INDUSTRIAL CONTROL SYSTEMS
Community of Interest

GUIDANCE: VISIBILITY FOR INDUSTRIAL CONTROL SYSTEM / OPERATIONAL TECHNOLOGY ENVIRONMENT ASSET MANAGEMENT

Introduction

NCSC has generalised asset management guidance which can be found here - https://www.ncsc.gov.uk/guidance/asset-management, while this article is part of a series of Industrial Control Systems (ICS)/Operational Technology (OT) specific guidance articles on Asset Management first introduced here . In this article we shall be focussing specifically on the asset visibility challenges and methods to overcome them in ICS/OT environments.

Asset visibility plays a vital role in any ICS/OT cybersecurity programme. Having a clear understanding and comprehensive inventory of all an organisations ICS/OT equipment provides the foundation that many other Cyber Security measures are built upon. The old adage ' You cannot defend what you do not know about' is important when securing the ICS/OT estate. Given the extent of the ICS/OT environment in a lot of companies, it may not be possible to physically survey every piece of ICS/OT equipment and understand how it is or not connected to the network. Even when a physical survey is possible, support and other vendor agreements may prohibit detailed inspection of "black box" system of systems components. And while a facility may have a list of assets from their integrator who first set up the facility, these are often out-of-date and not trusted, especially if the company has been a subject of mergers and acquisitions.

A lot of organisations believe they know about their ICS/OT assets attached to their core business processes but may not necessarily be aware of rogue or hidden components that open their ICS/OT environment to enhanced risk and may have neither technology nor processes in place to detect new unauthorised or even deliberately planted malicious components in real time.

Given the challenges highlighted below that organisations are faced with, such as remote sites and/or large and complex facilities. This could be a laptop that someone has connected at a remote site for a technician to provide on-site troubleshooting, to an old, retired external USB storage device for backups that remains plugged into the central facility network. An advantage of segmentation employed within ICS/OT environments is that organisations should be able to physically locate them once discovered.

This type of unknown asset is most likely to surprise the ICS/OT security professional while also likely to be something that a threat actor could take advantage of.

Challenges

Grasping the importance of asset discovery to ICS/OT security requires looking no further than the old adage mentioned above. More specifically, without adequate visibility into the engineering workstations, programmable logic controllers (PLCs), remote terminal units (RTUs), sensors, actuators, internet of things (IoT) devices, and other assets that comprise an ICS/OT environment, it is largely impossible to adequately secure it.

Indeed, this is precisely why widely adopted cybersecurity frameworks and guidelines from the International Organisation for Standardisation (ISO), the National Institute of Standards and Technology (NIST), NCSC's Cyber Assessment Framework (CAF) and many others all recommend asset discovery and an external connectivity audit as the first step on the ICS/OT security journey. ICS/OT security practitioners looking to take this step should consider that the following variables often cause or exacerbate an array of related challenges to asset discovery:

- **Proprietary Protocols:** Unlike their information technology (IT) counterparts, most ICS/OT assets communicate using vendor-specific proprietary protocols. Not only are such protocols incompatible with traditional (i.e., IT-oriented) inventory and security tools, but many are also not even supported by all ICS/OT-specific auto discovery solutions. Generally speaking, if a solution's protocol coverage does not include all protocols used within a given ICS/OT environment, the solution will be unable to provide full visibility into that environment. A common question that ICS/OT Security teams ask themselves is "do I need to have security concerns over network communications that are NOT Ethernet-based, such as Profibus DP, Profibus PA, Modbus, DeviceNET etc". Some ICS/OT security teams have the opinion that the non-Ethernet-based physical layers are so far down the network you would normally have to be physically on that bus segment to have any effect. A counter example might be that an attacker could reach the Ethernet side of a PLC or RTU and possibly try to disrupt Process variables that have come into that PLC via its lower networks such as Profibus, Modbus, DeviceNET etc. This perspective is something that needs due consideration within an organisations Risk Assessment process.
- **Non-standardised Technology:** Another key difference between IT and ICS/OT assets is that the latter can have a lifespan of several decades. As such, it is common for industrial organisations to amass an idiosyncratic set of new and legacy ICS/OT assets from a range of vendors. This lack of standardisation increases the volume of different protocols, prevalence of unsupported systems and unfamiliar technologies, and overall complexity of the ICS/OT environment, thereby further complicating asset discovery efforts.
- **Fragility**: Beyond the aforementioned protocol and non-standardisation issues, an additional reason why IT-centric inventory and security tools are incompatible with ICS/OT environments is that these environments tend to be uniquely fragile and unable to accommodate the extent of traffic generated by such tools. Certain assets — and, thus, the physical processes they control or otherwise support — can even be compromised to the point of impacting operational availability, integrity, and/or safety in situations where an unsuitable tool is used within the ICS/OT environment.
- **Intentional Network Segmentation and Segregation:** Designing an ICS/OT environment utilising the Purdue Model and following standards such as IEC62443 means that network segmentation and segregation are employed as part of the cyber security model, which in turn can provide a challenge to achieving full visibility of all assets easily, although Asset discovery tools are useful in places, such as defining the IT and ICS/OT environments and boundary, allowing IT asset management tooling to cover the IT

