foxguard

Asset Inventory

The First Step in Securing Your Operational Technology

2285 Prospect Dr. NE
Christiansburg, VA 24073
877.446.4732
foxguardsolutions.com

Introduction

We often encounter organizations saying, “We don’t have an asset inventory,” or “We had no idea that was even connected to the network.”

Asset inventory and baselining probably don’t spark much excitement in cyber security, we get it. However, no cyber security plan is complete without a comprehensive understanding of the assets you’re working to protect. Achieving this clarity is easier said than done, particularly in the realms of Operational Technology (OT) and Industrial Control Systems (ICS). Traditional automated asset discovery methods often fall short or even risk disrupting operations in these environments. So, what makes asset identification so unique in the OT world? **Two key factors**: the distinctive nature of OT assets and the potential operational impact.

Why have a complete asset inventory?

The answer is straightforward: to secure business operations. You can’t protect what you don’t know exists. Documenting every piece of equipment and its purpose is essential for evaluating vulnerabilities, applying patches, and monitoring for potential issues. Beyond asset security and business continuity, a thorough inventory is vital for assessing the impact of equipment failures and developing contingency plans to mitigate risks effectively.

OT Assets

OT assets differ significantly from those in traditional IT environments. While there is some overlap—such as HMIs, Historians and SCADA systems, which are often built on conventional servers and workstations—OT also includes specialized equipment like PLCs, switching relays and protection systems. These purpose-built devices are vastly different from the general-purpose assets common in IT. Achieving a comprehensive and accurate asset inventory requires specialized knowledge of OT operations.

The operational impact of OT systems is fundamentally different from that of IT systems. OT assets directly influence real-world physical parameters, not just data on a server. When OT systems malfunction, the consequences can be severe: pipelines may shut down, reactor output could fluctuate dangerously, or— worst of all— safety measures might fail. The criticality of these systems highlights the importance of asset inventory while demanding that discovery processes be carried out with utmost care and precision.

So, how should we go about this inventory?

Assets may include:

Operating systems | 3rd Party Applications | Network Devices | Field Devices | Drivers | Firmware

In addition- HMIs, SCADA and firmware systems may have distinct software packages and/or sub-components that need to be monitored.

Active Asset Recovery

Active asset discovery provides a comprehensive view of networked devices, capturing a wide array of information. This process typically involves scanning network devices by sending packets to every IP address within a specified range and waiting for responses. Once "live" assets are identified, the scanner probes each port to determine which are open for communication.

Although this method is suitable for IT environments with infrastructure capable of handling such traffic, the high volume it generates can lead to risks in OT environments.

In OT settings, availability is critical. Equipment outages, even if temporary, are typically unacceptable outside of maintenance windows.

However, many OT devices can be safely discovered automatically through the network, leveraging the same methods used by engineering software. Industrial protocols like Modbus, Ethernet/IP, Profinet, and Windows Remote Management (WinRM) offer commands to access device identity and configuration. These can be utilized effectively and safely for OT asset discovery without compromising system performance.

What is the alternative to network-based asset discovery if active network scanning is not possible?

Passive Monitoring

Passive monitoring is the preferred method of network-based asset discovery in an OT environment. In passive asset discovery, network traffic is observed and analyzed, generating a list of assets and a profile of how devices are interacting on the network.

This method can be much more time-consuming due to the possible infrequency of asset communication. Without the ability to "interrogate" assets for additional information, such as open ports, possible operating system information, etc., passive monitoring can result in an incomplete picture.

The advantage of this method lies in its ability to observe existing communications with minimal risk to operations. The network is only modified by configuring a span port on a switch/router to mirror traffic to a monitoring system or by using network "taps" to achieve the same result.

After monitoring the network for a specified period and capturing the traffic, analysis tools are used to examine the data and identify assets. Additionally, several purpose-built tools for passive OT network monitoring can perform asset discovery and alert for unexpected or suspicious traffic.

Physical Asset Walkdown

In the OT environment, many assets are either disconnected from the network, part of a closed network, or may not communicate for extended periods, preventing their discovery through digital means. As a result, physical walkdowns are often necessary to ensure complete asset discovery and inventory in OT settings.

A good starting point is the "as built" documentation, if available. However, many OT environments have evolved over years, with equipment added or replaced by various vendors, sometimes without proper documentation or any record of changes. In many cases, operators are only familiar with the equipment's function and lack knowledge of the underlying network. This knowledge gap is a primary reason for incomplete or missing asset inventories. To address this, a physical site walkdown is essential to uncover assets that have been omitted from documentation or undetected by scanning technologies.

Several key characteristics should be recorded during physical asset walkdowns:

- Physical location of the asset
  - Is the physical location of the asset secure? For example, is the asset stored in a locked room or cabinet? Are there additional security measures in place, such as surveillance cameras, to ensure its protection?
- Are there any signs that the equipment has been tampered with?
- Equipment vendor, product and version
- Software running on the system
- Network connections to and from the system
- Other physical connections to the system
- User accounts
- Does the system have a password that can be changed?
- Can software be added?
- What protocols are in use by the device?
- Does the device have wireless capabilities?
- Can removable media be attached?
- What types of physical port connections does the device have?
- Does the device keep log data?

These are just a few of the many questions that need to be addressed during asset discovery and inventory, preparing you for the next steps in securing your environment. This asset walkdown should not only include the devices you can see; it also needs to be a thorough walk-through. Open the cabinets, look in the closets and trace out that wire. Sometimes this means accessing an equipment rack suspended from the ceiling, but you need to get in there.

While the task at hand is undeniably challenging, it is an essential pillar of your cyber security strategy.

Conclusion:

Identifying your assets is just the beginning. To maintain an effective cyber security posture, it's essential to manage and update this inventory regularly. Leveraging technology for asset tracking ensures compliance, enhances efficiency, and forms the core of your cyber security strategy. This aligns with the 'Identify' phase of the NIST Cybersecurity Framework and makes it possible to manage all other security functions effectively.

How Foxguard Helps

At Foxguard, we understand the challenges utilities face in achieving and maintaining NERC CIP compliance. That's why we offer integrated solutions that unify patching, compliance, and vulnerability management through tools that simplify asset consolidation, enabling a streamlined, end-to-end approach tailored to critical infrastructure.

With Foxguard, utilities can:

- Consolidate IT and OT asset inventories
- Identify and prioritize vulnerabilities with actionable remediation
- Maintain compliance without operational disruptions

Trusted by over 800 customers across the energy, nuclear, and transportation sectors, our track record includes a $4.3M cooperative agreement with the U.S. Department of Energy (DoE) to develop a national Patch & Update Management Program.

Rather than managing siloed tools and vendors, Foxguard unifies cyber security requirements into a single, streamlined framework. This simplifies complexity, reduces overhead, and enables seamless integration across IT and OT environments. The result: improved visibility, fewer gaps, and a stronger, more efficient security posture.

About Foxguard

Foxguard is your trusted advisor at every stage of your cyber security, custom computing, and digitization journey. For critical infrastructure, we enhance operational safety, quality, and uptime by strengthening your cyber security maturity. We also meet your custom computing needs through end-to-end system integration of hardware and software solutions, ensuring a secure supply chain and effective lifecycle management. Foxguard is a wholly owned subsidiary of Framatome Inc. and a key part of the Framatome Cybersecurity Solutions line.

7k+	1.5M+	30k+	40+
Patch availability reports produced	Asset patching supports	Customer computing deployments	Years in business, since 1981

Contact:
877.446.4732
2285 Prospect Dr. NE
Christiansburg, VA 24073
foxguardsolutions.com