can together produce over 12,000 megawatts of electricity—enough to power 7 million homes. As part of the greater interconnected power grid, combined cycle power plants are a vital element in the power mix. Due to the high risks associated with threat events against OT, we performed an audit of logical, physical, and general security controls at one combined cycle plant.

¹ OT systems and devices monitor or control physical processes or events.

² OT cybersecurity is the application of cybersecurity controls to OT. OT cybersecurity programs should be part of OT safety and reliability programs at the plant site and within the enterprise cybersecurity program.

³ NIST Special Publication 800-82 (Revision 3), Guide to Operational Technology (OT) Security, September 2023, < <https://doi.org/10.6028/NIST.SP.800-82r3>>, accessed on 2/13/2024.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if logical, physical, and general security controls were (1) appropriately designed to reduce cybersecurity risk and (2) operating effectively. The scope of this audit was limited to the OT at one combined cycle plant. To achieve our objective, we:

- Reviewed applicable TVA Standard Programs and Processes to gain an understanding of TVA's processes related to logical, physical, and general security controls.
- Reviewed Power Operations SSPs to gain an understanding of cybersecurity control requirements.
- Identified and assessed internal controls to the extent necessary to address the audit objective, including:
 - Identified internal controls associated with configuration management; awareness and training; audit and accountability; assessment, authorization, and monitoring; contingency planning; incident response; media protection; physical security; access control; and systems and communication protection.
 - Assessed design of internal controls by comparing TVA policies, procedures, and work instructions to identified best practices.
 - Assessed implementation of internal controls by reviewing configurations, training records, and Standard Programs and Processes documentation.
 - Assessed effectiveness by reviewing network diagrams, system configuration information, vendor documentation, system inventory, logical access, and physical access related to the OT for the combined cycle plant.
- Conducted interviews with TVA Technology and Innovation, Power Operations, and TVA Police personnel to gain an understanding of TVA's logical, physical, and general security controls.
- Performed a site walkthrough in September 2023, which included the following steps:
 - Reviewed the OT network asset inventory and network diagrams provided by TVA and compared them to the devices observed on-site.
 - Reviewed physical and environmental controls on-site.
 - Performed wireless scanning to identify wireless devices on-site.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FINDINGS

We reviewed logical, physical, and general security controls and determined the following areas were appropriately designed and operating effectively:

- Logical controls used to manage logical system protection.
- Physical controls used to manage personnel access to areas of the plant with OT systems.
- General controls used to provide awareness and training as well as security authorization.⁴

However, we found the following general security control deficiencies that were significant to our audit objective:

- Contingency plans were not documented.
- OT inventory was incomplete.
- System baselines were not in place.
- Cybersecurity monitoring was incomplete.

In addition, we determined a risk assessment had not been completed for the site's OT systems.

The following provides a brief summary of our findings. Specific details of the issues we identified were omitted from this report due to their sensitive nature in relation to TVA's cybersecurity but were formally communicated to TVA management in a briefing on March 21, 2024.

CONTINGENCY PLANS NOT DOCUMENTED

Contingency planning involves restoring systems and implementing alternative business processes in the event of system compromise or breach. TVA SSPs require contingency plans be developed as part of the implementation of cybersecurity controls. According to TVA personnel, there was no documented contingency plan for the OT system at the site. Without a documented and tested contingency plan, Power Operations is at risk of extended downtimes and production losses in the event of system failure.

OT INVENTORY INCOMPLETE

We compared Power Operations' OT inventory listing to network diagrams and other documentation and identified inaccuracies. In addition, during our on-site

⁴ Security authorizations are official management decisions by senior officials to authorize the operation of system and explicitly accept the risk to organizational operations and assets based on the implementation of security controls.

walkthrough, we identified five network devices that were not included in the OT inventory as required by Power Operations' Standard Operating Procedure. An incomplete inventory could lead to unmanaged and unprotected devices within the OT environment. Additionally, TVA has an ongoing inventory project for the OT at this site that has not been fully implemented.

