







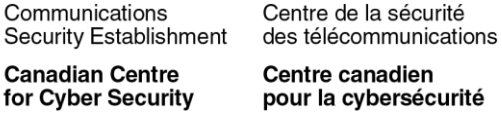






Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products

January 13, 2025

U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency
U.S. Federal Bureau of Investigation
U.S. Environmental Protection Agency
U.S. Transportation Security Administration
Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security
Directorate General for Communications Networks, Content and Technology, European Commission
Germany's Federal Office for Information Security
Netherlands' National Cyber Security Centre
New Zealand's National Cyber Security Centre
United Kingdom's National Cyber Security Centre

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) and partners warn that cyber threat actors, when compromising operational technology (OT) components, target specific OT products rather than specific organizations. Many OT products are not designed and developed with Secure by Design principles[1] and commonly have weaknesses, such as weak authentication, known software vulnerabilities, limited logging, insecure default settings and passwords, and insecure legacy protocols. Cyber threat actors can easily exploit these weaknesses across multiple victims to gain access to control systems.

When security is not prioritized nor incorporated directly into OT products, it is difficult and costly for owners and operators[2] to defend their OT assets against compromise. This Secure by Demand guide, authored by CISA with contributions from the following partners, describes how OT owners and operators should integrate security into their procurement process when purchasing industrial automation and control systems as well as other OT products.

- U.S. National Security Agency (NSA)[3]
- U.S. Federal Bureau of Investigation (FBI)
- U.S. Environmental Protection Agency (EPA)
- U.S. Transportation Security Administration (TSA)
- Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)
- Canadian Centre for Cyber Security (CCCS)
- Directorate General for Communications Networks, Content and Technology (DG CONNECT), European Commission[4]
- Germany's Federal Office for Information Security (BSI)
- Netherlands' National Cyber Security Centre (NCSC-NL)
- New Zealand's National Cyber Security Centre (NCSC-NZ)
- United Kingdom's National Cyber Security Centre (NCSC-UK)

[1] CISA's Secure by Design campaign urges technology providers to take ownership of their customers' security outcomes by building cybersecurity into design and development. As part of CISA's campaign, CISA and partners developed three core principles to guide software manufacturers in building software security into their design process. For more information, see joint guide Secure-by-Design - Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software.

[2] European Union (EU) legislation refers to essential and important entities, such as critical infrastructures as well as entities in the manufacturing sector.

[3] NSA manages the National Information Assurance Partnership (NIAP) program and is piloting the Operational Technology Assurance Partnership (OTAP) program. These oversee evaluation of Commercial Off-the-Shelf (COTS) IT and OT products for use in National Security Systems (NSS) and develop security functional requirements and assurance activities for the product evaluations.

[4] This document does not interpret European Union law nor is it meant to be a guidance for implementation of Union law. The document does not bind the European Commission. DG CONNECT contributed to the drafting of the document in order to cooperate on and emphasize shared cybersecurity principles. However, as this document is a multilateral effort, not all of its elements reflect Union law. Entities falling within the scope of Union law might use this document for information purposes only.

When procuring products, OT owners and operators should select products from manufacturers who prioritize the following security elements:

1. **Configuration Management:** The product supports controlling and tracking modifications to configuration settings and engineering logic. Seek out manufacturers whose products backup and deploy system configurations in a secure and simple manner.
2. **Logging in the Baseline Product:** The product supports logging of all actions—including changes to configuration, security events, and safety events—in the baseline versions using open standard logging formats. Seek out products that come with standardized access and change logs for building incident response capabilities.
3. **Open Standards:** The product uses open standards to support secure functions and services and for migrating configuration settings and engineering logic. Seek out products that support open, interoperable standards to facilitate replacing or adding products.
4. **Ownership:** The product gives owners and operators full autonomy over said product, including maintenance and changes. Seek out products that enable operator autonomy while minimizing dependency on the vendor.
5. **Protection of Data:** The product protects the integrity and confidentiality of data, services, and functions, including a product's configuration settings and engineering logic. Seek out products that treat operational data as valuable and protect it at rest and during transit to and from vendors and manufacturers.
6. **Secure by Default:** The product is delivered secure out of the box, reducing the attack surface and removing the burden on owners and operators. Seek out products that include all security features in all versions; eliminate default passwords; allow for appropriate length and complexity for passwords; use secure up-to-date versions of protocols with older insecure protocols (e.g., SNMPv1/2, Telnet, SSL, TLS 1.0/1.1) disabled by default; do not unnecessarily expose external interfaces; and provide authorized users the ability to reset product configuration to its original state.
7. **Secure Communications:** The product supports secure authenticated communication with digital certificates deployed that fail loudly (e.g., when a certificate expires) but allows critical processes to continue. Seek out products that simplify digital certificate deployment and renewal such that operators do not need to be cyber experts to achieve secure authenticated communications.
8. **Secure Controls:** The product is resilient to threat actors sending malicious emergency, safety, or diagnostic commands; protects the availability of essential functions; withstands active security scanning; and minimizes the impact of an incident on the overall system. Seek out manufacturers who can demonstrate trusted safety-critical controls and explain how operators can continuously verify and regain that trust.
9. **Strong Authentication:** The baseline version of the product, especially safety-critical equipment, protects against unauthorized access through appropriate control measures, including role-based access control and phishing-resistant multifactor authentication. Seek out manufacturers that have eliminated the use of shared role-based passwords in their products.

