INDUSTRIAL
CONTROL
SYSTEMS
Community of Interest

GUIDANCE: MANAGEMENT OF INDUSTRIAL CONTROL SYSTEM / OPERATIONAL TECHNOLOGY FIELD DEVICES

Introduction

This guidance is intended to enable organisations with Industrial Control System (ICS) / Operational Technology (OT) environments to implement appropriate controls to ensure appropriate management where local access to field devices such as smart instruments, variable speed drives, Remote Terminal Units (RTUs) is required. It is part of a series of articles focused around securing the ICS/OT boundary.

Local access to field devices could be required to perform one of many different functions such as:

- Configuration or Calibration of a device using a laptop.
- Calibration of a device using a proprietary calibration device.
- Retrieval of data, either process data, or device performance data, from a device using a laptop is a common operation. In such cases it is important to follow the controls identified in this related article on handling removable media within ICS/OT environments, to ensure proper data management and security.
- Monitoring and support of the device, including SNMP, SYSLOG, fault finding and initial configuration.
- Maintenance and administration of the device, implementing modifications to the device, e.g., updating firmware, changing device configuration parameters.
- Asset Performance Data – information relating to the condition and performance of the asset, typically being transmitted to asset management solutions and/or Artificial Intelligence (AI) / Machine Learning (ML) solutions to predict potential asset failures, or the impact of proposed changes.

In the context of this guidance, this local access could be achieved through either:

- direct connection to the device (e.g., through a serial port on the device), this includes instances where initial configuration of a device requires a dedicated wireless connection to be made to the configuration device.

- a dedicated out-of-band maintenance network - this is restricted to being within the facility and has no connectivity to any other networks (e.g., using separate network interfaces on a group of PLCs, connected to a managed switch to which a maintenance device is then connected). If implemented, such a network should be considered as a separate zone (as defined in ISA/IEC 62443) and managed appropriately.

It is also important to note that more devices are supporting local configuration via Bluetooth (or other local wireless protocols).

A key aspect of the design of any ICS/OT system is to understand all such scenarios requiring local access to the device such that appropriate controls can be implemented.

This guidance is provided on the understanding that the legacy aspects often experienced within ICS/OT environments mean that in some situations local access/configuration is still required either directly connecting to the device or via a local out-of-band site-based maintenance network, whereas there is a movement on newer implementations to be able to undertake all configuration over the network via secure network remote access means. NCSC has existing guidance to help secure remote access into CNI, that also covers the need for network infrastructure to support remote access.

Differences between IT and ICS/OT

A key difference between ICS/OT and IT environments is the extent to which local access to a device/asset is required. While in an IT environment, network connectivity allows the majority of operations to be undertaken remotely, in an ICS/OT environment, especially one containing legacy equipment, many activities require local access to the device. In many cases such local access is the only way by which access to the device can be obtained.

The different data streams associated with ICS/OT assets should also be recognised, along with the different potential consequences from a compromise of the Integrity, Availability, or Confidentiality of those data streams. Typically, these data streams can be segregated into:

- Process Data – information relating to the status of a process being transmitted between sensors, RTUs, PLCs, SCADA etc.
- Asset Performance Data – information relating to the condition and performance of the asset, typically being transmitted to asset management solutions and/or AI/ML solutions to predict potential asset failures, or the impact of proposed changes.
- Engineering Data – asset configuration data, administration and management data, or programs, used to control the operation and performance of the asset.

Ideally, streams should be segregated within the system, such as transmitting different data streams on different protocols. However, if this segregation hasn't been implemented, additional compensatory controls may be necessary, especially in cases where access to a system for asset performance data retrieval could also enable changes to engineering or process data.

Security Principles

The first step in securing an ICS/OT environment is to understand what assets you have (see related guidance here), and the options they have for secure management (see NCSC guidance here). The primary principles required to ensure the secure management of local device access require that:

- Physical access controls should be used to ensure only authorised personnel have access to devices.
- All support devices requiring connection to a field device (e.g. laptops, calibration devices) should be appropriately managed (and should follow NCSC guidance such as Browse Down.)
- Access to devices is only allowed to those authorised to work on the device.
- Records should be kept of all connections made to the device.
- Disable unneeded physical interfaces and disable unneeded management services.

