INDUSTRIAL CONTROL SYSTEMS
Community of Interest

Securing Industrial Control Systems/Operational Technology environments in periods of heightened threat.

Introduction

There are a number of interventions that UK CNI operators could employ within their Industrial Control System (ICS)/Operational Technology (OT) environments if the risk of compromise is higher than usual. For some CNI operators these will be a variation on existing controls, for others then these will be new controls that could be implemented.

Some of the interventions noted in this article will require elements to be considered during the design and architecting of ICS/OT environments, either when being built or during subsequent upgrades, otherwise CNI operators will find it difficult to implement them.

It is important to note that not all the interventions detailed in this article are appropriate for all ICS/OT environments, and the cost of implementing them may outweigh the benefits gained. Operators should use the interventions detailed as a suite of options that are available to them. They should always be fully tested before implementing them, with assurances gained on how effective they are within the operators specific ICS/OT environment. Furthermore, any interventions implemented for short term risk management, should always be tested to ensure they are fully reversible.

While this article has been written specifically for UK CNI Operators, it is relevant to the likes of System Integrators and those involved in the supply chain for UK CNI OT environments.

While the suggested interventions can be implemented prior to an incident and taken into account in the general work to secure ICS/OT environments, consideration should be given to them also being included as part of an operators Incident Response Plan (IRP).

The ICS COI has published guidance to help UK CNI Operators develop OT focused IRPs which can be found at:

- Considerations for Cyber Incident Response Planning within Industrial Control Systems/Operational Technology
- Incident Response Planning for Industrial Control Systems / Operational Technology - Meet Admin Corp

A further suggestion is for UK CNI operators to develop a pre-incident, heightened-risk period playbook, to help with implementing the suggested controls.

The Interventions detailed in this article have been broken down into 4 categories:

1. **Increase situational awareness -** *Increase and/or improve the information available to defenders.*
2. **Hardening -** *Prioritise typical resilience actions to reduce the attack surface area of devices, networks.*
3. **Change the environment -** *Step change to significantly limit the opportunities for actors to cause disruption, which may incur business cost.*
4. **Weathering the storm -** *Adapt ways of working to be more tolerant of disruption and prepare to adapt further in crisis scenarios.*

Proposed Interventions

The following 18 interventions have been identified that could be implemented by UK CNI operators during a period of heightened threat to the ICS/OT environments. While some of these may have no cost associated (to build and implement the controls), others will require significant prior investment to build the capability. The interventions could have possible costs to the operator's business, due to impacting the efficiency of providing their essential service, and therefore consideration and discussion across the business is required to understand the impact versus the risks being mitigated.

Increase situational awareness:

1. Automated response to monitoring enabled.
2. Increased Monitoring/Auditing of ICS/OT Systems
3. Threat Hunting Activities

Hardening:

4. Enforced Segregation
5. Enforced Island Mode
6. Turn off unrequired ICS/OT and IT
7. Advance plans for updates/patching

Change the environment:

8. Restricted Remote Access
9. More Restrictive Firewall filtering
10. Restricted Data Transfer – removable media
11. Restricted use of third-party IT
12. Revoke Account Access to ICS/OT Environment
13. Implement Geo Fencing on remote access connections
14. Implement full Multi-Factor Authentication on Physical Access Controls

Weathering the storm:

15. Workforce Communication
16. Invoke a change freeze
17. Implement Immediate Back Up
18. Review of ICS/OT Incident Response Plan

For these interventions to be enacted, it is suggested that the risk owner may well need to seek Board or Senior Management level agreement that the organisation is operating in a

period of heightened threat, where there is a threat actor with intent and capability to target operational technology (to also help ensure budget and resources are made available). This requires understanding of the threat, which can come from the work of their own threat analysis resources, or from external sources, such as government statements. Delegation of responsibility for decision-making also has to have been agreed before the period of heightened threat occurs.

Relevant CAF IGPs:

A1.a Board Direction - “You have effective organisational security management led at board level and articulated clearly in corresponding policies.”

A1.b Roles and Responsibilities - “Your organisation has established roles and responsibilities for the security of network and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.”

A1.c Decision-making - “You have senior-level accountability for the security of network and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the operation of the essential function(s) are considered in the context of other organisational risks.”