environment, and specific ICS/OT asset management tooling to cover the ICS/OT environment.

- **Legacy:** Some ICS/OT environments have been in place for 30 years plus, and therefore there may be old networking equipment providing connectivity or devices that are unable to run the latest type of technologies. With regards networking equipment, legacy network switches, or basic, unmanaged network switches can mean that features such as being able to have SPAN/Mirror ports are not available or are limited (not lending themselves well to segmentation either). Legacy elements also impact where the OEM software will only run on a legacy operating system, thus limiting options for the likes of Host based Agents to be deployed without investment in upgrading hosts and virtualising instances of legacy operating systems.
- **Limited Maintenance/Upgrade Windows:** Maintenance windows in which upgrades can be made are usually highly constrained in ICS/OT environments. Upgrading an asset often requires the asset to be shutdown thus impacting the physical process it controls, which risks operational downtime.
- **Variety of communications media:** Given the legacy aspect and the non-standardised technologies from different vendors, and the way ICS/OT environments are built then there is likely to be a plethora of communications media, such as serial, ethernet, copper and optical in use.
- **Network complexity:** ICS/OT environments even on one site can be inherently complex. Installations that have complex distributed environments, remote and central sites, with multi and sole vendor turnkey or inhouse build solutions, combined with the additional aspect created by mergers and acquisitions, then network complexity can represent a significant challenge for visibility in ICS/OT environments.
- **Unidirectional connectivity** - A key aspect of reducing the attack plane for threat actors is the restriction of the nature and directionality of data between segments, zones, and facilities within an ICS/OT environment.
- **Device Aggregation** - ICS/OT environments are often an aggregation of pretty much every device type, IT, Enterprise IoT, IIoT and ICS/OT. Therefore, it is important for ICS/OT organisations to take the approach to have "ICS/OT network" visibility and not just "ICS/OT asset" visibility (the latter being a subset of the first). This is very important because the techniques and solutions (multiple or singular) chosen should be broad enough to provide good coverage for all devices deployed within the ICS/OT environment and the relationships among them.

In this article we will examine why asset visibility is both integral to all ICS/OT security use cases and uniquely challenging for ICS/OT environments, introduce the most common methods for creating and maintaining an asset inventory, and detail the pros and cons of each method.

Asset Visibility Methods

There are several ways of achieving visibility within an ICS/OT environment:

- Passive Monitoring
- Active Monitoring
- Artefact Parsing
- Host Based Agents

These are all in addition to the point in time manual/physical survey that is covered in another guidance article in depth.

Some network and asset discovery solutions will also have the ability to integrate with various other systems such as change management tools and will be able to not only feed them with asset information but also extract asset information from them to enrich their understanding of the ICS/OT environment.

Each of these techniques has their own Pro's and Con's which we will now explore, and any deployed solution may well include use of several of these techniques to gain the asset visibility coverage that is required.

It is important to note the difference between a point in time approach to asset visibility and having continuous ICS/OT asset visibility. The latter providing enhanced insights into:

- Insecure configuration of ICS/OT assets (including reconfiguration).
- Rogue/newly connected ICS/OT assets
- Connectivity and communications channels/flows
- Threat actor actions
- Vulnerability Management

Continuous monitoring of ICS/OT assets can determine what vulnerabilities are currently applicable to the assets monitored, including closing vulnerability records where firmware updates have been completed, removing vulnerabilities, whereas a point-in-time approach can only give a point-in-time view of vulnerabilities.