10. **Threat Modeling:** The product has a full and detailed threat model. Seek out products that have an up-to-date threat model that articulates the ways in which it might be compromised, along with security measures implemented to reduce these threat scenarios.
11. **Vulnerability Management:** The manufacturer has a comprehensive vulnerability management regime in which products are rigorously tested to help ensure they contain no known exploitable vulnerabilities. Each product has a clearly defined support period during which vulnerabilities are managed and patches are supplied free of charge. Seek out manufacturers who include hardware and software bill of materials with product delivery and who commit to timely remediation of vulnerabilities through a vulnerability disclosure program.
12. **Upgrade and Patch Tooling:** The product has a well-documented and easy to follow patch and upgrade process and supports moving to a supported operating system version at no extra cost if the original operation system is soon to be no longer supported. Seek out products that can be verified and that support owner-controlled patch management.

By rigorously enforcing purchasing decisions that require and prioritize the purchase of products that enforce these elements, critical infrastructure organizations can help mitigate current and emerging cyber threats to critical infrastructure and create a path away from legacy environments. Additionally, OT owners and operators will send a message to manufacturers to stimulate the supply of Secure by Design products. Manufacturers that implement these considerations can establish a resilient and flexible cybersecurity foundation in their products that OT owners and operators can build on over the coming decades. Additionally, owners and operators may need to consider regulatory requirements, such as the European Union's (EU's) NIS2 Directive, during digital systems acquisition. [5] Where applicable, owners and operators should ensure that the products they buy are compliant with applicable legal obligations and carry required marks of regulatory compliance.[6]

[5] The NIS2 directive requires critical infrastructures and certain other entities providing services in the Union to take measures to ensure that the products deployed on their networks are secure. In addition, several countries and regions have started laying down security-by-design in law, such as the EU's Delegated Regulation on the Radio Equipment Directive, which will apply from 1 August 2025, and the Cyber Resilience Act, entered into force on December 10, 2024.

[6] The CE marking is required by the EU's Cyber Resilience Act for products with digital elements placed on the Union market and that products have been subjected to legally required conformity assessment procedures that are in line with the intended purpose and the risk profile of the product.

Table of Contents

Introduction

Critical infrastructure and industrial control systems manage essential services, such as energy, water supply, and transportation, making them prime targets for cyberattacks that could result in severe disruptions. Effective cybersecurity for these systems is crucial and helps ensure stability, safety, and economic well-being of nations.

The burden of industrial cybersecurity costs falls disproportionally on OT owners and operators rather than manufacturers, who have the greatest ability to improve the security of their products and reduce risk for their customers. There are ongoing efforts around the world to shift the balance towards more secure products, such as CISA's Secure by Design initiative, which aims to ensure customers can trust the safety and integrity of technology, and the EU's recently agreed Cyber Resilience Act, which mandates security by design for manufacturers of hardware and software products.

This document is part of CISA's Secure by Demand series, focused on helping customers identify manufacturers dedicated to continuous improvement and achieving a better cost balance by implementing Secure by Design principles. Achieving the right balance is more important than ever as threat actors increasingly target OT products.

Threat actors are successfully targeting particular OT products, rather than specific organizations, because vulnerabilities span multiple victims and critical infrastructure sectors, and OT products can be access points to control systems. Threat actors can easily exploit common weaknesses in OT products, such as weak authentication and authorization, known software vulnerabilities, and limited logging. It is difficult and costly for asset owners to defend themselves against these threats if security is not considered and implemented in the design and development of their OT products.

This document is intended to help owners and operators purchase OT products, particularly industrial automation and control system products, with priority secure by design elements. (Owners and operators purchasing products are referred to as "buyers" hereafter.) This document also supports OT owners and operators in meeting the applicable legal requirements and equipping themselves with products that will help ensure the resilience of their systems.

The priority elements were selected to mitigate current cyber threats to OT and adhere to common legal requirements to encourage business practices that empower asset owners to recover the infrastructure they are responsible for and develop foundational security elements that are uncommon in OT. Selecting manufacturers that implement these considerations can help buyers establish a resilient and flexible cybersecurity foundation in their OT systems that they can build on over the coming decades.

By ensuring the deployment of secure products on their networks, critical infrastructure owners and operators can reduce the potential damage from cyber threats and protect their systems from exploitation. Making these systems resilient is essential for maintaining public trust and the smooth functioning of modern societies.

Considerations for OT Product Selection

Buyers should look for the following key security elements when selecting OT products:

1. Configuration Management
2. Logging in the Baseline Product
3. Open Standards
4. Ownership
5. Protection of Data
6. Secure by Default
7. Secure Communications
8. Secure Controls
9. Strong Authentication
10. Threat Modeling
11. Vulnerability Management
12. Upgrade and Patch Tooling

The key elements above collectively enable buyers to consider how manufacturers are including security in the design and development of their products. These elements are not in priority order. As buyers are checking for these elements, they should ensure their manufacturers are familiar with the Secure by Design principles of taking ownership of their customers' security outcomes, embracing transparency and accountability with their own security progress, and business leadership for integrating cybersecurity from the start of design decisions. (For more information, see the joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software.) Buyers should look for manufacturers that demonstrate their adoption of Secure by Design and International Society of Automation (ISA) 62443 standards.[7] Manufacturers can demonstrate their adoption of Secure by Design by publishing roadmaps that detail how they are adopting these practices.

