Field Insights: Strengthening Digital Assurance Through On-Site Network Monitoring

INL/RPT-25-89299

INL Center for Securing Digital Energy Technology (CSDET)

SEPTEMBER 2025

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

CONTENTS

ACRONYMS

AOO	Asset Owner/Operator
BESS	Battery Energy Storage System
BMS	Battery Management System
CESER	Cybersecurity Energy Security and Emergency Response
CIE	Cyber-Informed Engineering
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Service
DOE	U.S. Department of Energy
EMS	Energy Management System
EWS	Engineering Workstation
GDO	Grid Deployment Office
GRIP	Grid Resilience Innovation Partnerships
HMI	Human Machine Interface
IBR	Inverter-Based Resource
ICS	Industrial Control System
IDS	Intrusion Detection System
INL	Idaho National Laboratory
IP	Internet Protocol
IR	Incident Response
IT	Information Technology
NTP	Network Time Protocol
OT	Operational Technology
PCAP	Packet Capture
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SSH	Secure Shell
TADA	Technical Assistance for Digital Assurance
U.S.	United States

Field Insights: Strengthening Digital Assurance Through On-Site Network Monitoring

1. INTRODUCTION

The accelerating deployment of digital energy infrastructure, ranging from inverter-based resources (IBRs), battery energy storage systems (BESS), to advanced grid control platforms, has brought unprecedented visibility, flexibility, and efficiency to the electric grid. However, this digital transformation also introduces new cybersecurity challenges, particularly in the form of supply chain risks and operational blind spots at the grid edge.

Over the past year, the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), though its Rapid Risk Assessment initiative, along with the Grid Deployment Office (GDO), through its Technical Assistance for Digital Assurance (TADA) initiative, have supported a series of on-site network engagements led by Idaho National Laboratory (INL). These engagements, conducted in partnership with asset owners across the country, have focused on identifying real-world vulnerabilities and misconfigurations in operational environments, many of which are not detectable through remote assessments or traditional compliance audits.

On-site network hunts and edge monitoring have proven to be essential tools in uncovering latent risks introduced through complex supply chains. These risks often stem from third-party components, firmware inconsistencies, or insecure default configurations that persist in the field long after deployment. By directly observing how digital energy equipment behaves in live environments, INL analysts identified systemic issues that could otherwise go unnoticed, offering asset owners actionable insights to strengthen their cybersecurity posture.

This mission extends beyond individual engagements. The program is designed to assist recipients of federal funding for energy resilience and capacity growth projects that rely on digital energy technologies. As part of this support, INL provides tailored technical assistance that includes equipment assessments and network monitoring to help partners ensure that their systems are responsibly deployed and configured securely. Eligible GDO partners for on-site network engagements are recipients of Grid Resilience Innovation Partnerships (GRIP) awards, which are projects focused on enhancing the resilience of electric system(s) and grid capacity growth. Supporting the security of these projects and CESER partner projects is important to help ensure asset owners remain uncompromised and that these projects are able to achieve their overall goals and objectives.

In parallel, INL also analyzes equipment and network data from sources outside of formal engagements to identify broader trends and common vulnerabilities. These insights help inform DOE strategy and provide the energy sector with field-validated lessons that can be applied across a wide range of operational contexts.

The goal of this report is to distill key findings and lessons learned during network hunt engagements from INL's fiscal year (FY) 2024 - 2025. It is intended to help asset owners—regardless of their participation in the program—better understand the evolving threat landscape and adopt practical measures to secure their digital energy infrastructure.

1.1. Key Observations

In this report, we provide a snapshot of our findings from various site engagements. Key observations include:

- Various types of third-party involvement with infrastructure management, often resulting in limited visibility over assets.

- A lack of demilitarized zones (DMZs) within operational technology (OT) networks.
- Incomplete network and asset inventories, with missing device and network information.
- The use of unencrypted and insecure communication protocols.
- Numerous known vulnerabilities in software and hardware equipment, indicating a need for regular patching and updates.
- Instances of unmanaged switches and gateways for asset controllers communicating externally, as well as obsolete devices connected to networks.
- Direct communications with the internet from OT networks.
- Staffing constraints and reliance on specific individuals for site information.
- A shift towards industrial control system (ICS) cloud usage.
- Issues with physical security, including unlocked human-machine interfaces (HMIs).

