EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Cyber Security Forensics for Industrial Control Systems

Summary of Utility Tabletop Exercises

3002013991

Cyber Security Forensics for Industrial Control Systems

Summary of Utility Tabletop Exercises

3002013991

Technical Update, December 2018

EPRI Project Manager

R. King

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THE FOLLOWING ORGANIZATION(S), UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

MITRE Corporation

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organization(s), under contract to the Electric Power Research Institute (EPRI), prepared this report:

MITRE Corporation
7515 Colshire Drive
McLean, VA 22102-7539

Principal Investigators
O. Alexander
M. Collins
C. Harvey
J. Hoyt

This report describes research sponsored by EPRI.

EPRI would like to acknowledge the support of the following organizations: Consolidated Edison, FirstEnergy, and Portland General Electric

This publication is a corporate document that should be cited in the literature in the following manner:

Cyber Security Forensics for Industrial Control Systems: Summary of Utility Tabletop Exercises. EPRI, Palo Alto, CA: 2018. 3002013991.

ABSTRACT

It is critical for utilities to continually evaluate and exercise their capabilities to effectively respond to events in their operational environments to determine if their processes satisfy operational requirements. With the increased usage of processor-based operational and communications infrastructure, the potential for operational events to occur or be influenced by malevolent cyber agents also increases. The tabletop exercises (TTX) described in this report review the approaches of electric power utilities to operational events. This report includes information regarding how the utilities currently engage cyber security and operational resources to address the increased potential for cyber-attacks. The report also describes the process and objectives of the exercise along with the scenarios that were evaluated, findings, and recommendations.

Keywords
Tabletop
Cyber security
Exercise

Deliverable Number: 3002013991

Product Type: Technical Update

Product Title: Cyber Security Forensics for Industrial Control Systems: Summary of Utility Tabletop Exercises

PRIMARY AUDIENCE: Chief Information Security Officers, Power Systems Operations Managers, Cyber Security Program Directors, Security Operations Managers, Cyber Security Architect, Cyber Security Engineers, Cyber Security Analysts, Physical Security Program Directors

KEY RESEARCH QUESTION

What are the organizational roles and responsibilities, processes and procedures, and technologies for effectively responding to cyber security events and conducting forensics investigations for those events in an operational technology (OT) environment?

RESEARCH OVERVIEW

It is critical for utilities to continually evaluate and exercise their capabilities to effectively respond to events in their operational environments to determine if their processes satisfy operational requirements. With the increased usage of processor-based operational and communications infrastructure, the potential for operational events to occur or be influenced by malevolent cyber agents also increases. The tabletop exercises (TTX) described in this report review the approaches of electric power utilities to operational events. This report includes information regarding how the utilities currently engage cyber security and operational resources to address the increased potential for cyber-attacks. The report also describes the process and objectives of the exercise along with the scenarios that were evaluated, findings, and recommendations.

KEY FINDINGS

- The coupling of IT and OT infrastructure components requires coordination, collaboration, and knowledge-sharing between the IT and OT organizations.
- It is critical to have clear processes and procedures in place to avoid conflicts between the forensics functions and the need to return to normal operations.
- The incident response and forensics processes should be routinely tested.
- Organizations should develop internal forensics talent and reduce reliance on vendors to perform the process.

WHY THIS MATTERS

The establishment of a baseline for ICS operational events will be one facet of EPRI's work in ICS forensics. Learnings from the reported tabletop exercises and follow-on discussions will improve information collection and analysis as the forensics research expands to engage the larger community.

HOW TO APPLY RESULTS

Utilities can use the results of the tabletop exercises to review and address potential gaps in their policies and procedures related to incident response in an increasingly complex and technology-rich operational environment. EPRI will also use the results as part of a baseline development of processes and procedures used by operational organizations in the electric sector. This baseline will be used as input for research on the application of forensics to industrial control systems (ICS) operational environments.

