INDUSTRIAL CONTROL SYSTEMS
Community of Interest

Attributes for Industrial Control systems/Operational Technology Asset Management

Introduction

NCSC has generalised asset management guidance which can be found here - Asset management, and one Industrial Control System (ICS)/Operational Technology (OT) specific guidance article relating to Creating and maintaining a definitive view of your OT architecture, which does cover some elements of Asset Management**. T**his article is part of a series of ICS/OT specific guidance articles on Asset Management first introduced here by the ICS COI.

ICS/OT asset management is the crucial practice of identifying, tracking, maintaining, and assessing the security all hardware and software assets (this includes supporting systems and their networks) within ICS/OT environments. This article explains the reasons for a good ICS/OT asset register, what information (attributes) it should contain and the rationale behind it.

Keep in mind that there is no perfect ICS/OT asset register, and any documented list is better than no list at all. At a minimum, the information documented in a register should be able to tell your cyber-security defenders:

- Which devices are present on the network,
- If something happens in the environment, where the device is located, and
- What firmware versions or applications are running on each device.

The list of asset attributes provided in this article are intended to be indicative of the information that is important. You should adapt the list to make it specific to your company and adopt internal descriptions to make it easier to use.

One point to consider for ICS/OT is that data collection may require manual activity, including site surveys. Due to the considerable time and effort this requires, it is important that the collection is focused on the most exposed and critical assets first. Attempting to capture every data point in ICS/OT environment without automation is unlikely to be an effective use of resources.

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.*

Who is this for?

This guide is for anyone looking to build or enhance an ICS/OT asset register or procure a new asset identification or management system.

Key Benefits of an ICS/OT Asset Inventory

An asset inventory provides organisations with a comprehensive understanding of their resources, enabling them to make informed decisions about resource utilisation, improve security, meet compliance requirements, and drive efficiency and growth.

- **Improved Asset Management:** An accurate asset inventory provides organisations with a comprehensive understanding of their assets, enabling them to better manage, maintain, and utilise these resources.
- **Increased Efficiency:** By having a clear understanding of their assets, organisations can streamline processes, reduce downtime, and make more informed decisions about resource allocation. An asset register can help with scheduling maintenance activities or patch management activities.
- **Clarity on what needs to be protected:** An asset inventory helps organisations identify and prioritise vulnerabilities, enabling them to implement the necessary security measures to protect against cyber-attacks and other threats.
- **Compliance:** Many industries have regulations and standards that require organisations to keep an inventory of their assets. An accurate inventory helps organisations to meet these requirements and maintain compliance.
- **Improved Decision-making:** An accurate and up-to-date asset inventory provides organisations with the information they need to make informed decisions about future investments and resource allocation, enabling them to stay ahead of the curve and remain competitive.
- **Enable asset refresh cycles:** An asset inventory enables organisations to identify underutilised or obsolete assets, allowing them to repurpose or dispose of these resources, improving efficiency and reducing waste.

Common Cyber Security specific use cases for an ICS/OT asset register

As mentioned above an ICS/OT asset register is a key foundational element to securing the ICS/OT environment from a Cyber Security perspective. You cannot protect what you do not know, and the more you know the better you can secure it, are often heard in discussions around ICS/OT asset management. The following Cyber Security specific use cases are key:

- Risk management: understanding and managing cyber risk depends on ICS/OT assets being accounted for. If assets are allowed to slip under the radar, it will not be apparent if appropriate security controls are missing, resulting in unmanaged risks.
- Managing legacy: in ICS/OT systems assets often have a much longer lifespan than in IT systems. Updating the asset registry when asset fall out of vendor support for instance. Using the asset register to identify assets that are no longer supported by the vendor, allows companies to assess the risk of not replacing them and create contingency plans for when they fail.
- Identity and access management: being able to identify users and devices is necessary to implement an effective identity and access management system. The asset register helps ensure all users and devices have unique identities and identifies assets and resources that need access controls applied.
- Vulnerability and patch management: patch management in ICS/OT systems can be controversial. It may be necessary to wait for a planned shutdown to apply patches, in some cases, applying patches will require testing or re-validating system functionality (which can be very expensive) and patches may no longer be available for legacy asset that can't be replaced. Using the asset register to identify which vulnerabilities present a realistic risk, then decide whether to transfer, tolerate, treat (with appropriate mitigations/controls) or terminate the risk. The asset register can also be used to record that decision so that when the situation changes, it can be revisited. The asset register is also used to help plan the list of things to do with regards patch management in the next planned shutdown.
- Incident management, response and recovery: Using the asset register provides a company with in-depth knowledge and understanding of their assets, allows them to determine which are most critical to the organisation (Via the likes of Crown Jewels Analysis) helps them plan for, respond to, and recover from incidents. By ensuring nothing important is missed and having the right information available, they can act quickly and minimise disruption. Configuration information can also provide a benefit to incident response/recovery planning, by utilising this as an opportunity to hash known good firmware/configurations for devices and take back-ups to support recovery efforts.
- It's not just cyber security: most business operations depend on some aspect of asset management. This includes IT operations, financial accounting, managing software licences, procurement, and logistics. While they may not all need the same information, there will be some overlap and dependencies between the respective requirements. The security aspect should not be considered in isolation or as the primary consumer of asset information, so integrating and coordinating asset management across your organisation will help reduce or manage any conflicts between these functions.

