SANS

A SANS Whitepaper

ICS Asset Identification: It's More Than Just Security

Written by **Mark Bristow**

June 2020

Sponsored by:

Tenable

Introduction

Without a solid understanding of the assets on your ICS network, it's impossible to develop and implement a strategy to manage risk and ensure reliable operations. Asset identification was the No. 1 concern of 338 ICS security professionals participating in the SANS 2019 State of OT/ICS Cybersecurity Survey.[1] Historically, asset identification has been associated with time-consuming and costly efforts to identify and maintain an accurate inventory, with more than half of operators spending 20–80% of their time just finding and validating plant information.[2] Despite this operational focus and perhaps due to mismatched expectations, this critical and fundamental step is not always the board's top priority for the CISO.

In this whitepaper, we provide recommendations and guidance covering:

- How to articulate not just security ROI, but business ROI—such as reducing mean time to recovery (MTTR)—to senior management and board members to obtain the resources needed to start an asset identification program
- How asset identification can support operations beyond cybersecurity
- How to get quick wins by leveraging information you already have to bootstrap an asset identification program
- What techniques you can use for ongoing asset identification maintenance with limited human resources

[1] "SANS 2019 State of OT/ICS Cybersecurity Survey," June 2019, www.sans.org/reading-room/whitepapers/analyst/2019-state-ot-ics-cybersecurity-survey-38995

[2] "Plantman Go: The future of asset lifecycle modeling," Sept. 22, 2016, www.controlglobal.com/articles/2016/plantman-go-the-future-of-asset-lifecycle-modeling

What Is Asset Identification?

You cannot defend what you cannot see. As previously mentioned, asset identification was the No. 1 concern among respondents in the SANS 2019 State of OT/ICS Cybersecurity Survey. Despite this priority—and, in many organizations, being supported by significant resourcing—asset inventories continue to be unreliable and incomplete, compounding problems during both emergency and routine events. Motivations for performing asset identification can vary from organization to organization. In some cases, regulatory requirements such as NERC-CIP-002 drive identification efforts, while ensuring appropriate depreciation schedules or looking for hidden operational costs drives efforts in others. Regardless of the motivation, asset identification comes in many forms and can be as simple as a walk-down inventory stored as a spreadsheet maintained by the operations team or something as complex as continuous automatic discovery scanning and network change management solutions. Generally, asset identification techniques fall into four categories:

- Physical inspection
- Passive discovery
- Configuration analysis
- Active discovery

Physical Inspection

Physical inspection entails tracing every piece of fiber, ethernet, serial cable and wire throughout your process facility to validate what systems are connected. If performed properly, physical inspection typically results in gathering the most comprehensive data and uncovers assets you would not be able to identify using other means. To get started, begin at the most upstream connection point on your network—likely your corporate network firewall—and trace every wire as it splits off various in-line devices. Physical inspection is particularly effective for initial asset inventory development. However, it does not have the scalable benefits and ease of automated updates found in passive or active discovery, nor the additional context available in configuration analysis. Physical inspection is extremely labor-intensive, making it the costliest method. But properly implemented, it can be a great way to build your asset inventory program.

Passive Discovery

Passive discovery consists of leveraging passive network, wireless and serial monitoring technologies to identify assets communicating in your system. This technique requires the installation of passive monitoring technologies in your communications system; but once the technology is installed, it is one of the lowest impact techniques for asset discovery. It can be left in place not only for continuous monitoring of assets, but also for network communication baselining and monitoring.

Passive discovery tools are more robust for traditional network technologies and protocols, such as ethernet or TCP/IP, and less robust for industrial protocols, such as Profibus or Modbus. Passive discovery can be a great tool for identifying assets at Purdue Model Level 2 and above rapidly. However, you will likely have difficulty identifying field devices and I/O without inferring their existence from the communication content, which may miss identifying critical devices (see Figure 1).

Some control devices—for example, ones in report-by-exception modes—do not produce much, if any, traffic during normal operations and, therefore, might be missed by passive techniques. Passive discovery can also be limited by devices behind network address translation (NAT) or multi-homed stations that relay traffic between networks but mask the end assets. It's also important to monitor the wireless spectrum in your plant because you may have WirelessHART, Zigbee, Wi-Fi or Bluetooth devices you were not accounting for that are not visible via other analysis techniques. Additionally, with older networking devices commonly found in ICS environments, the equipment may not have sufficient computational capability or memory available for a SPAN/mirror port configuration, which can introduce latency or packet loss on the network. Passive discovery may not be the ideal technique for building a comprehensive initial asset inventory, but with properly implemented open source or commercial tools, passive discovery can help maintain existing inventories.