The following sections provide buyers with guidance on questions to ask manufacturers, considerations for the OT context, and why these considerations matter. **Note:** This guidance aligns with established cybersecurity standards, including National Institute of Standards and Technology (NIST) 800-213a for industrial internet of things or NIST 800-82 for OT and Security Level 3 of ISA/IEC 62443-4-2 and 62443-3-3 for cybersecurity features in industrial automation and control systems.[8] This guidance aligns to technology-neutral and objective-oriented approaches contemplated by the Cyber Resilience Act (CRA).[9]

[7] ISA writes standards for automation professionals to improve safety, security, and efficiency. The ISA/IEC 62443 multi-part standard is internationally recognized as defining requirements and processes for implementing and maintaining electronically secure OT products, systems, and development lifecycles.

[8] NSA recommends maintainers of National Security Systems (NSS) use the forthcoming OT NSS profile in ISA.

[9] The EU's CRA lays down technology-neutral and objective-oriented essential requirements, which manufacturers are required to implement through concrete technical measures in light of the nature of their products. The European Commission intends to request the development of vertical (product-specific) standards by the European Standardisation Organisations. These standards aim to facilitate the compliance of manufacturers by proposing concrete technical solutions for specific product categories.

Configuration Management

Selection criteria: Products support controlling and tracking modifications to configuration settings and engineering logic.

Questions to ask: Does the product enable authenticated backup recording and deployment for configuration settings and engineering logic? Does the product have tamper prevention or detection? Does the manufacturer provide custom processes and response plans for interruptions involving their products or services?

Why this matters: Without strong configuration management, it is difficult to validate changes to infrastructure. Asset owners and operators need this validation to detect and prevent a threat actor from establishing persistence on OT devices. Recording and protecting backups of OT products is necessary for an operator to recover quickly and independently after a product failure.

The goal of this consideration is to help ensure OT owners and operators can swiftly identify unauthorized configuration changes and recover critical infrastructure after an incident occurs to minimize societal impact and downtime.

Owners and operators must be able to recover from incidents in which a threat actor establishes a foothold or wipes a component on the OT network. Buyers should look for manufacturers who can offer the following:

- Alerts for known insecure configurations or attempts to change to less secure configurations,
- The ability to authorize or restrict configuration changes,
- The ability to uniquely identify an OT device to support asset management,
- Open standards for backup files, and
- Documented interfaces for creating backups and restoring from backups in person or over the network.

As OT software manufacturers adopt best practices, buyers should seek out resilient products that can rapidly recover and update themselves with very little downtime. For example, immutable containers would allow operators to make configuration changes with minimal downtime by hot-swapping containers. For more on how manufacturers can support resilience with their business practices, see the “Ownership” consideration.

Logging in the Baseline Product

Selection criteria: The baseline product version supports security and safety logging of all actions using open standard logging formats.

Questions to ask: Does the product log, restarts, logins, or changes to the product? Does the product provide telemetry and logs that help predict and prevent process failure? Does the product log security events and safety events by default?

Why this matters: Logging will help OT network defenders gather evidence of intrusions into OT networks.

The goal of this consideration is to include logging in baseline OT products to preserve evidence of an intrusion throughout product lines. Logging should not be an add-on or paid feature.

Logging is necessary to detect incidents, provide indicators of compromise, and track threat actor behavior. Traditionally, real-time compute constraints and limited bandwidth on legacy products and networks complicated OT logging and resulted in limited host logging and telemetry. This problem is becoming easier to address as network operators migrate from serial connections to IP-based networks. Even in scenarios where the logs cannot safely be aggregated over the network into a security tool, OT products with local logging already enabled through their default function will support incident responders.

Buyers should seek products with a minimum set of logs enabled by default (which should be standardized across products and manufacturers). Log types that buyers should look for include:

- Open standard formats.
- Authentication events, both successful and unsuccessful.
- Deletion or modification of logs.
- Changes to the device, such as updated engineering logic, firmware updates, or a change in configurations.
- Data events including create, read, update, and delete.
- Error or exception events.

All event records should include a timestamp, source address and port, affected account details, correlation identifier, and event description. Buyers should then seek manufacturers that supplement minimum log types with information from the manufacturer's written threat model (see the Threat Model section).

Without logs, cyber threat actors can establish persistence through configuration or logic changes, or degrade operational efficiency, without leaving a record of the action for the operator or incident responders. For further guidance on OT logging, see the joint guide Best practices for event logging and threat detection.

Open Standards

Selection criteria: The product uses open standards to support secure functions, services, and migrating configurations and logic.

Questions to ask: Does the product support open, interoperable standards to simplify replacing or adding products? Is the manufacturer demonstrating their alignment to industry regulations or international standards (e.g., ISA/IEC 62443)?

Why this matters: Open standards enable interoperability that allows buyers to pick the best product available.