1. Automated response to monitoring enabled.

Category: **Increase situational awareness -** *Increase and/or improve the information available to defenders*

Due to the impact that an automated response to alerts within an ICS/OT environment can have, for example shutting down a potentially compromised process, or automatically isolating a host, this type of capability when deployed, is normally disabled.

During a period of heightened threat, given the change in risk posture, a CNI operator may wish to revisit whether it is now acceptable to run operations with this functionality enabled.

As with all the interventions in this document, care should be taken to test the impact of any change ahead of making a change in response to heightened threat. Particularly in the case of automated response, care should be taken to consider the impact of automated action being taken in contexts such as safety critical processes. A risk-based decision should be taken as to their appropriateness, with consideration given to the potential impact to safe operations and wider compliance.

It should be noted that a sophisticated actor who understands how automated response is configured to respond within an environment, could seek to use this themselves to engineer an outcome with an impact to operations (e.g. an unwanted shut down, or isolation of operationally critical hosts and processes).

The ICS COI has published guidance on logging and monitoring within ICS/OT environments that can be found here. In addition the NCSC has published principle based guidance on logging for security purposes that can be found at:https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.

Relevant CAF IGPs:

- **C1.a Monitoring Coverage** - "The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s)".
- **C1.c Generating Alerts** - "Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts".

- **C1.d Identifying Security Incidents** - “You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response”.
- **C1.e Monitoring Tools and Skills** - “Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential function(s) they need to protect”.

2. Increased Monitoring/Auditing of ICS/OT Systems

Category: **Increase situational awareness -** *Increase and/or improve the information available to defenders*

While monitoring of ICS/OT systems is a normal practice, additional resources (both human and machine) can be utilised to increase monitoring of control systems and auditing of ICS/OT system activities, particularly around third-party activities on site and site SCADA activity, during a period of heightened threat.

The ICS COI has published guidance on logging and monitoring within ICS/OT environments that can be found here. In addition the NCSC has published principle based guidance on logging for security purposes that can be found at:https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.

Relevant CAF IGPs:

- **C1.a Monitoring Coverage** - “The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s)”.
- **C1.c Generating Alerts** - “Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts”.
- **C1.d Identifying Security Incidents** - “You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response”.
- **C1.e Monitoring Tools and Skills** - “Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to

use. Monitoring staff have knowledge of the essential function(s) they need to protect".

3. Threat Hunting Activities

Category: **Increase situational awareness -** *Increase and/or improve the information available to defenders*

Threat hunting activities are not consistently undertaken within Operators. Provision of specific information relating to the threat actors Tactics/Techniques/Processes that the heighted threat is attested to, along with support on how to hunt, along with the operators SOC function putting additional resources to the task, could be implemented during a period of heightened threat. In addition, threat hunting should also look at the latest trends being used by other threat actors.

NCSC has published principle based guidance on threat hunting that can be found at:https://www.ncsc.gov.uk/collection/building-a-security-operations-centre/detection/detection-approaches#section_4.

Relevant CAF IGPs:

- **C1.e Monitoring Tools and Skills** - "Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential function(s) they need to protect".

4. Enforced Segregation

Category: **Hardening -** *Prioritise typical resilience actions to reduce the attack surface area of devices, networks*

Where ICS/OT environments connect to IT environments there is the opportunity for malware to propagate via the IT environment, given its wider exposure to threat actors. (note ICS/OT systems are also often connected directly to the Internet to provide remote access or 3rd party connections without going via the IT environment).

During normal operations there can be elements of communications and data transfer between the IT environment and the ICS/OT environment, which are controlled via the likes of firewalls, unidirectional gateways and diodes. However, an additional level of security can be maintained by enforcing a physical airgap, pulling all physical connections/cables, or using hardware to mechanically isolate cables from ports, between the IT and ICS/OT environments. This has previously been undertaken by UK CNI operators in their response to an incident within their IT environment to protect their ICS/OT environment.

The best form of isolation, physical isolation, may not always be possible initially / quickly without additional labour resources depending on operational requirements between linked upstream or downstream sites. Physical isolation requires suitably skilled and authorised personnel to attend site to perform the isolation and then re attend to re-enable. Documented and detailed understanding of the control systems communication patterns is essential to aid this.

The business need for data/control and security need for a shared integrated view to enable security detection and response within an ICS/OT environment may present a natural conflict with the full airgap aspect.