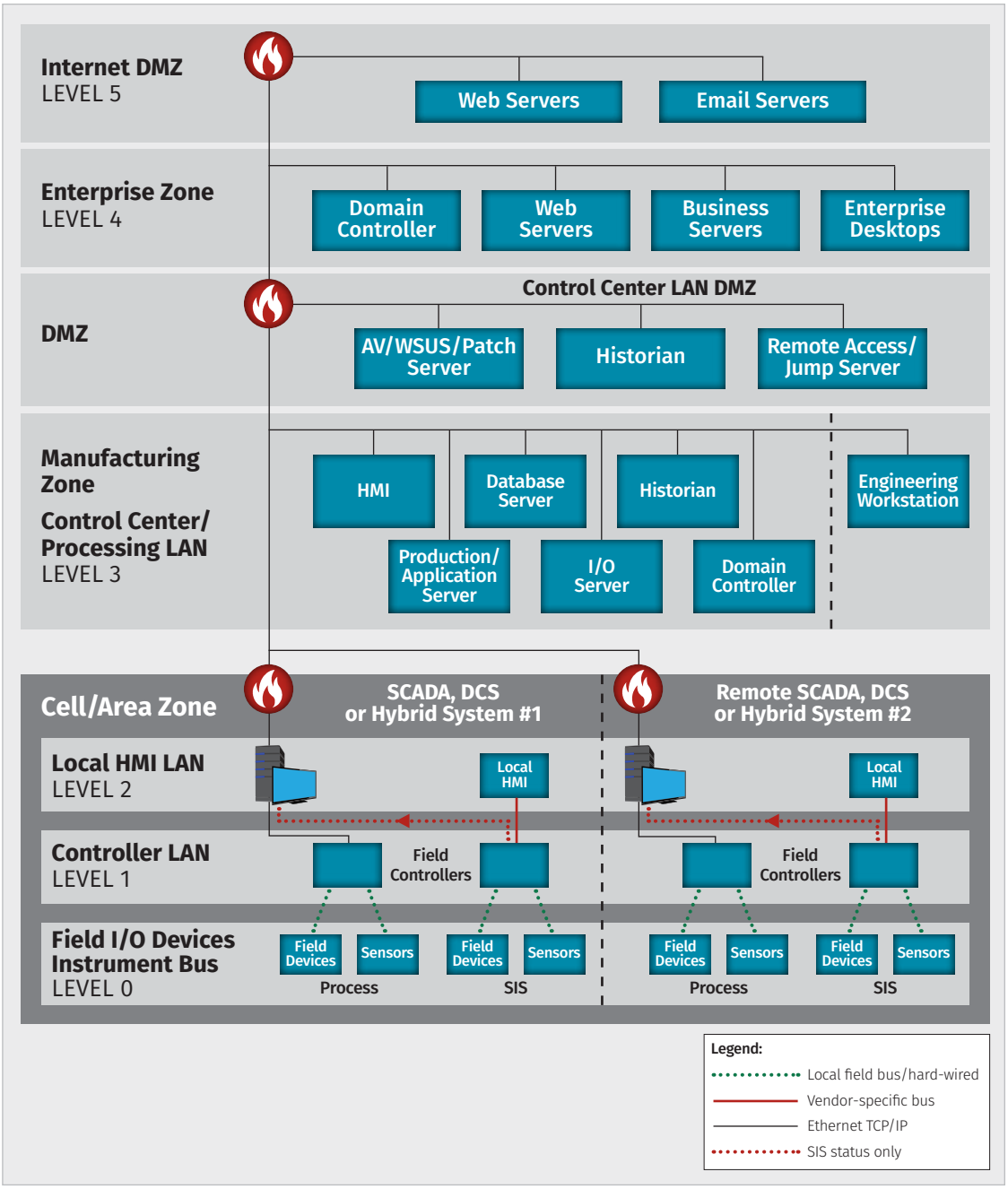

Figure 1. Recommended Secure Network Architecture Using the Purdue Model (ICS-CERT)[3]

[3] "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies: Industrial Control Systems Cyber Emergency Response Team," Sept. 2016, www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf, p. 17, Figure 5.

Configuration Analysis

Configuration analysis is a technique that takes existing configuration data from process control systems, networking devices, process diagrams and other configuration sources to create a picture of known assets. Configuration analysis can be completely passive, similar to passive discovery leveraging static configurations, or more active by leveraging automation to evaluate configurations continually. Unlike physical inspections, configuration analysis techniques can scale to the entire plant rapidly by leveraging just a few staff hours compiling and normalizing multiple configuration sources, as illustrated in Figure 2.