SYSTEM BASELINES NOT IN PLACE

Configuration management focuses on establishing and maintaining the integrity of devices and has a direct impact on the security posture of TVA systems. We determined Power Operations did not have configuration baselines for vendor developed OT systems as required by TVA policy. Establishing a secure baseline configuration provides a strong secure infrastructure for system components that minimizes risks and reduces the threat of vulnerabilities or malware.

CYBERSECURITY MONITORING INCOMPLETE

Cybersecurity monitoring involves receiving logs and analyzing them for signs of cybersecurity incidents. One segment of the OT network was not subject to logging and monitoring of cybersecurity events as required by TVA SSPs. TVA personnel agreed cybersecurity monitoring at the combined cycle site was inadequate to provide visibility of network intrusions, malicious code, or other nefarious acts that an adversary would be taking against a gas operations plant. In addition, we determined TVA does not have policies to collect, store, monitor, or analyze audit logs generated at the combined cycle site. Incomplete cybersecurity monitoring increases the risk that a security incident may go unnoticed, leading to additional damage or disruption.

RISK ASSESSMENT NOT CONDUCTED

A system level risk assessment determines the risk to an organization by identifying threats, vulnerabilities, the harm that may occur, and the likelihood that harm will occur. According to TVA personnel, there was no documented risk assessment for the OT system at the site. TVA SSPs require risk assessments be conducted as part of the implementation of cybersecurity controls. Without a system level assessment of risk, the selection of security controls applied to the system could be inadequate.

RECOMMENDATIONS

We recommend the Senior Vice President, Power Operations, and the Vice President and Chief Information and Digital Officer, Technology and Innovation:

1. Develop a contingency plan for the OT at the site.
2. Complete the ongoing inventory project for the OT at the site.
3. Document and implement OT system baselines and monitor systems for changes.
4. Design and implement cybersecurity monitoring, as appropriate, for the OT.
5. Perform a risk assessment and update as needed.

TVA Management's Comments – In response to our draft audit report, TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

June 13, 2024

David P. Wheeler, WT 2C-K

REQUEST FOR COMMENTS – AUDIT 2023-17433 – OPERATIONAL TECHNOLOGY
CYBERSECURITY - COMBINED CYCLE PLANT

Power Operations and Technology & Innovation (T&I) would like to thank Andrew Jurbergs and Sarah Huffman for their diligence, support, and recommendations for improvement as we are continuously improving the reliability and resiliency of our Combined Cycle Plant cyber security.

In response to the OIG memorandum dated May 10, 2024, Power Operations and T&I have reviewed your draft report and have the following comments and responses.

Recommendations

We recommend the Senior Vice President, Power Operations:

1. Develop a contingency plan for the Operational Technology (OT) at the site.

Response

Power Operations agrees with this recommendation.

2. Complete the ongoing inventory project for the OT at the site.

Response

Power Operations agrees with this recommendation.

3. Document and implement OT system baselines and monitor systems for changes.

Response

Power Operations agrees with this recommendation.

4. Design and implement cybersecurity monitoring, as appropriate, for the OT.

Response

Power Operations agrees with this recommendation.

5. Perform a risk assessment and update as needed.

Response

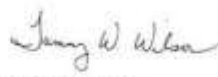
Power Operations agrees with this recommendation.

David P. Wheeler, WT 2C-K
Page 2
June 13, 2024

Thank you for the time to allow us to review and provide feedback on the draft audit. We appreciate the opportunity.



Allen Clare
Senior Vice President
Power Operations



Tammy Wilson
Vice President
Chief Information & Digital Officer

TDL

cc:

Brett A. Atkins
Kenneth C. Carnes
Sherri R. Collins
Samuel P. Delk
David P. Fountain
Greg G. Jackson
T. Daniel Lunsford
Todd E. McCarter
Donald A. Moul
Dustin C. Pate
Ronald R. Sanders II
John M. Thomas III
Josh Thomas
Kay W Whittenburg
OIG File No. 2023-17433