These principles **are consistent with IEC 62443-3-3 based design and** support objective B4 (System Security) of the NCSC CAF, in particular B4.c (Secure Management).

There are several different methods by which these principles can be implemented detailed below:

Physical Access Controls

A layer of protection can be implemented through the use of a variety of physical access controls (see related guidance from NPSA here) to the ICS/OT devices. These could take the form of:

- Devices installed in locked cabinets (or segregated enclosures within a cabinet), with access only available to those authorised to work on the device,
- Support tools used with the device kept in locked cabinets, with access only granted to authorised personnel,
- Communication port locks, preventing the connection of another device, again with access only available to those authorised to work on the device,
- Operating mode keys (e.g., a Run/Remote/Program key on an RTU), removed from the device and only available to those authorised to work on the device.

To support these controls (including procedures/protections that may be needed to provide access provisions in case of an emergency), management arrangements should ensure that records are kept of all authorised access to a device, e.g., through recording activities in a Maintenance Management System. It is recognised that keeping such records is a time consuming and expensive process. Detailed records are necessary however, when trying to recover from a cyber-attack, given the provide important insight into how a system has been attacked, and this aid the recovery and mitigation process. This requirement is detailed in the CAF logging and monitoring IGP.

It is important to note that more devices are supporting local configuration via Bluetooth (or other local wireless protocols).

Support Device Controls

PC based devices owned and managed by the operator.

The preferred approach for all support devices is for them to be owned and managed by the operator. This includes devices that are to be used by 3rd parties, where the recognised good practice is for the operator to provide user accounts to specific personnel from the 3rd party once they have demonstrated their competence.

Typical controls that can be applied to this scenario include:

- Devices should be securely locked away with access restricted to authorised personnel who have demonstrated the required levels of competence (including in relation to cybersecurity), with default accounts/passwords disabled.
- Devices should be hardened with, where possible, fully patched applications and operating system, and only have the software required for their specific function installed, and not corporate applications such as MS Office, e-mail, and should conform to NCSC's Privilege Access Workstation (PAW) guidance.
- Devices should not be capable of being connected to both the target device and another network concurrently. Devices should be restricted to accessing only specific ICS/OT networks for safe import of data and updates, they should not be connected directly to the IT network or internet.
- Devices should be managed as a component of the system(s) to which they have access and be subject to the rigour of change control required for those systems.
- Only program files, or device configurations, needed for the specific piece of work shall be loaded onto the device.
- Multi-factor authentication to use a device.

PC based devices owned and managed by a 3rd party.

Where a 3rd party is required to provide and use a support device as part of a support contract, and it is deemed acceptable by the asset owners, then the key controls that should be implemented include:

- ·assurance shall be provided that devices are hardened with, where possible, fully patched applications and operating system, and are free from malware prior to use and should conform to NCSC's Privilege Access Workstation (PAW) guidance
- assurance should be provided of the competence of 3rd party personnel, including in relation to cybersecurity.
- the degree of assurance provided should be proportionate to the sensitivity of the asset being accessed, noting that this can be hard to gain from 3rd parties.
- Controls should be implemented to ensure that any sensitive information relating to the asset is removed from the support device prior to it being removed from the operator's site.

As many of the above controls as possible should be incorporated into contractual requirements.

Proprietary devices owned and managed by the operator.

While most of the controls mentioned earlier are applicable in this context, it's worth noting that proprietary devices often have more limited functionality compared to PC-based devices or laptops. As a result, enforcing controls like the requirement for AV scanning may not always be possible. Additionally, as these devices also tend to have less granular capabilities in respect of user access control, additional physical/managerial controls require to be implemented to record the usage of the support tool. Due to their proprietary nature, there is a higher likelihood of these devices needing to be taken offsite, e.g., for repair. This requires the consideration of additional controls regarding the information stored on the support device.

Proprietary devices owned and managed by a 3rd party.

The principles for controls identified above also apply in this scenario, though the limited capabilities of the devices should be recognised.

Access Authorisation Controls

A key requirement is to ensure that all configuration activities are only undertaken by personnel who have demonstrated the level of competence (including in relation to cybersecurity) required to undertake the activity, with records kept of all authorised personnel and their competence status. It is important that the principle of least privilege needed to undertake the task is also followed (see NCSC guidance). This principle should be applied to 3rd party engineers as well as personnel from the operating company. Additional controls which should also be considered include:

- no use of corporate IT credentials to access ICS/OT systems,
- ensure all default usernames and passwords are removed or, as a minimum, disabled,
- apply 2-person rule for access to all sensitive/critical systems, and
- do not allow unsupervised access to 3rd parties.