The goal of this consideration is to confirm buyers can switch between vendors and manufacturers as well as leverage advances in general security standards in OT environments. The use of open standards means that advances, such as new encryption algorithms, naturally apply to OT environments rather than lagging enterprise security improvements. Open standards also mitigate the risk of buyers being trapped with unsupported hardware or software if a manufacturer goes out of business.

Proprietary technologies are common in OT environments for communication between devices made by the same manufacturer, as well as for internal logging and control processes. These technologies arguably allow for improved efficiency, yet this benefit comes at the expense of interoperability between products from different manufacturers. The lack interoperability may:

- Complicate asset management governance,
- Require owners to buy additional hardware when adding new manufacturers, and
- Impede safety by introducing friction for acquiring the newest safety and security capabilities.

Open standards provide flexibility for owners and operators to move between manufacturers based on the most viable product available, rather than the best manufacturer product available when their system was originally built. These standards might apply to logging formats (sysmon), networking protocols (OPC-UA), programming languages (IEEE 61131-3), encryption protocols (TLS), or any element of a device that would benefit from cross-vendor communication.

Buyers should prioritize open standards when evaluating new features to avoid any risks of vendor lock-in. However, international standards take time to update. Manufacturers will, rightfully, want to add functionality and features that are ahead of international standards. When this occurs, buyers should seek out manufacturers that actively support interoperability, such as those who publish parsers or participate in interoperability working groups.

Ownership

Selection criteria: The product gives owners and operators full autonomy over the product, including maintenance and changes.

Questions to ask: Does the product enable OT operators to do what is needed without an onward dependency on the vendor? Does the manufacturer allow for support contracts with local engineering firms? Does the warranty policy for the product allow for adding security software or products (e.g., firewalls, gateways, continuous monitoring, diodes) to the environment?

Why this matters: Asset owners and operators need to be in control of their dependencies to respond and recover quickly with clear roles and responsibilities for everyone involved.

The goal of this consideration is to enable operators to control and recover their systems without unintended or unnecessary dependencies.

Buyers should seek out vendors and manufacturers with explicit roles, responsibilities, and onward dependencies for their services or products. Owners and operators across many sectors depend on vendor or manufacturer support contracts to maintain and operate their systems. This is only an issue if the responsible party for a given system is unclear, the buyer's dependency on the manufacturer is unintentional, or the buyer's dependency on the manufacturer is required by the product but unnecessary. Products that discourage third-party or on-premises configuration and management may interfere in the timely remediation of safety and security issues. These barriers may manifest as:

- Restriction of data to an ecosystem or partition owned by the manufacturer and inaccessible to the asset owner,
- A warranty policy that limits an asset owner's ability to perform an upgrade, a security examination, or vulnerability testing beyond the limitations necessary for safety compliance, or
- A manufacturer selling device security functionality as an additional service.

Given that modern process automation involves technically complex components and architectures integrated with third-party vendors or contractors for maintenance and monitoring, buyers should seek out products unrestricted by the barriers listed above. To improve security across critical infrastructure, buyers should seek manufacturers that equip end users with the tools and skills necessary to engage in a business continuity plan that involves maintaining system functionality, operating through a degraded state, and bringing critical components back online safely. For guidance on the recommended minimum system functionality to aim for, U.S. organizations should consult their appropriate sector risk management agency.

Protection of Data

Selection criteria: The product protects the integrity and confidentiality of data, services, and functions, including configurations and logic.

Questions to ask: Does the product encrypt data at rest? Does the product have a way to verify the integrity of its data? Does the product share or sell its data to anyone?

Why this matters: OT data rarely changes and is valuable for threat actors trying to understand a system. An understanding of operational data is often needed to bypass safety checks and cause sustained harm.

The goal of this consideration is to protect customer data and limit harm to operational environments.

Buyers should seek out products that minimize access and sharing of OT data. This data underpins the engineering of the system and gives a threat actor the information needed to create a targeted effect beyond denial of service. Look for manufacturers and vendors that can explain how they protect copies of this data.

Buyers should seek out manufacturers that rely on data pushed out of the OT network as necessary, rather than pulling data out of the OT network. This shift enables the buyer to maintain control over their data and restricts any external connections into the OT network. These external connections are often used for maintenance and management purposes for complex systems. If two-way connections are required, buyers should seek out products that require an operator's approval to establish a connection. Including this check in the product helps mitigate the impact of segmentation misconfigurations.

For more information on OT data protection see the joint guide Principles of operational technology cyber security.

Secure by Default

Selection criteria: The product is delivered secure out of the box, resilient against the most prevalent threats and vulnerabilities, without requiring additional configuration from users or administrators.

Questions to ask: Has the manufacturer eliminated or is working to eliminate default passwords? Does the product enable by default and use the secure, up-to-date, versions of protocols (e.g., Secure Shell [SSH], SFTP [SSH File Transfer Protocol])? Are older insecure protocols disabled by default (i.e., SNMPv1/2, Telnet, Trivial File Transfer Protocol [TFTP])?

Why this matters: Insecure default settings expose asset owners to more risk and increase security costs.