LEARNING AND ENGAGEMENT OPPORTUNITIES

- EPRI Cyber Security Forensics Working Group
- EPRI PDU Advisory Meetings
- EPRI PDU Cyber Security Technology Transfer Meeting
- EPRI PDU "Birds of a Feather" Incident and Threat Management Workshop

EPRI CONTACTS

- Ralph King, Program Manager, Cyber Security
- Ben Sooter, Senior Project Manager, Cyber Security

PROGRAM: PDU Cyber Security, 183

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

What is a Tabletop Exercise

A tabletop exercise (TTX) is a facilitated, scenario-based discussion that tests an organization's ability to respond to a potential scenario in a practice environment. It enables participants to review and discuss in detail the actions they would take to validate operational processes, procedures, and reporting structures. The key outputs of the TTX are an identification of people, process, or technology gaps and recommendations for addressing them.

This report describes the process, execution, and results from three industrial control system (ICS) TTXs held with three individual utilities. Separate detailed reports that document the exercise and results were provided to each respective utility. This report provides a summary of the TTX workshops and generalizes the results to protect security information and business sensitive information that may have been utilized in the exercises.

Objectives of the Tabletop Exercise

Each TTX was a one-day onsite workshop at a participating utility. Staff members from these utilities with pertinent responsibilities for the processes to be evaluated attended the workshop along with the EPRI cyber security team members and staff from MITRE Corporation. A planning meeting was held with each utility prior to the exercise workshop to identify the appropriate utility staff that would attend and to determine logistics of the meeting. The exercise was intended to evaluate the roles and responsibilities, processes and procedures, and technologies for responding to a cyber event and conducting forensics investigations for those events in an operational technology (OT) environment. The objectives of the exercise are listed below.

1. Identify how to address a non-obvious cyber event normally attributed to a maintenance problem.
2. Refine the processes and procedures that operational engineers follow in a cyber event such as a series of actions typically taken in response to a critical incident for the operators in the field.
3. Identify roles, responsibilities, and authorities, to include:
    - Who is the primary authority?
    - Who performs cyber-related analysis of the operational environment?
    - Who are the stakeholders?
    - How is information shared?

Requirements for the Tabletop Exercise

The following were key requirements for the exercise:

1. The exercise had to be conducted in a learning environment wherein policies, procedures, and technologies could be evaluated.
2. The exercise scenario had to be plausible, with events occurring as they were presented.
3. Exercise simulation had to contain sufficient detail to allow the Blue Team to react to information and situations as they were presented as if the simulated incident were real.
4. The utility needed to have cross-functional representation to perform the Blue Team roles and responsibilities.
5. Incident response policies and procedures were available for consultation during the event.
6. Network diagrams depicting the OT assets and the information technology (IT) networks and hosts that manage and monitor the OT were available for consultation during the event.

2
DEFINTIONS AND ACRONYMS

This chapter provides definitions and acronyms for key terms used in this document.

Definitions

Tabletop Exercise: A facilitated, scenario-based discussion that tests an organization's ability to respond to a potential scenario in a practice environment. It enables participants to review and discuss in detail the actions they would take to validate operational processes, procedures and reporting structures. The key outputs of a TTX are an identification of people, process or technology gaps and recommendations for addressing them.

Acronyms

EMS	Energy Management System
HMI	Human Machine Interface
IED	Intelligent Electronic Device
IT	Information Technology
OT	Operational Technology
PLC	Programmable Logic Controller
SME	Subject Matter Expert
TTX	Tabletop Exercise

3
OVERVIEW OF THE TABLETOP EXERCISE

Scenarios for the Tabletop Exercise

The process for the exercise utilized event scenarios to evaluate the response of the utility. Each scenario focused on addressing different aspects of incident response and the forensics process in the OT environment. The following five scenarios were utilized in the three utility exercises.