ICS/OT Asset Attributes:

The tables below show what attributes should be included in an asset register and their importance to Incident Response and Vulnerability Management.

Some attributes will appear to provide similar information to other attributes. This is intentional as it allows for information to be inferred or acts as a starting point even if key asset attributes are missing. For example, if you know the department responsible for an asset, you would likely be able to find a point of contact for the asset even if this information is missing from the asset register.

The suggested attributes should be tailored to your needs. For simple ICS/OT sites, not all attributes will be as necessary as they would be for an overly complex site.

Abbreviations:

Abbreviation:	Meaning:
C	Critical
U	Useful
IR	Incident Response
VM	Vulnerability Management

Initial Attributes (Essential)

Attribute Name	Meaning	Rationale	IR	VM
Unique Asset Name	Descriptive asset name that is unique	Using unique asset IDs helps to prevent asset duplication and identify errors in asset registers. It also allows simple correlation of events from different tools to ensure that both onsite and central support personnel understand what asset is being discussed. Use of descriptive IDs (e.g., LONCC-CTRLRM-OT-OPPWS-001 for a Control Room OT Operator Workstation in the London Control Centre) helps personnel quickly understand the asset's location, type, or function without needing to look it up in a database.	C	C
Asset Name Alias	Descriptive name alias that may be used for the same asset	If a unique name is not used, adding aliases improves collaboration between different teams and systems where multiple names are used to describe the same asset.	C	U
Asset Description	Description of the asset.	Describe the physical attributes of the asset or the purpose of the asset.	C	C
Asset Purpose	Description of the purpose of the asset	Understanding the function of the asset aids in assessing its criticality and potential impact if compromised.	C	C
Asset Type	Description of the type of the asset e.g. PLC, HMI, RTU, Sensor	Helps categorise assets for inventory, risk assessment, and prioritisation in incident response.	C	U
Asset Criticality to Safety	How critical is the asset to the safety of the process/site.	Helps prioritise assets during VM and IR activities.	C	C
Asset Criticality to Operations	How critical is the asset to the operational process/essential service	Helps prioritise assets during VM and IR activities.	C	C
Asset Criticality to Security	How critical is the asset to the security of the environment/network/site	Helps prioritise assets during VM and IR activities.	C	C

Attribute Name	Meaning	Rationale	IR	VM
Impact if Compromised to Safety	Impact to safety of the process/site if asset is compromised and control/view etc lost	Helps prioritise assets during VM and IR activities.	C	C
Impact if Compromised to Operations	Impact to operational process/essential service if device compromised and control/view etc lost	Helps prioritise assets during VM and IR activities.	C	C
Impact if Compromised to Security	Impact to the security of the environment/network/site if the asset is compromised	Helps prioritise assets during VM and IR activities.	C	C
Asset Risk Score	A score of the risk of the asset. Score criteria common to all company assets.	Operational risk ranking, typically 1-10 or 1-100[1]	C	C
Asset Source	How was the information about the asset detected	How was it detected (typ. passive, active, manual, agent, etc.)	C	C
Asset Owner - Department	The department name that the asset belongs to - could be operations team, security team etc	Essential for identifying the business area responsible for the asset.	C	C
Asset Owner – Job Title	The job title that the assets belongs to.	Essential for contacting the asset's owner during IR and VM activities.	C	C
Asset Vendor - Hardware	OEM/Vendor name of the asset	Knowing the hardware vendor helps in identifying vulnerabilities, sourcing support, and managing warranties or recalls.	C	C

[1] Risk scores will depend on the methodology that the organisation is using for risk assessment.