There are other options to physically isolate to enforce segregation, most notably, logically, either by disabling the communications link or a network port, or by deploying a block-any-any firewall rule.

NCSC has published guidance on how to design, use, and maintain secure networks**,** that can be found here: https://www.ncsc.gov.uk/guidance/network-security-fundamentals, in addition to guidance on secure system administration that can be found here: https://www.ncsc.gov.uk/collection/secure-system-administration.

Relevant CAF IGPs:

- **B5.a Resilience Preparation** - "You are prepared to restore the operation of your essential function(s) following adverse impact."
- **B5.b Design for Resilience** -You design the network and information systems supporting your essential function(s) to be resilient to cyber security incidents. Systems are appropriately segregated, and resource limitations are mitigated."

5. Enforced Island Mode

Category: **Hardening -** *Prioritise typical resilience actions to reduce the attack surface area of devices, networks*

Within UK CNI ICS/OT environments there are a range of large to small sites, some remote from each other, and a range of ICS/OT systems within each site. Additional enforced segregations, creating Islands of ICS/OT Systems, either isolating sites within the ICS/OT environment (ideally physically pull cables from ports or using hardware to mechanically isolate cables from ports), or by segregating further between the Purdue layers, forcing control to be done locally at site versus at the higher Purdue layers.

All segregation activity should be fully tested, both to provide the assurance it works, but also to fully understand if and how it impacts normal operational procedures, and that the ICS/OT environment can be restored to its previous state.

Operators may also look at enforcing island mode by type of site, some being more at risk than others from a threat actor (for instance putting freshwater treatment works into island mode, but not sewage works).

Having knowledge of the threat actor, and their motive and intentions, would help understand the risks to various aspects to the various sites/systems within an Operators OT environment.

Virtual isolation (as a less harsh option, by turning off Virtual Private Network tunnels) may also be used to enforce Island mode with the benefit of being performed from a central point, this enables the isolation to be controlled centrally and re-enabled if required to aid site operational support. Virtual isolation may also not always be possible initially / quickly without additional labour resource depending on operational requirements between upstream or downstream sites.

In-depth knowledge of the operator's architecture and networking would be required to implement this intervention successfully.

Relevant CAF IGPs:

- **B5.a Resilience Preparation** - "You are prepared to restore the operation of your essential function(s) following adverse impact."
- **B5.b Design for Resilience** -You design the network and information systems supporting your essential function(s) to be resilient to cyber security incidents. Systems are appropriately segregated, and resource limitations are mitigated."

6. Turn off unrequired ICS/OT and IT

Category: **Hardening -** *Prioritise typical resilience actions to reduce the attack surface area of devices, networks*

Within any ICS/OT environment there will always be servers, control centre or site-based hosts, Human Machine Interfaces (HMI's) and panel PCs that remain switched on, connected to the network, when not required. These provide opportunities for threat actors to leverage them and the access/role that they provide. Ensuring unrequired ICS/OT and IT is powered down during a period of heightened threat can reduce the attack surface available to a threat actor.

Where the required infrastructure exists, it may be more viable to electronically isolate the network port to the device to prevent communication. This could be carried out by a central ICS/OT function but would require 24x7 support to re-enable if required as the response needed may be urgent and of a critical nature.

Relevant CAF IGPs:

- **B5.b Design for Resilience** – "You design the network and information systems supporting your essential function(s) to be resilient to cyber security incidents. Systems are appropriately segregated, and resource limitations are mitigated."

7. Advance plans for updates/patching

Category: **Hardening -** *Prioritise typical resilience actions to reduce the attack surface area of devices, networks*

The likes of software updates/patching and Anti-Virus updates within an operator's ICS/OT environment are scheduled for a suitable operational window in the future (maintenance period etc). In a time of heightened threat, reclassifying such updates/patching as safety-critical or operationally critical (depending on the plant type) would mean that they are implemented as soon as possible, versus possibly months or years in the future, thus improving the resilience of the ICS/OT environment, against threat actors.

NCSC has published guidance on Vulnerability Management that can be found at: https://www.ncsc.gov.uk/collection/vulnerability-management, in addition to keeping devices and software up to date that can be found at:https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date and patching for cross-domain solutions (such as IT to ICS/OT) that can be found at:https://www.ncsc.gov.uk/collection/cross-domain-solutions/using-the-principles/patching.