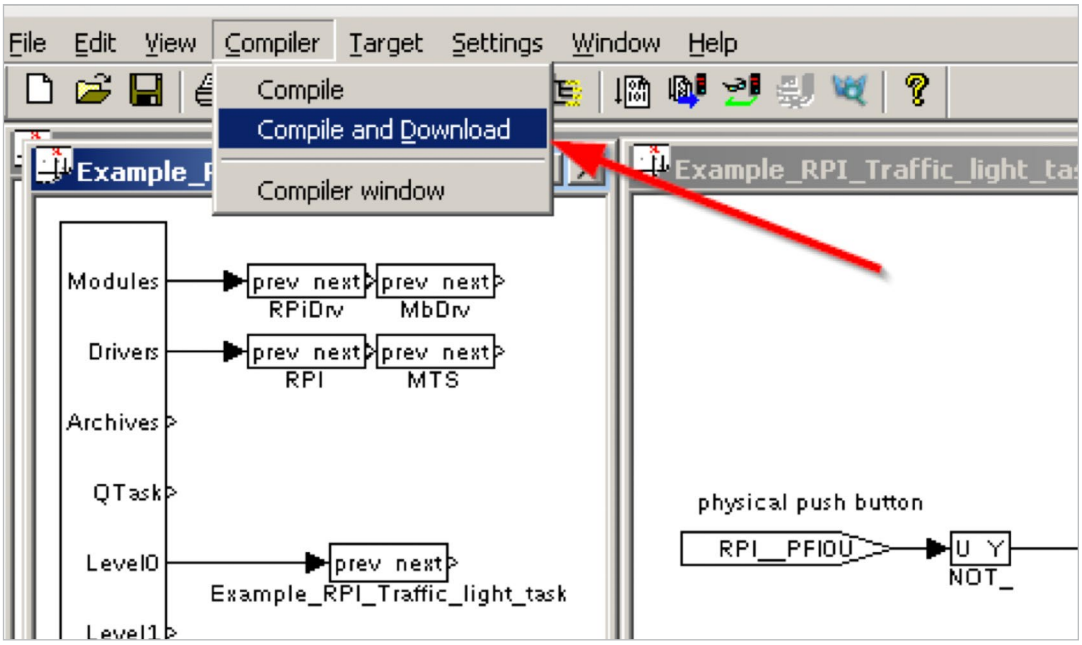

Figure 2. Ladder Logic (Source: ICS515 Workbook)[4]

Most configuration analysis tools and methodologies on the market focus on more traditional IT devices such as network switch and firewall configurations. In OT environments, these devices are often configured in incredibly permissive ways—for example, firewall rules allowing any/any on a segment, and therefore are not of high enough resolution to provide comprehensive results. In OT environments, there are often rich datasets for configuration analysis from the control system itself. Some configuration analysis tools specific to the ICS domain process logic files, controller or I/O configurations, or other process configuration data from the engineering workstation. Pulling in historian data can provide a robust set of information—and correlating it with other configuration sources can also help build a compressive asset inventory.

Using the OT system configuration information is the most economical way to get discovery information from Level 1 and Level 0 devices to ensure a comprehensive inventory. The challenge with configuration data analysis is pulling from non-homogeneous control environments with multiple vendors or models to process and normalize the configurations into a consumable format. Completing these normalization transformations can be a complex process requiring development and maintenance of the normalization process, or asset owners can acquire commercial professional solutions that can perform transformations up to date. Creating appropriate transformations may be time-consuming in complex systems, but once a set of suitable transformations is developed or acquired, it can be re-used.

[4] www.sans.org/course/industrial-control-system-active-defense-and-incident-response

Because configuration data is based on the operator-intended configurations and reflects a snapshot in time, it will not reveal unauthorized systems in an environment, such as a "rogue" workstation that is not part of the official configuration of the plant but has been installed by field technicians. Some tools on the ICS marketplace are being leveraged to do continuous or "active" configuration management analysis. This continual evaluation of configuration data—to include, in some cases, retrieving this data by uploading it directly from controllers—allows for nearly real-time updates of asset inventories, as is possible with passive and active discovery methods.

Configuration analysis is one of the best ways to get comprehensive OT information into your asset inventory and can provide a great baseline and contextual process information that cannot be obtained by other asset identification techniques. This might be the only technique that is practical to leverage against isolated and disconnected environments such as safety systems.