The goal of this consideration is to configure security into OT products such that protection against the most prevalent threats is included by default at no additional cost to the buyer. Secure by Default is of particular importance for today's OT systems because of their long lifecycles, their limited availability to be taken offline for patching, and the priority given to their continuous operation.

The key aims to achieve a Secure by Design product are:

- Making customer security a core business requirement, not just a technical feature.
- Including default configurations that protect against prevalent threats.

- Eliminating default passwords.
- Introducing continuous friction for connecting internal OT devices to the public-facing internet.
- Ensuring security functionality is available on the device at no additional cost.
- Embedding secure deployment guidance or hardening guides into the product by default; the guide should clearly state security risks introduced by operators changing default configuration options.

Eliminating default passwords is especially important because nation-state affiliated groups and hacktivists have recently exploited devices by leveraging default passwords. By using default passwords, a manufacturer creates a security risk in their product that a customer is not reasonably aware of. Even when a customer changes insecure defaults, it is likely that they eventually will make a mistake, particularly in distributed control system environments that have dozens of vendors. To remove this risk, buyers should seek products without default passwords for user login or embedded into the product's firmware, removing the possibility of an operator or integrator making a default password mistake. This is vital for passwords for remote access. For further guidance on eliminating default passwords, see CISA's Secure by Design Alert: How Manufacturers Can Protect Customers by Eliminating Default Passwords.

Additionally, buyers should seek manufacturers that document the level of security included in their products, with the most secure default configuration preset removing the burden of hardening from operators.

Buyers should also ask for security implementations that work with their existing operator workflows and allow for gradual security improvements. Backwards compatibility is often embedded into new devices to help ensure they work with existing deployments. However, this compatibility often requires that security features in new devices are not enabled by default to help ensure the legacy components can communicate seamlessly. This can be seen in lengthy secure deployment guidance that details how to turn off old insecure services. This operating model makes it difficult for an asset owner to use operational funds and eventually "flip the switch" to enable the secure option across their infrastructure. Buyers should seek manufacturers that develop backwards compatibility operating models that prioritize security features with negotiated downgrades when necessary. In the long term, this deployment model, along with open standards, will allow for a gradual digital transformation as equipment fails, rather than a large-scale rip and replace operation. For example, instead of replacing all the devices in a portion of the system at once, an owner/operator could deploy a newer secure device with an embedded protocol gateway that translates it to observed legacy devices while still communicating securely by default. Operational realities do not always need to result in less cybersecurity. Buyers should look for manufacturers that are performing voice of customer research to embed cybersecurity within existing workflows and deploy functional products with security enabled by default.

For more information on Secure by Design, see the joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software. This guide urges manufacturers to make it harder, or even impossible, for the operator or integrator to make a cybersecurity mistake.

Secure Communications

Selection criteria: Products should support authenticated communication with device certificates deployed that fails loudly but that allows critical processes to continue.

Key considerations: Does the product simplify the deployment and renewal of certificates for devices? Does the manufacturer need asset owners and operators to be cyber experts to sustain secure communication?

Why this matters: Secure communication is necessary to validate the integrity and authenticity of the messages controlling critical infrastructure.

The goal of this consideration is to improve the usability and uptake of secure machine-to-machine communications in OT networks.

Standard operating processes for most OT networks use unauthenticated and unencrypted traffic. Without authentication, cyber threat actors can impersonate any device and send safety-impacting commands across the network; without encryption, cyber threat actors can read sensitive network traffic. Retroactively adding cryptography for authentication and encryption is often not feasible due to cost and computer processing restrictions. The demand for backwards compatibility in legacy environments then results in newer devices not supporting cryptography or operators leaving cryptography capabilities disabled for the lifecycle of the product.

Another consideration risk for operators is that enabling authentication or encryption requires them to manage certificates and Public Key Infrastructure (PKI). It is easy for mistakes to occur, such as failure to replace an expired certificate, resulting in downtime. That is not a risk many critical infrastructure owners and operators are willing to take when even mature IT organizations can make mistakes. However, critical infrastructure owners and operators must be able to verify the integrity of their system, which requires authentication. Much like the needed progression to open standards, as critical infrastructure sectors mature, there should be a move towards more ubiquitous authentication and integrity for data in transit. Moreover, as secure communication capabilities mature, buyers should ask for products that support cryptographic agility to allow system upgrades if a product's cryptography becomes vulnerable. Cryptographic agility is particularly useful in OT due to the long lifecycles of products.

Buyers should mandate that secure communication solutions are easy for operators or integrators to deploy securely, resistant to operator error, and do not require operators to be cyber experts. As certificate management is not common in OT environments, operators may consider the equivalent of a TLS sign-only (unencrypted but still signed with a private key) or opportunistic TLS mode as an interim safety solution, where an expired certificate will generate logs but not prevent communication. Secure communications capabilities designed late in product development are likely to be difficult to use. A well-integrated secure communications capability acts as the foundation for defense in depth and a modern Zero Trust network. Buyers should seek manufacturers that understand common operator workflows and embed secure communications into those workflows.

Secure Controls

Selection criteria: The product assumes a threat actor is operating on the network and protects itself against malicious emergency, safety, or diagnostic commands.