Attribute Name	Meaning	Rationale	IR	VM
Asset Vendor - Operating System	The operating system on the asset.	Identifying the OS vendor is essential for patch management, compatibility checks, and vulnerability tracking.	C	C
Asset Vendor - Applications	Applications that are running on the asset	Application vendor information supports license management, security patching, and compatibility assessments.	U	C
Asset Product Name/Family	What product family does the asset belong to.	Helps to identify the type, age and function of a device.	U	C
Asset Product Version	Version number of the asset from a hardware perspective.	Helps to identify if an asset is vulnerable to a certain vulnerability.	U	C
Location - Country	The country the asset is located in.	Important for identifying anomalous communication and for grouping assets into regions to better understand the scope of an incident or impact to operations. Country may already be included in site address below.	C	U
Location – Site Address	Address of the site that the asset is located at.	A good understanding of where the asset is will help better understand the risks associated with vulnerabilities and allow onsite personnel to better assist in incident response activities.	C	U
Location – Room	Room number/name that the asset is located in.	A good understanding of where the asset is will help better understand the risks associated with vulnerabilities and allow onsite personnel to better assist in incident response activities.	C	U
Location – Cabinet	Number or name of the cabinet the asset is located in.	A good understanding of where the asset is will help better understand the risks associated with vulnerabilities and allow onsite personnel to better assist in incident response activities.	C	U
Location - Rack	Location within the rack that the asset is located in.	A good understanding of where the asset is will help better understand the risks associated with vulnerabilities and allow onsite personnel to better assist in incident response activities.	C	U
Network Exposure	Generalisation of the assets network exposure.	Indicates the device's direct connectivity to networks that are not local to the device. E.g. the device could be standalone, within a local OT network, or be directly connected to the IT network or the	C	C

Attribute Name	Meaning	Rationale	IR	VM
		Internet. Understanding exposure to threats aids risk-based VM and IR.		
Primary IP Address	IP address allocated to the asset.	Essential for network management, monitoring, and incident response.	C	U
Secondary IP Address	Secondary IP address allocated to the asset.	Essential for network management, monitoring, and incident response.	C	U
Management IP Address	IP address allocated to the assets management interface.	Essential for network management, monitoring, and incident response.	C	U
Any other associated IP Addresses	Other IP addresses allocated to the asset.	Essential for network management, monitoring, and incident response.	C	U
Other Network Identifiers	Network address of non IP assets such as a DNP node address.	Useful to identify assets that have communication interfaces that don't use IP or MAC addresses.	C	U
IP Subnets	IP subnet(s) that an asset has interfaces connected to.	Allows for correlation of interconnectivity between devices and the possible location of a device under investigation.	C	U
Primary MAC Address	MAC address of interface that primary IP address is assigned to	Useful for device identification and network access control.	C	U
Secondary MAC Address	MAC address of interface that secondary IP address is assigned to	Useful for device identification and network access control.	C	U
Management MAC Address	MAC address of management interface	Useful for device identification and network access control.	C	U
Any other associated MAC Addresses	Any other associated MAC addresses (Bluetooth, Wi-fi etc)	Useful for device identification and network access control.	C	U
Expected Open Network Ports	Open TCP ports relating to services running on the asset.	Identifies potential attack surface and aids in vulnerability assessments.	C	C

Attribute Name	Meaning	Rationale	IR	VM
Expected Network Protocols	Detail of network protocol the asset used e.g. Modbus TCP, DNP3	Essential for identifying protocols using non-standard ports and/or identifying non-TCP/UDP protocols	C	C
Directly Connected Assets[2]	Detail of assets that are directly connected to the asset.	Provides valuable situational awareness when investigating an asset or performing VM tasks. Also supports creation and verification of network diagrams.	C	C
Controller Rack/Slot Information/backplane UUID	Unique identified for assets hardware within a systems chassis.	It helps locate devices and detect vulnerabilities in parts of the OT network that may not be visible to detection tools.	C	C
Controller run-state[3]	The state that the controller is currently in.	Running | remote program | Faulted | stopped | backup, etc.	U	U
Virtual or Physical	Is the asset physical or in a virtualised environment.	Differentiates between asset types for inventory accuracy and helps in applying appropriate security controls.	C	C
Hardware Firmware Version	Firmware version describes the low-level code running on a hardware device	Important for tracking vulnerabilities and ensuring firmware is up to date.	U	C
Hardware Management Version	Management version describes the software managing the hardware.	Important for understanding potential attack paths and ensuring all elements of a device are managed.	U	C
Operating System Version	Version of the OS running on the asset	Critical for vulnerability management and identifying the assets' potential attack surface.	U	C
OT Application Version (depending on classification type such as controllers)	Version of the OT application running with the OS on the asset.	Critical for vulnerability management and identifying the assets' potential attack surface. It can be used to infer the expected communication protocols.	U	C

[2] Ideally this links to a network diagram for reference, given a diagram is the best way to understand connectivity.
[3] This would likely only be available if asset information was being automatically gathered.

