National Cyber Security Centre
a part of GCHQ

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

CISA CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

Federal Office for Information Security

National Cyber Security Centre
Ministry of Justice and Security

National Cyber Security Centre
NEW ZEALAND

Creating and maintaining a definitive view of your Operational Technology (OT) Architecture

How organisations who deploy or operate OT systems should build, maintain and store their systems understanding.

This guidance defines a principles-based approach for how operational technology (OT) organisations should build, maintain and store their systems understanding. It is aimed at cyber security professionals working in organisations that deploy or operate OT across greenfield and brownfield deployments. Integrators and device manufactures can also use these principles to ensure their solutions enable effective asset and configuration management.

Table of Contents

This guidance has been developed with contributions from partnering agencies and is part of a series of publications aiming to draw attention to the importance of cyber security in Operational Technology.

It is produced by the UK National Cyber Security Centre (NCSC) in partnership with the Australian Signals Directorate Australian Cyber Security Centre (ASD's ACSC), the Canadian Centre for Cyber Security (Cyber Centre), US Cybersecurity and Infrastructure Security Agency (CISA), the US Federal Bureau of Investigation (FBI), Germany's Federal Office for Information Security (BSI), Netherlands National Cyber Security Centre (NCSC-NL), and New Zealand's National Cyber Security Centre (NCSC-NZ).

Introduction

OT systems are a prime target due to their criticality and the potential impact if these systems are disrupted. As the number and capability of threat actor targeting OT increases, so too does the need for robust cyber security controls. However, the complexity, scale, and long-standing nature of OT systems often means organisations can lack a holistic view of their environment, which undermines their ability to implement effective cyber security measures.

Traditionally, OT networks were isolated (or 'air-gapped') from the internet and external systems. However, modern operational demands have led to increased connectivity as networks now integrate with enterprise systems, third-party vendors and cloud services. This makes designing appropriate security controls increasingly critical, to reduce the risks to previously isolated systems.

To design appropriate and effective controls a holistic system understanding is required. In this guidance, the term **definitive record** is used to describe a continually updated, accurate and up-to-date view of the system. A definitive record is an evolving collection of information that will change over time, with all system changes recorded to maintain its accuracy and authority.

Establishing a definitive record of your organisation's OT will allow you to effectively assess risks and implement the proportionate security controls. Rather than focusing solely on individual assets, a holistic approach enables you to consider the broader context which leads to a better assessment of the criticality and potential impacts of compromises.

Note: The process of establishing a definitive record should be collaborative, with both OT and IT teams involved. Use the NCSC cyber security culture principles to support this approach.

Key priorities

Your organisation should aim to create a definitive record of **all** OT systems that it owns and operates. Since this task can be complex and time-consuming, you should prioritise systems based on:

1. The impact of the system to either your business function or the potential of national impact.
2. Third party connections, particularly where these connections can change the configuration of system components (or have direct control over the process).
3. The overall exposure of the system, taking into account how many connections the system has to external services where your organisation does not set the configuration of security controls.

Principles-based guidance

This guidance outlines the principles that organisations should aim to achieve when documenting their OT. They are intended as goals rather than minimum requirements.

Cyber security professionals should use these principles as a framework to develop a comprehensive record of their systems. This will require time and may present complexities, particularly in brownfield deployments. However, much of the information necessary to establish a definitive record is likely already available within your organisations. This information may be found in configuration files, existing documentation, or through monitoring and security tools. Identifying these existing resources is crucial for minimising the burden of ongoing maintenance of the record.

Integrators and device manufactures are encouraged to make these principles easier for organisations to achieve, through freely providing comprehensive documentation for supplied systems and offering tools that enable effective asset and configuration management. It is especially important that this documentation is available for 'turn-key' solutions, allowing operators to understand the design and implement appropriate security controls throughout the system's lifecycle.

Terminology

A few quick points on terminology before we start.

Asset Any physical or virtual component within your OT system such as field devices, digital sensors, digital actuators, networking equipment, protocol gateways and computer platforms. Assets do not only include physical components but also digital services and software.

Asset inventory An organised, regularly updated list of an organisation's systems, hardware, and software. The inventory includes fields that describe the asset attributes such as manufacturer, model, and supporting communications protocols.

Architecture A holistic design that not only encompasses the components of a system (including technology, security controls, people and process), but how these elements integrate into larger business functions and objectives. The architecture is not just about technology; it is about how *people* and *processes* interact with it.

Brownfield An existing OT environment that is already deployed and operational. Brownfield environments present unique challenges when integrating new technologies, requiring careful planning to retrofit, secure, and modernise without disrupting critical operations.

Definitive record A definitive record describes a continually updated**,** accurate and up-to-date view of the system (or element of a system). The definitive record will change over time with all system changes recorded to maintain its accuracy and authority.