Relevant CAF IGPs:

- **B4.d. Vulnerability Management** - "You manage known vulnerabilities in your network and information systems to prevent adverse impact on the essential function(s)."

8. Restricted Remote Access

Category: **Change the environment -** *Step change to significantly limit the opportunities for actors to cause disruption, which may incur business cost*.

Compromising Remote Access is a common vector used by threat actors to gain access to ICS/OT environments and IT environments alike. Removing the ability to remotely access an ICS/OT Environment in a period of heightened threat level improves the cyber security of an ICS/OT environment. There is a plethora of staff from the likes of Vendors/OEMs, System Integrators and Operators' own staff that have the privilege of remote access into an operators ICS/OT environment.

Restricting remote access privileges to just operators own staff is one additional level of security that could be implemented, with further levels of security being implemented restricting all remote access to the ICS/OT environment. This response would also look to cover OEM remote access to an Operators' ICS/OT environment that the OEM owns and is not logically controlled by the operator but can be physically disconnected by them.

Knowledge/audit of all remote access accounts would be required to support this intervention.

Consideration would need to be given to any scenario where vendor support was required during a follow-on incident/compromise.

NCSC has published guidance on securing remote access to UK CNI operators here: https://www.ncsc.gov.uk/blog-post/cni-system-design-secure-remote-access in addition to the use of secure Privileged Access Workstations(PAW) that can be found here: https://www.ncsc.gov.uk/collection/principles-for-secure-paws and Privileged Access Management (PAM) that can be found here: https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management.

Relevant CAF IGPs:

- **B2.a Identity Verification, Authentication and Authorisation** - "You robustly verify, authenticate and authorise access to the network and information systems supporting your essential function(s)."
- **B2.b Device Management** - "You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential function(s)."

- **B2.c Privileged User Management** - "You closely manage privileged user access to network and information systems supporting the essential function(s)."
- **B2.d Identity and Access Management (IdAM)** - "You closely manage and maintain identity and access control for users, devices and systems accessing the network and information systems supporting the essential function(s)."

9. More Restrictive Firewall filtering

Category: **Change the environment -** *Step change to significantly limit the opportunities for actors to cause disruption, which may incur business cost*.

During normal operations there may be data flowing to and from the ICS/OT environment, which while it supports business activities, the business can survive for short periods of time without this data, with no major impact to its operations (processes can still run, but maybe not as efficiently for instance). This data can be identified beforehand, and specific firewall rules can be written to block this traffic and configured on the firewall appliance but not implemented. Then when the threat level is heightened, these additional firewall rules can be implemented. This could be done in two stages, inbound data only first and then both inbound and outbound data. Both Network and Host based firewalls can be included.

NCSC has published principle based guidance on the use of how to design, use, and maintain secure networks using firewalls that can be found at: https://www.ncsc.gov.uk/guidance/network-security-fundamentals. In addition NCSC has published principles for Cross Domain Solutions that can be found at: https://www.ncsc.gov.uk/collection/cross-domain-solutions.

Relevant CAF IGPs:

- **B4.a Secure by Design** -" You design security into the network and information systems that support the operation of the essential function(s). You minimise their attack surface and ensure that the operation of the essential function(s) should not be impacted by the exploitation of any single vulnerability".
- **B4.b Secure Configuration** - "You securely configure the network and information systems that support the operation of essential function(s)".

10. Restricted Data Transfer – removable media

Category: **Change the environment -** *Step change to significantly limit the opportunities for actors to cause disruption, which may incur business cost*.

During a period of heightened threat level, all use of removable media can be suspended to limit the attack surface. However, it must be noted that this control could also limit the ability to deploy viable security updates and patches within the ICS/OT environment. Additional physical checks on any removable media entering or leaving the ICS/OT environment could also be conducted (ideally this control should be default under normal operating conditions given the threat posed by removable media).

Where there is use of contractors, use of removable media could be restricted to the operator's staff only, who may be more vetted from a security perspective than contractors.

Given that the use of removable media is normally related to a privileged change occurring within an ICS/OT environment, then consideration for enforcing a two person do and check rule should be given.

The ICS COI has published guidance to manage the use of removable media that can be found here.

