



INDUSTRIAL CONTROL SYSTEMS

Community of Interest

Asset Management within Industrial Control System /
Operational Technology environments

Aims of this guidance

If you are responsible for the management or maintenance of Industrial Control System (ICS) / Operational Technology (OT) assets, this article will help you to navigate the challenges you may encounter when adopting mature management practices of these assets to maintain their cyber security.

In May 2021 NCSC published [implementing asset management for good cyber security guidance](#). Based on the NCSC's experience of providing support to IT and ICS/OT assets across UK Government and Critical National Infrastructure (CNI) systems, these principles are intended to help asset owners manage their assets securely across their full-service lifecycle.

The guidance caters for both IT and ICS/OT systems, but it can be difficult sometimes to see exactly how it should be applied in any given case. So, in this example, we're going to walk through specifically ICS/OT asset management lifecycle, led all the way by our guidance. We have done this to help those with ICS/OT environments and assets best understand how good asset management should be conducted, and how it can be very different in certain circumstances from IT asset management.

It should be read in conjunction with the latest guidance issued by NCSC in September 2025, [Creating and maintaining a definitive view of your OT architecture](#), which also covers Asset Management principles.

Having effective asset management practices in place also supports several outcomes within the Cyber Assessment Framework (CAF), namely: A3.a, B3.e, B4.b, B4.d, C1.c, & C1.e. A summary of the relevant IGPs is shown at the end of this case study.

Important Note: While the ICS COI is supported by the NCSC, and NCSC staff are involved in a range of its activities, no formal review of this guidance article has been undertaken by the NCSC. The ICS COI and its members strive to produce relevant ICS/OT specific cyber security guidance to supplement principles based cyber security guidance published by NCSC and have taken care to reference this guidance where applicable. This guidance article will be reviewed every 18 months to ensure that it has not been superseded by guidance published by NCSC, relevance and that any references are still accurate. The ICS COI and its activities are purely voluntary, with guidance articles produced that are deemed needed by UK Operators and their supportive industry partners. The fact that this guidance article has been published by the ICS COI has no relevance to the priority and focus of guidance published by NCSC.

Meet 'Admin Corp'

Let's imagine we're following a fictional organisation who is 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, they must take steps to ensure the continued safety of the Adminox production process.

Adminox processing plant

The process for producing Adminox involves several steps, with the final product stored under pressure in a tank.

Admin Corp's system, therefore, has two critical non-functional requirements:

- As a responsible and safety regulated company, they need to keep the local environment safe from the release of Adminox.
- Maintaining the availability of the product for customers in order to continue as a profitable company.

We will look at how Admin Corp applied NCSC's guidance for 'Implementing asset management for good cyber security' within their ICS/OT environment.

Overview of network

The Adminox processing plant has a fairly typical arrangement for this type of facility:

- **Process Control System (PCS) network.** This network hosts the main Industrial Control System (ICS) for the Adminox process. It comprises primarily of Programmable Logic Controllers (PLC)s that automatically operate the process, with some Human Machine Interfaces (HMI)s providing operators with localised viewing and control of individual process areas. The network is an IP based network comprising of managed Ethernet switches. The network is logically separated into VLANs to allow segregation of individual process areas.
- **Control Room.** This provides a centralised position for operators to control and monitor the plant using a SCADA system comprising of servers and workstations. The SCADA system operates in a dedicated VLAN.
- **Business Network.** This hosts IT infrastructure that is not involved in the production of Adminox; however, has connectivity to the control room and PCS networks to allow:
 - Consumption of process data by IT systems to support business operations.
 - Verified system updates to be passed from IT systems to the ICS/OT infrastructure.
- **Network firewall.** Controls the data connection between both the ICS/OT VLANs, and between the ICS/OT and IT environments.
- **Safety Instrumented System (SIS) network.** This network is physically isolated from the control room and PCS networks, and ensures the plant reverts to a safe operating condition should a dangerous fault condition occur within the processing plant. It does, however, have a data-diode on the network allowing outbound event data to be sent to the SCADA system, but without any inbound communication paths that could be used as an ingress point for threats.

Importance of asset management

Effective asset management will significantly contribute to Admin Corp operating a secure, resilient processing plant that limits exposure to cyber security threats. Without this in place it will be difficult to:

- **Understand authorised assets.** Without a good understanding of the assets that are supposed to be in operation across the environment, it is difficult to identify unknown devices that may pose a threat to the processing plant. Admin Corp often uses third-party suppliers and system integrators to maintain the processing plant which they do with their own laptops. However, it is vital that the cyber hygiene of these devices is verified before they are allowed to undertake work, so being able to identify such assets on the network can help enforce this. Admin Corp has previously discovered remote access devices connected to the plant network by well-meaning but misinformed suppliers who felt this would allow them to provide a better service. However, devices such as these can also present a gateway for threats to gain access into the network, so distinguishing these from legitimate devices is vital.