External connectivity Any connection that leaves the OT network boundary, including connections to any third parties, vendors and/or enterprise systems.

Internal connectivity Any communications with assets within your organisation OT system. This includes all LAN and WAN components.

Information In this guidance, information can refer to raw data (sensor values or industrial protocols), documents (reports or diagrams), configurations (settings or policies), records (logs or audit trails) and procedural/process data (workflows or operating plans).

Principle 1: Define processes for establishing and maintaining the definitive record

To create a definitive record of your organisation's OT systems, you should first determine how your organisation will gather, validate and maintain this information. Establishing a robust change management process is crucial to ensure the ongoing accuracy and **r**elevance of this record over time. Your process should answer the following 3 questions:

1. How will information be collected?

Once you've established the OT systems that you need to collect information on, you need to identify what sources you can use. When selecting information sources for the definitive record you should also consider any identified information gaps within the organisation.

Information sources could include, but are not limited to:

Asset Inventory
An OT asset inventory should list OT systems, hardware, and software with their attributes, including supported communications protocols.

Existing designs and documents
OT systems undergo extensive design work before they are commissioned to ensure they function as intended. Use any existing design, process or safety documentation as an initial step towards creating a definitive OT system architecture record.

Your staff
Many OT systems have evolved in line with business needs. If a change management process has not been implemented, it is likely this information is still known by your organisation's experts. Work with system owners to identify what knowledge is already documented, and how current it is.

Passive monitoring
Use passive monitoring tools to help build your OT architecture record. These tools can also aid in spotting undocumented changes to the OT system. If you find differences between your documented designs and monitoring results, you must validate if the changes were planned and where this is the case, document the changes.

Configuration information

Use configuration information stored on support and management components in the environment. This could include project files and related configurations for assets like programmable logic controllers and remote terminal units. This should also include the configuration of network devices within the OT environment.

SBOM and HBOM

A Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM) can be requested from your manufactures. These can provide visibility into underlying components and help identify potentially vulnerable components. Prior to purchase, an organisation can use the SBOM/HBOM as part of their product risk assessment. The US Cybersecurity and Infrastructure Security Agency (CISA) has published a HBOM framework as well as a number of resources on SBOMs. This NCSC blog will also help you to understand where SBOMs can add value in your organisation as well as their limitations.

Point-in-time active scanning

Conducting a point-in-time active scanning assessment can help you identify additional assets and their configurations within your environment. Before you conduct any actives scanning in OT environments, you should be aware that this process has the potential to overwhelm legacy devices that may have limited processing power, leading to performance degradation, freezing or crashing. Thoroughly consider and test for these implications before implementation.

Note: If your organisation decides to use active scanning, ensure that it employs native ICS/OT protocols and tools, and that the scanning methods have been tested and validated by the original equipment manufacturer (OEM) of each asset.

Where your OT system is monitored, it is crucial to inform your Security Operations Centre about your active scanning plans, including the date, time, and scope of the activity. This will help prevent any malicious active scanning from being overlooked after data collection. Planned maintenance windows can further ensure that this assessment does not impact your operations.

Summary: Your organisation should have a documented systematic approach to collect OT systems information. You should understand the sources of information available to you for the definitive record and how you can use this data. You should look to gather information from a range of sources, including from people, documentation, scanning and configurations.

2. How will information be validated?

Your process should also define how you validate any information you have collected. This is a critical step in ensuring you are building an up-to-date and definitive view of your OT system architecture. You will likely need to look at a several factors, including:

- **Completeness** How complete is the information? Does it capture all the details, or is it a draft document that will need additional information?
- **Accuracy** Does the documentation match your engineers' understanding of the system? Ensure that subject matter experts verify accuracy.
- **Consistency** Does the information confirm findings contained in other sources or are there conflicts? Any conflicts should be investigated to get to a consistent understanding of the current state of the system.
- **Timelines** When was the document produced? Combining this information with known business maintenance/planning windows can help you assess the likelihood that the documentation is representative of the current system state.

Validation is especially important in brownfield environments, where systems often change from their original designs.

Summary: Your organisation should have a documented approach to validate OT systems architecture records. Implementing a strong validation framework will enable you to establish an accurate and complete architectural overview. The process should ensure that you can create a single source of truth that shows the “as is” state of the OT architecture.

3. How will the definitive record be maintained?

Once a definitive record of the OT architecture has been established, it is critical to maintain the integrity and accuracy of this record. Change management processes and controls are vital for achieving this.

An effective change management process ensures systematic review, approval, and documentation of modifications, minimising the risk of errors. This process should define roles and responsibilities of key stakeholders, focusing on their potential impact on both operational efficiency and cyber security. Additionally, implement version control mechanisms to create a clear audit trail of all changes, enabling easy tracking of design evolution over time.