The remainder of this report highlights these observations in greater detail and includes a complete table in Section 3 of findings.

2. DEPLOYMENT OVERVIEW

Each engagement followed a structured process—from pre-assessment planning and architecture reviews, equipment deployment, network traffic analysis, and final reporting. The goal was not only to detect signs of adversarial activity, but to uncover misconfigurations, visibility gaps, and systemic risks that could compromise the resilience of critical energy systems.

Section 2.1-2.4 outlines the technical approach used during these engagements, including the tools and methodologies applied, the types of data collected, and the collaborative process that was followed with each partner. While the findings presented later in this report reflect observations from specific sites, they are representative of broader trends seen across diverse environments. The intent is to share these insights in a constructive and transparent manner, enabling other asset owners to evaluate their own systems and apply relevant mitigations to strengthen their cybersecurity posture.

2.1. Pre-Engagement Reviews

Before visiting a site for evaluation, INL gathers available data provided from the partner that includes any relevant information about the system(s) and devices involved. This may include information regarding existing asset inventories, the partners' overall network architecture, and potential deployment locations. This helps the INL team build a baseline view of the system, identify where to install sensors for proper visibility, and develop hypotheses to validate during the assessment.

During the engagement, INL analysts meet with the partner throughout the planning process to review requirements for sensor installation, validate safe methods to install the sensors in the desired location with minimal-to-no impact on operations, and ensure that the configuration enables the analysts to accurately capture communication flows. INL thoroughly reviews the partners goals for the engagement to ensure that the captured data will provide insights that are useful to the partner. Logistics expectations are also discussed (e.g., shipping equipment, identifying a space for analysts to conduct research during the engagement, etc.).

2.2. Sensor Deployment

At the beginning of each engagement, the INL team installs a Malcolm[1] server and Hedgehog[2] sensors at the requested locations, which are usually at IBR assets on the grid edge. Sensors can be installed via mirrored span ports or network TAPs. The kit relies on a NetGate routers running pfSense+, which must be assigned static IP addresses on the partners network, to transfer data from the Hedgehog sensors to the Malcolm server. Once they are powered on, they immediately establish pre-configured, routed IPsec tunnels. The tunnels from the routers allow the sensors to forward Zeek logs from the sensor to the server, where they are indexed by Malcolm. An example of Malcolms network connection flow is shown in Figure 1.

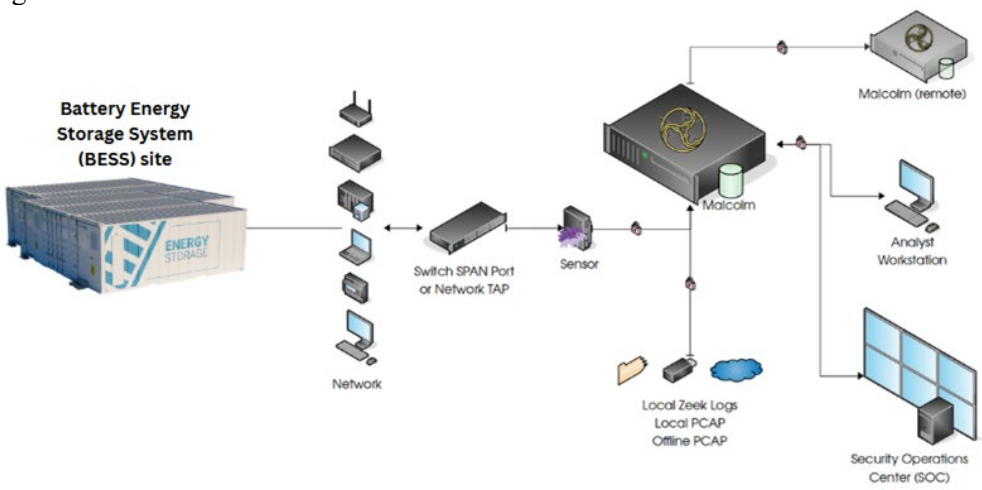

Figure 1. Example of a Malcolm network flow connected to a BESS site.

