CIS Critical Security Controls® v8.1

Industrial Control Systems (ICS) Guide

July 2024

Center for Internet Security®

CIS Controls™

Acknowledgments

CIS would like to thank the many security experts who volunteer their time and talent to support the CIS Controls® and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editors

Adam Boeckman
Bryan Ferguson
Kevin Klingbile
Justin Opatrny
Robin Regnier, CIS
Justin Young, CIS

Contributors

Ben Carter, CIS
Josh Franklin, CIS
Michael Wicks, CIS

Creative Commons License

July 2024

Contents

Overview

CIS Critical Security Controls

Appendix

Overview

Introduction

The CIS Critical Security Controls® (CIS Controls®) are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. They are developed by a community of information technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others. While the CIS Controls address the general practices that most enterprises should take to secure their systems, some operational environments may present unique requirements not addressed by the CIS Controls. CIS has expanded its efforts to include experts from the engineering Industrial Control Systems (ICS) and Operating Technology fields to provide the CIS Controls Industrial Control Systems (ICS) Guide.

The Center for Internet Security, Inc. (CIS) is a 501(c)(3) nonprofit organization whose mission is to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats.

For additional information, go to https://www.cisecurity.org/

ICS help run much of the world's critical infrastructure. ICS or some type of industrial automation is used and implemented in ways suited to the processes that are running or monitoring. Operational Technology (OT) primarily interacts with the physical world using hardware and software to control industrial equipment. OT teams maintain critical infrastructure and industrial environments. OT teams often rely heavily on vendor technologies, products, systems, and services. Many industrial control system vendor systems are designed and deployed using combinations of open and proprietary technologies and it is not uncommon for an ICS, once installed, to be accompanied with warranties and guarantees of that system's reliability and performance. These types of agreements are sometimes deemed critical by ICS asset owners since they help provide added assurance of the system's operational integrity, while they can also aid in cost-recovery associated with system downtime. ICS vendors often provide such agreements as a way to assume or offset aspects of risk as an automation and control system supplier to an asset owner. Such agreements are offered because the vendors conduct extensive engineering, testing, and validation of software and hardware combinations in these systems to help rule out potential compatibility and interoperability issues that may impact ICS operation. However, such agreements often place restrictions on ICS asset owners for what adjustments they can make to an ICS without voiding such a warranty. In some cases, even the addition of a simple security control to an ICS, or a minor configuration change, can void a warranty. Therefore, these agreements must be considered when determining how to best implement critical security controls to an ICS.

ICS environments may also have many embedded internet protocol (IP) connected devices. These devices often lack the capability to support traditional Information Technology (IT)-grade security control technologies since many run specialized firmware and Real-Time Operating Systems (RTOS), utilize proprietary protocols such as Profibus, Connection Oriented Transport Protocol (COTP), ThroughPacket (TPKT) Modbus, and EtherNet/IP, or do not have the capability to support contemporary endpoint or supplicant software that is commonly used in IT systems. Additionally, for ICS, the primary security focus tends towards ensuring operational integrity in the systems, rather than to data protection and privacy. Therefore, availability is a primary concern when developing a security program to address an enterprise's risk associated with its OT systems.

Consisting of a combination of routable and non-routable communication paths, ICS network architectures often differ from traditional IT environments. The overriding themes for applying security for ICS are segmentation and boundary control between the IT and OT domains, and best practice being segmentation within levels of ICS networks as well, with careful controls around local and remote connectivity to reduce attack vectors that threat actors can utilize to gain access to ICS networks.

Enterprises may look at each control as needing its own solution. However, one well-resourced solution may be able to account for multiple controls. Next Gen Firewalls are an example. In some cases, adding a software module license may be cheaper or more effective than implementing a separate solution to meet the same goal. It should be understood that traditional firewalls, Next Gen included, can be less effective if not ruggedized for some hostile ICS environments, and must be ICS protocol aware. That is, have the intelligence to fully dissect ICS specific protocols that are in use.

This Version of the Controls

CIS Controls version 8.1 (v8.1) is an iterative update to version 8.0. As part of our process to evolve the CIS Controls, we establish "design principles" that guide us through any minor or major updates to the document. Our design principles for this revision are context, clarity, and consistency. Context enhances the scope and practical applicability of Safeguards by incorporating specific examples and additional explanations. Clarity aligns with other major security frameworks to the extent practical, while preserving the unique features of the CIS Controls. Consistency maintains continuity for existing CIS Controls users, ensuring little to no change due to this update.

How to Use This Guide

In this document, we provide guidance on how to apply the security best practices found in CIS Controls Version 8.1 to ICS environments. For each top-level CIS Control, there is a brief discussion of how to interpret and apply the CIS Control in such environments, along with any unique considerations or differences from common IT environments. The applicability or not of specific Safeguards is addressed and additional steps needed in ICS environments are explained. Throughout this guide, we take into consideration the unique mission/business requirements found in ICS environments (with a focus on performance and real-time requirements), as well as the unique risks (vulnerabilities, threats, and consequences), which in turn drive the priority of the security requirements (e.g., availability, integrity, and confidentiality of process data).

