INDUSTRIAL CONTROL SYSTEMS
Community of Interest

# Active Discovery/Intelligent Device Interrogation in an Industrial Control System / Operational Technology Environment - Meet Admin Corp

### Introduction

NCSC has generalised asset management guidance which can be found here - Asset management, while this article is part of a series of Industrial Control System (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 having a close look at Active scanning/intelligent device interrogation asset discovery techniques. Further articles from the ICS/COI can be found here.

This article is aimed at those responsible for ICS/OT environments and understanding what assets are within them.

There is a quite often misunderstood myth that while use of active scanning techniques within IT environments is something that is a widely accepted practise, it is something that is inherently dangerous within ICS/OT environments, in the fact that use of such techniques could provide a wide range of unintentional consequences that would impact the operations being controlled within the environment.

Active scanning and intelligent interrogation techniques are in fact very capable methods of gaining understanding of the devices within the ICS/OT environment, but they must be conducted by staff who are aware of and understand ICS/OT environment, with the right tool selection, and who understand possible un-intentional consequences and have the skills to recover the environment if required.

## 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 Regulation. 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 using OG86 , they must take steps to ensure the continued cyber Security of the Adminox production process.

## Asset Discovery Review

Now that Admin Corp has an entry point into automating their asset inventory detailed in the article found here where they are utilising a purely passive monitoring capability, they have now been taking time and consider how this information can be used. Admin Corp have also decided it's a good time to test where their approach may have limits - in essence where their blind spots are and what they are blind to. As part of this review Admin Corp have considered a range of aspects that they documented during their initial project.

Firstly, Admin Corp are aware that passive monitoring is a continuous process that relies on interception of traffic between assets. By performing protocol analysis on the traffic, asset details can often be determined, such as the asset type and function (controller, workstation, switch, etc.).  It is not a perfect process as it very much depends on the quality of the traffic seen, but since it is continuous, classification errors made early on can be corrected by observing later traffic.

Admin Corp note that many industrial Programmable Logic Controllers (PLCs) respond to engineering station queries with detailed manifest information, enabling accurate

assessment of the controller asset. However, this level of query detail may only be available during the commissioning of a controller or modification of its running logic. Once the process code has been debugged and downloaded and the device placed into run-mode, identification opportunities may be limited as the traffic from the controller is just process telemetry (e.g., temperature, pressure readings, widget counts) and start/stop state-change instructions. Admin Corp must be mindful of this and have patience in waiting for an accurate assessment.

Admin Corp also note another important consideration is the length of process cycle. Since passive monitoring relies in other devices doing the talking, Admin Corp are aware that different systems may communicate during different parts of a process cycle. Thus, all process cycles should be executed before Admin Corp can consider that the asset discovery cycle is complete. And even after this, there may be some devices missed, as some of the taps they have installed are on switch uplinks and devices communicating within the switch domain (Human Machine Interface (HMI) to PLC, for example) may never generate traffic that leaves the switch, although where it was possible they did also utilise the switches SPAN port to catch inter-switch network traffic.

Admin Corp have reflected that the passive traffic solution they have implemented gives a reasonable picture of the assets and traffic flow within their ICS/OT environment, with engineering stations, control stations, switches, PLCs, Remote Terminal Units (RTUs) and field devices identified. Furthermore, (if the controller protocols are not encrypted) configuration changes are also being logged. Passive traffic is also providing a good indication of the security posture of the ICS/OT environment, as the solution they have chosen does an element of asset matching to vulnerabilities. Placement of taps at the key cross IT- ICS/OT points in the network will catch intrusion and exfiltration activities coming in from the IT environment, and the taps on most of their switches will catch much lateral movement (including some that bounded by the switch itself).

## Asset Knowledge supporting Vulnerability Management Review

When they implemented their asset discovery and monitoring solution, Admin Corp had in mind that this would also support their ability to undertake vulnerability management within their ICS/OT environment.