Active Discovery

Active discovery is a technique that uses active network communications to identify devices in the environment. These probes can be generic to the communications technology, such as an ICMP ping, or specific to the protocol, such as a Modbus unit identifier scan. Active discovery is able to identify devices that are otherwise dormant on a network. It might, however, miss devices that are configured to respond only under specific circumstances, such as a specific Master ID. Active discovery can cause negative interactions with some older equipment with non-compliant protocol implementations, causing them to lock up network interfaces or exhaust CPU resources. Because of this, organizations should test their active discovery processes on representative equipment prior to deploying it in production environments. Active discovery can also introduce additional latency into the environment, which could have negative process consequences in low-bandwidth, high-latency communications networks. Many active scanning tools are adapted from IT security or asset management tools and are not likely to provide comprehensive identification of devices using non-TCP/IP or serial protocols.

Over the past several years, multiple vendors have developed purpose-built OT-specific asset discovery tools that mitigate many of the risks of using IT tools in an OT environment. These OT-specific tools use the ICS protocols themselves to interrogate the environment, which allows security teams to incorporate more ICS-specific context into the scanning. Even with these new tools, it is critical that active scanning be tested on representative equipment before being leveraged in a production environment.

Bootstrapping an Asset Identification Program

Often a small team of engineers is assigned the task of creating a comprehensive asset inventory without many resources or much direction. Bootstrapping an asset identification program may initially seem to be a gargantuan task. By following some simple steps, as outlined in Figure 3, a small team can compile an asset inventory for a large and complicated system with ease. Oftentimes the hardest part is getting started.

Start Small

The most common misstep in an asset identification process is not properly setting the scope. Teams often want to start by putting in passive monitoring points all over the plant. The best approach is to start small and pick a subprocess—or even an unrelated process—to hone the process that will best suit your environment.

New asset identification programs often try to start by using active or passive asset discovery methods due to their perceived low barriers to entry. While these are great tools for growing and maintaining an asset inventory, many times starting with a small set of assets and conducting a physical inspection, combined with manual configuration analysis, yields the most complete results and more rapidly identifies deficiencies in the asset identification process. Once an initial asset scope has been mapped and the processes have been refined, adding in automated configuration analysis as a next step can help make your inventory more comprehensive. Note that adding automation might require additional investment to process the configuration information—so ensure your configuration tools work with the types of process control equipment you have. Finally, when transitioning from a building mode to a refining one, adding in active and passive methodologies for discovery and maintenance helps ensure your inventory stays up to date.

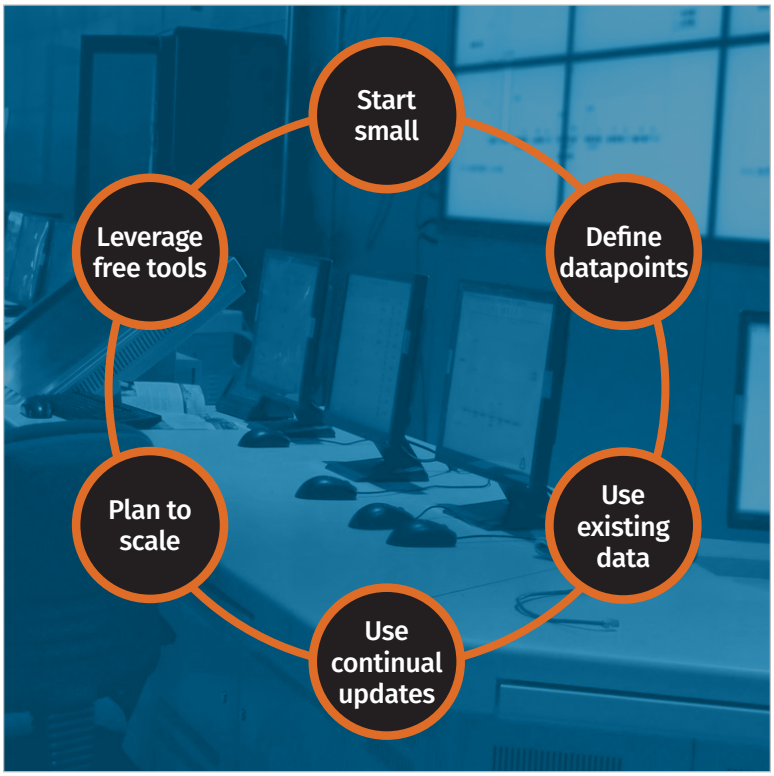

Figure 3. Compiling an Asset Inventory

EXPERT ADVICE:

Your initial scope does not necessarily have to be part of your main process control system. For example, one team started by mapping out the management building's HVAC system as a way to refine the process for a lower-stakes system before moving to the plant. Starting in a training/test environment can also increase success with initial efforts.