By walking through CIS Controls Version 8.1 with this Companion guide, the reader should be able to tailor the CIS Controls in the context of a specific IT/OT enterprise as an essential starting point for a security improvement assessment and roadmap.

As part of CIS Controls v8.1, the Implementation Groups (IGs) are a guideline to help enterprises determine a starting point for implementation of the CIS Controls. Enterprises will, at times, find the need to implement CIS Safeguards in a higher IG. When integrating new technology into an environment, such as cloud, an enterprise should fully consider, and assess the security risks and impacts to assets and data; that understanding should drive the selection and implementation of appropriate CIS Safeguards regardless of IG.

Methodology

A consistent approach is needed for analyzing CIS Controls in the context of ICS. For each of the CIS Controls, the following information is provided:

- **ICS Applicability:** This assesses the degree to which a CIS Control and Safeguard functions or pertains to ICS.
- **ICS Challenges:** These are unique issues that make implementing any of the relevant CIS Controls, or associated Safeguards, for ICS difficult.
- **ICS Additional Discussion:** This is a general area for any guidance that also needs to be noted. For instance, relevant tools, products, or threat information that could be of use can be placed here.

If you have questions, comments, or have identified ways to improve this guide, please write us at controlsinfo@cisecurity.org.

CIS Critical Security Controls

CIS CONTROL 1

Inventory and Control of Enterprise Assets

Overview

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure, physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

ICS Applicability

The first CIS Control is considered to be the most important because it's necessary to first identify the systems and devices that need to be secured. CIS Control 1 is about taking inventory. Understanding and solving the asset inventory and device visibility problem is critical in managing an enterprise security program. This is especially challenging in ICS where network segmentation, dual-homing, and isolation are common themes. Mixtures of old and new devices from multiple vendors, lack of up-to-date network diagrams, unique industry, and application-specific protocols, some of which are not based on IP, and the difficulty in conducting physical inventories in dispersed or hostile environments compound these challenges.

ICS Challenges

The conventional approach of using ping responses, Transmission Control Protocol (TCP) SYN or ACK scans can also be problematic in ICS due to device sensitivity since even seemingly benign scanning employed in IT environments can disrupt communications, or in some cases even impact device operations. Methods that are more passive to locate connected assets are preferred, as they are less likely to impact system availability or interact with vendor systems in a manner that could cause warranty issues. Where practical, non-intrusive scanning methods should be leveraged including media access control (MAC) – address resolution protocol (ARP) tables, domain name system (DNS) records, active directory, or a variety of ICS-specific tools employed to control and collect data in these systems all for the purpose of locating the variety of connected assets.

ICS Additional Discussion

For this CIS Control consider the following additional steps:

- Consider the life cycle and acquisition costs; for example, National Institute of Standards and Technology (NIST®) 800-82r2: Component Lifetime. Typical IT components have a lifetime on the order of three to five years, with brevity due to the quick evolution of technology. For ICS, where technology has been developed for very specific use and implementation, the lifetime of the deployed technology is often 10 to 15 years and sometimes longer.

Ensure that all equipment acquisitions and system modifications contain cybersecurity language during the procurement process. Be sure to follow an approval process and ensure the technical drawings (if applicable, automated inventory systems) are updated at the time of the change.

Safeguards

Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Asset Type: Devices	Security Function: Identify	IG1 IG2 IG3

Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

Applicability

This is especially challenging in OT where network segmentation, dual-homing, and isolation are common themes.

These challenges are compounded by mixtures of old and new devices from multiple vendors, lack of up-to-date diagrams, unique industry, and application-specific protocols, some of which are not IP-based, and the difficulty in conducting physical inventories in dispersed or hostile environments.

OT systems are made up of multiple components, like most hardware. Components, firmware, etc., all have vulnerabilities, and can be attack vectors. Be aware of the supply chain of the hardware and components.

The life cycle of the components will have different time frames that will impact support for the components. Understand how the whole system is impacted if one component becomes obsolete or vulnerable.

In addition to mobile device management (MDM) options, use any existing management tools (e.g., Factory Talk Asset Centre) or other vendor equivalents as information sources.

There is a unique scenario within OT; many systems may exist on non-routed networks that are either more isolated or attached to devices that have a secondary connection to a routed network. While there are methods to gain visibility to these back-end networks, we should not miss the opportunity to include that a manual walk-down may be necessary to provide a full inventory.

Safeguard 1.2: Address Unauthorized Assets

Asset Type: Devices	Security Function: Respond	IG1 IG2 IG3

Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

Applicability

Ensure there is a process for how to specifically authorize a device to be added to the network, whether by a workforce member or vendor/integrator to ensure unexpected devices are detected.

While not easy, the OT environment is generally more conducive to a manual walk-down. The process may include having the workforce quickly but regularly check for unexpected devices when opening panels/enclosures.