Where such controls are not practical, alternative approaches such as requiring the 3rd party to contact an authorised person before connecting to any plant, and providing an assured log of all activities undertaken, or implementing a monitored Maintenance Zone (detailed below), should be considered.

Maintenance Zone Controls

Where a single location contains multiple endpoints capable of supporting dedicated management interfaces, consideration could be given to implementing a Maintenance Zone using interfaces separate from the process zone. Zones such as this could simply provide connectivity for a laptop, or could include additional services (e.g., authentication services) used with the laptop and target device. While the additional infrastructure associated with such an architecture requires additional support, it can provide many security benefits including:

- Providing additional security controls restricting the devices which can be connected to the zone (and hence to the endpoints)
- Providing additional monitoring and logging capability which can be used to detect unauthorised activity, especially where 3rd parties are undertaking the activity.

As noted in the introduction section, ideally endpoints should be networked and configured, with zoning/segmentation as required, to facilitate secure remote access and configuration, bringing other security benefits such as facilitating better logging and monitoring capabilities.

Access Records

To support any potential incident response, a record of all authorised interventions should be maintained. Ideally this should be linked to the maintenance records of the asset. These records should identify:

- the user, including the specific user account(s) accessed,
- the devices used during the activity, and
- all actions undertaken.

Where possible the record of these actions should be verified either by a second individual (e.g., when the 2-person rule is being followed), or via independent means especially when assurance of 3rd party activities is required.

Meet Admin Corp

With the principles above it can be difficult sometimes to see exactly how a principle should be applied in any given case. In this "Admin Corp" example, we're going to walk through the selection and usage of a solution to securely manage media in an element of their ICS/OT environment**.**

For this example, we will re-use fictional case study "Admin Corp" previously used by the NCSC to explore the application of the Secure Design Principles.

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 EU NIS Directive. This means that Admin Corp's network, information systems and technology needed for the production of 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.

The process for producing Adminox involves a number of steps, with the final product stored under pressure in a tank. Clearly, no one would benefit from the unconstrained release of this Adminox, with the potential for additional red tape clogging up local services for years.

We now look at two different components of Admin Corp's production environment, its Safety Systems and its Batch Reactor PLC, and the solutions employed for local access.

Admin Corps Approach to securing local access to Safety Systems

Admin Corp use two laptops to support the maintenance and configuration of an isolated Safety System. In addition to the controls already implemented relating to the use of media with these laptops following NCSC's guidance, given the significance of the potential consequence of a compromise of the associated safety system, additional controls were considered to improve the security of the laptops and safety systems themselves.

Admin Corp's use of Physical Access Controls - When looking at the access arrangements and physical security of the safety system, it was identified that non-authorised personnel could access the cabinet in which the system was installed as it was shared with other services. To improve this position, the following additional controls were implemented:

- An additional lockable cover, segregating the safety system controller from the other equipment in the cabinet was installed which prevented access to the systems communication ports without removal of the cover.
- The operating mode key on the system was set to the Run position, removed from the cabinet, and stored with the laptops.

A procedure to support emergency access by authorised personal was also implemented.

Admin Corp's use of Support Device Controls - When reviewing the configuration of the laptops, although significant controls had been implemented to support the required media management controls, a number of areas for further improvement were identified, including:

- The support laptops themselves were stored in a locked cabinet, with access only granted by the operational shift manager to authorised individuals. This includes access to laptops to allow them to be maintained and patched utilising removable media (following the guidance here).
- The build of the laptops was reviewed with all unnecessary software (e.g., MSOffice) being removed.
- The laptops were added to the plants asset register, as components of the safety systems.

Admin Corp's use Access Authorisation Controls - To ensure the safety systems were only accessed by authorised personnel, a register of authorised personnel was created. This was made available to the operational shift managers (to allow the required level of control of access to the support laptops). Additional training in cybersecurity was provided to these personnel, and successful completion of that training added to their training records to underpin the necessary demonstration of competence.