2.3. Assessment Techniques

Network activity is monitored through the deployed Hedgehog sensors and forwarded to the Malcolm server (which converts the packet capture (PCAP) information into a digestible format). This process takes place for several weeks, allowing time for the Hedgehog sensors to gather the PCAP data needed to conduct a thorough analysis.

After PCAP data is done, INL analysts begin analyzing the collected data and building out an asset inventory to identify all devices connected within the network. Typically, this is done when INL analysts are in-person on site for approximately 2 weeks. Through inspection of the corresponding MAC addresses, INL analysts can identify device types and the manufacturer of the device, to include in the asset inventory. This information can also be cross-referenced with the partners provided existing asset inventory to identify any missing devices or improperly decommissioned assets within the network.

The next step involves beginning building out a network architecture diagram. The result of this step is a visual diagram of IP connections between devices and the sources and destinations of ingress and egress traffic. By building out a network architecture diagram, analysts can identify unexpected traffic patterns and provide partners with a visual of connections within their network architecture.

Malcolm provides PCAP information in a digestible format to so analysts can (1) identify the volume of network traffic, (2) identify the protocols that are being used within the network, and (3) identify

[1] Github. https://cisagov.github.io/Malcolm/ - Network traffic analysis tool suite designed to collect and analyze network traffic in OT environments.

[2] Github. https://cisagov.github.io/Malcolm/docs/hedgehog.html - Sensor designed to collect the network traffic to be analyzed by Malcolm.

potentially suspicious geographical locations ingress and egress traffic is communicating to and from. The hunt team is trained to look for misconfigurations and suspicious traffic patterns that may introduce risk in the asset owner's environment.

2.4. Sharing the Findings

INL reviews key findings with the engagement partner while INL analysts are on-site. This allows an opportunity to have open discussions about key findings, ask or expand on questions that may have been raised during the analysis and provides an opportunity to provide actionable insights to the partner. In many cases, INL analysts collaborate with the partner to make changes and/or set up additional monitoring while they are on-site to provide the partner with immediate assistance and continual support beyond just the engagement for their network monitoring.

After the engagement is completed, the INL team provides a thorough report that includes documented details including the key findings from the engagement. In addition to the direct observations INL analysts made during the engagement, the outcomes focus on providing recommendations, risk-based mitigations, and Cyber-Informed Engineering (CIE)[3] considerations for the partner. The final report also includes the compiled asset inventory, and the network architecture mapping that was compiled during the engagement. Further insights in the report include any relevant information regarding network segmentation, user management, firewalls and DMZs, and physical security. The engagement reports also recognize areas of excellence that were observed, highlighting best practices that have already been implemented by the partner. This report provides documentation that the partner can return to for ongoing insights, and it can be used in discussions with engineers or management about investments needed to improve the security of the site. Custom requests from the partner can be made and included in these reports if there is a specific area they would like an emphasis on.

3. LESSONS LEARNED FROM ONSITE ENGAGEMENTS

Through TADA and Rapid Risk Assessment engagements, INL executed three network analysis engagements in FY 2024-2025. Although no significant evidence was uncovered during the engagements indicating the presence of adversarial activity, each engagement identified important findings and suggestions to help mitigate vulnerabilities and risks within the analyzed infrastructure. The following table outlines the common findings across all engagements conducted from FY24-25.

The purpose of sharing these findings is not intended to single out any of the engagement partners, but to highlight recurring patterns and observations that have emerged across a wide range of environments. By surfacing these shared insights in Table 1 below, we aim to provide other asset owners with an opportunity to reflect on their own systems and consider proactive steps to address similar challenges. The lessons presented here are meant to support continuous improvement and broader awareness of risks that may otherwise go unnoticed.

Table 1. Summary of observed engagement findings.

Category	Key Finding(s)
Third-Party Controls and Communications	• Various types of third-party involvement with infrastructure. • Controls and communications managed through a third party.

[3] Cyber-Informed Engineering is a strategic initiative championed by Idaho National Laboratory (INL) to integrate cybersecurity into engineering practices for critical infrastructure.