Depending on the technology implemented, there may be multiple ways to address this. For instance, if a managed switch is in use, sticky MACs, port access control, or other measures may be available. Empty ports on switches should be disabled and only enabled when necessary. See CIS Controls 12 and 13.

If a next generation firewall (NGFW), intrusion detection system/intrusion protection system (IDS/IPS), security information and event management (SIEM), or other tool is monitoring the segment, and is capable of identifying traffic by device, it may be able to provide a report of devices. If those technologies are not an option at the source, determine if there is an upstream option, especially if a device attempts to talk outside the segment.

Device spoofing could be used to potentially defeat this Safeguard and potential mitigations for this should be investigated, but it provides another layer of security.

An enterprise may encourage the consideration of additional controls that can be met when acquiring or upgrading hardware or software.

Weekly review is a baseline recommendation. However, the needs of the OT environment may dictate the frequency.

Safeguard 1.3: Utilize an Active Discovery Tool

Asset Type: Devices	Security Function: Detect	IG2 IG3

Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.

Applicability

This Safeguard is relevant with the caveat that active discovery is done with purpose-built tools, designed to provide more due diligence, using known, in-use industrial protocols, with minimal additional traffic and precise timing of interactions. This is preferred over a less targeted approach which may generate high volumes of mostly extraneous traffic, and it will minimize potential disruption to OT devices. Such tools should be properly validated to ensure no OT disruption prior to moving into production.

Safeguard 1.4: Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory

Asset Type: Devices	Security Function: Identify	IG2 IG3

Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.

Applicability

For this Safeguard, DHCP may be less commonly used in the OT space. However, reserved IPs may be in use. Additionally, you may see this is in regard to industrial internet of things (IoT) use cases.

It would be more likely that static IP address is used so that traffic can be segmented, routed, inspected, and more controlled specific to the OT environment.

Safeguard 1.5: Use a Passive Asset Discovery Tool

Asset Type: Devices	Security Function: Detect	IG3

Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.

Applicability

For this Safeguard, ensure you are deploying engineering approved and ICS-specific controls that support the safety and reliability of operations.

Passive collection minimizes the potential for adverse events, as it only collects information already traversing the network. However, it is far less likely to have visibility of all devices, depending on placement and monitoring saturation, as the only information it directly collects is through packet collection and analysis.

If the device(s) is(are) communicating downstream and no data flows across the collection point, these inventory items will most likely be missing.

This can be addressed somewhat by compensating controls from other tools performing OT monitoring.

If traffic used by an active discovery tool is not able to traverse a certain point in the IT or OT network, a device may not be seen by an active discovery tool residing in another segment. Passive discovery, when used as a complimentary method of detection, may be able to discover additional devices as that traffic traverses past this point. One applicable example is an environment that employs a core switch that only routes North/South traffic through the firewall, but not East/West traffic.

Using both active and passive tools is a useful way to check one against the other to ensure detection of as many assets as possible.

CONTROL 2

Inventory and Control of Software Assets

Overview

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

ICS Applicability

This CIS Control offers steps needed to identify, track, and account for software and firmware used in the OT environment. Actively managing software can be a challenge in ICS. Much of the software is provided by vendors and is tied to specific hardware platforms. This software often has commercially available components that are also tied to the hardware.

ICS Challenges

Safeguards related to network isolation may be more challenging to implement or may not be possible.

Due to the network communication requirements of much ICS software, true isolation may not be possible.

Additionally, depending on original equipment manufacturer (OEM) vendor offering and support, for example, virtualization may not be supported. Instead, utilize transparent firewalls or subnet-wide segmentation to mitigate high-risk applications.

Using automated software inventory tools can pose a challenge in ICS. Many collection methods rely on active scanning or endpoint software. Large parts of ICS networks are comprised of devices sensitive to scan or unable to support endpoint software. Exercise caution when considering automated software inventory tools as these may cause stability issues on some systems.

For Safeguard(s) related to whitelisting, utilize application allowlisting technology only where feasible. Allowlisting can be manual for some systems; thinking of air gapped for instance. Only authorized administrators should be able to install authorized software. They can update the inventory during that process, if manual. Depending on system criticality, unauthorized software can cause alerts or can be blocked from executing on systems. If blocking, make sure operations has a method to bypass when/if needed as an emergency. For embedded devices that utilize firmware, leverage firmware signing (or something similar) if available.

ICS Additional Discussion

For this CIS Control consider the following additional steps:

- Ensure ICS manufacturers and vendors provide a list of recommended and supported software and versions that are required for each system.
- Consider upstream and downstream requirements prior to upgrade.
- Forecast operating systems and application life cycle cost in alignment with typical COTS (commercial off-the-shelf software) End of Life and End of Support (EoL/EoS) notifications.

Ensure cybersecurity requirements are a consideration within procurement/sourcing processes. Specifically, ensure vendors leverage a secure development life cycle.