Relevant CAF IGPs:

- **B3.a Understanding Data** -You have a good understanding of data important to the operation of the essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to the operation of essential function(s).
- **B3.b Data in Transit** - You have protected the transit of data important to the operation of the essential function(s). This includes the transfer of data to third parties.
- **B3.c Stored Data** - You have protected stored soft and hard copy data important to the operation of the essential function(s).

11. Restricted use of third-party IT

Category: **Change the environment -** *Step change to significantly limit the opportunities for actors to cause disruption, which may incur business cost*.

During normal operations, build/configuration and maintenance periods it is common practice with UK CNI operators for third party IT to be connected to ICS/OT environments. While best practice is to only allow Operator controlled and enforced Privilege Access Workstations, there are various use cases where third party IT is connected within the ICS/OT environment. While controls to secure this usage may be in place (either contractually or via point in time laptop drive scanning stations), the assurance that they offer may not be as great as the operator managed PAW. Therefore, restricting their use during a heightened period of threat can reduce the attack surface available to a threat actor.

Consideration could be given to reducing the amount of project work and third-party activities being carried out during very high threat levels, although this would need to be assessed and controlled carefully.

NCSC has published guidance on the use of secure PAWs that can be found here: https://www.ncsc.gov.uk/collection/principles-for-secure-paws, in addition to guidance on Privileged Access Management (PAM) that can be found here: https://www.ncsc.gov.uk/collection/secure-system-administration/use-privileged-access-management.

Relevant CAF IGPs:

- **B2.a Identity Verification, Authentication and Authorisation** - "You robustly verify, authenticate and authorise access to the network and information systems supporting your essential function(s)."
- **B2.b Device Management** - "You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential function(s)."
- **B2.c Privileged User Management** - "You closely manage privileged user access to network and information systems supporting the essential function(s)."
- **B2.d Identity and Access Management (IdAM)** - "You closely manage and maintain identity and access control for users, devices and systems accessing the network and information systems supporting the essential function(s)."

12. Revoke Account Access to ICS/OT Environment

Category: **Change the environment -** *Step change to significantly limit the opportunities for actors to cause disruption, which may incur business cost*.

Operators may have "user access groups" that facilitate large numbers of staff/users being able to access the ICS/OT environment from the IT environment. These staff/users would be something that a threat actor could compromise, so given a heightened threat level, these "user access groups" could have their access to the ICS/OT environment revoked. A smaller "user access group" that only has key personnel (or break glass users), would remain implemented.

If a centralised ICS/OT IDAM solution is employed then it would require all users access groups to be disabled, with revert to break glass local accounts/users only implemented. (the term "break glass" refers to a method of bypassing security controls that normally guard a system or service, normally in an emergency situation).

Where there is use of contractors, account access could be restricted to the operator's staff only, who may be more vetted from a security perspective than contractors.

Knowledge/audit of all ICS/OT access accounts would be required to support this intervention.

NCSC has published guidance on Privileged Access Management that can be found here: https://www.ncsc.gov.uk/collection/secure-system-administration/use-privileged-access-management.

Relevant CAF IGPs:

- **B2.a Identity Verification, Authentication and Authorisation** - "You robustly verify, authenticate and authorise access to the network and information systems supporting your essential function(s)."
- **B2.c Privileged User Management** - "You closely manage privileged user access to network and information systems supporting the essential function(s)."
- **B2.d Identity and Access Management (IdAM)** - "You closely manage and maintain identity and access control for users, devices and systems accessing the network and information systems supporting the essential function(s)."

13. Implement Geo Fencing on remote access connections

Category: **Change the environment -** *Step change to significantly limit the opportunities for actors to cause disruption, which may incur business cost*.

Operators can implement Geo Fencing against the Internet Protocol (IP) number ranges that users connect from. This can be restricted to IP networks that staff are known to operator from (with prior research being undertaken, e.g. IP number allow listing), or by use of IP number geolocation sources, restricting access for instance to UK based IP number ranges.

This control has limited effectiveness, with known issues around if the threat actor's infrastructure is also based in the UK and are all users requiring remote access based in the UK (a likely issue for those with international OEM support or operators who are international companies).

Because of the limited effectiveness of this intervention, applying and gaining assurance from this control needs to be carefully considered.