Admin Corp understand that their passive-only deployed solution can provide them with vulnerability mapping and passive vulnerability detection. Vulnerability mapping is the process of matching vulnerabilities to a specific configuration. This strategy works best for systems that have limited configuration variability (or degrees of freedom in configuration),

such as closed systems containing ICS/OT devices (such as PLCs, RTUs, field devices) and some network devices such as wireless access points, switches, etc.). Passive vulnerability detection uses passive traffic monitoring and protocol analysis to determine what clients and servers are running in an asset, cross-referencing with vulnerability databases. This is good for detecting services and "vulnerabilities in transit".

Admin Corp recognise in their review, that vulnerability mapping is not so effective with devices with large degrees of freedom (such as Windows and Linux general purpose servers). This approach breaks down because you cannot reliably identify all applications installed on a server just by waiting for them to talk, given that some installed applications may never talk or if they do, may not communicate their version numbers.

Admin Corp recognise that passive vulnerability detection and vulnerability mapping work would only be exposed to the communications that are allowed if firewalls are configured with least-trust rules, i.e., only allowing communications across the network for the ports actually used by the applications. They note that an external scan by an adversary should therefore only reveal the presence of services that should have already been detected by the passive discovery system. However, Admin Corp recognise that if an adversary gains a foothold in the internal network and can scan from there, it is a very different situation.

## Best Case Analytics

In the best case, Admin Corp recognise that they have visibility of all machines that communicate across the network, identification of PLCs, RTUs, field devices, Windows, Linux/Unix, switches and other network equipment, this covers the DMZ and Levels 3 to 0, as per the diagram below. They may identify many vulnerabilities on devices where the service and application versions are clear, though false positives may be a problem. They will have a security monitoring capability and anomaly detection capability as well as potentially a configuration drift detection capability.