Safeguards

Safeguard 2.1: Establish and Maintain a Software Inventory

Asset Type: Software	Security Function: Identify	IG1 IG2 IG3

Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, decommission date, and number of licenses. Review and update the software inventory bi-annually, or more frequently.

Applicability

When collecting a software inventory, it is important to assess all systems for software that may not have a license requiring purchase, as there will be no financial records associated with this software.

In an OT environment, it is possible the suggested list of software and component details may be difficult to obtain. Develop a strategy and process to capture details about any software presenting such challenges. At minimum, all deviations should be documented.

Safeguard 2.2: Ensure Authorized Software is Currently Supported

Asset Type: Software	Security Function: Identify	IG1 IG2 IG3

Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.

Applicability

This Safeguard's intent is to identify currently supported software that is authorized for use, and to document exceptions for unsupported software following the enterprise's established exception policy. Software, which is not on the current release, but is supported, is acceptable so long as no known security vulnerabilities exist. If any vulnerabilities exist in such software, they must be documented and a mitigation strategy should be developed if mitigation is possible. Determine and document the enterprise's acceptable risk, including risk associated with supported software that contains known security vulnerabilities.

It is important to note that often software is comprised of multiple other software components combined together. There may be instances where one piece of the overall software package becomes unsupported.

Some vendors may not patch their software, rather resolving vulnerabilities in the next release.

Safeguard 2.3: Address Unauthorized Software

Asset Type: Software	Security Function: Respond	IG1 IG2 IG3

Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.

Applicability

This Safeguard focuses on the exception process for when unauthorized software cannot be removed from a system, and an exception is necessary. The goals here are related to licensing issues and documentation of risk (documented exception and thus risk). The exception process has some characteristics that need to be determined; i.e., what is adequate due diligence for the approval process; can expired software licenses be renewed, and thus regain vendor support; how long is such a renewal valid; how does this impact the accepted enterprise risk, etc.

Safeguard 2.4: Utilize Automated Software Inventory Tools

Asset Type: Software	Security Function: Detect	IG2 IG3

Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.

Applicability

This Safeguard focuses on the exception process for when unauthorized software cannot be removed from a system and an exception is necessary. The exception process has some characteristics that need to be determined. Examples: How long is the approval process? Once expired, can it be renewed and for how long? etc.

An enterprise may have more than one automated solution. If multiple solutions are deployed, where possible utilize both solutions and compare for best results, and to identify gaps. Purpose-built OT tools may be required to adequately satisfy this Safeguard.

Safeguard 2.5: Allowlist Authorized Software

Asset Type: Software	Security Function: Protect	IG2 IG3

Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.

Applicability

Allowlisting may be difficult to implement in the OT environment by nature, as such tools are typically implemented on certain commercial operating systems that may not be relevant. Operating systems with an inherent limited ability to install additional software may also satisfy this Safeguard. OT environments are sometimes also reliant on third-party vendors which may deploy assets where this control is difficult to implement due to limited control of the asset. Every effort should be made to work with vendors to comply with this Safeguard, exceptions should be documented, and risk assessment should be performed. Depending on the operating system, some built-in controls can be leveraged.

Safeguard 2.6: Allowlist Authorized Libraries

Asset Type: Software	Security Function: Protect	IG2 IG3

Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, and .so files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.

Applicability

As with the previous Safeguard, allowlisting may be difficult to implement in the OT environment by nature, as such tools are typically implemented on certain commercial operating systems that may not be relevant. Operating systems with an inherent limited ability to install additional libraries may also satisfy this Safeguard. OT environments are sometimes also reliant on third-party vendors which may deploy assets where this Control is difficult to implement due to limited control of the asset. Every effort should be made to work with vendors to comply with this Safeguard, exceptions should be documented, and risk assessment should be performed. Depending on the operating system, some built-in controls can be leveraged. Solution agents can also be used, such as network access control (NAC) triggered via automated detection of unauthorized libraries running on the system; however, this may prove impractical.

If antivirus/anti-malware is in use, those may be able to detect an attempt to load libraries and prevent known insecure or malicious libraries from loading. Some libraries may also trigger a detection in behavioral detection systems.

Safeguard 2.7: Allowlist Authorized Scripts

Asset Type: Software	Security Function: Protect	IG3

Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, and .py files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

Applicability

As with the previous Safeguard, allowlisting may be difficult to implement in the OT environment by nature, as such tools are typically implemented on certain commercial operating systems that may not be relevant. Operating systems with an inherent limited ability to run scripts may also satisfy this Safeguard. OT environments are sometimes also reliant on third-party vendors which may deploy assets where this Control is difficult to implement due to limited control of the asset. Every effort should be made to work with vendors to comply with this Safeguard, exceptions should be documented, and risk assessment should be performed. Depending on the operating system, some built-in controls can be leveraged. Solution agents can also be used, such as NAC triggered via automated detection of unauthorized scripts running on the system; however, this may prove impractical.

If antivirus/anti-malware is in use, those may be able to detect the attempt to run scripts and prevent unauthorized scripts from running. Some scripts may also trigger a detection in behavioral detection systems.