1. **Scenario 1 – Ransomware**: An OT Operator notices a pop-up ransomware alert on the human machine interface (HMI) console.
2. **Scenario 2 – Programmable Logic Controller (PLC) Device Failure**: The OT Operator receives an alert that a device (for example, PLC) has stopped communicating in a substation.
3. **Scenario 3 – Rogue Device**: A circuit breaker trips unexpectedly. The circuit breaker is replaced but the same symptom repeats.
4. **Scenario 4 – State Estimation**: A metering device begins sending incorrect measurements to the state estimator.
5. **Scenario 5 – Multi-feeder Event**: A feeder breaker at a substation supplied by multiple feeders trips on over current.

Tabletop Exercise Team Participants

Three teams comprised the TTX: a White Team, Red Team, and Blue Team, with subject matter experts (SMEs) having the skill sets necessary to support the execution of these scenarios as they apply specifically to the utility. The description of the teams, their respective roles and responsibilities, and desired skill sets or knowledge base are shown in Table 2-1 below.

Table 2-1
TTX Team Participants

Player	Roles and Responsibilities	Expertise or Skills
White Team	Facilitates exercise discussion. The Facilitator is responsible for keeping the discussion focused on exercise objectives and ensuring that all key issues are explored within time constraints. Resolves any issues that may arise, handles all requests for information or questions. A key objective of the White Team is to identify decision points and what goes into the decisions.	Possess functional area expertise of the power industry. Background in ICS processes, ability to translate events into cohesive and succinct script.
Red Team	Emulates cyber adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to demonstrate the impacts of successful attacks and share details needed by the Blue Team for their analysis and response.	Background in cyber adversary exploitation for IT and OT environments.
Blue Team	Responds to the symptoms/injects presented based on their respective SME knowledge of current plans, procedures, processes, and technologies.	Utility personnel who are responsible for maintaining, monitoring, and responding to cyber events within the utility. • Operators who monitor the HMI • Personnel who understand the IT side of the utility (for example, network architecture, systems architecture) • OT engineers who maintain the OT equipment and are responsible for responding to events on OT • IT/OT personnel who have deep knowledge of the utility policies and procedures as they relate to incident response • Cross-functional representation from generation, transmission, distribution, cyber security, operations centers, and substation operations

The Tabletop Exercise Process

The White Team facilitated the execution of the TTX. At the start of the event, the White Team reviewed with the participants the TTX goals and objectives, key assumptions and dependencies, the roles of the various teams, and the scenarios. Following this, the White Team presented the scenarios and facilitated a discussion with the Blue Team members on how they would respond to the issues or events described in the general scenario or from specific injects. During these discussions, the White Team also elicited input from the Red Team on cyber adversary details and further injects for the scenario. The following diagram depicts the general flow of this

interactive technique used during the TTX execution.

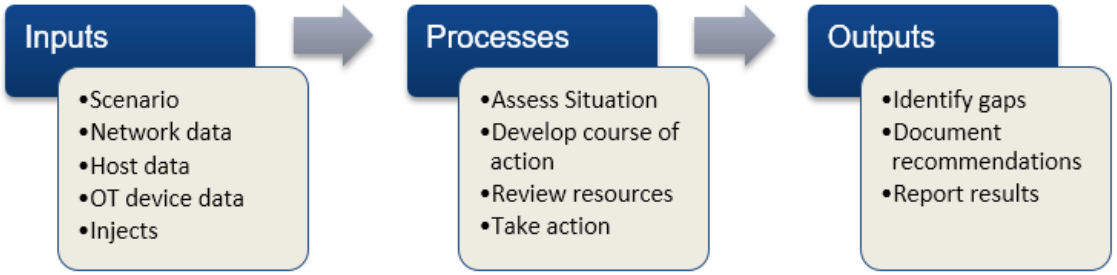

Figure 2-1
TTX Process Flow

After the conclusion of each scenario, there was a hot wash that allowed the participants to discuss what went well, what needed to be improved, and what gaps needed to be addressed to improve ICS forensic response in the future. This discussion provided valuable input to the identification of recommended changes to policies, procedures, and technologies.

4
SCENARIO RESULTS

Scenario 1 – Ransomware

In the first scenario, ransomware is identified on an HMI machine delivered via an external media device used for updating the HMI screens. The update occurred during a planned maintenance period by an outside vendor, but the ransomware did not lock out the system until two weeks later.