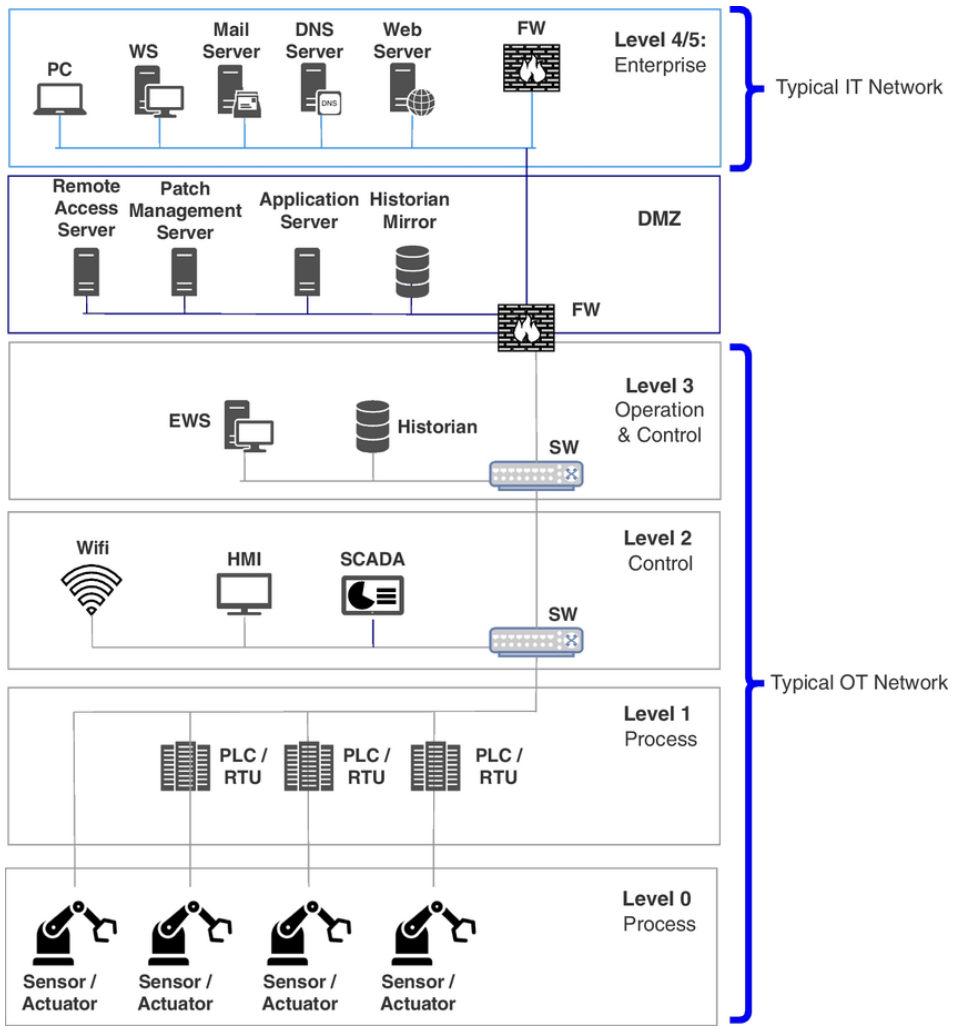


Figure 1: Purdue Model

Admin Corp's utilise their chosen solution which combines security monitoring, asset and vulnerability data to calculate a cyber-exposure risk/impact metric. Armed with this metric for every device, Admin Corp are looking to develop and implement a remediation workflow that minimizes their real-time risk/impact.

Admin Corp develop these risk/impacts by developing and analysing specific scenarios. This work is conducted jointly with the cyber security team work closely with the engineering and operational teams to ensure understanding from both a process control and safety aspect is included.

But how can they align with executive-risk concerns, such as asset linked financial risk, safety risk, environmental risk, reputational risk and the risk of service impact?

Admin Corp extend the fields in their asset knowledge database that implements a risk/impact matrix detailed below. For each asset, they assign a profile comprising 5 key-value pairs:

| CUSTOM FIELDS | |
|---|---|
| OTRISK-REP | OT RISK INDEX - REPUTATION |
| OTRISK-AFC | OT RISK INDEX - ASSET-LINKED FINANCIAL COST |
| OT-RISK-INT | OT RISK - INTERRUPTION (of Service) |
| OTRISK-SAF | OT RISK INDEX - SAFETY |
| OTRISK-ENV | OT RISK INDEX - ENVIRONMENTAL |
| OTRISK-SUBSYS | SUBSYSTEM ASSET IS LOCATED IN |

Table 1

and assign appropriate category values (A-E) according to the assessment of the asset. Information to the value scores is gained by on-site visits, questionnaires and interviews with local operations/engineering staff, who have clarity of knowledge on which devices are vital, dangerous (from the safety perspective) or not important at all, to the key processes to support the production of Adminox.

Admin Corp in doing this exercise realise it cannot easily be automated, but shortcuts can be taken to establish an early baseline. One early shortcut is to first assign a master field, OTRISK-SUBSYS to each asset and tie this to the part of the production process that the asset is involved in, then set a profile of values for the production process. Then, Admin Corp assigns the individual assets as per the OTRISK-SUBSYS profile and finally, tweaks each asset accordingly.

RAISE Risk Model Example

| RISK INDEX | REPUTATIONAL DAMAGE | ASSET-LINKED FINANCIAL COST | INTERRUPTION (of Service) | SAFETY | ENVIRONMENTAL IMPACT |
|---|---|---|---|---|---|
| A | No harm or slight client concern | Potential equipment or asset damage or financial loss < $1K | < 1 minute | Slight, injury without work absence | None to low |
| B | Minor harm to public reputation or client concern | Potential equipment or asset damage or financial loss $1-10K | 1 hour - 1 day | important, injury with absence | Temporary, on-site, non-toxic odor |
| C | Harm to local reputation, multiple client complaints | Potential equipment or asset damage or financial loss $10-100K | 1 day - 1 week | severe, lasting injry with absence | Minor, on-site, cleanup needed |
| D | Harm to regional reputation, loss of business, compensation claims | Potential equipment or asset damage or financial loss $100K-1M | 1 week - 1 month | very severe, fatality | Major, spills into environment |
| E | Harm to international reputation, loss of multiple clients | Potential equipment or asset damage or financial loss > $1M+ | multiple months | disaster, multiple fatalities | Disaster, major environmental impact in the area |

Table 2

Fortunately, this exercise only needs to be done once per process line, as nearly all their ICS/OT systems are static over their lifetimes.