It is also important to identify the level of ICS/OT asset visibility that is required by an organisation. Organisations that follow the Purdue model may want to have full ICS/OT asset visibility from layer 3.5 to layer 1 (or even layer 0). Reaching down into Purdue Layer 1 from a higher layer is often prevented, for example, because of the PLC backplane supporting only vendor-proprietary communications. For instance, a Profinet Ethernet segment will be un-reachable by trying to "route" across a PLC backplane. Asset Discovery tools that rely solely on passive monitoring, operating at Layer 2 of Purdue will therefore not see anything beyond the PLC such as lower level Profinet and other Ethernet-based networks. This challenge can be solved when tools are used that support artefact parsing and/or host-based discovery, in addition to the necessary protocols.

Passive Monitoring

Passive monitoring has long been considered the default, go-to discovery method for ICS/OT environments. Passive monitoring involves the capture and copying of data moving across the ICS/OT environment. The three options for passive monitoring/packet capture are:

- Network Cards
- SPAN Ports: Switch Port Analysers (SPAN) provide port mirroring, which provides a copy of all network packets on one port (or an entire VLAN) to another port.
- Network Taps: These are hardware tools that allow you to access and monitor your network by capturing both send and receive data streams simultaneously on separate dedicated channels.

Span Ports and Network Taps are the main options utilised within ICS/OT environments, each having its own strengths and weaknesses such as:

SPAN Port	**TAP**
Advantages: • Low cost, using existing switch capabilities. • Remotely configurable through the network. • Captures intra-switch traffic and so can detect unauthorised equipment additions.	**Advantages:** • Captures send and receive data streams simultaneously, eliminating the risk of dropped packets. • Provides full visibility into full-duplex networks. • Captures everything on the wire—including Physical Layer errors—even when the network is saturated. • Once installed is invisible on the network and if a data diode TAP is deployed then data can never be induced back into the network through the monitor port(s)
Disadvantages: • Drops packets when the volume of mirrored traffic exceeds the capacity of the mirror port network interface. • Filters out Physical Layer errors. • May place a burden on the switch's CPU to copy data. • May change frame timing, altering response times and slowing network performance. • Is an integral part of the network that exposes a potential vulnerability as it has a physical receive path • Legacy ICS/OT network switches may not support SPAN ports, may not support them reliably, or might support only 1:1 port mirroring. • To implement may require equipment to be upgraded/swapped out and therefore has additional costs associated.	**Disadvantages:** • Requires the purchase and installation of additional hardware. • Analysis device may need dual-receive capture interface (when a breakout tap is deployed or when a Network Packet Broker is not used). • Only captures data between network devices; can't monitor intra-switch traffic. • Network segment needs to be interrupted to insert the Tap. • Very few taps are certified as unidirectional. • Requires manual intervention / Tap installation to start monitoring communications, and so is blind to prior unauthorised or malicious equipment additions. • Requires the aggregation of large amounts of raw data into something understandable, which also requires special aggregators.

Network Taps or network taps or unidirectional gateways providing protection for a SPAN port, may be favoured due to 2 main benefits:

- **Guarantee Unidirectional Traffic -** Unidirectional, or one-way data flows, are often required in ICS/OT networks (dependent on the CNI sector). These safeguard the network from external threats while also providing the out-of-band data necessary to monitor the network for cybersecurity purposes. TAPs can have built-in Data Diode functionality. This sends unidirectional copies of the traffic to out-of-band tools for monitoring purposes, without any effect on the link between the two network elements. Since there is no physical connection between a Data Diode TAP's monitoring and network ports, there's no possibility of intrusion from the destination.
- **No Impact on Production environment -** it is critically important to keep power plants generating power and water treatment facilities providing clean drinking water. Anything that would impact production has serious consequences. One benefit of using a passive TAP fabric is the lack of impact on production. With low-speed network TAPs that are passive and deployed out-of-band should a TAP go down for some reason, or if any of the devices connected to the TAP were to lose power, there wouldn't be any impact on a organisation's operations. Many ICS/OT networks are copper based and run at 1G or higher, and in these environments an Active TAP would be required. In these instances, "Failsafe" technology within the TAP is used to ensure that network integrity is restored in the result of a power loss. (Typically, it will take 27ms to failover).

It is important to note where a passive TAP fabric is used, that the actual insertion of a TAP does require an outage, whilst connections are disconnected, attached to the TAP and then reconnected. This of course would need to be scheduled during a maintenance window to minimise impact.