Regular training sessions should be conducted to ensure that personnel involved in design and documentation understand the protocols and their significance.

Summary: Your organisation should have an established change management process to govern your definitive OT record. The change management process should establish clearly documented personnel roles, version control, and ongoing training to ensure the integrity and accuracy of the record is maintained over time.

Principle 2: Establish an OT information security management programme

The definitive record will be a collection of documents that consolidates a wide range of information about your organisation and OT environment. This makes it a high-value target for an attacker. As you build your definitive record, it is important to consider how it will be secured and your broader approach to OT information security management.

Skilled threat actors will seek to gain insight into a target system to support their capability development and attack planning. The easier it is for an attacker to build an understanding of your OT system, the more likely an attack will be successful. Since physical assets in an OT environment are operational for long periods, any exposed information is likely to remain relevant for longer (when compared to planning attacks on conventional IT systems).

Your organisation could use standards such as ISO/IEC 27001 to aid in the implementation of an OT information security management system. At a minimum, your OT information security management programme should enable you to answer the following 3 questions:

1. What is in scope of the OT information security management programme?

You should understand and create a record of all the information your organisation holds or shares relating to your OT systems. This could be as a standalone inventory or as part of the wider definitive record. Your organisation should record the purpose of the information, any relevant data flow diagrams as well as any key properties such as access permissions, retention and data format.

Standard information types (such as documents) may be stored in a data repository that already produces a record of all or many of these attributes. For less standard information types (such as data generated from OT devices), this may need to be manually produced.

This guidance identifies five key groups of OT information:

Design information
Focuses on providing a clear view of how a system is structured and arranged, and defines the architecture, specifications and/or configuration of an OT system. Examples include network diagrams, asset inventories, configuration files and technical system diagrams. Design information also includes details specific to individual sites such as locations of physical assets.

Business information
Focuses on how the OT system functions in the context of business objectives and relationships with stakeholders. This includes (but is not limited to) data on service areas, customer or user locations and supplier contracts.

Identity and authorisation data
Encompasses information that is essential for the authentication and authorisation of users and systems within the OT environment. Identity and authorisation data includes user credentials, details of personnel, encryption keys, access control lists and access logs.

Operational data
Refers to the information involved in the real-time control of an OT system. This includes the unrefined data from OT devices/software. Examples include sensor readings, system logs and alerts. Operational data also captures analytical output generated from unrefined data such as predicted reporting of component and/or system performance.

Cyber and safety risk assessments
Contains information on weaknesses in the system design, its components and the potential consequences of risks if they were to occur. Examples would include HAZOP assessments or results of penetration testing.

Tip: IEC 62443-2-1:2024 offers advice on the protection of data related to industrial automation and control systems, as well as examples of the types of information/data that are within scope.

Summary: You should have a comprehensive and structured record of all the information your organisation holds or shares relating to your OT systems. This record should clearly identify each information/data component's purpose and relevant properties. This record will support informed decision-making as you build and deploy an effective OT information security management programme.

2. What is the value of the OT information to an attacker?

An attacker targeting an OT environment typically aims to disrupt, damage and/or destroy industrial systems and processes. They may also target OT systems to gain an economic advantage by stealing intellectual property or datasets that would enable competitors to improve their own processes. To achieve these aims, threat actors require information on how your system is architected, secured and operates.

There are three primary ways that threat actors can use OT information to finesse their cyber attacks:

Inform

Data can help a threat actor understand the broader context of their target system. This could include network architecture, access opportunities, and process dynamics for the underlying operational system. Threat actors may seek information on dependent systems that rely on, or contribute to, the correct operation of the target system.

Target

System information can be used to begin targeting components within your environment with the aim of achieving a specific outcome. This will likely focus on developing capabilities to enable an attacker to enter and move within a network. This may involve identifying systems running outdated or vulnerable software. It could also include identifying possibilities for physical sabotage.

Exploit

Data can be used to cause an effect within the target system. Examples would include set-point limits and privileged access credentials. Deep knowledge of how the system works can also allow attacks that target 'difficult to replace' or long-lead items, with the intention of extending the duration of any disruption.

A good approach is to consider the information an attacker would require within your threat modelling. After identifying the relevant information for each threat scenario, you can then analyse how an attacker might exploit that information and assess how critical its compromise is to their overall success. This helps you to determine the value of the information to an attacker, and to tailor your protections accordingly.

A data aggregation risk arises when threat actors have access to a collection of information that, when combined, can lead to development of capabilities that would not be possible using the individual pieces alone (this is described as latent intelligence). You should understand how information could be combined by a threat actor to chain together attack paths. Managing data aggregation risks requires an understanding of what information is already available, and what may become available as a consequence of future data sharing arrangements.