	• Limited to no visibility over assets managed or integrated by third parties. • Devices exposed to the internet and communicating with external endpoints discovered at one third-party managed site. • Third-Party Controls and Communication observations are further detailed in Section 3.3.
Network Segmentation	• Lack of true demilitarized zones (DMZs) within operational technology (OT) networks. • Devices like EWS and printers were found to be communicating on both IT and OT networks. • Network Segmentation observations are further detailed in Section 3.2.
Incomplete Network and Asset Inventories	• Missing device and network information in most inventories. • Each engagement partner tracked and shared information differently. • Incomplete Network and Asset Inventory observations are further detailed in Section 3.4.
Unencrypted and Insecure Communication Protocols	• Use of unencrypted and insecure communication protocols observed (e.g. Telnet or secure shell (SSH)). • Included plaintext protocols and protocols for remote access without proper control.
Device Vulnerabilities	• Many known vulnerabilities were identified in software and hardware equipment. There was a common need for patching and updates on the devices.
Device Exposures	• Unmanaged switches and gateways for asset controllers communicating externally discovered. • Obsolete devices connected to the network due to improper decommissioning in one engagement.
OT Network Comms to the Internet	• Direct communications with the internet observed. • Devices reaching out for updates and DNS queries made. • EWSs, a BESS controller, cameras, and several meters communicating directly to the internet. • OT Network Comms to the Internet are further detailed in Section 3.1.
Staffing Constraints	• Staffing constraints and dependence on specific individuals for site information. • Lack of expertise and availability could delay addressing issues or changes in system and network behavior.

Cloud Usage	• Most partners are shifting towards industrial control system (ICS) cloud usage.
Physical Security	• Some sites lacked proper locking mechanisms. A Human machine interface (HMI) was left unlocked at one of the observed sites.

3.1. OT Network Comms and the Internet

INL analysts observed at multiple sites that devices on OT networks could communicate directly with the internet, owing in part due to poor network segmentation and a reliance on third-party providers. Some examples of direct communication with the internet include devices reaching out for updates, and DNS queries being made. Devices such as engineering workstation (EWS), a BESS control server, Internet Protocol (IP) cameras, and several meters were also observed communicating directly with the internet.

Direct communication between OT networks and the internet increases risk by providing a path for adversaries to enter an otherwise restricted network, particularly in environments with poor segmentation and visibility. The INL team recommended that asset owners limit external network communication and route it through their data centers to enhance visibility.

3.2. Network Segmentation

The INL team observed that the OT networks at many sites were "flat," or unsegmented, meaning devices were connected without separation, allowing unrestricted communication. Examples of unsegmented networks found by the INL analyst team include those lacking a strict DMZ between the OT network and external networks. These networks allowed devices on the OT network to communicate freely with each other, even when unnecessary. Additionally, devices like EWS and printers were found to be communicating on both IT and OT networks.

Unsegmented networks pose similar risks to direct communication with the internet – there aren't safeguards to prevent adversaries from entering the OT network. In addition, unsegmented networks allow a single compromised device to grant adversaries access to the entire network. Segmenting a network compartmentalizes it, limiting communication between segments. This reduces the attack surface and restricts an adversary's lateral movement within the network.

3.3. Third-Party Providers

Many asset owners rely on one or more third party services to manage equipment and network configurations. This reliance limits the asset owners' ability to monitor network and device activity, reconfigure and segment networks, and patch vulnerabilities. Additionally, these third parties require remote access to the OT network over the internet.

The reliance on third parties can be risky in several ways. The lack of control over devices and networks limits the actions asset owners can take to mitigate vulnerabilities. Remote access requirements also create potential paths for adversaries to access a network, particularly in the event of a vendor compromise. Third parties also have different standards of security which may not be sufficient for BESS systems. The INL team provided network segmentation recommendations and suggested asset owners limit vendor access to the devices they manage.

Additionally, third-party providers are increasingly posing risks to asset owners because often when contracts are signed there are limitations for the asset owners to limit third parties from having access to

systems. We encourage asset owners to follow leverage procurement guidance to ensure that contract terms align with proper security standards.[4]

3.4. Asset Tracking and Inventory Management

Throughout the network engagements, the INL team utilized documentation provided by asset owners to help identify devices on the network and their purposes. There were instances of mislabeled devices, inconsistent documentation, and unidentified devices on the network. The lack of incomplete asset inventories posed a challenge during engagements, because each IP conversing throughout the networks had to be identified to verify it wasn't a malicious connection. Analysts compiled any missing asset inventory information and provided it back to the partner.