Other aspects that need to be considered with passive monitoring is the use and placement of TAPs. An in-depth understanding of the ICS/OT environments networking is required, both physical and logical to insure considerations such as the physical communication medium in use and therefore the type of TAP required; Optical or Copper, Ethernet or Serial (RS232/R485), the communication protocol being used, and if the use of physical (serial to ethernet) or protocol gateways would also aid more effective monitoring/TAP points, and the traffic flow/direction over the network.

Once the data is copied it is typically then sent to an "on premise" Network Packet Broker (usually a hardware device) or a cloud based server (many organisations would not want their sniffed network data pushed up onto a cloud-based server due to a lack of confidence in the security protection of data provided on these platforms, so would choose 'on premise' solutions, but this this view is slowly changing as confidence grows in cloud-based security), that will aggregate, 'shape', and then direct the combined traffic to multiple monitoring and/or security tools for further processing via deep packet inspection (DPI), which analyses each packet to identify the respective assets and their vendor, model, operating system, firmware, and other details. The depth and accuracy of these details are critical to the effectiveness and efficiency of a broad range of subsequent ICS/OT security and operational use cases such as change management, vulnerability and risk management, network segmentation, threat detection, and incident response.".

The following table details some of the Pro's and Con's of passive monitoring for Network Visibility:

Pros of Passive Monitoring	***Cons of Passive Monitoring***
Non-Disruptive: Once deployed successfully, passive monitoring has no impact whatsoever on the ICS/OT environment and thus poses no risk to operational availability, integrity, or safety. **Generally Effective:** Passive monitoring can typically identify and provide rich details on *most* types of assets within *most* types of ICS/OT environments. One caveat is that the respective discovery solution must support the full depth and breadth of both communication protocols and physical media found in the environment in order for passive monitoring to deliver the desired results. **Multipurpose:** Beyond discovering assets in ICS/OT environments, passive monitoring can also deliver visibility into communication baselines and deviations, operational behaviours, network traffic patterns, and other types of valuable information that support subsequent ICS/OT security and operational use cases. Examples include change management, vulnerability & risk management, segmentation, threat detection, incident response, and more.	**Asset Communication Limitations:** Since passive monitoring works by inspecting network traffic, it is not ideal for assets that seldom communicate (and thus seldom generate traffic including from rogue or maliciously installed equipment). For example, ICS/OT environments in electric grids usually contain redundant assets that only communicate in failover situations. **Asset Protocol Limitations:** The specific protocol an asset uses impacts the details shared (and those that passive monitoring can identify) in its communications. Modbus TCP, for instance, is a protocol widely used in ICS/OT environments but shares very few asset details in its communications. **Slower time-to-Value:** Passive monitoring usually requires physical or virtual sensors to be installed in strategic locations across the environment. This, combined with the aforementioned limitations, can yield a time-to-value that is comparatively slower than that of other asset discovery methods.

Passive monitoring of RF/wireless networks is undertaken by monitoring the switch that the Wireless Access Point is connected with. This is the norm where RF/wireless networks exist, although has possible visibility limitations of the RF/wireless connected devices that may not communicate further across the ICS/OT environment and thus transit the upstream switch.

Active Scanning

Active scanning works by sending targeted queries to certain segments of the ICS/OT environment and reporting back on which assets and related details are present. It is often used to supplement passive monitoring and other methods in situations where deeper details about a specific asset or segment are needed.

For instance, using the above example regarding the protocol Modbus. Passive monitoring would likely be able to discover only the presence, vendor, and few other details of a controller that communicates via Modbus. Active scanning could then be used to query that controller to fill in the remaining visibility gaps — or, in other words, to identify the controller's firmware, installed applications, and other key details that passive monitoring would be unable to pinpoint.

It is imperative to note, however, that when executed incorrectly, active scanning can be hazardous to ICS/OT environments due to their fragility. This method is generally only safe when:

- Queries and responses are only sent in a way that is guaranteed to not interfere with the ICS/OT system controlling live plant, and
- Queries are sent exclusively in each asset's native ICS/OT protocol or,
- Queries are sent in a manner that has been tested and verified by each asset's original equipment manufacturer (OEM)

The above criteria help ensure that any solution that uses active scanning is doing so in a manner that essentially mimics the type and volume of traffic each respective asset routinely receives, that it is designed to receive as part of its standard operating procedures, or that the vendor and engineering team have verified pose no threat to normal operations.