The asset states can now be analysed to develop impact/risk mitigation strategies that are more aligned to corporate goals. In the case of Admin Corp, Adminox is highly volatile, where concentration build up and ignition can lead to widespread, and often fatal paper cuts. So, a subsystem score for Adminox production might look like this:

- OTRISK-REP:D
- OTRISK-AFP:E
- OTRISK-INT:C
- OTRISK-SAF:E
- OTRISK-ENV:C

But individual storage of the non-reactive ingredients has a different profile:

- OTRISK-REP:C
- OTRISK-AFP:D
- OTRISK-INT:C
- OTRISK-SAF:B
- OTRISK-ENV:A

While historian and data logging systems might look like this:

- OTRISK-REP:B
- OTRISK-AFP:C
- OTRISK-INT:B

- OTRISK-SAF:A
- OTRISK-ENV:A

Once implemented, Admin Corp can then create remediation workstreams around criteria such as:

- Assets with cyber risk scores > 80%, for systems if compromised that have a financial cost > £1m and a regional reputational harm and loss of business.
- Assets with risk scores > 20% that if they fail can lead to fatalities.
- Assets with risk scores > 60% that if they fail would require notification to the Environment Agency.

## Expanding Asset Detection techniques - an opportunity

Admin Corp, have as detailed in other examples, had the challenges of acquiring other ICS/OT assets through the mergers and acquisitions process, as the company as a whole looks to expand. They have now purchased several processing plants that produce products based on Adminox, such as Graftol™, Toilurine® and AntiSlack©. The Admin Corp security team now have an objective to bring the new plants under their security umbrella, apply their risk models and optimize their remediation paths to keep their corporate risks manageable.

From their initial meetings with their counterparts in the newly acquired processing plants, the Admin Corp security team already know that the acquired plants are operating in steady state (little engineering change / programming is ever done), are highly distributed and segmented network-wise, being built recently, but built not necessarily with security in mind. It is clear to their architects in the security team that, unlike their own network, a passive-only tap approach will be expensive and time-consuming and might not yield good results for the PLCs. They are also concerned that limited tap points will result in poor asset detection as many assets such as HMIs are entirely bound by their switch domains.

The Admin Corp Security team decide that this is an ideal time to try more of a developed hybrid approach to asset discovery. Their initial risk analysis identifies roughly 5% of the plant involves potentially explosive areas where Adminox is handled in its raw state. In these areas, they will invest in taps and port mirrors, upgrading to intelligent managed switches and passively discover assets. In the rest of the plant, they have identified that there are no life-critical environments - so these ICS/OT environments will be good candidates for the security team to explore what assets can be discovered via the Intelligent Device Interrogation querying capability of their chosen asset discovery solution.

Admin Corp decide to run Intelligent Device Interrogation query-based discovery on four lines. As a control test, they deploy on a fifth line entirely passively, with the sensor tapped into the uplink from the process line back to their process information servers. This passive deployment is the first test they initiate, as data collection takes longer and can be left running during the other testing phases.

Admin Corp do undertake some limited testing in the pre-production environment, although recognise that this is not truly fully representational, as in some cases it only contains one of every device (for type testing/patch testing), and because of this network topographies are considerably different to the production and safety environments.

They set an initial Intelligent Device Interrogation querying testing run to occur in one plant that has two lines down for maintenance work. They deploy their chosen vendor's devices on the first line with a network line of sight of all assets (e.g. all reachable over IP). For this phase they opt to start with a limited ping sweep to discover asset IPs and then entirely manual probes to classify the IPs. This approach allows them to observe the devices at all stages of discovery to determine how the classification works, what extra information is retrieved and if any queries cause issue. The manual queries cause no issue, classification is excellent, and the extra data retrieved is comprehensive.