Define Datapoints

When beginning an asset identification program, be sure to include at least the following essential information for each asset, including any additional datapoints that might be relevant to your system. It's critical to capture not only the physical asset information, but also the logical information and the planned communication pathways and protocols. Be sure to include:

- Unique asset ID
- Business unit
- Device type
- Asset name
- Manufacturer
- Model number
- Serial number
- Sub-assets (such as daughter cards)
- Asset function
- Impact on operations
- Physical location
- Firmware revision
- Patch levels
- Primary network information (ethernet, serial, fiber)
- Secondary network information (microwave, backup cellular, VSAT)
- Connected wire tags/circuit information
- ICS protocols in use
- Location of configuration information
- Location of configuration offline backup
- Associated I/O points or tags
- Asset owner and contact Info
- Process owner and contact Info
- Links to parent assets
- Links to child assets

In the first pass, you will likely not be able to collect all of this information—and some of these data points might not apply to every asset type. Still, this list helps to orient your process. As your process expands, you will begin to have subassemblies and correlations between assets as well, so plan for linkages in your initial data model.

Use Existing Data

New asset identification efforts often overlook existing documentation and data repositories that can be helpful for identifying assets. Look for existing network maps or other documentation that might shed light on assets in the field. Review process and historian data that may include configuration and asset information. Review vendor documentation from recent system upgrades. Be sure to review build, wiring, piping and instrumentation diagrams. Even if they are not fully up to date, they can help you get your process started with minimal effort.

Use Continual Updates

Far too often, asset identification programs are successful in creating a comprehensive asset inventory but are never updated. When starting a new program, be sure to define program update intervals at the beginning of the process. A best practice is to build asset identification updates into your change control processes to ensure that, as changes are

processed, they also get updated in the asset inventory database. If you are leveraging ongoing assessment tools (such as active or passive monitoring), ensure that proper network segmentations are in place (such as data diodes) so the asset monitoring system cannot be used as a back door into your process. Although asset identification is a continual process, you should revisit your processes no less than annually.

Plan to Scale

One mistake many initial asset identification programs make is keeping the asset data as a "close hold" dataset that is in spreadsheet format and accessible only to a handful of core team members to preserve integrity. Such practices all but guarantee that asset inventories will be frequently out of date and not applicable to the rest of the business. Use a shared platform and allow anyone involved with the process to propose updates to the asset inventory. If an update outside of an identified asset identification process is proposed, validate and accept the change—and investigate how the change was not captured by previous efforts or through integration with the change management process. If asset inventories are viewed as living documents and are frequently referred to by operations personnel, those same personnel can make small corrections when they are identified.

Asset inventory data is an incredibly valuable asset, both to you and an adversary. Ensure you have proper access control and non-repudiation to protect this critical data from confidentiality or integrity breaches. To ensure availability, periodically store encrypted offline backups of this information so it's available in the event of a catastrophic failure.

Leverage Free Tools

Recent market developments have increased the sophistication and diversity of asset identification products in the marketspace. While professional tools allow for more advanced features, enhanced workflows, expert support, ICS integration and ease of use, there are a handful of free ICS asset identification tools that can be used for budding ICS asset identification programs. Organizations can and have successfully leveraged many of these free and open source tools to implement large-scale and robust asset identification programs. The savings in capital costs for the free tools frequently requires more labor hours to implement than their correlating professional tools, so we recommend you do a cost/benefit analysis. Remember, though, free tools, such as the ones described in the following sections, can help prove out the pilot effort benefits with minimal investment.[5]

GRASSMARLIN

GRASSMARLIN[6] is an open source passive discovery tool that can map ICS into a visual or exportable topology map. GRASSMARLIN can analyze live network tap, span traffic or existing packet captures and attempts to perform device fingerprinting, network communication flow fingerprinting and other passive analysis techniques.

---

[5] This paper mentions product/solution names to provide real-life examples of how ICS tools can be used. The use of these examples is not an endorsement of any product/solution.

[6] https://github.com/nsacyber/GRASSMARLIN

CyberLens

CyberLens[7] is a free, passive discovery ICS network visibility tool. CyberLens performs deep packet inspection on a handful of ICS protocols from live or offline captures and can identify I/O and protocol commands of IP-based communication to build and map an asset inventory. CyberLens identifies ICS assets by passive discovery and inference of control data flows based on deep packet inspection.

Snipe-IT

Snipe-IT[8] is an open source asset management platform for tracking IT assets. Snipe-IT is not designed to track ICS assets, but it is customizable and can replace basic spreadsheets to provide more robust asset management tools. Using an asset management tool allows for more advanced features such as nesting assets and asset families, which can allow for easier searches of complex asset interactions in control environments.