Questions to ask: Does the product have a method to establish trust for commands to/from critical components? Does the product prevent or ignore commands if they create known safety concerns? Does the product behave differently if commands meant for maintenance periods are sent during active operations? Can the product alert on breaks from a standard or specification? Can the product remain stable during security scans, such as vulnerability assessments or asset inventory tools?

Why this matters: OT environments need safety systems and processes to keep people safe. Without security checks, safety systems are easy and valuable targets.

The goal of this consideration is to improve the resilience of OT systems by encouraging components that do not inherently trust the entire network or trust that all components are acting according to the rules of a standard or specification. Components should assume threat actors are on the network.

OT systems are designed for safety and resilience, with mechanisms built into products and their underlying communication protocols to degrade safely and recover from errors. While these systems work well in a trusted environment, they are obvious targets for threat actors seeking to rapidly degrade OT systems. For example, existing protocols include commands to take control from the main computer or disable other computers in case of failure, such as a stuck transmitter. A threat actor can recreate those conditions or send a command to weaponize safety features against the system. Products must mitigate the risks from a threat actor compromising a trusted device or intentionally violating a standard to do harm.

Buyers should ask for products that are designed to withstand the malicious use of commands. Third-party security solutions, which largely operate on communications data, have limited capacity to effectively detect unverified, invalidated, or unauthorized commands. Often these products have to model the entire system and have significant integration challenges to get the engineering process data they need. By contrast, OT components are well positioned to understand their context within the system and identify deviations in that context. For average components, this could mean documenting how the component responds to conditions impacting safety or security. For example, a manufacturer could document how a component responds if another device impersonates it, how it verifies error states and diagnostic commands, or how it handles active scanning. This understanding is akin to a process alerting system determining whether an incident is a communications disruption or a process malfunction. Identifying illegitimate behavior is particularly important for roots of trust, such as a primary controller. Components do not need to merely log anomalous behavior. If the intended system architecture or specification is broken or does not follow the operational context, then a component may be able to ignore or respond to the anomalous behavior. Examples of system specifications being broken include: a singular Modbus client or bus controller being impersonated, network arbitration designed to disable an existing system such as a new engine appearing while a vehicle is in operation, or maintenance commands and updates mid process.

Buyers should look for products that are designed to operate through security scans. Legacy OT products are prone to crashing during noisy scans. This fragility is a security weakness that makes it difficult for operators to maintain an accurate view of a network and limits the implementation of Zero Trust in OT.

Moreover, buyers should seek out manufacturers that considered the security of unauthorized commands throughout the design process. Asset owners and operators should consider consulting the Department of Energy's Cyber-Informed Engineering Implementation Guidance to incorporate cybersecurity decisions into their engineering and design process.

Strong Authentication

Selection criteria: The baseline version of the product supports role-based access control (RBAC) and multifactor authentication (MFA), particularly for changes to safety-critical equipment.

Questions to ask: Has the manufacturer eliminated or is working to eliminate the use of shared role-based passwords in their products? Is MFA included in the baseline version?

Why this matters: Strong authentication allows for defense-in-depth and enables identity and access management best practices.

The goal of this consideration is to use human-to-machine authentication mechanisms that are sufficient to support modern identity and access management best practices. This consideration is focused on two elements of strong authentication:

1. RBAC and/or attribute-based access control (ABAC)
2. Phishing-resistant MFA

Buyers should seek products with RBAC and ABAC rather than relying on common accounts. RBAC and ABAC, or a control that can restrict users to viewing information versus the ability to change information, is key for limiting the ability to make network changes to authorized individuals. A singular admin account is not uncommon in OT devices, and encourages risky behavior like sharing accounts, which make passwords easier to steal in addition to making it difficult to identify who made any given change.

Buyers should look for products with phishing-resistant MFA included in the baseline version. In OT environments this might be MFA for engineering workstation or SCADA software with controllers designed to recognize if supervisory control is authenticated. Phishing-resistant MFA is a key security control for limiting the damage a threat actor can do in an OT environment. Some critical infrastructure sectors already use MFA in unique ways. For example, in the Freight Rail Subsector it is commonplace for wayside interface units to require a local button press on the controller and a dynamic code along with a password to change vital (safety-critical) signaling logic. It would be simpler for rail companies to change safety-critical logic without having a signaling engineer drive out to a waystation, but requiring a signaling engineer to press the physical button reduces risk and enhances safety. MFA is a critical tool for preventing unwanted changes to an environment and keeping the system and people safe.

Physical controls combined with MFA, or MFA enabled for modifications on every component, is likely to be difficult in an operational environment. Jump hosts are a way to add MFA restrictions to OT networks. However, segmentation is difficult to maintain, and critical components warrant that additional layer of

protection. Segmentation is a highly valuable security control, but CISA and partners have consistently observed accidental breaks in segmentation. An organization of any size may want assurance that even if a single control (segmentation) fails, that there is a backup security control to prevent safety impacts. In the freight rail environment, this higher level of change control is restricted to safety-critical logic. Not every tiny sensor or cheap component necessarily needs to support MFA in the near term, but baseline versions of industrial automation control systems should support MFA from supervisory control (e.g., engineering workstations, SCADA, HMI).

Threat Modeling

Selection criteria: The product has a full and detailed threat model.