For the second line, they choose a more automated approach: a ping sweep followed by automatically issued classification intelligent device queries on discovered assets. Again, they observe no problems, and the entire discovery and classification process is complete within 5 minutes.

For the third test they choose an operational line. They revert to the strategy employed on the first line - ping sweep and manual classification queries. Again, no issues.

For the fourth test, they choose another operational line where they run the ping sweep and auto-classification. This time, they encounter an apparent problem - the production line is stopped. After 30 minutes of sharp looks and muttering by process line supervisors, the problem is identified as physical and unrelated - an item on the assembly line was incorrectly positioned and tripped a limit sensor. The security team had encountered an all too familiar issue - *last system deployed always gets the blame*. However, they are familiar with this from the corporate side and ensure the event root cause is clearly and promptly communicated without prejudice to all stakeholders.

## How does Intelligent Device Interrogation work and what are the risks, advantages and limitations?

Admin Corp security staff understand that Intelligent Device Interrogation is a method whereby a security product can interact with target devices to gain information about them. In many ways, it is a close cousin to vulnerability scanning, except that it is specifically designed for use in ICS/OT environments and thus has to be safe to use and must not alter the behaviour of the target system in any way.

A golden rule in Intelligent Device Interrogation is to not query the target system with commands that it may be unable to handle, and this can be done with progressively more targeted queries. The queries mimic the exact amount and type of traffic an ICS/OT asset is already accustomed to receiving from the other assets with which it communicates. This traffic is also sent in the asset's native protocol, further ensuring it does not encumber the network and cannot be distinguished as related to anything but the ICS/OT environment's standard operations.

If the security system has access to passively acquired data, then there may already be enough information to classify the type of device, for example:  server, workstation, network device, controller. From here, a decision tree can be followed to selectively learn and target the device with more specific query commands as shown in the table below:

| **Classification** | **Query protocols / existing data** |
|---|---|
| Unclassified | Media Access Control (MAC) Address hardware lookup, open ports from passive traffic analysis, restricted port scan |
| Workstation | Network Basic Input/Output System (NETBIOS), Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP) |
| Server | NETBIOS, WMI, SNMP, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) Secure (S) |
| Network device | SNMP, teletype network (TELNET), Secure Socket Shell (SSH) |
| PLC | Common Industrial Protocol (CIP), Siemens S7, Modbus, BACnet, Omron FINS, 7T IGSS, Inter-Control Centre Communications Protocol (ICCP) COTP, Profinet, DNP3, vendor-specific protocols |

An example decision tree may look like this:

- Identify hardware from MAC (Schneider, Siemens, Rockwell, etc.)
- Identify ports from passive traffic (NETBIOS -> Windows/Linux, WMI -> Windows, TCP/102->ICCP (Siemens), TCP/44818->Ethernet/IP (Rockwell).
- Perform a light SYN-based port scan (is port open) on 40 common ports (e.g. NETBIOS, WMI, SNMP, CIP, ICCP, MODBUS, Ethernet/IP)
- If CIP open, perform query device -> identifies device.
- If SNMP open, perform SNMP query ->identifies device.
- If device identified, perform detailed vendor-specific queries to retrieve information.

What kind of device details are available with these queries? MAC addresses have the hardware vendor in encoded in the first 3 bytes of the 6-byte MAC address - these 3 bytes can be searched for to retrieve the vendor. Both CIP and SNMP can return vendor, device, make and model, serial number, device revision. WMI can return hardware and software details as well as software inventory, including publisher, software version and installation date. NETBIOS can return server names. Reverse DNS queries can return fully qualified domain names (FQDNs) given IP addresses. FTP, Telnet and HTTP scraping can often return make, model serial, firmware details. These methods may be useful for smaller devices that do not support management protocols such as SNMP, for example cameras and IoT devices.

Some discovery protocols have the advantage that they are extensible. For instance, SNMP has an extensible structure that allows almost any type of information to be encoded into the reply. Data is provided back in a tree-like structure called a Management Information Base (MIB) of object identifiers (OIDs). Different vendors will encode different types of information into SNMP - for example switch vendors can encode network port states, controller vendors can encode memory card details and serial numbers. Workstations can include running processes. The security tool normally has the means to identify security-pertinent information by make and model, and the classification decision tree may request different OIDs according to device type discovered.

## Limitations and risks

Admin Corp security staff understand that a lot of their activities contain an element of risk, even querying a controller with the vendor's engineering station software. Applications can have bugs; devices may have memory leaks. Intelligent Device Interrogation typically use the identical query formats as an engineering station issues, so if a bug can be activated by such a query, it will also be activated by the security monitoring software. They

do however realise that these are vanishingly small risks as such bugs are normally identified and corrected early on in a product lifecycle.

Other limitations may be present, such as a service partner not configuring SNMP on a device, or firewalls are in place that prevent queries from machines other than authorized engineering stations. Admin Corp staff understand that these limitations can be overcome though. They also recognise that there may be incomplete support of a vendor protocol in their chosen security solution - for example basic information (make, model, firmware) may be available but advanced information (backplane module configuration etc) may not be. Fortunately, the basic information is usually enough to determine the asset and vulnerability disposition of the device.

Another limitation that has been identified by Admin Corp staff is if a protocol is being translated using a protocol gateway, for example if the protocol is a serial protocol being translated into TCP/IP, for example Modbus Serial to Modbus/TCP or Profibus. In these environments, the security product's capability of asset discovery may be limited to the protocol gateway itself. However, the security monitoring aspect of their chosen solution can detect rogue commands being issued to the asset via the gateway, providing a protective service even if the asset identification is imperfect.

Admin Corp also recognise this method works by exchanging communications with ICS/OT assets, it is ineffective at discovering assets that lack properly functioning communication mechanisms. Although it is relatively rare, they recognise that an original equipment manufacturer (OEM) or the engineers could have disabled an ICS/OT asset's ability to respond to queries.

Admin Corp undertook work to explore the risk of increasing the attack plane by introducing a new security component, and related security fabric, when their chosen solution was first implemented purely in passive mode. However, they revisited this work given their decision to enable the chosen solutions active capability. This included aspects around the associated supply chain for their security solutions, and of course it went through their full and rigorous change management process.

## Overcoming encryption and authentication limitations

Admin Corp Staff, realise that if they continue to acquire new sites with newer technology implemented within the ICS/OT environment, that it may well utilise newer protocols for secure transport and authentication. This may impact the usefulness of purely passive traffic monitoring solutions to determine device information. Intelligent Device

Interrogation queries then become a key method to determine what a device is, as an Intelligent Device Interrogation query takes part in an encrypted session.

Admin Corp staff also realise that, if encryption is required, so are credentials, so the security system will need access to the usernames/passwords of the devices. For Windows systems using WMI, specialized, limited accounts will need to be set up (no-interactive, information-only) for such queries, ensuring confidentiality of user accounts and their data. Many PLCs have read-only accounts, and it is these account types are preferred for credentialled Intelligent Device Interrogation queries. They recognise that there may be a need for multiple account credentials required to effectively cover their ICS/OT environments, and therefore look to understand better how their chosen asset discovery solution handles the requirement for multiple accounts, specifically, does it try each account in turn, or can it bind account credentials to a list of devices? They also check how are these credentials are securely stored and if the solution matches Admin Corps intended encryption requirements as a whole.

## Is general scanning that bad in an ICS/OT environment?

Admin Corp recognise that there is a place for general Nmap type scanning in ICS/OT environment but only the if the degree of configuration freedom of a device is large, then you are going to get better results from scanning it than in mapping vulnerabilities to it. Admin Corp recognise that these devices are always general compute platforms such as servers and workstations, which are higher in the Purdue model, and are not in the process control environment, and therefore have implemented only at Purdue Layer 3 and above.

Admin Corp recognises that ICS/OT devices such as PLCs, RTUs and instrumentation, may be too sensitive to withstand general Nmap type scanning, noting this is especially true of older devices, identifying they may be sensitive for any of the following reasons:

- Limited CPU power: They can be overwhelmed when too many requests are added to their process control duties.
- Real-time communications: The protocols involved often expect an unbroken stream of readings from a device. If they're delayed substantially, they may have issues re-establishing communications. A full vulnerability scan probes many areas of a device very quickly, which can overly burden the limited CPU power and delay communications.
- Custom operating system and software: ICS/OT devices generally do not run widely used and widely tested operating systems, such as Windows or Linux. They may include a small HTTP server, but it likely includes a limited feature set. When a

vulnerability scanner attempts to check SSL, which may not have been implemented, the embedded HTTP server could crash.

## Are Intelligent Device Interrogation queries vendor-supported?

Admin Corp have put thought into gaining understanding if their use of Intelligent Device Interrogation queries is supported by the ICS/OT vendors. They realise from talking with their chosen solution provider that this question is tied to the history of how Intelligent Device Interrogation queries were developed by security vendors. Many ICS/OT vendors are very proprietary - they do not share protocol information and have limited APIs, therefore security vendors initially reverse-engineered the communications protocols to obtain the information required. Whilst not initially condoned by the ICS/OT vendors, many of them now are pragmatic on the issue, recognising that customers need to secure their ICS/OT network as a whole and that the security vendor products are often better than the tools the ICS/OT vendors themselves provide. Many ICS/OT vendors have active agreements or part ownership of security tool vendors, enabling them to meet customer demand for better security. Admin Corp undertake an element of due diligence and are knowledgeable of the relationship/agreements that their chosen solution provider has with the ICS/OT vendors that they have deployed within their ICS/OT environments.

## Summary of Admin Corps Testing of Intelligent Device Interrogation

Admin Corp, on analysis of the data from all tests, they note the following key observations:

- Asset detail on actively discovered assets is more comprehensive.
- 40% less assets are discovered on the passively monitored line.
- Vulnerability detection on the actively discovered assets is more accurate.

These results were in agreement with Admin Corps predictions for the testing:

- The PLCs were in run-mode, passive traffic provided for limited detection opportunity as there was no metadata available for analysis. Many assets had positive vendor identification (from hardware MAC address) but were identified as "Server", "OT Device" or "Generic Device".
- The HMIs communicated with PLCs only, not with PI servers and therefore traffic from them was not present on the switch uplink.
- On the passive line, vulnerabilities detected were ones only present in communicated traffic. (Fortunately, Admin Corps chosen solution used a sparse matching strategy for vulnerabilities mapped using incomplete information. Had

they used a different vendor with a 'greedy' matching strategy, their vulnerability false positive rate would have been unacceptably high.
- The passive line monitor had an advantage that it detected real-time events.

The four tests have provided Admin Corp with a level of confidence that they can expand from a passive-based discovery solution and roll out a hybrid-based discovery system quickly in the sites that they have newly acquired, as they do not have to install multiple tap points on every switch and arrange transport of the monitored traffic through the infrastructure. They would continue to use passive detection on the 5% of systems that were safety-critical, and at distribution switches. With the addition of automatic polling of systems where active query was used Admin Corp believe they have a good balance of monitoring capabilities, asset discovery and deployment cost.

The Admin Corp Cyber Security team also note during this exercise, that from discussions with engineering staff around what would happen if the active approach had an undesired consequence, with the engineering staff volunteering that they could replace/swap out devices if needed, that they also need to undertake asset management across their range of spares, which currently reside in a multitude of locations and states, in addition to asset management across equipment still held but not considered serviceable, including developing a documented disposal process.

## 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 Tenable 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). 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. This document is provided on an information basis only, Tenable and ICS-COI members have used all reasonable care in verifying the guidance contained within using the data sources available to it, they provide no warranty as to its accuracy or completeness. To the fullest extent permitted by law, Tenable and the ICS-COI accept no liability whatsoever for any 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 Tenable or the ICS-COI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.