Summary: You will be able to identify the OT information that supports different threat scenarios, understand the ways threat actors seek to exploit this information and recognise how aggregating OT information increases this risk. This knowledge allows you to focus security measures where they are most needed.

3. How do you secure your OT information?

All information your organisation holds or shares relating to OT systems should be secured using appropriate and proportional controls. Your organisation should have clearly documented policies and procedures on how each type of information should be secured.

When protecting information it is important to consider all the components of the CIA triad:

Confidentiality

Confidentiality controls focus on ensuring that information is only accessible to systems and users that are authorised to have access. Core elements of confidentiality management comprise:

- **Storage** Where to store information should balance ease-of-access against the ability to apply effective security measures to minimise exposure. If your OT environments lack the ability to implement adequate controls, it may be appropriate to store information in IT systems where they support modern security controls. Where this is implemented in the IT environment, additional management and oversight of export risks should be put in place.
- **Access** should follow the principle of least privilege, meaning only users who need the information to perform their role are granted access. For high-value information, stronger authentication methods such as multi-factor authentication should be employed.
- **Sharing** It's important to assess risks before sharing information about an OT system. One example of a set of handling rules is the Traffic Light Protocol (TLP) designation, which provides a standardised framework to ease the secure sharing of information. When third parties are involved, confidentiality must be protected through carefully defined and contractually enforced agreements.

Integrity

Integrity means proving that information is complete, intact, and trusted and has not been modified or destroyed in an unauthorised or accidental manner. Validating integrity is essential for all types of information in the OT environment. For example, if designs stored at rest lose integrity, a maintenance engineer might misconfigure equipment. Similarly, unauthorised modification of operational data in transit could cause a programmable logic controller to operate incorrectly.

Integrity controls can be broadly divided into two categories, those that focus on maintaining integrity and those aimed at validating it:

- **Maintain** The usability of OT information depends on maintaining its integrity which involves regulating how information is created, updated, deleted, or changed, alongside monitoring these processes to detect anomalies. This includes restricting write permissions to authorised users, and enforcing version control to provide a complete audit trail and enable rollback of changes if needed.
- **Validate** Validation controls aim to verify that information has not been tampered with or corrupted. Cryptographic methods, such as digital signatures, serve as validation tools to ensure authenticity and integrity.

Availability

Availability controls focus on ensuring that organisations appropriately protect information and systems from outages, delays, and service degradation, ensuring they remain accessible to authorised users whenever needed. This includes building resilience through redundancy, backup and disaster recovery capabilities, as well as monitoring system health to detect and respond quickly to issues. The availability of information in OT is critical when looking to recover systems in the event of an incident. When deciding where this data is stored, you should consider how it would be accessed in different incidents. It is critical that backups are implemented to be ransomware resistant to protect their availability.

Summary: You should have a clear and documented understanding of the security controls applied to all information your organisation holds or shares relating to OT systems. These controls should be aligned with the value of OT information and target appropriate security attributes.

Principle 3: Identify and categorise assets to support informed risk-based decisions

Your organisation should understand the role of each of the components within your OT system. This is critical to enable you to create appropriate and proportionate security controls within your environment.

Tip: This guidance focuses on the broader process required to define your system architecture. There is additional international guidance on delivering an asset discovery programme which can be referred to, including:

- Security for industrial automation and control systems (IEC 62443-2-1)
- The Industrial Control System Community of Interest Asset Management guidance
- Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators | CISA.

For each asset you should be able to define three factors; criticality, exposure and availability.

Criticality

Criticality describes how important the functioning of the asset is to the wider OT system, in terms of its impact on:

- **Business** Would a failure cause the process to stop or result in a lower yield?
- **Safety** Would a failure cause harm or damage to people, equipment, and/or the environment?
- **Security** Would a failure result in the system being exposed to an unacceptable level of risk?

To gain a complete understanding of an asset's criticality, it should be examined in the context of the wider system. This will require combining the criticality of the asset with information about your wider system connectivity.

Exposure

Exposure refers to the discoverability and accessibility of networked devices within an organisation, which could make them vulnerable to potential threats. This should account for what defence in depth controls might add to its security. Exposure should consider several factors including:

- the time of exposure (for example is it accessible 24/7 or only accessible when required?)
- the type of connectivity being used (for example direct connections to the public internet are inherently more exposed than private fibre links)
- communications flow (for example does the system accept inbound connections?)
- proximity to external networks such as the internet or remote access points
- physical accessibility (are there opportunities for unauthorised physical interaction, such as plugging in devices or physical presence near the system)

Availability

Availability refers to the timely, reliable access to data and information services for authorised users. OT availability should include what business or operational functions would be lost in the event of that single asset being unavailable.