CONTROL 3

Data Protection

Overview

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

ICS Applicability

This CIS Control's focus is on data protection and the relevance greatly varies based on ICS environment. These environments often do not contain much if any sensitive data in the traditional sense (PII, credit cards, etc.) In many ICS networks, control data consists of physical measurements such as flow, temperature, pressure, or valve readings and specific commands issued by logic control devices that control an overall process. This information is sometimes not deemed to be especially sensitive, or proprietary on its own, and, in some cases, it is absent of any particular protections in the way it is collected, transferred, stored, and analyzed. However, some enterprises consider this same information sensitive since it can indeed provide insights into an ICS design, connected products, proprietary process, production data, process variables, system schedules, configuration changes, and a bevy of other data that can provide significant intelligence to potential attackers.

ICS Challenges

For ICS environments that do contain sensitive data, all the Safeguards are applicable.

In some ICS environments information that is highly guarded and the ability to keep it confidential is key to business success. This is often seen in the manufacturing space where recipes or formulas are used to make foods or chemicals. It is a growing concern for critical infrastructure ICS because it is recognized that such data leakage can aid an attacker in developing a strategy.

What constitutes sensitive data is up to each enterprise to determine. If it is concluded that no sensitive data is present, then this Control becomes less important for an ICS environment but still should be addressed. However, such a conclusion is expected to be a very rare exception.

ICS Additional Discussion

Safeguards related to automated and scheduled scanning might adversely affect the reliability of the system. Only scan for sensitive data when it is safe to do so. Rather than scanning and introducing risk to safety and operations, it would be highly recommended to speak with and work with engineering staff to understand data repository locations etc.

Also, consider that encryption may not be feasible on all devices. For example, some embedded devices or network components may not be able to decrypt/encrypt data on removable media. Even when encrypted ICS protocols are available, they may add operational risk, new attack vectors, and will reduce visibility of OT traffic that is being pursued in many environments.

Consider establishing a means to passively capture data from ICS using a variety of tools such as sniffers, protocol anomaly detection tools, and to periodically evaluate traffic streams for data leakage that could lead to misuse or abuse by a would-be attacker.

Safeguards

Safeguard 3.1: Establish and Maintain a Data Management Process

Asset Type: Data	Security Function: Govern	IG1	IG2	IG3

Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, consideration is given to the OT environment; IT environment data management is addressed in the standard CIS Controls. There can be many storage locations, legal or regulatory considerations, and production schedules may be different per department, all of which can affect this data management process. ICS vendors may need to be involved in data management, and possibly managing these systems entirely. The inventory of ICS data may be more challenging as there may be gaps in the data inventory. Understanding where data exists, especially sensitive data, is important. Note that ICS data may also exist on the IT network examples being engineering system design documents, “as built” documents, ladder logic, control device configurations.

Safeguard 3.2: Establish and Maintain a Data Inventory

Asset Type: Data	Security Function: Identify	IG1	IG2	IG3

Establish and maintain a data inventory based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.

Applicability

For this Safeguard, the inventory of data in the OT environment may be more challenging as there may be gaps in the data inventory. Understanding where all data resides, backups and/or replicas are examples. Data sources that may be overlooked include support and maintenance related email, volume shadow copies, email archive and storage files, data archives, system snapshots, restore points, cache, etc. Encryption may create additional challenges due to lack of visibility into such data. Consider a data inventory that extends beyond just sensitive data, including RAW data from the OT environment.

Safeguard 3.3: Configure Data Access Control Lists

Asset Type: Data	Security Function: Protect	IG1	IG2	IG3

Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.

Applicability

For this Safeguard, not all OT components may have this level of configurability/options. It is important to follow proper access control when onboarding and off-boarding, as well as transfers for data access control lists. If groups are used for access control, understanding inheritance can be important. Consider group policy/active directory challenges faced by the users at point of process (i.e., users on the factory floor), remote access to lock to a machine vs individual, long-term storage vs real time, access control list (ACL) around environment to collect info. Such methods may be most feasible at data aggregation points, such as at an application server, or via database access roles. Consider a requirement the ICS/OT network has it's own, Active Directory / Domain(s), separated out from IT, with no-trust relationships with IT's Active Directory and Domains.

Safeguard 3.4: Enforce Data Retention

Asset Type: Data	Security Function: Protect	IG1	IG2	IG3

Retain data according to the enterprise's documented data management process. Data retention must include both minimum and maximum timelines.

Applicability

For this Safeguard, in ICS it is key to understand retention schedules, hesitancy to delete, capability of a system to enforce a schedule, legal and regulatory requirements, legacy systems, and who is responsible for retention compliance in a non-automated environment. OT and IT should be aware of the process and timelines to limit challenges.

Safeguard 3.5: Securely Dispose of Data

Asset Type: Data	Security Function: Protect	IG1	IG2	IG3

Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.