Questions to ask: Can the manufacturer articulate the attack vectors they have considered when designing their product? What security measures does the product implement to reduce these threat scenarios? Does the manufacturer have a roadmap to address gaps in their threat model?

Why this matters: Threat models are necessary for asset owners to understand the risk from a product and prioritize their security controls.

The goal of this consideration is to give buyers the opportunity to make informed choices when evaluating the security mitigations in a product. Threat modeling is a structured process designed to identify and analyze risks. Transparent threat models and corresponding mitigations allow buyers to understand the risk from disabling product mitigations and determine if a product is maintaining pace with modern threat actors.

Buyers should seek out threat models that track and incorporate threat sources, such as MITRE EMB3D, so that threats are aligned with modern threat actor capabilities. Public threat sources allow manufacturers to communicate threats and mitigations using a shared language, making it simpler for buyers to understand how a product fits into their overall security model. In legacy OT environments, that security model is likely to rely heavily on segmentation. Buyers should avoid products that rely entirely on a threat actor never accessing the OT network. Mitigating the impact of a successful compromise requires defense in depth, and defense in depth is challenging without secure products.

Buyers should search for manufacturers that use threat modeling throughout the software development lifecycle to understand where and how security measures should be prioritized and implemented to protect their product from malicious actors. Manufacturers that document and update threat models, hardening guidance and secure lifecycle development, are more likely to build products that will be resilient against both known and emerging threats. Asset owners and operators should partner with a manufacturer's threat modelling capability to prioritize upgrades and patches that impact their OT system. Additionally, threat models enable manufacturers and buyers to answer the following questions:

- What security products (e.g., EDR, network monitoring, firewalls) or security controls and policies (segmentation, password policies) does the manufacturer assume are protecting the product?
- What communication capabilities does the product have? Does the product ever communicate back to the manufacturer?
- What environment is the product intended for and how can it be used securely?

- How have they designed to protect against common classes of coding error and how might adversaries take advantage of common coding errors if the product is vulnerable?
- How does the manufacturer protect against supply chain attacks?

Vulnerability Management

Selection criteria: Product manufacturers should have mature vulnerability management processes based on the CVE Program. The processes help ensure that vulnerabilities in their products are identified and remediated across the entire life cycle. In addition, manufacturers need effective communication channels with users and the wider public, enabling them not only to share and publicly disclose information about vulnerabilities and mitigations, but also to receive information about newly discovered security flaws in their products.

Questions to ask: Has the manufacturer drawn up a software bill of materials? Does the manufacturer have a track record of remediating vulnerabilities in a complete, accurate, and timely manner and is relevant information about vulnerabilities and remediation shared with users and the public? Will security advisories be automatically retrievable according to the Common Security Advisory Framework (CSAF) standard? Does the manufacturer have a coordinated vulnerability disclosure policy? Does the manufacturer make it easy to report security vulnerabilities by providing an RFC 9116 compliant security.txt?

Why this matters: It is difficult to design and develop products without any vulnerabilities given the complexity of modern operational technology, the possibility of human error, and supply chain risks. Transparency of vulnerability handling is necessary for buyers to make informed decisions and manufacturers to continuously improve their secure development practices.

The goal of this consideration is to keep OT secure across its entire life cycle. Industrial control systems and other technologies deployed by operators are often in use for decades. It is essential that operators can rely on mature vulnerability handling processes put in place by the manufacturers of such products.

A mature vulnerability handling process is based on the CVE Program and established international standards, mainly ISO/IEC 29147 and ISO/IEC 30111, complies with all application legislation (such as the EU's Cyber Resilience Act), and should contain at least the following elements:

- Complete, accurate, and timely identification and documentation of vulnerabilities and components contained in operational technology, including a software bill of materials in a commonly used and machine-readable format.
  - Vulnerabilities should be assigned an identifier (CVE number) and published to CVE Program.
- Risk-based remediation of vulnerabilities without delay, including security updates.
- Public disclosure of information about available security updates, including an accurate description of the vulnerabilities, the root cause, the common weakness enumeration (CWE), information allowing users to identify the products affected, the impacts of the vulnerabilities, the severity, and clear and accessible information to help users to remediate the vulnerabilities as security advisories.

- Security advisories provided in an automatically retrievable, machine-processable format. This enables the operator to match security advisories against its own assets and reduce the human resources needed to find and evaluate the information. Vendors can use CSAF standard to automate retrieval of security advisory information.
  - **Note:** Information in BSI TR-03191 may provide the basis for procurement requirements. Please consult your legal advisor.
  - Vulnerability Exploitability eXchange (VEX) statements indicating the "not affected" or "under investigation" status for "celebrity vulnerabilities" (i.e., Log4Shell-type vulnerabilities) should follow the CSAF standard.
- A policy on coordinated vulnerability disclosure setting out how the manufacturer intends to responsibly share information about discovered security vulnerabilities with affected parties and the public.
  - **Note:** Entities should follow well known and established coordinated vulnerability disclosure (CVD) best practices. See CERT Coordination Center (CERT/CC)'s for more information.[10]
- Measures to facilitate the sharing of information about potential vulnerabilities in operational technology as well as in third party components contained in such products, including by providing a contact address for the reporting of discovered vulnerabilities. This should also be supplied according to RFC 9116 as a security.txt on the manufacturer's website.
- Mechanisms to securely distribute updates for products to fix or promptly mitigate vulnerabilities.
- Dissemination of security updates without delay. Updates are accompanied by advisory messages providing users with relevant information, including on potential action to be taken.