The White Team gave the Blue Team the following initial symptom on the failure and an additional item of information to influence their analysis:

- Initial symptom: HMI screen in a manned central control station gets replaced with a ransom message, and it is immediately noticed by the OT Operator.
- Additional information: This has occurred on a single workstation; other local and remote stations are still operating fine.

The White Team and Red Team members asked leading questions of the Blue Team regarding response actions, recovery actions, and technical capabilities in the context of the scenario. The result was a free-flowing discussion between the participants regarding response actions, recovery actions, and technical capabilities in the context of the scenario. The list of questions included:

- How do you maintain control? What is the fallback order for control?
- How do you validate control? Is it documented?
- Do you have hot backups? Do you have cold backup? Do you have archives?
- How do you reconstitute control?
- Who does an operator call to report the problem?
- Does an operator require authorization to make a change in the environment (for example, move to backup workstations)?
- What are the initial actions that will be taken with the machine?
- Do you unplug the device from the network?
- Do you unplug power from the device?
- What does your network look like? Can you prevent it from jumping?
- How do you know this is the only affected machine?
- For incident response actions:

- Who is responsible for the investigation?
- Do you check network logs?
- How do you investigate the use of universal serial bus?
- What other artifacts are incorporated in the investigation?
- What direction is provided by incident response playbooks?
- How do you identify/log changes to the system? Traceability of work?

Goals for Scenario 1 – Ransomware

This scenario was focused on the control center since it is the OT infrastructure that is closest to IT infrastructure in terms of network connections and device types in use. This allowed for evaluation of the IT response to a cyber-attack in the OT space. The goals for this scenario were as follows:

- Gain insight into interaction between IT and OT security personnel.
- Understand all internal organizations involved and who has authority.
- Determine procedures for software and patches transitioning from development to test to operational systems.
- Identify data sources in the control center.
- Determine forensics capability in IT-centric environment.
- Exercise policy and procedures for recovery and handling of affected devices.

Scenario 2 – Intelligent Electronic Device (IED) Failure

In the second scenario, malicious firmware was unintentionally installed during an update. The malicious firmware subsequently bricked the substation device while attempting to install itself. The firmware file had a delayed effect so that the failure did not occur until triggered by a load condition in the substation.

The White Team gave the Blue Team the following initial symptom on the failure and an additional item of information to influence their forensics analysis:

- Initial symptom: OT personnel noticed a loss of communication to an IED which is a high-value critical asset (for example, may have received an alert on the energy management system (EMS) HMI, “Loss of communication to IED XXX”).
- Additional information: A month later, another IED of the same make and model has the same symptoms after being serviced.

The White Team and Red Team members then asked the Blue Team the following questions in the course of the discussion. The result was a free-flowing discussion between the participants regarding response actions, recovery actions, and technical capabilities in the context of the scenario.

- How do you maintain control? What is the fallback order for control? Can you staff local stations?
- How do you validate control? Is it documented?
- Do you have hot backups? Do you have cold backup? Do you have archives?
- How do you reconstitute control?
- Do you reroute power?
- What are diagnostic/forensic processes for malfunctioning OT equipment? Who does the diagnostics/forensic? Vendor? On-site OT engineers? What is the timeline for conducting the diagnostics?
- How do you determine if there is a systemic problem?
- How do you track asset management and configuration control?
- Can you get a copy of the firmware that was installed? How do you validate it (for example, a hash check)?
- Is there a test environment on site?
- What is documented in the ticketing system? What work is performed?
- What kind of validation is done on firmware prior to being implemented?
- How was the firmware upgrade performed? Vendor laptop? Removeable media? How is the laptop or removeable media scanned/vetted prior to being introduced?