NCSC has published guidance on securing remote access to UK CNI operators here: https://www.ncsc.gov.uk/blog-post/cni-system-design-secure-remote-access. While the NCSC doesn't specifically endorse or use geofencing for security, the technology can be used in conjunction with other security measures.

Relevant CAF IGPs:

- **B2.a Identity Verification, Authentication and Authorisation** - "You robustly verify, authenticate and authorise access to the network and information systems supporting your essential function(s)."
- **B2.c Privileged User Management** - "You closely manage privileged user access to network and information systems supporting the essential function(s)."
- **B2.d Identity and Access Management (IdAM)** - "You closely manage and maintain identity and access control for users, devices and systems accessing the network and information systems supporting the essential function(s)."

14. Implement full Multi-Factor Authentication on Physical Access Controls

Category: **Change the environment -** *Step change to significantly limit the opportunities for actors to cause disruption, which may incur business cost*.

It is common within ICS/OT environments to secure access to rooms/cabinets with Multifactor Authentication (MFA) physical access controls, however, often while they are deployed, the full multi-factor element is not enabled (e.g. swipe card access but no pin usage). These physical access controls are in place to mitigation risks due to poor IDAM controls on equipment within the room. During a period of heightened threat all elements of MFA physical access controls should be enabled.

NCSC has published principles based guidance on identity and access management that can be found at:https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management.

Relevant CAF IGPs:

- **B2.a Identity Verification, Authentication and Authorisation** - "You robustly verify, authenticate and authorise access to the network and information systems supporting your essential function(s)."
- **B2.d Identity and Access Management (IdAM)** - "You closely manage and maintain identity and access control for users, devices and systems accessing the network and information systems supporting the essential function(s)."

15. Workforce Communication

Category: **Weathering the storm -** *Adapt ways of working to be more tolerant of disruption and prepare to adapt further in crisis scenarios*

In addition to Security Operations Centre (SOC) staff, brief the plant operations, maintenance and engineering personnel that there is an increased potential for malicious communications via the likes of voice, email, network intrusion, postal distribution of portable media with the intention of disrupting operations. Reinforce phishing training, reinforce the need to report any suspicious communications by whatever means or via whichever media form. Having standardised forms of wording available for specific threat levels should be considered.

Workforce Communication will need to be approved by the board/senior management, and thought should be applied to the type and level of technical depth of the communication, depending on the audience.

NCSC has published guidance on creating a positive cyber security culture on a workforce that can be found at: https://www.ncsc.gov.uk/collection/board-toolkit/developing-a-positive-cyber-security-culture.

Relevant CAF IGPs:

- **B6.a Cyber Security Culture** - "You develop and maintain a positive cyber security culture."
- **B6.b Cyber Security Training** - "The people who support the operation of your essential function(s) are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed."

16. Invoke a change freeze

Category: **Weathering the storm -** *Adapt ways of working to be more tolerant of disruption and prepare to adapt further in crisis scenarios*

Given the period when changes within an ICS/OT environment are being made might provide an access vector for a threat actor, especially if the changes being implemented are complicated, require remote access and take a long period of time to implement, then a change freeze is one option that an operator can take in a period of heightened threat.

In addition, if the changes are complicated, they may have an impact on the ability of the ICS/OT cyber security fabric to understand and monitor the environment effectively in the short term (any changes may be unintentionally seen and triaged as potentially malicious). Thus, having a change freeze helps the operator to understand exactly what their ICS/OT environment currently looks like. How long this freeze is maintained will need to be given careful thought, especially if any needed changes enhance the cyber security resilience of the environment.

17. Implement Immediate Back Up

Category: **Weathering the storm -** *Adapt ways of working to be more tolerant of disruption and prepare to adapt further in crisis scenarios*

Due to the way ICS/OT environments sometimes operate, the operator may not hold a current back up of key nodes. During a period of heightened threat, the operator should ensure it has current back-ups of all key nodes, and if not held, implement the back-up process immediately. All back-ups should then be stored offline/isolated. Isolation of all software and documentation repositories that would be needed to recover ICS/OT systems should also be undertaken.

NCSC has published principles based guidance on making on-premises and cloud backups resistant to the effects of destructive ransomware that can be found at: https://www.ncsc.gov.uk/collection/ransomware-resistant-backups/principles-for-ransomware-resistant-cloud-backups.