Applicability

For this Safeguard, be aware of the different data destruction methods for varying types of storage. Methods can differ depending on the hardware in use and whether data is stored on premises or in the cloud. Terminology in this area can be confusing as there are different terms used (e.g., sanitize, overwrite, shred (file level or disk?), erase, wipe, destroy). Consider embedded devices, external storage cards, whether a service was used (confirmation being done and perhaps described via contract), enterprise data management. Is the data stored in multiple locations?

Safeguard 3.6: Encrypt Data on End-User Devices

Asset Type: Data	Security Function: Protect	IG1	IG2	IG3

Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

Applicability

End-User Devices per CIS Controls v8.1 glossary: Information technology (IT) assets used among members of an enterprise during work, off-hours, or any other purpose. End-user devices include mobile and portable devices such as laptops, smartphones and tablets, as well as desktops and workstations. For the purpose of this document, end-user devices are a subset of enterprise assets.

For this Safeguard, far less efficacy as many OT devices do not have this level of capability. OT focus would appear more towards transient devices (e.g., vendor or engineer laptops) and storage device. Encrypted storage drives may not work correctly with OT devices.

Safeguard 3.7: Establish and Maintain a Data Classification Scheme

Asset Type: Data	Security Function: Identify	IG2	IG3

Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as “Sensitive,” “Confidential,” and “Public,” and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, consider when working with vendors, contractors, partners, etc., that the classification terms, criticality of data used for real-time decisions, and CIA triad effectiveness, with safety being first in an ICS environment is understood, should be understood fully by all involved.

Safeguard 3.8: Document Data Flows

Asset Type: Data	Security Function: Identify	IG2 IG3

Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, if a workforce member, contractor, or any system sending data is compromised, knowing data flows and location can shorten the time required to determine the breadth of the compromise. Data flow considerations should also be considered when data is sent to a cloud instance or to a third party. Data classifications, volumes, dependences, criticality, are all elements needed on top of knowing a data flow exists.

If one vendor is used for multiple solutions, (e.g., object or resource reuse may occur in a vendor's cloud tenant) ensure the vendor uses best practice cloud practices to properly secure and separate data from other clients. Intrusion detection being more difficult due to industrial protocols, finding what is not normal is a way to find unusual, unexpected, and/or potentially malicious traffic. It is useful to understand and document how data gets from field devices through control up to the supervisory control and data acquisition layer and beyond. Consider methods to identify document flows for any sensitive information that might not have traditional enterprise data classification.

Safeguard 3.9: Encrypt Data on Removable Media

Asset Type: Data	Security Function: Protect	IG2 IG3

Encrypt data on removable media.

Applicability

For this Safeguard, transient removable media can be connected, utilized, and then detached. Transient removable media can be a necessity in the industrial space (e.g., lack of network connectivity, the way the OT device functions, OT device lacking encryption support for encrypted drives, speed of deployment, etc.). With encryption primarily concerned with the confidentiality protection of the device and information, this may be more useful for when data is leaving the environment and reducing the risk of it doing so in the clear. However, the risk is typically more due to the fact of having to use that device in the industrial space, especially given that many OT devices do not support encrypted removable devices.

It is recommended there be a process/procedure for using transient removable devices when necessary (i.e., having a malware scanning process if external drives are permissible, or a copy process where data is migrated to a trusted drive - e.g., red (untrusted) drive has to have data scanned and transferred to green (trusted) drive, etc.).

Safeguard 3.10: Encrypt Sensitive Data in Transit

Asset Type: Data	Security Function: Protect	IG2 IG3

Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

Applicability

For this Safeguard, where applicable and possible encrypt sensitive data if it is leaving. In ICS, most protocols do not support encryption. Consider if encapsulating protocols might work for this Safeguard. Systems/device administration should be considered sensitive and treated accordingly. Some environments may not benefit from in transit encryptions as much due to the nature of the environments, i.e. air-gapped or non-internet connected.

Safeguard 3.11: Encrypt Sensitive Data at Rest

Asset Type: Data	Security Function: Protect	IG2 IG3

Encrypt sensitive data at rest on servers, applications, and databases. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

Applicability

For this Safeguard, where applicable and possible, encryption of the data at rest should be used. Considerations could include an approach from the disposal side (i.e., during a hardware refresh), third parties that store data externally, historical data that is written and stored, databases accessing other databases, and ensuring the encryption of sensitive data. There may be other compensating controls available.

Consider prioritizing the data historians on the IT (i.e., read-only or replica data historians for example). Historians, backup environments, secondary systems leveraging process data, and log aggregators.

Safeguard 3.12: Segment Data Processing and Storage Based on Sensitivity

Asset Type: Data	Security Function: Protect	IG2	IG3

Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.

Applicability

For this Safeguard, this can become difficult in environments that are utilizing shared services and common storage environments. In the cloud, subscriptions and resource groups become important. As each environment is segmented, costs for cloud resources will scale with that. In some cases, it may exceed any cost savings associated with utilizing cloud services. Understanding the full system architecture is important in the planning phase so that costs do not grow out of scope as shared resources are converted to isolated resources. In some cases, where there is a comparison of costs between on-premises versus cloud, this may become critical. If under specific regulation, it may be necessary to have physically separate environments. It is possible security controls within a virtual environment, in combination with proper architecture, could make shared processing and storage environments more feasible and acceptable.