Goals for Scenario 2 – Intelligent Electronic Device (IED) Failure

This scenario focused on the lowest level electronic devices involved in power distribution; this allowed the scenario to explore the response from OT personnel who may not be as familiar as IT personnel with the vulnerabilities of devices or the data sources that may be available to detect cyber-attacks. Goals for the scenario included:

- Determine procedures for software and patches transitioning from development to test to operational systems in substations.
- Identify data sources in the substations.
- Identify remote troubleshooting abilities.
- Determine forensics capability in OT-centric environment.
- Identify policy and procedures for recovery and handling of affected devices.
- Identify configuration management for field devices.
- Identify configuration management and security for transient assets.

Scenario 3 – Rogue Device

In the third scenario, an adversary gained access to the substation network and is attempting to move laterally to compromise OT devices.

The White Team gave the Blue Team the following initial symptom on the failure and an additional item of information to influence their forensics analysis:

- Initial symptom: A circuit breaker trips unexpectedly.
- Additional information: There are no physical reasons for the trip. The circuit breaker is replaced but the same symptom repeats.

The White and Red Team members then asked the Blue Team the following questions about actions that would be taken with respect to the substation environment. The result was a free-flowing discussion between the participants regarding response actions, recovery actions, and technical capabilities in the context of the scenario.

- How would you detect a rogue device on the network?
- How is the network instrumented to allow detection?
- How many places do you have to monitor in a substation?
- What tools are available to you to identify and isolate the rogue device?
- How long would you capture traffic on a substation network where the rogue device was detected after removing it?
- What is done in terms of whitelisting?
- If you see a command come across the network and it matches that of the remote terminal unit, what do you do?
- On the substation local area network, do you have access control for individual ports?

The points raised by the participants during the discussion were recorded by the individual White Team members and, after the TTX, correlated, discussed, and distilled down to the set of findings presented in the next section.

Goals for Scenario 3 – Rogue Device

Adding a rogue device to the substation allowed for continued focus on the lowest levels of the OT infrastructure. The rogue device scenario also exercises the understanding of communications and interaction between the control center and the remote substations. Goals for the scenario included:

- Identify data sources in the substations.
- Identify remote troubleshooting abilities.
- Determine network forensics capability in OT-centric environment.

- Detail communications from control center to substations and within substations.

Scenario 4 – State Estimation

In another scenario, an adversary inserted a modified metering device into the supply chain. The device was installed and then sometime later began reporting incorrect data.

The White Team gave the Blue Team the following initial symptom on the failure:

- Initial symptom: A metering device begins sending incorrect measurements to the state estimator.

The White and Red Team members then asked the Blue Team the following questions about actions that would be taken with respect to the substation environment. The result was a free-flowing discussion between the participants regarding response actions, recovery actions, and technical capabilities in the context of the scenario.

- How are state estimation errors discovered?
- How would a suspicious device be handled?
- What procedures are in place for verifying new devices?

Goals for Scenario 4 – State Estimation

This scenario targets newer technology in the OT environment as well as the supply chain. The goals included exercising OT personnel and establishing what testing was done prior to devices being put into service. Goals for this scenario include:

- Understand OT operators' ability to identify malicious activity.
- Determine sophistication of the state estimation to determine inappropriate behavior.
- Understand procedures for installing new devices in the infrastructure.
- Understand testing and commissioning procedures.
- Determine limits of OT forensics capabilities at the utility.
- Test limits of knowledge around OT cyber events.

Scenario 5 – Multi-feeder Event

In the final scenario, an adversary obtains persistence on an EMS server in the control center. Methods of access were not discussed during the exercise but could include infected updates from manufactures or contractors, unwitting insiders connecting an infected device, or witting insiders.

The White Team gave the Blue Team the following initial symptom on the failure and an additional item of information to influence their forensics analysis:

- Initial symptom: A feeder breaker at a substation supplied by multiple feeders trips on over current.

- Additional information: The feeder breaker on one of the other feeders at the station has mechanically failed, forcing excess current through the remaining feeder. The mechanical failure of the breaker was not indicated in the EMS system.

The White and Red Team members then asked the Blue Team the following questions about actions that would be taken with respect to the substation environment. The result was a free-flowing discussion between the participants regarding response actions, recovery actions, and technical capabilities in the context of the scenario.