Further to this, Admin Corp also decided that, due to the sensitivity of the safety systems and its inability to provide a record of activities undertaken on it, they would apply a 2-person rule for all access to these systems to allow for independent verification of all activities undertaken.

Admin Corp's use of Access Records - Although part of their standard maintenance arrangements, in relation to these systems Admin Corp reinforced to the authorised personnel the need to record all details of work undertaken on the systems accurately to allow it to be entered into their Maintenance Management System. Details required to be recorded included:

- the user, including the specific user account(s) accessed,

- the specific laptop used to undertake the activity, and
- all actions undertaken, with reference to any authorised change requests, or other authorisations.

Admin Corps Approach to securing local access to Batch Reactor PLCs

The batch reactor building contains several PLCs to which access is required by 3rd parties for maintenance, data retrieval, and modification. As these PLCs had the capability for multiple ethernet interfaces, it was decided to connect a dedicated ethernet port on each PLC to form an isolated Maintenance network to which a single programming laptop, which would be used by the limited number of authorised engineers within Admin Corp, and a 3rd party service provider, could be connected.

Admin Corp's use of Physical Access Controls - When implementing the access arrangements and physical security of the maintenance network, steps were taken to ensure that no unauthorised personnel could access the cabinets in which the equipment was installed.

Admin Corp's use of Support Device Controls - The laptop to be used for the maintenance activities would be used by personnel from the 3rd party service provider, as well as Admin Corp personnel and, to ensure that it could only be used for the purposes identified above, was built to a specification which included:

- Restricting its access to only the maintenance network (with no connectivity to the IT network or internet) and preventing it from being connected to multiple networks concurrently.
- Installing anti-malware software, which was maintained current, and confirmed as being free from malware prior to use.

Additionally:

- The support laptop was stored in a locked cabinet, with access only granted by the operational shift manager to authorised individuals, including the 3rd party engineers.
- The laptop was added to the plant's asset register, as a shared component of each of the PLCs.

Admin Corp's use of Access Authorisation Controls - To ensure the PLCs were only accessed by authorised personnel, a register of authorised personnel was created. This was made available to the operational shift managers (to allow the required level of control of access to the support laptops). Additional training in cybersecurity was provided to these personnel, including those from the 3rd party service provider, and successful completion of that training added to their training records to underpin the necessary demonstration of competence.

Further to this, to support the use of the laptop by personnel from the 3rd party service provider, dedicated accounts for use by those engineers were created. Given the limited number of engineers from Admin Corp and the 3rd party required to access this single laptop, which is the only device authorised to be used with these PLCs, it was decided to use local user authentication on the laptop itself, rather than install the additional infrastructure required to implement centralised authentication services for the maintenance zone.

Additional controls were then implemented including:

- The laptop was configured to log all user activity to relevant system logs.

- The network switch to which the PLCs, and laptop, were connected was secured to prevent unauthorised devices from being connected to it, and was also configured with a RSPAN port to enable the logging of all events (e.g. connection of the laptop, changes in switch configuration).

These controls were to ensure that all activity on the maintenance network was monitored, following NCSC guidance, such that activities by the 3rd party could be verified.

Admin Corp's use of Access Records - Although part of their standard maintenance arrangements, in relation to these systems Admin Corp reinforced to the authorised personnel, including those from the 3rd party service provider, the need to record all details of work undertaken on the systems accurately to allow it to be entered into their Maintenance Management System. Details required to be recorded included:

- the user, including the specific user account(s) accessed,
- the specific laptop used to undertake the activity, and
- all actions undertaken, with reference to any authorised change requests, or other authorisations.

CAF Indicators of Good Practice Summary

This case study discusses measures that contribute to the following CAF V3.1 Indicators of Good Practice (IGP)s:

- **B3.A**: You have identified all mobile devices and media that may hold data important to the operation of the essential function.
- **B3.E:** You catalogue and track all devices that contain data important to the operation of the essential function (whether a specific storage device or one with integral storage).
- **B3.E:** All data important to the operation of the essential function is sanitised from all devices, equipment, or removable media before disposal.

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), with support from the National Cyber Security Centre (NCSC). This guidance is not intended to replace formal NCSC guidance where already available, and care has been taken to reference such existing guidance where applicable.

This document is provided on an information basis only, ICS-COI members and NCSC 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, the NCSC 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 the ICS-COI or NCSC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.