TLP:CLEAR

Secure by Demand Fact Sheet

Priority Considerations for Operational Technology Owners and Operators When Purchasing Digital Products

Key Secure by Demand Elements for Operational Technology

This fact sheet addresses key elements for operational technology (OT) owners and operators to consider when purchasing digital products that automate physical processes, e.g. programmable logic controllers (PLCs), human-machine interfaces (HMIs), and remote terminal units (RTUs). CISA strongly advises buyers to consider these key security elements when making procurement decisions. **Note:** CISA has based this list on the joint guidance *Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products*[1] and is providing it without ranking or priority.

Element	Why This Matters	Questions I Should Ask
Configuration Management	Asset owners and operators need to detect changes establishing persistence on OT devices. Recording and protecting backups of OT products allows for quick and independent recovery.	• Does the product enable authenticated backup recording and deployment for configurations 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?
Logging in the Baseline Product	Logging helps defenders gather evidence of intrusion into OT networks.	• Does the product log logins, restarts, 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?
Open Standards	Open standards enable interoperability that allows buyers to pick the best product available without lock-in.	• 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?
Ownership	Asset owners and operators need to be in control of their dependencies to respond and recover quickly with clear roles and responsibilities.	• 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 to the environment?
Protection of Data	Threat actors need to understand OT data to have an impact.	• Does the product encrypt data at rest? • Does the product have a way to verify its data integrity? • Does the product share or sell its data to anyone?
Secure by Default	Insecure default settings expose asset owners to more risk and increase security costs.	• Has the manufacturer eliminated default passwords? • Are older insecure protocols disabled by default?

[1] https://go.dhs.gov/Ujv

As of April 2025

Element	Why This Matters	Questions I Should Ask
Secure Communication	Secure communication is necessary to ensure integrity and authenticity of the messages controlling critical infrastructure.	• 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?
Secure Controls	OT environments need safety systems and key control processes to keep people safe. Without security checks, these systems are easy and valuable targets.	• Does the product assume a malicious actor? • Can the product remain operationally normal during security scans?
Strong Authentication	Strong authentication allows for defense-in-depth and enables identity and access management best practices.	• Has the manufacturer eliminated, or is working to eliminate, the use of shared role-based passwords? • Is multifactor authentication (MFA) included in the baseline version?
Threat Modeling	Threat models are necessary for asset owners to understand the risk from a product and prioritize their security controls.	• 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?
Vulnerability Handling	Transparency of vulnerability handling is necessary for buyers to make informed decisions and for manufacturers to continuously improve their secure development practices.	• Has the manufacturer produced a software bill of materials? • Will security advisories be automatically retrievable according to the Common Security Advisory Framework (CSAF) standard? • Does the manufacturer have a coordinated vulnerability disclosure policy?
Upgrade and Patch Tooling	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 even in downtime windows. These patches also need to be easy for an operator to deploy themselves.	• Does the manufacturer test patches and report the results to (1) check for compatibility issues with software/firmware/binaries and (2) ensure the patches do not overwrite existing configurations? • Does the manufacturer update all software to modern operating systems if the underlying operating system is end-of-life? • Does the manufacturer publish product end-of-life dates? • Does the manufacturer allow the buyer to verify an update is authentic? • Are security patches available free of charge and disseminated securely?

Where can I go to obtain additional information or get help?

After reviewing the guidance document, CISA recommends that U.S.-based users engage with Sector Risk Management Agencies (https://www.cisa.gov/sector-risk-management-agencies) and regional Cybersecurity Advisors (https://www.cisa.gov/regions), who can provide further support regarding implementation. SRMAs and CSAs can provide guidance on individual procurement cycles, current and potential solutions, workflows, and relationships with third parties.

For additional information on CISA's Secure by Design work, visit https://www.cisa.gov/securebydesign. For information about CISA's role in OT and industrial control system security, visit https://www.cisa.gov/topics/industrial-control-systems.