Where systems are highly critical, they are likely to be deployed for high-availability with redundancy built in and automated failover systems. This wider system availability may lower the availability requirements of some individual assets, making them easier to update and maintain.

Information to record on availability could include but is not limited to:

- timescales for known downtime, such as repeat scheduled maintenance windows
- high-availability deployments, including its architecture and the identification of the paired high-availability device or service and/or automated failover systems
- ability for the system asset to support rolling deployments, where updates can be provisioned with zero downtime

Tip: Vendors should provide categorisations of their updates so users can understand how the update will impact the asset's functionality. This should also include clear guidance on how quickly the update should be applied, in line with NCSCs Vulnerability management guidance best practice timelines.

Key categorisations may include ‘update’ (where a bug or unintended behaviour is being removed), ‘security’ (where a vulnerability is being remediated) or ‘feature updates’ (where new functionality is being added). The vendor should also highlight if the

vulnerability is being actively exploited, and ensure it is added to the CISA Known Exploited Vulnerability List.

For 'security' updates, vendors should publish a security advisory that is automatically retrievable according to the Common Security Advisory Framework (CSAF) and includes links to one or more complete and accurate CVE records. The NCSCs Vulnerability management guidance should be referred to for further advice.

Criticality, **exposure** and **availability** factors should be recorded as part of the definitive record to enable your organisation to take effective risk based decisions when considering new or revised security controls. For example, consider three common assets in an OT environment: a safety controller, a firewall and a regional supervisory control and data acquisition (SCADA) platform.

1. The safety controller is crucial for system safety, so it is typically designed to have minimal network connectivity with other assets. It also needs to be highly-available to ensure the process is protected during operations.
2. In contrast, a firewall for external connectivity is located at the edge of the network and provides important functions like secure remote access. While this is useful, it is less critical to day-to-day operations; however, it also more exposed to potential threats. Where this external data flow is essential to the process, this will likely be deployed as a high-availability pair.
3. A regional SCADA platform deployed on a virtualisation platform needs connectivity to all your OT systems and is likely critical to the business. It is also likely more exposed to external services than most of your OT assets, potentially exporting data to business systems. Where this is critical, it is also likely to be deployed as a high-availability pair.

When looking at updating in this scenario, you might choose to prioritise updates or maintenance of the firewall due to its exposure to threats, despite the fact it is less critical to the OT system. The fact that it is in a high-availability pair may allow you to update one asset at a time to prevent any impacts on operations. For similar reasons you may be able to routinely maintain your SCADA platform where you can fail over to the warm standby system during the maintenance process.

Your organisation should use a comprehensive risk management framework to inform these decisions, such as the NCSC's risk management framework (which aligns with international standards such as ISO 27001 and includes vital techniques such as threat modelling and attack trees). Note that IEC 62443-3-2 provides some additional advice specific to industrial automation and control systems.

Summary: You should have each asset systematically assessed and categorised by its criticality (business, safety, security), exposure within the OT system architecture and any availability constraints. The documented factors, recorded in a definitive record should be used to support risk-based decision-making. Enabling informed decisions regarding security controls, maintenance and updating.

Principle 4: Identify and document connectivity within your OT system

Most modern OT systems no longer operate in air-gapped environments by default. Instead, they require external connectivity to support business functions, streamline maintenance activities, and enable enhanced security controls. It's the connectivity and interactions between assets within a system that allow it to work to perform the intended function. Understanding how these assets work together within the wider system is essential for building effective and proportionate security controls..

When designing connectivity, reducing your organisation's vulnerability to potential attacks is paramount. For instance, the use of wireless communication technologies can elevate risks, as threat actors may not need to be physically present to exploit the system.

An effective understanding of the communications each of your assets require is critical to being able to design and articulate your networks zones and conduits as described in IEC 62443-3-2. Having this documented will enable your organisation to implement effective network controls such as network segmentation.

At a minimum, you should be able to answer the following 5 questions for each asset in your architecture:

1. What does the asset need to communicate with to perform its function?

You should maintain a clear record of the connections each asset has with other systems, devices, or services. This should clearly demonstrate which assets it depends on to function, and those assets that depend on it. This could include connections such as centralised control systems or remote database access.

As well as technical details, documentation on connectivity for all new and existing asset connectivity should include:

- a business case, detailing the connectivity requirement, which is centrally recorded and approved

- a reference to the how the record is maintained in line with existing change management policies
- a process for periodic reviews to confirm the necessity of each connection against associated risks to the OT network and evolving threats

Additional risk assessments should be performed for external connections to assess if connectivity is required, as well as the security controls implemented.