One aspect of "active scanning" is to simply use the vendor supplied tools to query assets on a regular schedule. Doing so can elicit the required responses from assets, which can then also be detected by passive monitoring tools and users will have OEM support if anything goes wrong, as the OEM's tooling was used.

One other type of 'active scanning' is to use network management systems (NMS) tools to actively query network devices such as switches and routers on a regular schedule. The responses can be directly consumed or again produce traffic that can also be detected by passive monitoring tools. This approach could provide a level of visibility of devices including IP address, MAC address, and locational information. Network devices can be actively queried for full configuration detail, which can then be used as part of artefact parsing. This information is then available to either point other active tools in the right direction in terms of what protocols to use for specific ICS/OT devices. It can also provide a scalable way to get at least partial information where placing a passive sensor everywhere is not an option, or where ICS/OT devices cannot be accessed by active queries.

The following table details some of the Pro's and Con's of active scanning for Network Visibility:

Pros of Active Scanning	***Cons of Active Scanning***
Generally Non-Disruptive: Active scanning via queries that are sent solely in each asset's native protocol and that have been OEM-verified pose little-to-no risk to ICS/OT availability, integrity, or safety. **Effective:** Active scanning, when conducted according to the above criteria, is extremely effective at identifying nearly all types of assets in nearly all ICs/OT environments. This method particularly excels in easily uncovering otherwise difficult-to-obtain asset details, such as the presence, version, and patch level of any windows-based and additional sorts of applications that may be installed on assets. Such information is critical to the execution of effective ICS/OT vulnerability & risk management and cannot be discovered by passive monitoring. **Fast Time-to-Value:** Active scanning typically returns robust results quickly, easily, and without requiring extensive sensors or other hardware installations.	**Asset Communication Limitations:** Passive monitoring and active scanning both have limitations related to how assets in the ICS/OT environment communicate, but their mechanics differ considerably. Specifically, some OEMs and operators turn off the communication mechanism that exists on the asset itself to answer queries, blocking the asset from being discovered via active scanning. Disabling this mechanism is considered a security control because some types of queries have been known to be exploited by attackers, but enforcing network segmentation is an alternative way to mitigate this risk without hindering discovery. **Prevalence of Risky Solutions:** ICS/OT asset discovery solutions that offer active scanning are growing increasingly common, but not all solutions are OEM-tested and verified and, as such, can increase the risk of sending queries that cause an asset to crash and potentially dangerous consequences to ensue. The only way to mitigate this risk is by using solutions that rely solely on native ICS/OT protocols formally certified by the OEM.

While active scanning techniques are normally not preferred, intelligent active querying is a developing capability being developed by a number of solution providers. The techniques used include use of tested scans, OEM approved querying of devices, and intelligent network device polling.

Artefact Parsing

Artefact parsing utilises specific technology to ingest and parse artefacts stored on support and management components in the environment. Such artefacts include configuration, project, and related files for assets like PLCs and RTUs, which are periodically backed-up on engineering workstations and within backup and restore systems. Artefacts can also include the configuration details of network devices within the ICS/OT environment.

Parsing these files to retrieve and then correlate data from multiple artefacts is a non-intrusive, efficient way to attain a detailed inventory of all the assets in an ICS/OT environment for those that are controlled from management systems.

An aspect of Artefact parsing is when a solution in the other categories is implemented, and the existing knowledge base of assets or asset register, is parsed and imported to help develop the baseline knowledge within the solution. Ideally the existing asset register will confirm to naming

standards that allow easy ingest. The Official Common Platform Enumeration (CPE) Dictionary that was developed by Mitre/NIST is one of these standards that allows easy ingest of asset information. It is a standardised method of describing and identifying classes of applications, operating systems, and hardware devices present among an organisations computing assets. Because of its use within the Common Vulnerabilities and Exposure (CVE) process, it facilitates Vulnerability Management. However, some organisations asset databases and registers, predate CPE, or CPE was not used when they were first established. Most ICS/OT Asset Discovery solutions can ingest outputs (via csv) or directly connect with asset database solutions; however, it is at this point, that quite often, database records being imported are rejected, and a significant amount of manual process is required to successfully import existing asset records.