Attribute Name	Meaning	Rationale	IR	VM
Other Application Versions	Versions of other applications running on the asset that are not core to its role.	Critical for vulnerability management and identifying the assets' potential attack surface. It can be used to infer the expected communication protocols.	U	C
Physical Installation Date	The date the asset was physically installed.	Useful for indicating if the device, has been replaced or is end of life and its potential vulnerabilities.	U	C
Last Updated	The date the asset record was last updated	Useful for understanding how up-to-date the asset information is.	C	C
Lifecycle Status	Is the asset still in support or not.	Active | end of sale (EOS) | end of life (EOL)	C	C
Lifecycle vendor link	Link to details about the asset on the internal documentation store.	Link to vendor page. This usually includes any significant dates, support dates, etc.	C	C
Alternative products	If the asset is no longer supported what other assets replaced it in the OEM/Vendor catalogue or company spares store.	Equivalent product if this asset is discontinued.	U	U
Discontinued Date	Date that asset reached End of Life.	Date product discontinued by vendor	C	C

Further Attributes (Collect where possible)

Attribute Name	Meaning	Rationale	IR	VM
Serial Number	Serial number of the asset	Useful for warranty tracking, support, and asset verification.	U	U
Photo of Device	Photo of the asset in location	Aids in the physical identification and verification of assets.	U	U
Link to Asset Configuration/Backup Files	Links to internal document store files relating to the asset	Enables quick identification and verification of backups.	U	U
Security Features Enabled	Details of specific security features enabled on the asset.	Where applicable, what features have been enabled – e.g. Threat protection module, Syslog forwarding.	U	U
Hardening Information	Details of what hardening actions have been undertaken on the asset.	Indicates the security posture of the asset and helps in compliance assessments.	U	U
CPE (Common Platform Enumeration)	Full CPE name of the asset which is key to matching CVE's as part of the vulnerability management process.	Enables standardised identification of software/hardware for vulnerability management and threat intelligence. These can be manually created or automatically generated using vulnerability management platforms.	U	U

Attribute Name	Meaning	Rationale	IR	VM
Link to vulnerabilities & exposures	Link to internal store of vulnerability information	Link to list of known vulnerabilities and detected weaknesses of the asset	U	U

Example Asset Register Entries

The following examples depict what an export from an effective asset register could look like. The underlying data may not be collated or stored in the same way as it is presented here, but the ability to quickly create an export of data is an essential element of an asset register.

OT Operator Workstation

Attribute Name	Example Value
Unique Asset Name	LONCC-CTRLRM-OT-OPPWS-001
Asset Name Alias	Flow control desk 1 workstation, FCHMI1
Asset Name Description	Operator Workstation 1, located in the London Control Centre
Asset Purpose	Used for monitoring and controlling energy flow across UK production sites
Asset Type	Operator Workstation
Asset Criticality - Safety	Medium – Important if manual intervention is required
Asset Criticality - Operations	High – Important for managing power flow
Asset Criticality - Security	Low – Does not perform a security-critical function
Impact if Compromised to Safety	Medium – Potentially increased risk to persons if normal software interlocks are bypassed
Impact if Compromised to Operations	High – Direct ability to operate equipment and disconnect circuits
Impact if Compromised to Security	Medium – Workstation could be used for lateral movement and/or collecting authentication tokens or passwords
Asset Owner - Department	Energy Corp Electricity Distribution – Control Centre Operations
Asset Owner – Job title	Contact the duty control centre system team: Internal - 4530 External - 07948930271 Email – CCST@energycorp. com
Asset Vendor - Hardware	Dell
Asset Vendor - Operating System	Microsoft
Asset Vendor - Applications	GE Digital, Rockwell Automation
Asset Product Name/Family	Dell OptiPlex 7090
Asset Product Name	7090-Tower
Location - Country	United Kingdom

Attribute Name	Example Value
Location – Site - Address	Energy Corp Electricity Distribution, Bright Spark Road, Wood Green, London, N22 1ZZ W3W – shining.lights.dazzle
Location – Room	Control Room
Location – Cabinet	Flow control desk 1
Location - Rack	N/A
Network Exposure	Connected to the Primary and Secondary LONCC-CTRLRM OT Networks. No direct internet or corporate network access.
Primary IP Address	10.10.1.10
Secondary IP Address	10.10.2.20
Management IP Address	N/A
Any other associated IP Addresses	N/A
Other Network Identifiers	N/A
IP Subnets	10.10.1.0/24
Primary MAC Address	84:7B:EB:3C:4D:5E
Secondary MAC Address	84:7B:EB:3C:4D:0D
Management MAC Address	N/A
Any other associated MAC Addresses	N/A
Expected Network Ports	TCP 502, TCP 491, TCP 475, TCP 80, TCP 139, TCP 443, TCP 3389
Expected Network Protocols	Modbus TCP, iFIX Web, Proficy Licensing, HTTP, NetBIOS, HTTPS, RDP
Directly Connected Assets	LONCC-CTRLRM-OT-PRISW-001, LONCC-CTRLRM-OT-SECSW-001
Controller Rack/Slot Information/backplane UUID	N/A
Controller run-state	N/A
Virtual or Physical	Physical
Hardware Firmware Version	UEFI 4.2.3 (Dell)
Hardware Management Version	N/A
Operating System Version	Windows 10 Enterprise LTSC 2021
OT Application Version	iFIX 6.5 ProficyLicenseClient 4.1
Other Application Versions	Internet Explorer 11.0.19044.57 Windows PowerShell 5.1.19041.394

Attribute Name	Example Value
Physical Installation Date	2023-03-15
Last Updated	2024-05-20
Serial Number	D3LL7090WS001
Photo of Device	Stored in CMDB
Link to Asset Configuration/Backup Files	Energycorp.shinybackups.local/loncc-ctrlrm-ot-oppws-001
Security Features Enabled	BitLocker, Microsoft Defender for Endpoint, Windows Defender Firewall, Windows Defender System Guard, Application Whitelisting,
Hardening Information	CIS Benchmarks applied – Level 2 profile, USB ports disabled, local admin disabled
CPE (Common Platform Enumeration)	cpe:2.3:o:microsoft:windows_10:2019:*:*:*:enterprise_ltsc:*:*:* cpe:2.3:a:ge:ifix:6.5:*:*:*:*:*:*:* cpe:2.3:a:ge:proficylicenseclient:4.1:*:*:*:*:*:*:* cpe:2.3:a:microsoft:internet_explorer:11.0.19044.57:*:*:*:*:*:*:* cpe:2.3:a:microsoft:powershell:5.1.19041.394:*:*:*:*:*:*:*

IT/OT Firewall

Attribute Name	Example Value
Unique Asset Name	LONDC-CTRLRM-SEC-CRFW-001
Asset Name Alias	ITOT-Gateway, Control Room Firewall
Asset Name Description	Firewall managing traffic between IT and OT networks
Asset Purpose	Segment the control room OT network, control access to and from the IT/OT network and route traffic between subnets.
Asset Type	Firewall
Asset Criticality to Safety	Medium – Important if an operator needs to remotely control equipment to protect people.
Asset Criticality to Operations	Critical – Essential for active power management performed by the OT SCADA servers.
Asset Criticality to Security	Critical – performs critical security functions
Impact If Compromised to Safety	Medium – Important if an operator needs to remotely control equipment to protect people.
Impact If Compromised to Operations	Critical – segments IT/OT networks and routes traffic between different subnets. Unauthorised changes could deny access and/or expose critical systems.
Impact If Compromised to Security	Critical – performs critical security functions
Asset Owner - Department	Energy Corp Electricity Distribution – Control Centre Operations
Asset Owner – Job title	Contact the duty control centre system team: Internal - 4530 External - 07948930271 Email – CCST@energycorp. com
Asset Vendor - Hardware	Palo Alto
Asset Vendor - Operating System	Palo Alto
Asset Vendor - Applications	N/A
Asset Product Name/Family	PA-3220 NGFW
Asset Product Name	PA-3220 Rev B
Location - Country	United Kingdom
Location – Site - Address	Energy Corp Electricity Distribution, Bright Spark Road, Wood Green, London, N22 1ZZ W3W – shining.lights.dazzle
Location – Room	Control Room System Room 1
Location – Cabinet	CAB001
Location - Rack	U36
Network Exposure	Connects to both OT and IT networks. No direct Internet Connectivity.

Attribute Name	Example Value
Primary IP Address	N/A
Secondary IP Address	N/A
Management IP Address	10.10.99.88
Any other associated IP Addresses	192.168.1.17, 192.168.1.215, 192.168.1.134, 192.168.1.84, 192.168.1.107, 192.168.1.190, 192.168.1.63, 192.168.1.212, 192.168.1.87, 192.168.1.206, 172.168.5.43, 172.168.5.37, 172.168.5.16, 172.168.5.1, 172.168.5.44, 172.168.5.21, 172.168.5.49, 172.168.5.40, 172.168.5.59, 172.168.5.55, 172.168.6.55, 172.168.6.12, 172.168.6.62, 172.168.6.23, 172.168.6.54, 172.168.6.33, 172.168.6.30, 172.168.6.18, 172.168.6.34, 172.168.6.42, 10.134.50.3, 10.134.50.12, 10.134.50.6, 10.134.50.11, 10.134.50.14, 10.134.50.7, 10.134.50.8, 10.134.50.4, 10.134.50.9, 10.134.50.10
Other Network Identifiers	N/A
IP Subnets	192.168.1.0/24, 172.168.5.0/26, 172.168.6.0/26, 10.134.50.0/28
Primary MAC Address	N/A
Secondary MAC Address	N/A
Management MAC Address	00:1B:17:AA:BB:AD
Any other associated MAC Addresses	00:1B:17:AA:BB:4D, 00:1B:17:AA:BB:63, 00:1B:17:AA:BB:79, 00:1B:17:AA:BB:85, 00:1B:17:AA:BB:28, 00:1B:17:AA:BB:AE, 00:1B:17:AA:BB:39, 00:1B:17:AA:BB:8A, 00:1B:17:AA:BB:1F, 00:1B:17:AA:BB:E3, 00:1B:17:AA:BB:CC, 00:1B:17:AA:BB:D3, 00:1B:17:AA:BB:50, 00:1B:17:AA:BB:88, 00:1B:17:AA:BB:DD, 00:1B:17:AA:BB:C8, 00:1B:17:AA:BB:EE, 00:1B:17:AA:BB:37, 00:1B:17:AA:BB:E4, 00:1B:17:AA:BB:DF, 00:1B:17:AA:BB:58, 00:1B:17:AA:BB:C7, 00:1B:17:AA:BB:DE, 00:1B:17:AA:BB:46, 00:1B:17:AA:BB:5A, 00:1B:17:AA:BB:25, 00:1B:17:AA:BB:E0, 00:1B:17:AA:BB:6C, 00:1B:17:AA:BB:E2, 00:1B:17:AA:BB:F4, 00:1B:17:AA:BB:BC, 00:1B:17:AA:BB:AA, 00:1B:17:AA:BB:27, 00:1B:17:AA:BB:C4, 00:1B:17:AA:BB:6D, 00:1B:17:AA:BB:60, 00:1B:17:AA:BB:5F, 00:1B:17:AA:BB:0E, 00:1B:17:AA:BB:68, 00:1B:17:AA:BB:5C, 00:1B:17:AA:BB:03, 00:1B:17:AA:BB:A5, 00:1B:17:AA:BB:4E
Expected Network Ports	TCP 443, TCP 80, TCP 139, TCP 3389, TCP 20000, TCP 502, TCP 1433, UDP 1434, UDP 18245, UDP 161, UDP 162, UDP 514, TCP 445, TCP 139, TCP 2010, TCP 53014, TCP 13000, TCP 14000
Expected Network Protocols	HTTPS, HTTP, NetBIOS, RDP, DNP3 over TCP, Modbus TCP, SQL Server, SQL Server Browser, GE SRTP, SNMP, Syslog, SMB/CIFS, iFIX, Historian, ICMP
Directly Connected Assets	Linked to LONDC-CTRLRM-NET-CRSW-001, LONDC-CTRLRM-NET-CRRTR-001

Attribute Name	Example Value
Controller Rack/Slot Information backplane UUID	N/A
Controller run-state	N/A
Virtual or Physical	Physical
Hardware Firmware Version	1.0.5
Hardware Management Version	PAN-OS 10.2.3
Operating System Version	PAN-OS 10.2.3
OT Application Version	N/A
Other Application Versions	N/A
Physical Installation Date	2017-1-8
Last Updated	2025-2-25
Serial Number	PA3220ITOT001
Photo of Device	Picture in CMDB
Link to Asset Configuration/Backup Files	Energycorp.shinybackups.local/loncc-ctrlrm-sec-crfw-001
Security Features Enabled	Unknown
Hardening Information	Default credentials changed, unused services disabled, logging enabled
CPE (Common Platform Enumeration)	cpe:2.3:h:paloaltonetworks:pa-3220:*:*:*:*:*:*:*:*

PLC

Attribute Name	Example Value
Unique Asset Name	NOTPS-TER-OT-TCPLC-001
Asset Name Alias	TGU, Turbine Controller
Asset Name Description	Turbine Control PLC 1, located in the turbine equipment room at the Nottingham power station
Asset Purpose	PLC for controlling and monitoring the steam turbine
Asset Type	PLC
Asset Criticality to Safety	Critical – performs safety-critical functions
Asset Criticality to Operations	Critical – required to generate revenue
Asset Criticality to Security	Low – no specific security function
Impact If Compromised to Safety	Critical – potential to disable or modify safety-critical systems
Impact If Compromised to Operations	Critical – If the PLC is compromised, the system will be immediately shut down for safety, preventing operation.
Impact If Compromised to Security	Low – no specific security function
Asset Owner - Department	Energy Corp Electricity Distribution – PS OPS
Asset Owner – Role title	Contact the duty PS OPS Manager: Internal - 1330 External - 07748930246 Email – PSOPS_DUTYMANAGER@energycorp. com
Asset Vendor - Hardware	Siemens
Asset Vendor - Operating System	Siemens
Asset Vendor - Applications	N/A
Asset Product Name/Family	Simatic S7-400
Asset Product Name	S7-400 - CPU 414F-3 PN/DP
Location - Country	United Kingdom
Location – Site - Address	Nottingham Power Station, Power Station Road, Liven, Nottingham, NG12 4ZZ W3W – ///opens.locked.amused
Location – Room	TGU Equipment Room R7.4
Location – Cabinet	X.7.4.1
Location - Rack	Middle of rack
Network Exposure	Connects to the OT TGU LAN. No direct Corporate or Internet Connectivity.
Primary IP Address	172.168.50.10
Secondary IP Address	172.168.60.20

Attribute Name	Example Value
Management IP Address	N/A
Any other associated IP Addresses	172.168.50.2, 172.168.60.3, 192.168.5.120, 192.168.5.130, 192.168.5.140
Other Network Identifiers	Modbus Unit ID: 1
IP Subnets	172.168.50.0/25, 172.168.60.0/25, 192.168.5.0/24
Primary MAC Address	00:0E:8C:AB:CD:EF
Secondary MAC Address	00:0E:8C:AB:CD:F0
Management MAC Address	N/A
Any other associated MAC Addresses	00:0E:8C:DE:AD:BE, 00:0E:8C:01:23:45, 00:80:2F:12:34:56, 00:80:2F:AB:CD:EF, 00:80:2F:01:23:45
Expected Network Ports	TCP 443, TCP 80, TCP 102, TCP20, TCP 21, TCP 502,
Expected Network Protocols	HTTPS, HTTP, S7comm, FTP Data, FTP Control, Modbus TCP, ICMP
Directly Connected Assets	Linked to NOTPS-TER-OT-PRISW-001, NOTPS-TER-OT-SECSW-001, to NOTPS-TER-OT-MODSW-001
Controller Rack/Slot Information/backplane UUID	CPU 414-3 PN/DP, CP 443-5, SM 336 AI, SM 326 DI, SM 326 DO
Controller run-state	Running
Hardware Management Version	N/A
Operating System Version	Unknown
OT Application Version	N/A
Other Application Versions	N/A
Installed Date	2017-2-6
Last Updated	2022-12-25
Serial Number	Unknown
Photo of Device	None
Link to Asset Configuration/Backup Files	Energycorp.shinybackups.local/NOTPS-TER-OT-TCPLC-001
Security Features Enabled	Unknown
Hardening Information	Unknown
Security Logging Configured	Unknown
Security Log Accessibility	Local (if at all)

Attribute Name	Example Value
Security Logs Actively Monitored	No
Security Logs Forwarded to a central log collector or SIEM	No
CPE (Common Platform Enumeration)	cpe:2.3:h:siemens:simatic_s7-400_cpu_414-3_pn_dp:7.0:*:*:*:*:*:*:*
Link to vulnerabilities & exposures	Energycorp.luminescence.local/NOTPS-TER-OT-TCPLC-001