When evaluating the requirement for a new external connection, you should consider the following:

- **Avoid duplication**: Instead of designing unique routes for each data flow, consider implementing a unified and secure data export pattern. Minimising duplicate data routes reduces management overhead and lowers the risk of misconfigurations in security controls.
- **Establish control**: Ensure that any data exiting the OT network is sanitised (removing sensitive material) and authorised (deemed suitable to be stored outside the environment). There should be safeguards in place to stop connectivity if required.
- **Data security**: Implemented connectivity should ensure that data leaving the OT network is encrypted both in transit and at rest. Particular attention should be applied to who requires access to the data, and the ongoing management of encryption keys. These controls should be designed in line with your information security management programme.

Data flow diagrams (DFDs) should be used to effectively record information about connectivity. Establishing a 'single source of truth' will reduce ongoing overheads and enable effective risk management.

Summary: You should have a maintained record of all necessary connections each asset has with other systems, devices, or services. This record should justify the need for each connection and document wider system or third party dependencies. Techniques such as DFDs are used to capture this information.

2. What communication protocols are required, and how are they secured?

A centralised record should be maintained which details the specific communication protocols (for example Modbus, DNP3, OPC UA) and the corresponding TCP/UDP ports required by each asset. This documentation is critical for configuring network equipment, such as firewalls, to enforce strict ingress and egress filtering.

Regular audits of these protocols should be conducted to ensure they adhere to current security standards. Where legacy or insecure protocols are in use (especially on external connections) organisations should seek to replace them with secure alternatives. If this is not feasible, compensating controls such as encapsulating traffic in additional protections (such as a VPN) should be implemented.

Protocol audits should also focus on ensuring the OT protocol incorporates all three pillars of the CIA triad. While **availability** is often prioritised in OT environments to maintain continuous system operation, a secure and resilient OT system requires a balanced approach that also safeguards data **integrity** and **confidentiality**.

- **Confidentiality** ensures that sensitive data within the OT system is protected from unauthorised access. This is especially critical for systems connected to external networks, where exposure to threats is higher. Protocol audits should evaluate how well the communication protocols safeguard data from eavesdropping or unauthorized disclosure.
- **Integrity** encompasses both the authenticity and accuracy of data. It ensures that the information such as sensor readings, control commands, or system configurations remains consistent and unaltered during transmission. Integrity also verifies that the data originates from a legitimate source, preventing unauthorised entities from issuing commands or manipulating system behaviour.

Implementing a balanced approach to the CIA triad in OT protocols helps block common attack vectors such as machine in the middle (MitM) attacks, packet replay, and the malicious use of legitimate commands

Key areas to document and audit are as follows:

- the use of cryptographic protections, such as digital signatures or secure authenticated protocols, including any key management or supporting infrastructure

- the use of compensating controls on communications, including how these are managed and maintained
- legacy protocol use, including reasons why they cannot be migrated to more modern protocols (and any plans to upgrade the asset out of service)
- how segmentation, additional monitoring or other complementing controls can manage this risk when protocol-layer security may not be feasible (such as in low-latency safety systems)
- the logging and monitoring of OT protocols within the system, including the protocols communications structure and flows
- normal traffic patterns (such as consistent packet sizes or used commands) as this understanding aids in identifying potential malicious activity on the network; variations in expected traffic could indicate issues or threats

Summary: For each asset you should have documented in use protocols, along with their corresponding TCP/UDP ports. This documentation should be used for configuring ingress and egress filters on firewalls. Additionally, a thorough audit of these protocols should have been conducted to ensure compliance with security standards, incorporating necessary encryption and integrity mechanisms.

3. What architectural security controls are currently implemented in the OT system?

Architectural security controls refer to any control that is implemented at a network layer level. As part of your definitive OT architecture record, you should document existing controls, which could include:

Network flow controls

This ensures that data only flows one way through the channel. Flow control does not stop a vulnerability being exploited within the destination system, but it can make it difficult for an attacker to perform command and control, export data, or simply learn more from the sensitive services being protected. A more capable attacker may look to use alternative export paths to exfiltrate data. Consider how resilient the control is. For example, it might rely on protocols like UDP, which need network enforcement. Alternatively, it could use fixed hardware such as a data diode, which is more resistant to change.

Continuous network monitoring and alerting

Maintaining persistent visibility enables you to detect anomalies, identify potential threats, and respond to incidents before they escalate. This should include monitoring the performance of critical systems and the application of security policies to ensure compliance with your organisation's standards. Monitoring should include rules based on an analysis of how your specific system could be attacked, and what would enable you to detect the attack.

Access control and centralised identity

Implementing centralised identity management enables you to enforce use of authenticated protocols so only permitted personnel have access to sensitive systems. This includes using multi-factor authentication, role-based access control (RBAC), and regular access reviews to reduce the risk of unauthorised access or insider threats. Proper access control measures not only protect critical assets but also aid in tracking user activities for compliance and auditing purposes.