Note: Entities that have mature vulnerability handling processes should consider becoming a CVE numbering authority (CNA) within the CVE Program. For more information, contact CISA at cvd@cisa.dhs.gov.

[10] https://vuls.cert.org/confluence/display/CVD

Upgrade and Patch Tooling

Selection criteria: The product has a well-documented and easy to follow process for patches and upgrades, and the manufacturer provides security patches at no extra cost. This includes porting supported software to new operating systems free of charge if the original operating system is no longer supported.

Questions to ask: Does the product employ resilient patching features to reduce the risk of downtime from a bad patch (e.g., golden images)? Does the manufacturer test patches and report the results to check for compatibility issues with software/firmware/binaries and help ensure the patches do not overwrite existing configurations? Does the manufacturer update software to modern operating systems if the operating system is end-of-life? Does the manufacturer publish end-of-life dates for their products? Does the manufacturer allow the buyer to verify an update is authentic? Are patches made available free of charge and disseminated via secure channels?

Why this matters: Patches are an excellent way to protect against known threats. Greater patch adoption in OT requires transparency, verifiability, and a confidence that patches will not break a critical process.

The goal of this consideration is to increase patch rates and reduce use of end-of-life software through increased patch availability, customer confidence, and transparency. These improvements are necessary to mitigate the operational concerns of patching an OT environment.

For increased confidence, buyers should seek manufacturers with resilient patching technologies, verification techniques, and transparency. For resilience, find manufacturers that develop and test patches in representative configurations to help address the risk of a faulty patch. For example, a patch may be incompatible with another piece of software, or a patch may overwrite the asset owner's configurations or engineering logic. Manufacturers can avoid incompatibility by using a developer preview program for the software used by the operator or their own testing environment that replicates client environments. Responsible manufacturers will test against common configurations and take environmental considerations into account. Buyers should also ask about automatic recovery features to protect them from any patching issues, such as golden images or safe modes.

For verification, buyers should be able to reliably determine the authenticity of an update. The delivery mechanism for that update needs to be over a secure channel to help guarantee integrity. Buyers should ask for the security controls the manufacturer uses to protect the update development, build, and delivery pipeline to help ensure their updates are legitimate.

For transparency, buyers should seek out manufacturers that release updates that provide users with relevant information (see Vulnerability Handling section), provide security updates free of charge, and are transparent about the length of the support period for a product. This support period should reflect the intended lifecycle of the product (i.e., a pump intended for remote areas may expect a greater period of support than a centralized manufacturing use-case). During the support period, a buyer can expect that security vulnerabilities in their products will be handled and security updates will be made available. An organization may have hundreds or thousands of retired devices in the field. Transparency around retirements helps buyers schedule their replacement hardware or invest in mitigating controls such as virtualizing the out-of-date system within a modern operating system. Notably, it is very common for warranty or support packages to be tied to an underlying end-of-life operating system, so that an operator

is forced to run an older version of an operating system even if the software is functional on newer operating systems. Operators should verify that running software on modern operating systems does not needlessly invalidate the support agreement. Without the planning that transparency allows, an operator may have to maintain a high-risk product for years.

Resources

Organizations face the difficult task of upgrading to secure by design products while simultaneously defending their current infrastructure. Individual elements of secure by design may be difficult to apply perfectly to the current processes of a sector or subsector. For further guidance, reach out to the appropriate Sector Risk Management Agency or SecureByDesignOT@cisa.dhs.gov. Additionally, CISA offers free products and services to help critical infrastructure owners and operators secure their current infrastructure. See our website for a full listing or contact a regional cybersecurity advisor.

Contact Information

U.S. organizations are encouraged to report suspicious or criminal activity related to information in this guide to:

- CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870) or your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
- For NSA cybersecurity guidance inquiries, contact CybersecurityReports@nsa.gov.
- State, local, tribal, and territorial governments should report incidents to the MS-ISAC (SOC@cisecurity.org or 866-787-4722).

Australian organizations visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

Canadian organizations report incidents by emailing CCCS at contact@cyber.gc.ca.

German organizations visit bsi.bund.de/EN/IT-Sicherheitsvorfall/it-sicherheitsvorfall_node.html to report cyber security incidents.

Netherlands' organizations visit ncsc.nl for advisories, and report incidents by emailing NCSC-NL at cert@ncsc.nl.

New Zealand organizations report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

United Kingdom organizations report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA and its co-sealers do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA and co-sealers.

This document is without prejudice to any type of legislation that is applicable in the jurisdictions of CISA and its co-sealers. This document does not bind CISA and its co-sealers and is not intended to provide guidance on the implementation of such legislation.

Acknowledgements

The U.S. Department of Energy, CESER, Energy Threat Analysis Center; U.S. Federal Railroad Administration (FRA); Interstate Natural Gas Association of America; IT Sector Coordinating Council; OPC Foundation; Open Policy; OT Cyber Coalition; Schneider Electric; and Xylem contributed to this guide.