- **Understand security controls in operation.** Admin Corp is seeking to operate periodic assurance audits across plant assets to verify expected security controls, such as identity and access management, malware protection, and security monitoring, are in place. However, any assets not identified may be missed out. This could lead to critical devices being exposed to threats, or devices in operation on the network that are not appropriately secured that provide a gateway for threats to impact the system.
- **Understand software or firmware versions.** Admin Corp operates frequent patching regimes across its IT estate and uses vulnerability scanning to gain insights into any remaining vulnerabilities. However, within the ICS/OT environment this is less straight forward. Due to the high availability requirements of the plant, they only apply software updates during specific maintenance windows, and only after the updates have been rigorously tested. Vulnerability scanning is also not conducted across the plants ICS/OT assets: Firstly, because most common scanning tools are unlikely to identify vulnerabilities in ICS/OT assets; and secondly, due to concerns that scanning may affect their operation. Admin Corp has, therefore, elected to adopt a manual approach to vulnerability identification, by assessing announced vulnerabilities relevant to its ICS/OT assets to determine if it affects their deployment. Accurate recording of asset and software version then becomes essential to support vulnerability assessment.
- **Identify assets for upgrade before becoming end-of-life.** ICS/OT assets are typically designed to be in service far longer than IT assets. Admin Corp expect to get around 5-7 years of service from most IT assets. However, they expect to achieve around 10-15 years of service from their ICS/OT assets. These operate bespoke SCADA programs and PLC code, which are written for the specific platform they are deployed. Moving to a platform that is 10-15 years more modern often means that the current programs and code cannot be run on the replacement platform. Replacement is likely to require significant time, effort, and investment, and so Admin Corp will need to make sure it plans ahead. NCSC's [Obsolete products guidance](#) can help further with managing legacy assets.
- **Responding to faults.** An unknown asset that performs an important function within a process may be difficult to support. If a fault were to occur, having knowledge of the product and the software to communicate with it will be needed to ensure prompt diagnosis and rectification.
- **Ensure assets are backed up.** Should a device fail and need replacing, a backup of the latest running configuration will be required for restore. Asset types like PLCs are likely to have complex bespoke code written specifically for its application. If this is lost, re-writing the code can be a lengthy activity, incurring significant costs; not just in development time, but due to the potential outage or work-around that may need to be put in place to overcome the outage.

Admin Corp's approach to asset management

For Admin Corp to apply appropriate and effective asset management, it must understand the assets that comprise the Adminox processing plant infrastructure. It is important to identify not just those assets directly critical to the operation of the plant, but also those assets that must be carefully configured and managed to maintain the security of the plant. This will typically be those that either contribute to the management of the critical assets or those that could in some way impact the operation of those assets. This may include underlying infrastructure such as the network devices interconnecting the critical assets, or ancillary systems such as data archivers or remote access gateways which could be used as a threat vector to exploit the critical assets. Finally, they must ensure there is good understanding of the assets that secure the environment, such as network firewalls, to ensure they can be effectively managed to maintain the security protection required.

Admin Corp senior management approved the establishment of an asset inventory to record Adminox processing plant hardware and software assets that:

- Are directly critical to the operation of the plant.
- Must be carefully configured and managed to maintain the security of the plant.

This will be the authoritative source of information that will be owned by an appointed Admin Corp Senior Manager. Once established any other mechanisms for recording assets will be retired. To support this, the asset inventory will be hosted on a centralised platform that all stakeholders can easily access if they have been provisioned access rights to do so.

Asset attributes to be recorded

To allow Admin Corp to achieve all its goals from asset management, it must ensure it records adequate details against each asset. Hardware and software assets will be recorded, with these two asset types requiring different attributes to be recorded. The ICS COI has produced an article - [Attributes for Industrial Control systems/Operational Technology Asset Management](#) – providing detail on the types of attributes that need to be recorded and what they can then be used for.