- Where would the investigation start?
- Where are maintenance logs of devices kept?
- When is preventative maintenance performed on devices?
- Are sources of data other than voltage, current, and phase used to monitor the system?

The points raised by the participants during the discussion were recorded by the individual White Team members and, after the TTX, correlated, discussed, and distilled down to the set of findings presented in the next section.

Goals for Scenario 5 – Multi-feeder Event

As the most complex scenario, this scenario works to test a variety of areas. Goals included:

- Bring OT and IT together to determine a root cause.
- Test the ability of OT and IT personnel to detect a sophisticated event involving obfuscation by the malicious actor.
- Evaluate what forensic data is available in the OT environment.
- Exercise recovery for control centers.
- Determine what data sources are available:
    - In the control center
    - In the substation
    - In the communications infrastructure
- Determine what alternative data sources could be used for forensics that already exist in the OT space.

5
GENERAL FINDINGS

The responses from each participating utility varied based on the application of their corporate security policies, incident response procedures, individual experiences, corporate structure, and network architecture. The observations that were common among all three utilities summarized below.

1. Any cyber event affecting OT will require interaction between IT and OT internal groups that must share knowledge and coordinate activities. This was exemplified in the scenarios that occurred in the control center, where the IT personnel have responsibility for workstations while the OT personnel have responsibility for the applications running on them. It was also demonstrated in the substation scenarios where the OT personnel are responsible for loading firmware and configurations on devices and IT personnel are responsible for the laptops used by OT personnel.

2. There are IT components in the OT environments (for example, HMI). IT and OT personnel need to be knowledgeable of cyber security policy and procedures associated with both IT and OT as well as incident response. Response actions will need to be executed in a timely fashion and be able to capture critical data, both IT and OT, minimizing impact to operations. Enhancing IT/OT incident response procedures to incorporate cyber as an attack vector in the OT environment is critical.

3. There is always going to be a conflict between forensics and operations. Forensic investigations benefit from as much data about the incident as possible. Returning to normal operations may reduce the amount of data available to forensics through loss of volatile memory when a device is powered down or network data is lost due to communications being disconnected. This is not an endorsement of leaving malware in place and observing its behavior but simply an acknowledgement of the possible loss of data that is useful for a forensic investigation. Identification of the data sources needed for forensics prior to an incident will aid in ensuring that adequate forensic data is saved while returning the system to operations status as quickly as possible.

4. Organizations lack sufficient in-house knowledge of OT forensics and rely on suppliers of equipment for detailed forensics. The types of forensic data available from OT-specific devices were not well understood by the organizations. Organizations overall had a good understanding of the devices they use in their infrastructure; however, they lacked the specific knowledge to do tasks such as retrieving firmware from a device.

5. Utilities had environments for developing and testing new configurations, firmware, and devices. These same environments should be leveraged to test incident response procedures, test the use of forensic tools as well as procedures for activities that impact security operations such as applying patches to firmware or software.

6. Policies and procedures were in place to spell out the process for testing and installing firmware on OT devices. In addition to the policies and procedures, technical controls must be put in place to ensure that firmware files are controlled from the vendor to the

end device and ensure accountability. Supply chain accountability for firmware is critical.

6
RECOMMENDATIONS

This TTX was designed to evaluate the roles/responsibilities, processes and procedures, and technologies for responding to an event in an OT environment, build an understanding of how OT and IT staff need to work collaboratively, and highlight significant areas of importance relative to a subsequent OT forensic investigation.

The following recommendations were derived from the discussions following each phase of the TTX and consolidation of individual participant feedback.

Process and Procedures

- Spell out detailed coordination and sharing across business units prior to an incident. Details should include what organization is in charge during a cyber incident.
- Define at what point within incident response cyber expertise should be brought in. Cyber experts do not need to be consulted every time a breaker trips but should be brought in when routine causes are eliminated. It is beneficial to at least consult with them before all non-cyber causes have been exhausted to enable them to understand the incident more thoroughly.