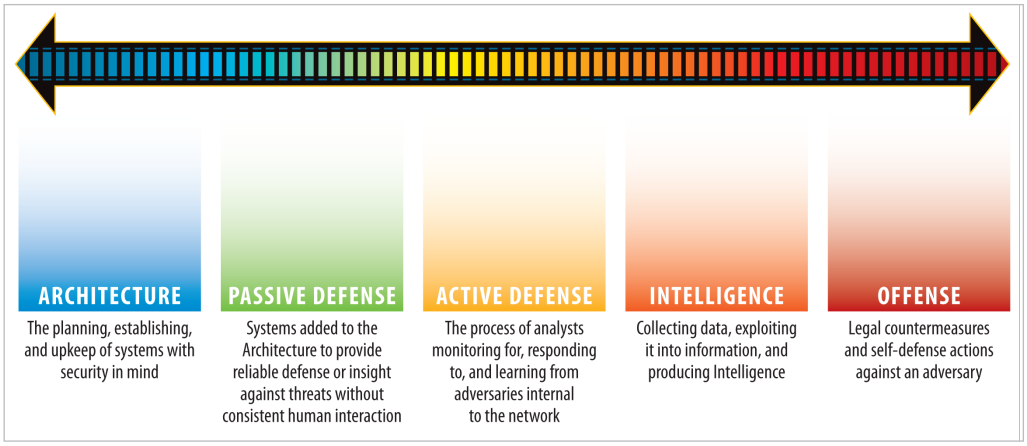

Figure 4. The Sliding Scale of Cyber Security[10]

Cybersecurity Application

Strong asset identification is a foundational step for ICS security efforts. As Rob M. Lee articulated in his paper "The Sliding Scale of Cyber Security,"[9] asset identification is a critical foundational step for all ICS security efforts, a precursor even to architecture design. Without asset identification, all of the subsequent steps of the sliding scale cannot be completed, because they rely on accurate, authorized asset inventories to be effective. See Figure 4.

Without comprehensive asset inventories providing that core foundation, other elements of a cybersecurity life cycle are not as effective. To understand why, we need to start by understanding the NIST Cybersecurity Framework, as illustrated in Figure 5.

Figure 5. NIST Cybersecurity Framework[11]

[7] https://dragos.com/cyberlens-download/

[8] https://snipeitapp.com/download

[9] "The Sliding Scale of Cyber Security," August 2015, www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240

[10] "The Sliding Scale of Cyber Security," August 2015, www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240, p. 2, Figure 1.

[11] "NIST Releases Version 1.1 of its Popular Cybersecurity Framework," Apr. 16, 2018, www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

Leveraging that framework, let's look at how asset inventories play a role in each of the phases:

- **Protect—**With a compressive asset inventory, you can ensure that defensive measures and controls have been applied or cover all of your assets. If there are gaps in coverage, they are apparent. Comprehensive asset inventories also enable some more advanced cybersecurity protective controls and defenses.
- **Detect—**With a comprehensive asset inventory, you know what should be in the system and how it should behave, enabling security teams to detect new or anomalous behavior in your system.
- **Respond—**Having a comprehensive asset inventory allows you to more rapidly identify where an issue has occurred and determine which other assets might also have also been impacted.
- **Recover—**When recovering from an incident, comprehensive asset inventories allow you to recover faster and with more surety and reduced unintended impacts. You can ensure you've completely remediated the environment before returning to normal operations.

These are only some of the cybersecurity benefits of asset identification. Many papers have been written on how asset identification supports cybersecurity efforts, such as the excellent paper by Dean Parsons and Doug Wylie, "Practical Industrial Control System (ICS) Cybersecurity: IT and OT Have Converged—Discover and Defend Your Assets."[12]

Non-Security Applications for Asset Identification

Asset identification, while often thought of in the context of compliance and cybersecurity, is critical in more than just the cybersecurity domain. Complete, accurate and up-to-date asset inventories can support a variety of non-cybersecurity purposes that rely on complete and accurate asset identification programs, as described in the following sections.

Failure Analysis

Every system or process will eventually fail. "A risk quantified is a risk mitigated" is a fundamental principle of risk management. Failure analysis is critical to industrial applications and processes because failure needs to be quantified so it can be mitigated with either redundancy or other compensating controls. Failure analysis techniques, such as Failure Modes & Effects Analysis (FMEA), Hazard and Operability Analysis (HAZOP) and Probabilistic Risk Assessments (PRA), all rely on complete and accurate asset inventories of both hardware and software assets as prerequisites to these processes.

[12] "Practical Industrial Control System (ICS) Cybersecurity: IT and OT Have Converged—Discover and Defend Your Assets," September 2018, www.sans.org/reading-room/whitepapers/analyst/practical-industrial-control-system-ics-cybersecurity-ot-converged-discover-defend-assets-38620 [Registration required.]