Safeguard 3.13: Deploy a Data Loss Prevention Solution

Asset Type: Data	Security Function: Protect	IG3

Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's data inventory.

Applicability

For this Safeguard, it might be necessary to update or modify the data loss prevention (DLP) tool to align with the OT environment. Consider focusing on Data historian on IT networks or ICS DMZ-read-only data historians and/or main hists inside ICS networks.

Safeguard 3.14: Log Sensitive Data Access

Asset Type: Data	Security Function: Detect	IG3

Log sensitive data access, including modification and disposal.

Applicability

For this Safeguard, enterprises need to understand where logging occurs. Scoping logging to fit the available technology and needs of the environment will be important. Don't assume that the logging data set is the correct data set. Logging too much data can be as big a problem as logging too little. Logging can instill a false sense of security if it goes to a SIEM, which is expected to correlate and alert if something is triggered. However, if not configured and tuned correctly, such tools can miss significant events, or create too many false positives/negatives, potentially creating inattentiveness and alert fatigue in those who monitor. If a SIEM is used for this, ensure all sources are accounted for. If a system is isolated, as OT systems may be, evaluate what options may be available to collect such logs. On the server side there may be more options; traditional OT devices may be limited in logging ability. However, OT devices may not have enough sensitive data to require immediate focus.

CONTROL 4

Secure Configuration of Enterprise Assets and Software

Overview

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

ICS Applicability

This CIS Control addresses the need to manage the configuration of network-connected devices using a change control process.

For additional context, we can more accurately reflect this Control in relation to OT: Establish and maintain the secure configuration of OT assets (end-user devices, including portable and mobile); OT devices (programmable logic controllers (PLCs), human machine interfaces (HMIs), engineering workstations); servers; network and security devices; and non-computing/Internet of Things (IoT) devices and software (operating systems and applications).

ICS Challenges

There is no single established standard or approach to doing secure configuration activities within an enterprise that require additional production OT-related considerations above those that occur on the enterprise side of the enterprise. The enterprise needs defined areas of responsibility whether there is a single team that manages all OT systems or whether the responsibility is split amongst multiple teams. This brings clarity to who will be developing, testing, and implementing the secure configuration activities. It is likely this will include IT and OT working together to develop a risk-informed secure configuration for the various device types/use-cases throughout the ICS environment. There needs to be a process to ensure proper application and monitoring of these activities.

Not all OT devices have the same secure configuration capabilities. For legacy OT devices that are insecure-by-default (meaning there are very few or no options for secure configuration, with the main vulnerability being access to the device), the secure configuration implementation is likely around placement within and access control to/from the device (not configuration of the device itself). For these types of devices, there should be an obsolescence program to ensure the enterprise moves towards devices with more secure configuration options.

For OT devices capable of a more secure configuration, develop a secure baseline configuration to meet the enterprise's risk needs. If centralized management is feasible, this provides for a more consistent method to develop, apply, and monitor these configurations. The enterprise needs to ensure the necessary, trained people have access to do these centralized activities. For those devices that do not offer centralized management (or if the enterprise does not authorize its use), methods such as baseline configuration and scripts may be helpful in applying the changes.

ICS Additional Discussion

For this CIS Control consider the following additional steps:

- Ensure firewalls are configured with a set of least privilege rules and denies other traffic by default (secure configuration should not be the first line of defense).
- If a location is not staffed or if critical process data flows through a perimeter device, ensure redundancy exists or device failure won't prevent this data from being received by its intended destination.

Portable end-user devices are uncommon in the OT environment; however, this is expected to evolve over time as Industry 4.0 pivots toward integration of new technologies in support of bringing modern technologies into OT environments and the "plant floor."

Safeguards

Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a documented secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, having a process to develop, manage, and monitor secure baselines helps ensure consistent configuration and deployment of assets. In ICS, some embedded devices may have no ability to change default behavior or may have limited configuration options. Document such systems and review software and firmware releases for updates that may add these features.

There should be a capability to evaluate configuration compliance periodically. Periodically means at least annually but certain types of devices or automation may allow this to be more frequent. Evaluate management and monitoring systems to ensure they can alert when there is a change to configuration. If the capability for assigning criticality exists, ensure it is configured and tested.

Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a documented secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, having a process to develop, manage, and monitor secure baselines helps ensure consistent configuration and deployment of networking and security infrastructure assets. These devices typically have many configuration items, making a standardized process even more important. Management, whether centralized or decentralized to individual locations, will require consideration. This should include additional architecture-related standards/requirements (e.g., industrial and non-industrial devices should not co-mingle on the same network and security infrastructure).

Safeguard 4.3: Configure Automatic Session Locking on Enterprise Assets

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.