Network segmentation

Network segmentation involves dividing the OT network into distinct zones to enhance security and reduce the attack surface. This control limits lateral movement and confines any potential breaches to a smaller segment of the network. By implementing techniques such as VLANs, DMZs, and dedicated subnets, organisations can enforce stricter policies and controls on which devices can communicate with each other. Segmentation also allows you to tailor security measures for specific components in your system, such as legacy systems that present additional risks. Granular segmentation enhances your overall resilience against attacks.

Protocol breaks

A protocol break will terminate the network connection, and the application protocol. The payload will then be passed via a simplified protocol to a receiving process, which re-builds the connection and passes the data on. A well-engineered protocol break will make a protocol-based attack against the destination system much more difficult

Content validation and inspection

Content validation enables you to gain assurance that data flows do not contain malicious data which could undermine the integrity of your OT environment. The NCSC has existing guidance on safely importing data and implementing secure application programming interfaces (API).

Isolation plans

Isolation can be a critical control of OT systems in an incident, removing connectivity to less-trusted systems. However, to ensure your organisation can isolate connectivity routes during an incident, it's important to clearly document potential impacts. This means that, if an incident occurs, you should know exactly how it will affect various systems, networks, and processes. These plans should also include how you will recover these systems and restore connectivity post incident.

You should use this information to evaluate gaps in your existing controls and determine areas needing further improvements. Frameworks such as the MITRE ATT&CK framework for ICS can be beneficial to map controls against potential attacks.

Summary: You should understand your existing architectural security controls and what protections they provide to the asset and the wider system. Network security controls should be designed to limit the ability for a compromised system impacting your wider OT network. The potential resulting impact from a compromise within the context of applied controls should be well understood and documented for effective risk management.

4. What are the network constraints in your OT environment?

When documenting OT networks, it is important to record any factors that could limit the ability to implement effective cyber security controls. This will help you to make informed decisions when planning future security programmes. These factors could include:

Bandwidth

What limitations are there on the data related to the asset, and how much of the available bandwidth is already being used by the OT process? If there is no spare capacity within the network, this may inform a need for future uplifts to support security functionality.

Exposure

Understanding the exposure of your data bearer is critical to inform the risk to data being carried. Over-the-air wireless bearers (including technologies such as wifi, Bluetooth and LTE) may pose additional risks due to them being openly accessible, this can drive the requirement for strong controls to handle jamming attacks and prevent replay or MiTM attacks.

Latency

Understanding acceptable latency levels is critical in shaping effective cyber security controls in time-sensitive environments like process control or emergency shutdown systems. High latency requirements may necessitate the use of lightweight encryption and/or streamlined authentication methods to avoid delays while maintaining essential security measures. There may be times where cyber security controls are avoided due to unacceptable added latency. Where this is the case, other mitigations through defence in depth should be in place.

Redundancy

What redundancy is in place in the system that would enable updating? Where are single points of failures where downtime is not feasible? Within redundancy, you should also seek to understand what backup communication routes would be used in the event the primary bearer fails. This backup bearer needs to be equally secure and not expose the OT system to additional risk.

Availability

Connectivity may need to be continuously available because it is critical to the function or resilience of the OT system. External functions with high availability requirements should be considered critical system dependencies.

Summary: The technical factors that may limit the implementation of cyber security controls in OT networks should be thoroughly documented. By identifying these constraints, organisations can make informed, risk-based decisions regarding future security enhancements. Effectively managing these limitations is essential to mitigate additional risks being exposed.

5. Would a compromise allow an attacker to bypass existing controls?

When assessing external connectivity into your OT network, it's important to understand how compromised routes or assets could impact connected systems. This could include - but is not limited - to considerations such as:

Security of edge routers in your WAN

What systems would an attacker be able to directly access if they compromised the edge router in your OT WAN? Your organisation should have confidence that defence-in-depth controls would prevent an attacker being able to reach directly into the critical OT components from this style of compromise.

Unsecured connectivity into your OT network

This could be the use of unsecure OT protocols between organisations that might not support security controls. You should consider how you prevent this data being manipulated to cause an impact in your OT system without requiring an attacker to directly compromise the system.

Legacy connectivity into the core OT network

This could include exposed wireless communication channels that do not support adequate encryption or authenticity controls. You should understand the scale of impact if one of these accesses is compromised.

If security compromises have been necessary in the external connectivity, you should have mitigating controls in place to limit the potential impact of a threat actor if a compromise occurs.

Summary: Your organisation should have a comprehensive understanding of the potential impacts of compromised external connectivity into the OT network. Where security compromises have been made, mitigating controls should be in place to limit the potential impact.