In the FMEA model, the first step in the process is to take an inventory of all assets that make up the target process so they can be assessed. If the initial inventory is inaccurate, the FMEA team cannot make assessments about probability or severity of the impact of a component-level failure on the overall process. Without a comprehensive inventory of assets, FMEA analysis would be incomplete and could lead to significant risks not being appropriately accounted for. See Figure 6.

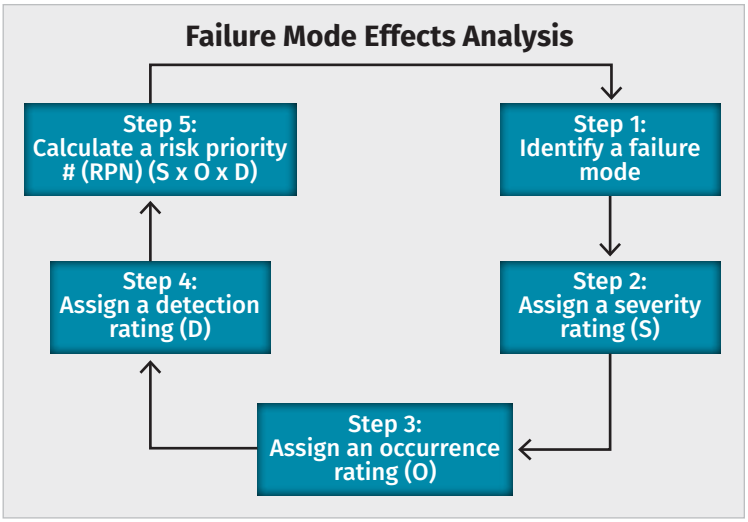

Figure 6. FMEA Process[13]

Similarly with a HAZOP analysis, asset identification plays a role throughout the entire process but is critical in the scope definition and data collection phases. If key components of a process are not assessed as part of the HAZOP analysis, the subsequent risk analysis and certification of safe operating procedures are inaccurate.

Mean Time to Recovery

Comprehensive risk analysis can help mitigate specific process components to lengthen the mean time to failure (MTTF). However, in nearly every environment, process failure occurs at some point. When it does, having a preexisting understanding of the process and its components is critical to identifying and mitigating the root cause. Having an accurate, comprehensive inventory directly reduces the mean time to recovery (MTTR).

Process Integrity and Safety

Without a comprehensive inventory of the assets and components in your process, as well as their designed functions, tolerances, systematic capability, failure likelihood and consequences, you cannot ensure that your process operates as intended. This lack of knowledge has implications such as lost production and unscheduled downtime. Asset identification is fundamental to analyses, including IEC 61850 or other safety systems standards for your industry. Having an incomplete asset inventory can impact your regulatory and/or insurance risks when you cannot complete safety integrity level (SIL) analysis. Ultimately, you can't have true safe and reliable operations without asset identification.

From the Field

Once, while supporting a coal-fired power plant, the author experienced an outage with the plant's continuous emissions monitoring system (CEMS) that required resetting the controller manually. The system had been installed without issue several years prior; however, none of the current staff could recall the physical location of the controller. With the potential regulatory risk of this outage, it became a key priority of the plant to find the errant controller to return to normal operations. With a comprehensive asset identification program, this information would have been readily available, resulting in a more rapid recovery.

[13] https://13485store.com/articles/using-fmea-to-manage-risk

Best Practices

With a robust asset identification program established, the following concepts will help your organization refine and improve the asset identification process. With these improvements, organizations can minimize costs and maximize utility from their asset identification program.

Use Multiple Analysis Techniques

One key mistake asset ID programs make is focusing on a single asset identification technique for their program: physical, passive, configuration or active. While it's recommended that organizations start with one or two of these techniques to begin their programs, mature programs combine multiple techniques to identify assets and keep their inventories up to date. For example, TCP/IP networking information, such as IP addresses, often change, so while a physical inspection may have been used to build a base asset inventory, using a passive monitor to update that IP information can reduce the frequency of manual updates. Consider matching on other network information such as MAC address and/or in-use protocols to align disparate data sources. Many asset ID programs also conduct active scanning during planned outages to further validate their inventory. It also can be useful to periodically validate that change control processes are effective by verifying configuration analysis data to determine whether the process configuration changed.