The following table details some of the Pro's and Con's of artefact parsing for Network Visibility:

Pros of Artefact Parsing	***Cons of Artefact Parsing***
Non-Disruptive: Artefact parsing has no impact on the ICS/OT environment and thus poses no risk to operational availability, integrity, or safety. **Effective:** When powered by appropriate technology, artefact parsing can usually identify nearly all types of assets and details in nearly all ICS/OT environments. This method is ideal for discovering assets in air-gapped or otherwise inaccessible segments of an environment, as well as those for which passive monitoring or active scanning is not effective or suitable. **Fast Time-to-Value:** Artefact parsing is generally capable of returning robust results quickly, easily, and without requiring hardware installations or reconfiguration.	**Timeliness Limitations:** The timeliness of the asset information extracted via artefact parsing is dictated by the date at which the respective files were most recently backed-up in the ICS/OT environment's engineering workstations and/or backup and restore systems. Although such backups happen extremely frequently in some environments, they seldom occur in others. Many security practitioners have little control over this frequency, which means they typically also have little control over the timeliness of the information retrieved via artefact parsing. As a result, outdated asset information is a possibility in some cases. It is quite often also noted that OEMs do not provide access to the back-up files, which again will cause operators difficulty using this method. **Scope limitations:** Assets not registered in existing inventories may not be backed up regularly, and so may be invisible to artefact parsing solutions. Such omissions may be due to poor record-keeping, unauthorised vendor or insider deployment of assets outside of change control procedures, or malicious insertion of attack assets into control systems. **Integrity of the Artefact:** Local changes made to an asset for whatever reason might not use the management system, so these Artefacts might become out of date. Local changes could be through malicious attacker actions, or via local user laptops for re-configuration in cases of localised problems or incident management.

Host-based Discovery

Host-based discovery works by installing a lightweight executable file on compatible "host" assets, which may include engineering workstations and other IT-oriented assets that are prevalent in ICS/OT environments. Upon execution of this file, host-based discovery essentially combines certain functional aspects of active scanning and artefact parsing to collect and correlate details from each host asset and all surrounding assets in the environment. It is worth noting that the compatible element of the host asset may be limited due to legacy operating systems, and also anti-virus solutions deployed need to be reviewed for compatibility.

Hosts such as Human Machine Interfaces (HMIs), engineering workstations. are often part of a system managed by a third-party vendor. Those systems are often Factory Accepted Tested (FAT) as a system and any changes to that system, including installation of software need to be approved and implemented (often at significant cost) by the vendor, otherwise the testing of the system can be invalidated. This can be a challenged faced by operators in implementing host-based discovery.

The following table details some of the Pro's and Con's of host-based discovery for Network Visibility:

Pros of Host-based Discovery	***Cons of Host-based Discovery***
Non-Disruptive: This technique is non-disruptive and should pose no risk to ICS/OT availability, integrity, or safety, when OEM approved and tested software is used.	**Point-in-Time Limitations:** The granular ICS/OT asset details that host-based discovery provides reflect the specific point-in-time at which the method is executed. This method does not provide continuous visibility or fully support the added monitoring, detection, and many security and operational other use cases enabled by passive monitoring, although some solutions will provide near real-time automated updates. As a result, whenever a new asset is added or other meaningful change happens within the ICS/OT environment, host-based discovery will need to be re-executed thereafter to ensure such changes are captured within the inventory. While this execution process is technically manual, it usually entails little more than the push of a button and takes mere minutes from start to finish. A security policy should dictate a standard build that includes the required agents. This can be further enforced with technology to ensure only compliant devices can get network access. This method's lack of continuous monitoring capabilities is also why practitioners may be inclined to combine host-based discovery with other methods to ensure an always up-to-date asset inventory.