Principle 5: Understand and document third-party risks to your OT system

Many OT systems are managed or maintained by third parties, such as manufacturers, integrators, or managed service providers (MSPs). When these groups have access to your environment, they add risks that require additional consideration, as you don't have direct control over the security of the delivered system.

The NCSC has produced supply chain security guidance on how to effectively manage these risks. IEC 62443-4-1 (*secure product development lifecycle requirements*) and IEC 62443-2-4 (*security program requirements for IACS service providers*) provides some additional advice specific to industrial automation and control systems.

At a minimum, you should be able to answer the following 3 questions for third parties connecting to the network:

1. What entities are involved in the external connection?

For each external connection, your organisation should have a detailed understanding of the entities the route is designed for. These are likely to fall into 3 trust levels:

Equal trust

Information sharing routes with other critical national infrastructure (CNI) organisations that operate within the same threat model, and where you have assurance over the technical controls they have implemented.

Partial trust

Connectivity to enterprise networks, where communications are within your organisation are able to assure the technical controls in place.

Low trust

Connectivity to external networks from third-party organisations such as vendors, integrators or managed service providers. This is where you have limited controls over the technical controls implemented.

The trust level of the network will dictate the kind of controls required to both protect your OT data and systems.

When evaluating the entities involved you should ensure they are following the 'browse-down' model, where high-trust systems administer systems of lower trust. No low-trust system should be able to administer systems of a higher trust. Where this appears to be required (such as a third-party providing administration) you need to have documented processes for establishing trust in their systems through validating their security controls are in line with your organisations standards.

Summary: Your organisation should have a detailed understanding of each external connection and its corresponding trust level, ensuring that these levels dictate the necessary security controls for protecting OT data and systems. You must verify compliance with the "Browse-Down" model, where high trust systems manage lower trust systems, and have processes in place to validate the security controls of third-party administration systems against your organisational standards.

2. What are the contractual requirements imposed by the third party?

It is common for third parties to add connectivity requirements to their contracts. This can allow a third party to set the expectations for how they expect to be able to access your environment. This can limit your ability to implement technical controls.

For example, a third party may require 24/7 remote access that would prevent your deployment of a ‘just-in-time’ administration model. Where possible, requirements that limit your ability to deploy technical controls should be removed. You should work with the third party to understand why they require levels of access, and where existing remote access process may be suitable. This will aid in preventing duplicate remote access methods being developed.

Where requirements cannot be removed, compensating controls should be in place to audit and monitor third party actions. You should ensure all other assets in your system are protected from this third-party access, through network segmentation and access controls. A third-party should only be able to access specified assets, and not any other elements of your system.

Regulated CNI sectors may have additional requirements where you may be mandated to supply data to specified third parties. This requirement imposed on the availability of this external connectivity will need to be factored into your isolation plans. Where the connectivity is always persistent the use of technologies that provide a continuous level of separation should be considered. This could include physical data diodes or the use of cross domain solutions (CDS).

Summary: Your organisation should have a documented and detailed understanding of how contractual or regulatory requirements from third parties impact your ability to apply security controls. This documentation should include any compensating controls in place that enable you to manage this risk.

3. Are the third party installing any out of band access?

If a third party is installing equipment within your environment you should ensure you understand the functionality and features of the assets being deployed. This should focus on out of band communication channels, both for asset-to-asset communications, as well as external communications. If deployed systems have connectivity into your wider network and your are unaware of installed out of band channels, you could be carrying substantial unmanaged risk.

Out of band communication channels include but are not limited to:

- 4G modems within devices, facilitating the third party unconstrained remote access to the system and potentially your wider environment. The third party should be encouraged to use an existing remote access mechanism to remove the risk of shadow IT in your environment.
- Other wireless technologies such as Bluetooth or wifi for configuration. In this case, you should understand if this functionality will remain enabled once the asset is deployed and how the connectivity will be hardened.
- Use of removable media to deploy configurations to devices. The product may support zero touch provisioning via removable media. In this case, you should understand what sensitive

data is included within this configuration, how the organisation is protecting this data and how removable media risks are being managed on site.

Note: The use of removable media should be restricted to approved items, as removable media introduces an additional attack vector through which a threat actor can enter the environment.

For example, a threat actor could use malicious USB device to emulates a trusted Human Interface Device (HID), such as a keyboard, to perform keystroke injection attacks. Once connected, the device can rapidly deliver pre-programmed keystrokes to execute commands, install malware, or alter system configurations.

The UK's Industrial Control Systems Community of Interest has published guidance on the management of removable media within OT environments.

Summary: Your organisation should have an established process to assess any new assets being installed by third-parties and to document any risks these assets may present to the wider system. Out of band management should be removed where feasible to remove these risks. Where this is not possible, you should have a clear documented understanding of the technical controls put in place by the third party to harden the access.