Don't Forget Plant Data

This is asset identification for operational technologies, not information technology! Especially because OT equipment sometimes behaves in unexpected ways to asset identification technologies designed to monitor IT systems, don't overlook the plant data. As an extension of the configuration analysis technique, examining plant data from the process control system itself can be extremely valuable. While plant and configuration data comes in a variety of formats, several commercial solutions exist that can process and normalize this data to discover previously unknown assets. This normalized data is directly derived from the intended plant configuration and can identify otherwise hard-to-discover assets. In more complex situations, it can correlate that asset inventory data with contextual process information such as process and historian tag information, which can accelerate root cause analysis.

Different Plant States

If you are using passive monitoring as a tool for asset identification, it's important to monitor the network during different plant operational modes. The network of a plant running in normal operations can appear differently during an outage, constrained operations or a safety event. Frequently, control equipment is not active in the network, except during report-by-exception events that can occur during different plant operation modes. Oftentimes, safety systems generate no network communications outside of a safety event. You can expect new communications pathways and flow, which are important to account for in your asset inventory baselines, to exist in different plant states.

Don’t Ignore IT Data

There is a tendency in the ICS community to be somewhat dismissive of IT challenges, protocols and concepts, focusing solely in the OT aspects. Because many OT networks run on IT platforms, such as Windows, Active Directory or Network File Systems, it can be helpful to consider the IT fabric under your OT network. The majority of traffic on OT networks, perhaps with the exception of field devices, is on IT protocols such as TCP/IP. Don’t ignore this rich data. IT networks also have several types of auto-discovery protocols and broadcast messaging, including NetBIOS, LLDP and Bonjour, that can be helpful with asset identification, even if it’s just to identify an IT device on the wrong network when using passive analysis techniques. Also consider how your asset identification program for OT can inform your IT asset management programs and vice versa, enabling the business to leverage consolidated reporting and management.

Articulate Value to the Business

Industrial control systems do not exist in a vacuum. These capital-intensive investments are built to increase efficiency and/or decrease costs for the production of the commodity that the system was designed to produce, be that corn chips or electric power. Security professionals don’t realize and often forget this context when proposing investments in security functions such as asset identification. Security initiatives are often viewed by the business as cost centers, not in terms that demonstrate the value to the business. Executive boards have a fiduciary responsibility to return value to their investors, so as security professionals, we need to ensure that we are effectively communicating value in terms the business leaders can understand and get behind.

You can directly attribute asset identification efforts to cost savings and/or profit increases in the following ways:

- Reduced MTTR increases productivity and profit. Having a comprehensive asset list allows engineers to recover operations more quickly. One day of extra uptime might pay for the entire program.
- Clear asset inventories can identify assets needing maintenance or replacement before they impact the process, increasing MTTF.
- Inaccurate asset inventories create unaccounted-for risk that cannot necessarily be managed using existing processes and tools, such as insurance.
- Having complete asset inventories ensures that your safety engineering and analysis is complete, as well as the safety of your personnel and assets.
- Comprehensive asset identification programs can reduce regulatory risk of “off the books” assets that don’t follow security compliance rules.
- Investments can initially be small with minimal scope and use free or open source tools to prove the process.
- Leveraging modest investments in automated asset identification can be instituted on a continual basis, reducing associated labor costs.
- Comprehensive asset inventories position the organization to better understand and manage cybersecurity risk.

Conclusion

Asset identification is a critical and fundamental step in ensuring the safe and reliable operations of your process. There are several key approaches to asset identification, physical, active, configuration and passive techniques. All have areas where they excel—but successful asset identification programs utilize more than one analytic technique. Asset identification does not need to be an arduous task; if you stay focused, utilize the resources you have at hand and follow a few key tips, you can successfully and rapidly build out your program.

Asset identification is not just a cybersecurity tool. You can use asset identification techniques to provide support for reducing recovery times and lowering organizational risk in other areas. When attempting to get resources for a new asset identification program, it might be best to articulate the benefits of such a program to reliable operations and safety instead of security. Such benefits will enhance your case to business leaders.

About the Author

Mark Bristow, a SANS instructor for ICS515: ICS Active Defense and Incident Response, is Branch Chief for Cyber Defense Operations at the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), using his expertise in incident response (IR), industrial control systems, network monitoring and defense to support national security interests. Before that, Mark was Chief of the ICS Cyber Emergency Response Team (ICS-CERT) incident response. He also worked for CSRA and Securicon, supporting a variety of private and public sector clients. Mark has been involved in high-profile IR efforts, including the Ukrainian power grid attack, intrusions into U.S. election infrastructure and Russian attempts to access the U.S. power grid.

Mark would like to thank Jonathan Homer, ICS Subject Matter Expert, and Dean Parsons, Certified SANS Instructor, Cybersecurity Leader & ICS Cyber Security Officer, for their contributions to and peer review of this paper.

Sponsor

SANS would like to thank this paper's sponsor: