INDUSTRIAL CONTROL SYSTEMS
Community of Interest

Logging and Monitoring within Industrial Control systems and Operational Technology environments.

Aims of this guidance

This article is designed to help organisations understand the importance of logging and monitoring in Industrial Control Systems (ICS)/Operational Technology (OT) systems and ultimately to better prepare for a cyber incident in an OT/ICS environment. It considers how organisations using ICS/OT can assess logging opportunities in their estates and how to implement best practice, in line with the NCSC secure design principles, in particular the principle of making compromise detection easier.

It specifically provides best practice advice for organisations in defining, implementing, operating and maintaining monitoring and logging activities. It will help your organisation devise an approach to logging, by addressing many of the questions asked when a cyber incident occurs in an ICS/OT environment. It is designed to complement the NCSC's general logging and monitoring guidance, while focusing on the specific and unique aspects relating to ICS/OT, being part of a series of guidance developed by the ICS COI.

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 principal 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 This guidance article will be reviewed every 18 months to ensure that it has not been superseded by guidance published by NCSC, relevance and that any references are still accurate.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 guidance for?

This guidance is for you if:

- your organisation currently has little or no ICS/OT logging capability, or you would like to assess if your current logging capability is suitable or sufficient
- you would like to understand the NCSC's expectations in basic good practice for logging

Structure of this guidance

The guidance is made up of a series of articles addressing different aspects of ICS/OT logging and monitoring:

- **Why** you need to log and monitor in an ICS/OT environment
- **What** you need to log and monitor in an ICS/OT environment
- **How** you undertake ICS/OT logging
- **Where** you undertake ICS/OT logging
- How you **verify** your logging in an ICS/OT environment
- How you **secure** your ICS/OT logging and monitoring capability
- How long to **store** your ICS/OT logging records and how to store them
- **Who** needs to monitor your ICS/OT logging and what skills are required
- How to **analyse** your ICS/OT logging

Differences between IT and ICS/OT

At a high level, the benefits of monitoring and logging are the same for ICS/OT and Information Technology (IT). But there are some key differences to consider between IT and ICS/OT, concerning the specific purpose of ICS/OT in plant operations.

Plant operations provide many opportunities for monitoring, beyond those typically deployed (or required) in an IT environment. As plants are cyber-physical systems, the integrity and availability of their ICS/OT functions is vital. For effective security monitoring in the ICS/OT environment, organisations need to know about and understand the full range of functions. Data from the physical processes of operational plants can be used as another source of security-monitoring data.

Within ICS/OT systems, the production process creates information that can supplement traditional IT monitoring. This provides greater visibility of ICS/OT functions and technologies that may lack built-in monitoring and logging capabilities.

Examples of logging and monitoring in plant operations:

- **Operator rounds**. Identifying anomalies in performance (such as excessive vibration or noise), as well as variances in process readings between a SCADA and what is displayed on local analogue instruments.
- **Maintenance activities**. Routine maintenance or management of ICS/OT equipment can also identify anomalies (such as unexplained changes in configurations or error messages in system logs) which may indicate suspicious activity.
- **Technical oversight**. Technical support teams, using data from ICS/OT historians (or similar), can identify unexpected trends in plant performance.
- **Monitoring** of process control variables and set point limits.
- **Monitoring** of control commands (such as pump start or stop) in ICS/OT network traffic and protocols.

The differences between IT and ICS/OT can cause difficulties for people, processes and technology when monitoring and logging in such environments. Examples of these difficulties include:

- **Aged assets and operational criticality**. ICS/OT assets are often close to end of life (EOL) and industrial networks aren't necessarily designed to consider spare capacity for future growth. As such, it may be necessary to upgrade networks and networking equipment to support the additional throughput required for active monitoring. Devices may also be aging and without software or firmware patches against the latest vulnerabilities.
- **Proprietary or less common protocols**. It's common to find a wide range of both open and vendor proprietary protocols in ICS/OT environments. Without fully understanding the data within certain protocols, it can be difficult to know if network traffic is benign or malicious. IT tools often don't correctly understand protocols and therefore provide limited benefits.
- **Skills shortages**. Organisations often have a skills gap between those maintaining and operating the ICS/OT environment, and those responsible for security at sites. Without knowledgeable staff who understand the monitoring and logging data from the ICS/OT environment, remediation activities may be more difficult, or operations may even be disrupted. Security Operation Centre (SOC) staff need to understand the context of any ICS/OT logging in place and be able to correlate it with IT or traditional security logging in place.
- **Sufficient availability of data**. While many ICS/OT environments are designed to meet operational demands, this design doesn't necessarily help forensic readiness or follow best security practices. Using unmanaged switches may create blind spots, or it could be difficult to provide meaningful logs for assets in an ICS/OT environment.
- **Reliance on non-ethernet connectivity**. While many industries have moved to ethernet based devices and protocols, some sectors are still very reliant on serial communications (such as RS-232 and RS-485 proprietary) which makes duplicating or tapping difficult.

Conversely, the difference between IT and ICS/OT can be beneficial because it can simplify the detection requirement within the ICS/OT assets:

- **Static design.** The design of ICS/OT network is fairly static and subject to strict change management processes. This allows for simplified and focused detection in the ICS/OT environment.
- **Controlled environment**. ICS/OT users are defined and operate in a controlled environment. Unlike large IT assets where a user's mode of operation, geographical location or other factors can be variable, ICS/OT asset users and operating modes are known and well defined.
- **Low volume of data**. The extent of operational and security data in the ICS/OT environment is often considerably lower than in IT environments. This provides for lowered storage and processing requirements at the edge.
- **Defined ICS/OT boundary**. The ICS/OT boundary should be well defined to help logging and monitoring, and to provide good visibility of key potential attack paths.
- **Traditionally Air gapped**. ICS/OT systems were often run in isolation without wider connectivity to enterprise systems. More recently this has started to change through digital transformation which brings operational efficiency; however, this may lead to inadvertently connecting legacy systems to networks which may have a transient link to public networks or expose ICS/OT systems to attacks for which they were not designed.

A note on the fictional organisation used in examples

Across this guidance, we are using the fictional organisation 'Admin Corp' also used in NCSC's Design Principles and Operational Technology) to explain different aspects of this topic. Each section provides examples of how Admin Corp implements the guidance.

The below diagram is a simple network diagram of the fictional Admin Corp:

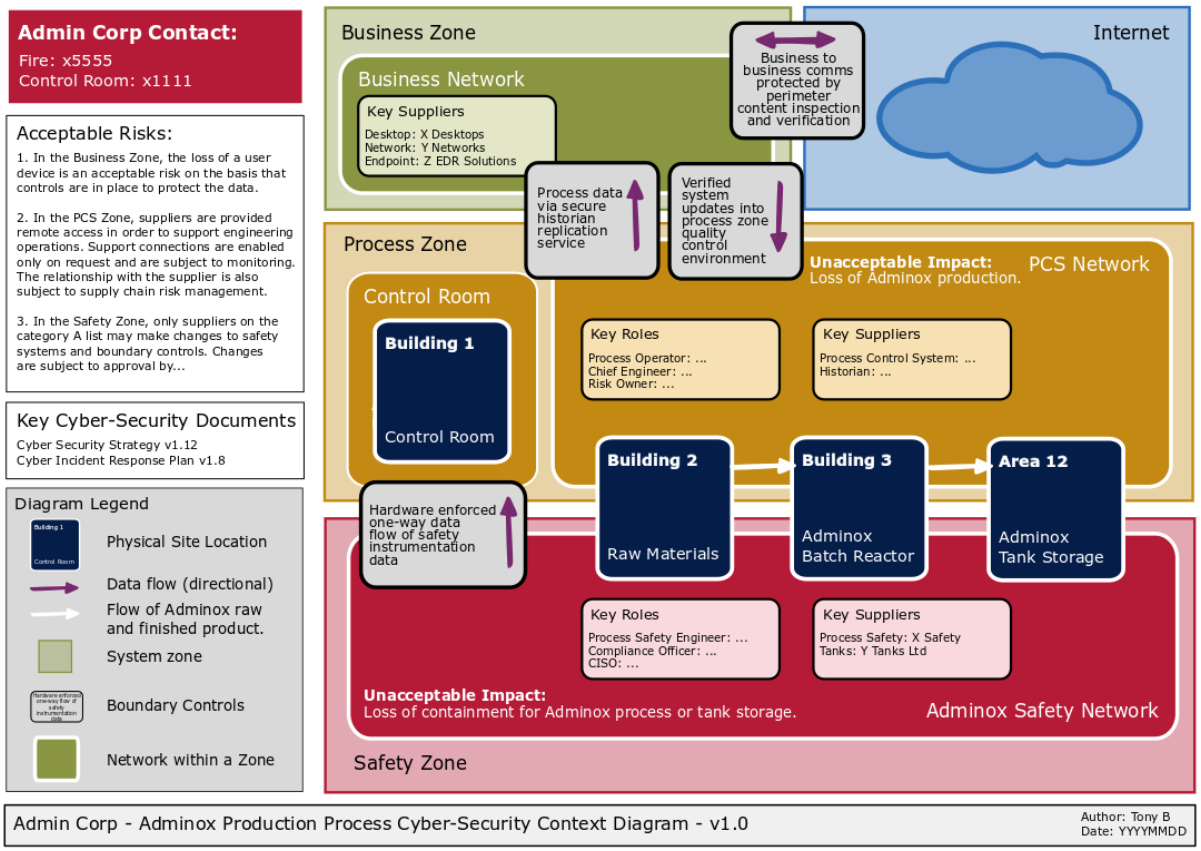

Figure 1 -The Admin Corp Network

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 v2.0 and was published on 20/10/2025. It will be reviewed every 18 months.