Hardware

The following will be recorded for all hardware assets:

- **Asset Type:** We firstly need to understand what the asset is, as the plant operates multiple hardware types. The list may be added to if additional hardware types require recording, but initially Admin Corp have decided they will be looking for the following (please note this is not designed as a definitive list):
 - Servers
 - Workstations
 - Human Machine Interfaces (HMIs)
 - Programmable Logic Controllers (PLCs)

- Remote Terminal Units (RTUs)
 - Network Switches
 - Security Appliances (E.g., Firewalls)
-
- **Name:** The actual name configured for each device
 - **Description:** This will typically be what the asset is known as. E.g., SCADA server, Batch Reactor HMI, Batch Reactor PLC etc.
 - **Vendor:** The asset vendor. Admin Corp will require this should they need to obtain vendor support. If possible, information around the procurement route/project would be useful also but this is not always available given historic implementation projects within ICS environments.
 - **Model:** The specific type of the device. May be a model name or a model code dependent upon the type of asset. Admin Corp will require this to allow it to understand if the asset is still in support and when it is due to become end-of-life.
 - **Version:** Dependent upon the type of device this will either be the firmware or BIOS version. Admin Corp will require this to allow it to understand if the asset is running up-to-date firmware/BIOS, or any vulnerabilities in the version in operation.
 - **IP Address:** ICS/OT assets within the Adminox processing plant are assigned an IP address manually. It is vital that IP addresses are tightly controlled to avoid any IP address conflicts that could affect network communications. Understanding which asset is using a particular IP is also needed when trying to identify network issues through network data analysis, such as packet captures and firewall logs.
 - **MAC Address:** This is the specific hardware address of an asset. Having an accurate recording of all the MAC addresses used by authorised assets, and the IP address they have been assigned to, is vital for being able to identify unauthorised assets on the network.
 - **Location:** Recording the physical location of the asset will allow Admin Corp to verify the information recorded is for the specified asset. It will also allow the asset to be promptly reached should there be a need to do so. For example, if it is causing disruption across the network.
 - **Criticality:** By recording the criticality of the asset based upon the importance to the operation of the plant, Admin Corp will be able to ensure it takes particular care when working with assets that could affect operations. When recording the criticality of assets, it will be important to consider not just those core assets that could directly impact the plant, but also any assets supporting underlying infrastructure that core assets depend upon, such as power and cooling.

Software

The following will be recorded for all software assets. This may be the operating system or an application:

- **Name:** The name of the operating system or application.
- **Host Name:** The host name on which the software is installed. Each instance of the software will be recorded to ensure that the version of each can be catalogued to identify any discrepancies.
- **Description:** The purpose of the application.
- **Vendor:** The software vendor. Admin Corp will require this should it need to obtain vendor support.
- **Version:** This is the specific version of the software. Dependent upon the version this may be recorded as the major/minor version of the software, or the build number.

For both hardware and software asset details, AdminCorp are keen to ensure utilisation for the hardware and software characterisation of the [Official Common Platform Enumeration \(CPE\)](#) Dictionary hosted and maintained by NIST.

Additional Attributes

Admin Corp will also record the following information against each asset:

- **Owner:** The assets used across the Adminox processing plant are the responsibility of different parties, so it's important to understand who is responsible for each. For example, the PLCs are the responsibility of the plant Engineering Manager, whereas the security appliances protecting the infrastructure are the responsibility of the Admin Corp Security Manager.
- **Modified Date:** It is useful to understand when the information for the asset was last updated to give an understanding of the currency of the data recorded.
- **Support Contract:** Some assets will require a support contract in place with the vendor to gain access to updates and receive vulnerability notifications. Admin Corp will need to ensure continuity of support to maintain its access to vendor support.

Populating the Asset Inventory

There are several mechanisms available to Admin Corp to perform the initial asset discovery (further details can also be found in the article developed by the ICS COI that looks [at visibility for asset management](#)):

- **Design documents.** Comprehensive design documentation was produced for the implementation of the Adminox processing plant. Unfortunately, it appears the documents have not been reviewed or updated since the plant was commissioned; however, they are very detailed, with location information allowing engineers to physically check if the asset is still in operation and get an up-to-date understanding of the asset. They also describe the function of each asset, allowing criticality to be understood.

- **SCADA system.** Admin Corp will need to record the hardware, OS, and software used for the SCADA systems server and workstation in its asset inventory. The SCADA OPC server will also show all the plant assets the SCADA system communicates with, such as PLCs. This can be used to identify any assets that may have been added to the plant since it was commissioned. Determining the control & monitoring provided by the PLC to the SCADA system, will also give an understanding of the criticality of the asset.
- **Packet Capture.** Admin Corp has configured a Switch Port Analyzer (SPAN) port on the core network switch providing connectivity of all PCS VLANs to the site network firewall, and on a switch port on the SIS network. SPAN ports output a copy of all data forwarded by the switch, which can be captured with network protocol analyser software. ARP broadcasts captured allow asset MAC addresses and IP addresses to be learnt. The first six digits of a MAC address are known as the Organisationally Unique Identifier (OUI) and are assigned to a manufacturer allowing identification of the product vendor. Some vendors use specific OUI for different product lines, allowing the model to also be identified.
- **MAC Address Tables.** Network switches use MAC address tables to map the MAC address of any devices that communicate through it with the switch port the device is accessible via. This information can be accessed by logging on to each switch individually; the approach used for the SIS. For the PCS, Admin Corp has recently deployed a Network Management System (NMS) to manage the configuration of network switches, such as assigning access ports to VLANs, and ensuring unused switch ports are shutdown. The NMS can retrieve MAC address tables from each switch via SNMP, which Admin Corp use to centrally collate MAC address data and build a map of their network. The additional value of this approach over packet capture is the ability to identify the location of the device due to also learning the switch port it is connected to.
- **Engineering workstation.** An engineering workstation on the PCS is installed with software tools for managing the ICS/OT assets. Engineers can use this to communicate with discovered assets to retrieve additional asset data, such as firmware version.
- **OT asset discovery tools.** There are many ICS/OT asset discovery tools available across the market; most using the passive packet capture techniques previously described. However, some also use native ICS/OT protocols to actively communicate with devices to gain more detailed asset data, such as firmware version. Admin Corp have no such tooling in place yet but certainly see this as something they may consider in the future to centralise asset visibility across their main production sites and their considerable remote site estate.
- **Physical survey of ICS/OT environment.** Admin Corp periodically undertake physical surveys of the ICS/OT environment with teams comprised of cyber security personnel and ICS/OT engineers. This allows them to survey the condition of assets and physical security controls in place to protect assets. During these surveys, they take the opportunity to validate the location of assets and identify assets that may not have been previously discovered. E.g. non-networked assets residing in package plant. The ICS COI has developed an article that looks at the approach to be taken for [physical survey of ICS/OT Environments](#).

Validating the inventory and detecting unknown assets

An important part of asset management is to detect any assets not recorded in the asset inventory. These may be legitimate devices or software that have been introduced without going through the formal change processes operated by Admin Corp. If these are not included in the inventory, they are likely to go unmanaged. This could lead to problems not only for the unmanaged assets, but potentially to the rest of the plant. They could cause network disruption through unstable firmware or incorrect IP configuration, or they could contain hidden vulnerabilities that are an entry point for cyber threats. An unknown asset may also be a direct cyber threat, such as a device under the control of an adversary. Admin Corp will use the following strategies to validate their inventory and identify unknown devices on the network.

- **Firewall logs.** Admin Corp uses automated tools to monitor its firewall logs. The logs will also be used to identify any IP addresses within the internal network attempting to connect out through firewalls that are not recorded in the asset inventory.
- **NMS data.** As they did for the initial discovery, Admin Corp will use their NMS to query network switch MAC address tables to identify any devices not previously seen on the network, with an alert generated should an unknown device be detected.
- **Loss of SCADA to PLC communications.** If the SCADA system shows an unexpected loss of communications to a PLC, this could be an indicator that the PLC's port has been used to connect an unauthorised device to the network and should be investigated. The NMS can also be used to identify this type of issue should a network port go down then back up again.
- **Physical survey.** Given Admin Corp have not yet invested in an automated asset monitoring and discovery tool, they will continue to undertake physical surveys for new/unknown devices, especially in locations known to be not visible to the NMS, such as those devices using non-IP ICS/OT protocols.

Maintaining the inventory

After all the effort involved in creating the asset inventory - and understanding the value it provides - Admin Corp wants to ensure it keeps the inventory up to date. It will do this through the following means:

- **Embedding asset management into change management.** Admin Corp operate rigorous change management across the plant, which includes governing the addition, change, removal of any assets. Its change management process will be updated to ensure it includes the need to update the asset inventory whenever changes are made. This will include whenever software or firmware updates are made.
- **Device connection procedure.** Admin Corp will adopt a new device connection procedure to manage the connection of any new asset to the plant. This will ensure the asset is safe to be connected, by ensuring it is properly configured and is using the allocated IP address, that it is running up-to-date software or firmware, and that it is not infected with malware. This procedure will also ensure the asset is accurately recorded in the asset inventory.

- **Controlling the network.** All unused network ports will be administratively shutdown on the network and only opened to allow the connection of an asset that has successfully passed through the device connection procedure.
- **Periodic asset validation.** Initially, a manual maintenance regime will be adopted, whereby each asset in the inventory is accessed to verify the details recorded for it are accurate. If Admin Corp do decide to use an OT asset management tool with active capabilities, then this will automate the process of interrogating assets to validate their properties. Managing Access to the asset inventory
- The Admin Corp asset inventory will contain a significant amount of sensitive data about the Adminox plant. Knowing the assets in use and the network settings of those assets could be very valuable to an attacker, who may be able to use the information to craft a targeted attack against the plant. Admin Corp will, therefore, host the inventory on a platform on which it can tightly control access to it for authorised personnel only, and following the principle of least privilege. It must also consider whether it allows data to be exported from the inventory, as it will be much more difficult to control access to it should this be allowed.

Asset management Lifecycle

Admin Corp will be undertaking periodic reviews of the assets within the inventory to understand the life expectancy of all its assets in service, so that it can plan accordingly for the replacement of any assets that may be nearing end-of-life. It must factor into this the time it may take to replace ICS/OT assets compared to IT assets, due to the re-engineering that may be required for the replacement.

When assets are decommissioned, this is not the end of the journey, and it will be important for Admin Corp to adopt procedures to ensure assets are sanitised of any sensitive data prior to repurposing or destruction. As with the data in the asset inventory, if the configuration data stored on assets fell into the hands of an adversary, this may be useful to allow an attack to be crafted against the Adminox processing plant. It may be sufficient to securely wipe any data from memory; however, granulation of the asset may also be needed to be certain of being unable to retrieve any data from the device.

Next steps

Having taken these steps, Admin Corp believe they have appropriate asset management in place to underpin secure operations across the plant.

Their next steps are to ensure they have embedded these asset management practices into the business to ensure their asset inventories remain accurate; while ensuring they use the data within the inventory to underpin critical cyber security activities, such as vulnerability and threat management.

As an operator of Critical National Infrastructure, Admin Corp ensure they continue to manage the Adminox process safely and effectively, becoming members of the ICS Community of Interest (COI) and maintaining a relationship with the NCSC Private Sector CNI Engagement Team.

CAF IGP Summary

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

- [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.
- [A3.a A02](#): Dependencies on supporting infrastructure (e.g. power, cooling etc) are recognised and recorded.
- [A3.a A03](#): You have prioritised your assets according to their importance to the operation of the essential function(s).
- [A3.a A04](#): You have assigned responsibility for managing all assets, including physical assets, relevant to the operation of the essential function(s).
- [A3.a A05](#): Assets relevant to essential functions are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.
- [B3.e A01](#): You catalogue and track all devices that contain data important to the operation of the essential function(s) (whether a specific storage device or one with integral storage).
- [B3.e A02](#): Data important to the operation of the essential function(s) is removed from all devices, equipment and removable media before reuse and / or disposal using an assured product or service.
- [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 function(s).
- [B4.b A02](#): All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment.
- [B4.b A04](#): You regularly review and validate that your network and information systems have the expected, secure settings and configuration.
- [B4.d A01](#): You maintain a current understanding of the exposure of your essential function(s) to publicly known vulnerabilities.
- [C1.c A03](#): Alerts can be easily resolved to network assets using knowledge of networks and systems. The resolution of these alerts is performed in almost real time.
- [C1.e A07](#): Monitoring staff are aware of essential function(s) and related assets and can identify and prioritise alerts or investigations that relate to them.

Statement of support

This guidance has been produced with support from members of the Industrial Control System Community of Interest (ICS-COI) for publication via the Research Institute for Trustworthy Inter-connected 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, and whilst ICS-COI members have exercised reasonable care in compiling the guidance, they provide no warranty as to its accuracy, completeness, or suitability for any particular purpose.

To the fullest extent permitted by law, neither the ICS-COI or its members accept any liability for any loss, damage, cost, or expense arising directly or indirectly from the use of and / or reliance on, this document. Users of this guidance are advised to exercise their own judgement and consider taking independent professional advice.

Any reference to commercial products, services, or entities by name or otherwise, does not constitute or imply endorsement, recommendation or preference by the ICS-COI. The views and opinions expressed in this document shall not be used for advertising or product endorsement purposes.

Document Details

This document was originally published in October 2023, with this version being v1.1 and was published on 20/10/2025. It will be reviewed every 18 months.