Pros of Host-based Discovery	*Cons of Host-based Discovery*
Comprehensive Host Data: Host-based enumeration is nearly always capable of identifying all characteristics of host assets across all segments of ICS/OT environments. This method delivers the broadest and deepest visibility out of all available asset discovery methods. As such, it is also ideal for addressing ICS/OT asset blindspots caused by limitations of other discovery methods.	**Vendor support agreements:** Some third-party agent software may not be supported by some ICS/OT equipment vendors and running such agents on this equipment may constitute a violation of support agreements.
Fairly Rapid Time-to-Value: Host-based discovery is capable of delivering a fully detailed ICS/OT asset inventory within minutes of installing the host software, without requiring any prior configuration or additional hardware, but it can take time to visit all compatible hosts and install and/or activate the agents, especially in environments under tight change controls due to safety or critical infrastructure reliability concerns.	**Possible incompatibilities:** Introducing third-party host agent software into legacy or sensitive ICS/OT environments risks introducing incompatibilities, performance issues or other issues that impair continuous, correct operation of the ICS/OT assets and environment.
Real time: Host based agents can generally run continuously and report regularly to asset management monitoring solutions and can often be configured to report on an exception basis, in real time, when host configuration changes are observed.	**Unauthorised equipment:** host-based agents are generally unable to detect unauthorised or malicious "leave-behind" equipment in ICS/OT environments when host-based reporting is not enabled in that unauthorised hardware.
Scheduled: An agent running on a time schedule say once every 12 hours, or once a 1 day, whatever is deemed appropriate for the type of environment it is in. This could also be varied under certain circumstances such as some ongoing maintenance work where 3rd parties are working continuously on the system, in which case monitoring interval may need to be reduced to shorter times.	

Meet 'Admin Corp'

Let's imagine we're following a fictional organisation who are responsible for managing the cyber security of a CNI processing plant.

Admin Corp runs a plant that produces Adminox, a highly volatile, refined form of administrative paperwork that is essential to every organisation in the country. It is created from volatile raw products using a continuous chemical process.

As an essential service, Admin Corp must comply with the UK NIS Regulations. This means that Admin Corp's assets needed to produce Adminox must be protected from cyber-attack.

Also, because Admin Corp are regulated for safety by the UK Health and Safety Executive, they must take steps to ensure the continued safety of the Adminox production process.

Asset Management in Admin Corp

Admin Corp have always undertook ICS/OT Asset Management to support their approach to Cyber Security within their ICS/OT environment, in addition to meeting UK NIS regulations, and self-assessment utilising the NCSC's Cyber Assessment Framework. Admin Corp's overall approach to ICS/OT asset management was first detailed here, with their initial manual approach detailed here. However, with the continued growth in the company through mergers and acquisitions, the dedicated ICS/OT Cyber Security Team have identified the need to explore use of automated Asset discovery tools, especially for use in some of their remote sites. The ICS/OT Cyber Security Team realise that visibility of ICS/OT assets is key to supporting the use of automated discovery tools and have set aside budget to support being able to provide visibility of its ICS/OT environment to the discovery tool that they eventually adopt.

Admins Corps Approach

For its large sites, mainly due to the complexity of the ICS/OT environments within them, the ICS/OT security team, are looking to utilise a passive TAP fabric approach using TAP devices certified for unidirectional communications, with out of band communications, to gain asset visibility. This has been chosen, although initially more costly, as the ICS/OT security team have identified that it is more appropriate for the complex environment and will provide the required visibility without the potential for disrupting production operations. In addition, the ICS/OT security team will undertake a project to update its knowledge on the networking across the ICS/OT environment to ensure the best placement of TAPs and will consider if traffic aggregation is required.

Admin Corp recognises that a TAP-based solution is unable to discover new or unauthorised assets connected to ICS/OT switches and accepts this limitation because they believe that their existing discipline of manual/in-person inspection of and control over their ICS/OT control and server rooms is adequate protection from unauthorised assets.

For its remote sites, with them having relative low bandwidth communications running over the switches, predominantly due to the small number of ICS/OT assets at site, the difficult of carrying out regular in-person inspections and the risk of new unauthorised hardware deployments on ICS/OT switches over time, the ICS/OT security team, are looking to utilise the SPAN ports on the existing switches. The ICS/OT security team have identified that even though some of these remote sites have been acquired through mergers and acquisitions, the switches are all

relatively recent models that should accommodate configuring SPAN/mirror ports without malfunction. Given the use of existing media gateway/converters and protocol gateways within most of the remote sites, the ICS/OT security team are confident that the SPAN port on the switches should be able to provide good insight on all assets within the remote site and keeps the costs down without the need for investment in a large number of network TAPs. They do however decide to implement a SPAN port network tap, to ensure unidirectional traffic flow (use of the SPAN port alone creating a bi-directional traffic flow opportunity that from a security perspective is undesirable for the ICS/OT Security Team). The Security Team also realise that they now need to put in place communications to feed the TAP data back into the central on-premises packet broker.