Data Sources

- Before incidents occur, identify what OT data is needed for forensics for each device that is fielded to enable quick acquisition during an incident.
- For forensic data identified for devices, determine how to collect the OT data to ensure the availability of the data when needed.
- Through discussion with device manufactures and testing, understand what forensic data might be lost during troubleshooting. This can lead to procedures to back up or capture specific data prior to performing troubleshooting to ensure the availability of the data.

Configuration Management

- Maintain accurate asset inventories of OT devices, including location, firmware, and configuration. The inventory can then be used to respond to vulnerability notifications.
- Maintain change history for firmware and configuration so devices can be restored in the event of an incident.
- Track who, when, and where any change was made for traceability during incident response.
- Maintain a “Gold Disk” image of critical systems, such as the energy management system, to enable quick restore. A “Gold Disk” would contain a complete base install of the system but may not include every operating system and application patch and update.

Incremental backups should be maintained for recovery as well, but in the event of an incident that has an unknown initial infection time, being able to restore to a known good state is important.

- If devices are restored to service after refurbishment, ensure that configuration management is addressed so devices return to a stable state.
- Provide ability to trace device history through refurbishment in the event the malicious activity is not fully remediated by the refurbishment.

Disposition of Devices

- Define a policy for disposition of devices involved in cyber incidents and have criteria for determining the decision.
- IT and OT devices may be treated differently after a cyber incident. Factors to consider include replacement cost and availability, as well as confidence in a refurbished device.

Laptops

- Maintain technical controls to reduce likelihood of infection on laptops used in field operations. Some options include:
- Re-image laptops often to maintain "clean" image.
- Use read-only hard drive to prevent persistent infection.

Infrastructure

- Use standard practices for securing networking equipment used in substations, including:
    - Port blocking, both logical and physical, on unused Ethernet ports.
    - Network segmentation to reduce lateral movement.
- Evaluate risk tradeoff of remote access to microprocessor-based protection relays and other devices in the substation:
    - Benefits include decreased troubleshooting time through remote troubleshooting.
    - Risks include increased attack surface due to additional connections to device.

Test Environment

- Establish process to bring devices from the field back to test labs for forensic analysis in a controlled environment.
- Consider procedure for vendors to work securely in utilities test labs to ensure traceability and security.

New Technology

- Implement new technologies that incorporate additional authentication of users and

firmware on the end devices.

- Technologies that vendors are starting to deliver include:
    - Digital signatures for firmware will help ensure that valid firmware is installed on devices.
    - OT device self-integrity checking of firmware can also reduce risk.

Training

- Cross-train IT and OT personnel.
- Expose IT personnel to OT operations/procedures/data sources.
- Expose OT personnel to IT operations/procedures/data sources.
- Tabletops and continued work:
    - Perform tabletop exercises to understand forensic procedures and identify gaps.
    - Perform realistic cyber security drills to test level of understanding of cyber security policies and incident response procedures at the operator and user levels.

7
SUMMARY

In summary, the tabletop exercises for incident response and forensics were a valuable process for the participating electric power utilities. The exercises also provide value to the large utility community by sharing the process, scenarios, findings, and recommendations resulting from the exercise workshops. Key points from the workshops include the following:

- The coupling of IT and OT infrastructure components requires coordination, collaboration, and knowledge-sharing between the IT and OT organizations.
- It is critical to have clear processes and procedures in place to avoid conflicts between the forensics functions and the need to return to normal operations.
- The incident response and forensics processes should be routinely tested.
- Organizations should develop internal forensics talent and reduce reliance on vendors to perform the process.

It is important to build upon this baseline analysis of the incident response and forensics capabilities of electric power utilities, particularly for the industrial control system components of the OT infrastructure. Forensic capabilities for industrial control systems are not mature and represent a gap in the cyber security industry. Therefore, EPRI will continue to work with utilities and industry partners to further the incident response and forensic investigative processes for industrial control system. These processes will continue to be a focus and part of the roadmap for the EPRI cyber security research program

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI members represent 90% of the electric utility revenue in the United States with international participation in 35 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

3002013991

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com