An inconsistent asset inventory can slow down incident response and make identifying suspicious or otherwise anomalous activity more difficult to spot. It can also lead to unused devices being forgotten and left on the network, consuming bandwidth and possibly increasing the attack surface of the network. The INL team recommended that asset owners implement inventory management systems to expedite responses to incidents and investigations into suspicious network activity.

3.5. Areas of Excellence

A few of the asset owners required Multi-Factor Authentication (MFA) for remote access to their systems, mitigating the risks posed by third parties. Additionally, some asset owners implemented security tools to enhance the security of network devices. Many were aware of the issues in their networks and were taking steps to address these issues in the future.

4. RECOMENDATIONS BASED ON COMMON FINDINGS

While each site presented its own unique context, many of the observations pointed to shared challenges that are broadly relevant to asset owners deploying digital energy infrastructure. This section distills those lessons into a set of practical recommendations and best practices. These are not intended as prescriptive requirements. Rather, they represent a synthesis of field-validated insights that can help organizations proactively strengthen their digital assurance posture. By applying these recommendations, asset owners can address common sources of risk, such as misconfigurations, insufficient segmentation, or limited visibility, and build more resilient systems that are better equipped to withstand evolving threats. Whether you are in the early stages of deploying digital energy assets or looking to enhance the security of existing systems, the practices outlined here offer a starting point for informed, risk-based decision-making.

- Segment networks and implement layered defenses, DMZs between IT and OT networks wherever possible. DMZs help separate devices that may be accessed remotely from those that should not be accessed. Networks should also be segmented to limit vendor access to the equipment they manage.
- Use technologies such as Virtual Private Networks (VPNs), Virtual Local Area Networks (VLANs), and Multi-Factor Authentication (MFA) to further limit and control the devices vendors interact with.
- Identify ways to bring network and device management in-house instead of relying on third parties.

[4] Idaho National Laboratory/. BESS Procurement Guidance and Sample Contract Terms. https://inl.gov/content/uploads/2023/11/FINAL-BESS-Supply-Chain-Security-Proc-Guidance-Sample-Contract-Terms-Compressed.pdf

- Deploy systems to collect, monitor, and analyze network and device activity to improve system visibility.
- Improve asset tracking and inventory management practices, including the use of systems that can track device firmware versions and vulnerabilities. This can assist in identifying and mitigating device vulnerabilities, as well as expediting investigations and incident response.

5. CONCLUSION

The findings from INL's network assessments underscore the need for stronger cybersecurity and physical security practices across digital energy infrastructure. While no evidence of adversarial activity was observed during these engagements, the assessments revealed a range of vulnerabilities and misconfigurations that, if left unaddressed, could be exploited by malicious actors to disrupt critical operations and impact stakeholders.

Across the sites evaluated, recurring issues included reliance on third-party network management, use of insecure communication protocols, insufficient network segmentation, incomplete asset inventories, and exposure of devices to the open internet. In some cases, devices were found to have known vulnerabilities or unrestricted external access. Physical security controls were also inconsistent, with some systems lacking basic protections (e.g., password enforcement; physical locks).

These vulnerabilities, individually and in combination, create opportunities for adversaries to breach networks, move laterally across systems, and potentially access sensitive OT assets such as HMIs, EWSs, or grid-edge controllers. Third-party management arrangements, while often operationally convenient, can impact an organization's visibility into its own network and introduce additional attack vectors. Similarly, incomplete inventories and unencrypted protocols make it difficult to detect abnormal behavior or prevent unauthorized access.

The goal of this report is to share field-validated insights that can help asset owners and operators (AOOs) strengthen their defenses. The recommendations provided are based on real-world observations and are intended to support proactive risk mitigation. By implementing these practices, AOOs can improve their resilience, reduce exposure to cyber threats, and ensure that digital energy systems remain secure and reliable.