For new investment at its main sites, the ICS/OT security Team, will look to ensure that integration with the existing passive TAP fabric, is built into the design and build stages. While at its remote sites, the ICS/OT security team is looking to standardise the use of existing switches, and use of a SPAN port network tap, predominantly to ensure that intra-switch traffic is visible.

The ICS/OT security team is keen to compare the results of automated asset discovery with the base line of asset knowledge that they have achieved via the comprehensive manual physical survey approach and are looking forward to the integration of continuous asset discovery to support their change management process, in addition to a range of additional cyber security monitoring capabilities they are looking to implement. The team have also decided to implement an on-premises packet broker as they would like the ability to provide additional feeds of data to a new network flow monitoring tool they are exploring.

Final Thoughts

Admin Corp recognise that a centralised and fully detailed inventory that includes detail on all assets from across their ICS/OT environment is essential to the success of their ICS/OT Cyber security program. To achieve this from an asset visibility perspective, they have ensured they have factored in the following aspects:

- Standard or otherwise IT-oriented asset discovery or related solutions are fundamentally incompatible with and can even be downright dangerous to their ICS/OT environments. The solution to be used within the ICS/OT environment must be purpose-built specifically for OT.
- The extent that any ICS/OT asset discovery solution is able to deliver an adequate asset inventory for a given ICS/OT environment generally depends on two key factors:
    - Protocol coverage: Most ICS/OT assets communicate via proprietary protocols that significantly impact the breadth and depth of visibility that a discovery solution can provide. The solutions to be used must include all protocols within Admin Corp's ICS/OT environment, otherwise the solution will be unable to provide full visibility into it.
    - Discovery method(s): Most of the numerous ICS/OT-specific asset discovery commercial solutions available support at least one of four different discovery methods, passive monitoring, active scanning, artefact parsing, and host-based discovery. While it may be impossible for a *singular* discovery method to deliver a truly comprehensive asset inventory for any ICS/OT environment, it may be possible, however, to achieve something greater by combining multiple methods in a manner that best accounts for the unique characteristics of each ICS/OT environment, something that they will review once they have had some time operating the solution they have selected.
- Admin Corp recognise that asset visibility is foundational to all subsequent and truly essential ICS/OT security use cases, from vulnerability and risk management, to

segmentation, to threat detection, and many more. As a result, the often-challenging path to full visibility is not only worthwhile but also essential for the companies ICS/OT Cyber Security strategy.

- Admin Corp also understand that the asset visibility solution is just part of their overall asset management process, which needs to be just as effective in its implementation, to give them the foundational assurances they are looking for from a fully informed asset register. For instance, it needs to ensure that if a PLC card goes down in the middle of the night and a technician replaces it that the new serial number/firmware version that this change is captured in the asset management process and that the asset register is updated.

CAF IGP Summary

This case study discusses measures that contribute to the following CAF IGPs:

- **A2.a A01:** Your organisational process ensures that security risks to networks and information systems relevant to essential functions are identified, analysed, prioritised, and managed.
- **A2.a A04:** Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential function.
- **A3.a A01**: All assets relevant to the secure operation of essential functions are identified and inventoried (at a suitable level of detail). The inventory is kept up to date.
- **B4.a A01:** You employ appropriate expertise to design network and information systems.
- **B4.b A01**: You have identified, documented and actively manage (e.g., maintain security configurations, patching, updating according to good practice) the assets that need to be carefully configured to maintain the security of the essential service.
- **B4.b A04**: You regularly review and validate that your network and information systems have the expected, secured settings and configuration.

In addition this case study supports the requirements within the HSE's OG86, Cyber Security for Industrial Automation and Control Systems (IACS) - notably Appendix 2, Cyber Security Management Systems, Section A3.

Statement of Support

This guidance has been produced with support from Claroty, Dragos, Garland Technology, Waterfall Security and members of the Industrial Control System Community of Interest (ICS-COI) for publication via the Research Institute for Trustworthy Interconnected Cyber-Physical Systems (RITICS), with support from the National Cyber Security Centre (NCSC). This guidance is not intended to replace formal NCSC guidance where already available, and care has been taken to reference such existing guidance where applicable.

expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using this document. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation or favour by Claroty, Dragos, Garland Technology, Waterfall Security, the ICS-COI or NCSC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.