RTU

Attribute Name	Example Value
Unique Asset Name	CDLPS-RTU-OT-PSRTU-001
Asset Name Alias	Candle Lane Sub RTU, Candle Lane 33 RTU
Asset Name Description	Candle Lane Primary Substation RTU number 1
Asset Purpose	RTU for control and monitoring of Candle Lane Primary Substation
Asset Type	RTU
Asset Criticality to Safety	Low – no specific safety function
Asset Criticality to Operations	Important – required to monitor and reconfigure electricity flow
Asset Criticality to Security	Low – no specific security function
Impact If Compromised to Safety	Low – no direct safety impact if compromised
Impact If Compromised to Operations	Critical – An attacker could turn off or reconfigure power flow, impacting customers and our ability to meet regulatory requirements
Impact If Compromised to Security	Low – no specific security function
Asset Owner - Department	Energy Corp Electricity Distribution – Field Operations
Asset Owner – Job title	Contact the Central Control Centre for a field ops point of contact: Internal - 4530 External - 07948930271 Email – CCST@energycorp. com
Asset Vendor - Hardware	Schneider Electric
Asset Vendor - Operating System	N/A
Asset Vendor - Applications	N/A
Asset Product Name/Family	Talus
Asset Product Name	Talus C10e
Location - Country	United Kingdom
Location – Site - Address	Candle Lane 33 Primary Substation, Candle Lane, Sandy Donington, Leicestershire, DE74 2SA W3W – ///overdrive.recovery.impose
Location – Room	Candle Lane 33 Primary Substation
Location – Cabinet	RTU and Telecoms
Location - Rack	Top
Network Exposure	Connects to the Candle Lane Protection Relay Modbus (RS485) ring bus and the RTU Radio Link. The radio link connects RTUs to the

	London Control Centre via radio relays. No direct Corporate or Internet Connectivity.
Primary IP Address	N/A
Secondary IP Address	N/A
Management IP Address	N/A
Any other associated IP Addresses	N/A
Other Network Identifiers	Modbus Unit ID: 1
IP Subnets	N/A
Primary MAC Address	N/A
Secondary MAC Address	N/A
Management MAC Address	N/A
Any other associated MAC Addresses	N/A
Expected Network Ports	N/A
Expected Network Protocols	N/A
Directly Connected Assets	CDLPS-PRT-OT-CCTOC-001, CDLPS-PRT-OT-CCTOC-003, CDLPS-PRT-OT-CCTOC-005, CDLPS-PRT-OT-CCTOC-007, CDLPS-COM-OT-SDRSD-001
Related Assets	London Control Centre OT Systems and Networks
Controller Rack/Slot Information backplane UUID	N/A
Virtual or Physical	Physical
Hardware Firmware Version	V1.3
Hardware Management Version	N/A
Operating System Version	Unknown
OT Application Version	N/A
Other Application Versions	N/A
Physical Installation Date	2013-6-6
Last Updated	2015-2-2
Serial Number	Unknown
Photo of Device	None
Link to Asset Configuration/Backup Files	Energycorp.shinybackups.local/CDLPS-RTU-OT-PSRTU-001

Security Features Enabled	Unknown
Hardening Information	Unknown
Security Logging Configured	Unknown
Security Log Accessibility	Local (if at all)
Security Logs Actively Monitored	No
Security Logs Forwarded to a central log collector or SIEM	No
CPE (Common Platform Enumeration)	Unknown
Link to vulnerabilities & exposures	Energycorp.luminescence.local/CDLPS-RTU-OT-PSRTU-001

Summary and Conclusion

Establishing a well-structured ICS/OT asset register is vital for enhancing your cybersecurity and operational resilience. This article outlines key asset attributes that enable effective incident response and vulnerability management—think of it as a starting point from which you can build off.

Focusing on high-value data, especially for critical assets, allows you to make informed decisions and respond rapidly to threats. While gathering data in ICS/OT environments can be challenging, prioritising impactful attributes ensures efficiency and significance.

Whether you are building a new asset register or improving an existing one, align your data collection with operational and security priorities. Adopt a practical approach: focus on what matters most and expand as you grow.

Further Reading

- CISA - Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators
- NIST - Guide to Operational Technology (OT) Security
- NIST - Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry

CAF Indicator of Good Practice Summary

This article discusses measures that contribute to the following CAF Indicators of Good Practice:

- 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.
- A3.a A04: You have assigned responsibility for managing physical assets.
- 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.
- 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 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, secured settings and configuration.
- B4.d A01: You maintain a current understanding of the exposure of your essential service to publicly known vulnerabilities.
- C1.c A03: Alerts can be easily resolved to network assets using knowledge of networks and systems.
- C1.e A07: Monitoring staff are aware of essential services 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 is version 1.0 and was published on 08/10/2025. It will be reviewed every 18 months.