Relevant CAF IGPs:

- **B5.a Resilience Preparation** - "You are prepared to restore the operation of your essential function(s) following adverse impact".
- **B5.c Backups** - "You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s)".

18. Review of ICS/OT Incident Response Plan

Category: **Weathering the storm -** *Adapt ways of working to be more tolerant of disruption and prepare to adapt further in crisis scenarios*

While some operators do regularly review and exercise their ICS/OT Incident Response Plan (IRP), not all will have done so within the last 6 months. Reviewing the ICS/OT IRP by all stakeholders should be done as quickly as possible during a period of heightened threat.

The ICS COI has published guidance to support the development of ICS/OT focused IRPs that can be found at: https://ritics.org/ics-coi/#downloads. In addition NCSC has published principles based guidance on developing an IRP that can be found at: https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes.

Relevant CAF IGPs:

- **D1.a Response Plan** - "You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function(s) and covers a range of incident scenarios".
- **D1.b Response and Recovery Capability** - "You have the capability to enact your incident response plan, including effective limitation of impact on the operation of your essential function(s). During an incident, you have access to timely information on which to base your response decisions".

CAF IGP Summary

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

- **A1.a Board Direction** - "You have effective organisational security management led at board level and articulated clearly in corresponding policies."
- **A1.b Roles and Responsibilities** - "Your organisation has established roles and responsibilities for the security of network and information systems at all levels, with clear and well-understood channels for communicating and escalating risks."
- **A1.c Decision-making** - "You have senior-level accountability for the security of network and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the operation of the essential function(s) are considered in the context of other organisational risks."
- **B2.a Identity Verification, Authentication and Authorisation** - "You robustly verify, authenticate and authorise access to the network and information systems supporting your essential function(s)."
- **B2.b Device Management** - "You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential function(s)."
- **B2.c Privileged User Management** - "You closely manage privileged user access to network and information systems supporting the essential function(s)."
- **B2.d Identity and Access Management (IdAM)** - "You closely manage and maintain identity and access control for users, devices and systems accessing the network and information systems supporting the essential function(s)."
- **B3.a Understanding Data** -You have a good understanding of data important to the operation of the essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to the operation of essential function(s).
- **B3.b Data in Transit** - You have protected the transit of data important to the operation of the essential function(s). This includes the transfer of data to third parties.
- **B3.c Stored Data** - You have protected stored soft and hard copy data important to the operation of the essential function(s).
- **B4.a Secure by Design** -" You design security into the network and information systems that support the operation of the essential function(s). You minimise their

attack surface and ensure that the operation of the essential function(s) should not be impacted by the exploitation of any single vulnerability".

- **B4.b Secure Configuration** - "You securely configure the network and information systems that support the operation of essential function(s)".
- **B4.d. Vulnerability Management** - "You manage known vulnerabilities in your network and information systems to prevent adverse impact on the essential function(s)."
- **B5.a Resilience Preparation** - "You are prepared to restore the operation of your essential function(s) following adverse impact".
- **B5.b Design for Resilience** -You design the network and information systems supporting your essential function(s) to be resilient to cyber security incidents. Systems are appropriately segregated, and resource limitations are mitigated."
- **B5.c Backups** - "You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s)".
- **B6.a Cyber Security Culture** - "You develop and maintain a positive cyber security culture."
- **B6.b Cyber Security Training** - "The people who support the operation of your essential function(s) are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed."
- **C1.a Monitoring Coverage** - "The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s)".
- **C1.c Generating Alerts** - "Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts".
- **C1.d Identifying Security Incidents** - "You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response".
- **C1.e Monitoring Tools and Skills** - "Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential function(s) they need to protect".
- **D1.a Response Plan** - You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function and covers a range of incident scenarios.
- **D1.b Response and Recovery Capability** - You have the capability to enact your incident response plan, including effective limitation of impact

on the operation of your essential function. During an incident, you have access to timely information on which to base your response decisions.

- **C1.a Monitoring Coverage** - “The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s)”.
- **C1.c Generating Alerts** - “Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts”.
- **C1.d Identifying Security Incidents** - “You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response”.
- **C1.e Monitoring Tools and Skills** - “Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential function(s) they need to protect”.

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 Interconnected 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.