Applicability

For this Safeguard, automatic session locking has the potential to impact the industrial process negatively if applied without sufficient consideration. Some systems may not support this option or be in an environment not conducive to frequently supplying credentials. This is a risk-based decision. There should be policies and procedures to ensure this does not lead to other insecure behaviors (e.g., posting the username/password on or near the device).

Other options may exist for securing systems' access (e.g., placing vulnerable systems in an access-controlled room), or using an alternative authentication method (e.g., badge or token).

Consider efficiency and impact depending on the system being configured for session locking. Tablets and smartphones, while not in wide adoption within the OT environment as of this writing, typically have robust authentication methods. However, by being transient they may be problematic if proper session locking is not enabled; such devices are easily misplaced or removed from secure locations. Laptops in use in OT environments, being transient as well, may need conventional automatic session locking enabled.

Safeguard 4.4: Implement and Manage a Firewall on Servers

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.

Applicability

For this Safeguard, being primarily systems with defined communication needs, this may be quite feasible in an OT environment. However, vendors may have insufficient documentation on necessary traffic flows, requiring the enterprise to expend effort determining, developing, and testing host firewall rules.

Asset criticality and systems architecture are key for this Safeguard. Host firewalls may be more critical in situations where data does not flow through a hardware firewall device. However, it is recommended to always enable host firewall if practical in whitelisting mode and alerting to reduce false positives would be safer until such time the control system traffic patterns we very well understood and known to not impede operations.

Safeguard 4.5: Implement and Manage a Firewall on End-User Devices

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Applicability

For this Safeguard, this may be only feasible on a subset of devices in an OT environment. Many ICS devices do not have this capability. Vendors may have insufficient documentation on necessary traffic flows, requiring the enterprise to expend effort determining, developing, and testing host firewall rules. Centralized management, if available, will help ensure consistent management of any host-based firewall capability.

Host firewalls on end-user devices limit attack surface of devices which may be most vulnerable to attack due to commodity operating systems, many software installations, or general portability of the device.

Safeguard 4.6: Securely Manage Enterprise Assets and Software

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.

Applicability

For this Safeguard, many ICS devices may use insecure-by-default or known insecure communications and management protocols. This may require special consideration of who and how people access these device management interfaces.

Secure management of network and security infrastructure should be a requirement. Traditional server infrastructure would likely be able to leverage more secure methods, and potentially alternatives to minimize potential exposure of credentials and configurations.

Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.

Applicability

For this Safeguard, in an ICS environment it is generally feasible for many assets. Configuration options will vary in respect to centralized versus individual management and should follow the processes set forth above.

For assets that do not permit changes to these credentials, monitor use of these default credentials. Document processes and exceptions associated with these assets and review periodically.

Safeguard 4.8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software

Asset Type: Devices	Security Function: Protect	IG2 IG3

Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

Applicability

For this Safeguard, this is most feasible on servers and many transient assets. Being part of an engineered system, many OT assets are unlikely to have extraneous services and software. However, such assets must be reviewed for confirmation. Extraneous services and software unable to be disabled or uninstalled should be documented.

Part of the difficulty of implementing this Safeguard in an OT environment is vendors may have insufficient documentation to articulate how their systems function. This Safeguard should be applied to such assets, if possible, including any traditional server or client systems.

This may be partially feasible on ICS devices that have limited configuration options (e.g., a PLC may not have additional services or software needing to be disabled). Field devices such as a drive, whether connected through Ethernet or another fieldbus, may have very few configuration parameters available.

There are also assets acquired or purchased through another vendor providing needed functionality (e.g., turbine generator power controls). Install, rigorously test, and validate these assets to work at a certain configuration level. While there are cases where any changes to the approved configurations may potentially void warranty, work directly with the vendor to determine if it is really a warranty issue, their preference, or an actual regulatory or certification requirement.

Safeguard 4.9: Configure Trusted DNS Servers on Enterprise Assets

Asset Type: Devices	Security Function: Protect	IG2 IG3

Configure trusted DNS servers on network infrastructure. Example implementations include configuring network devices to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

Applicability

For this Safeguard, assets using DNS should be configured to utilize trusted DNS servers. There may be instances where managing a HOSTS file is preferable to manage versus a DNS deployment and the associated DNS dependencies or related potential issues. It is highly unlikely an enterprise will be using an externally available DNS server, and any such use should be scrutinized.

There are times where vendors/original equipment manufacturers (OEMs) pre-configure devices with externally available DNS servers, but a procurement, Factory Acceptance Test (FAT), or Site Acceptance Test (SAT) assessment should catch this before commissioning, and log review for already in-service devices can help surface these cases.

Safeguard 4.10: Enforce Automatic Device Lockout on Portable End-User Devices

Asset Type: Devices	Security Function: Protect	IG2 IG3

Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.

Applicability

For this Safeguard, portable devices are currently uncommon in the OT environment; however, that will likely continue to change as Industry 4.0 pushes more “connected worker” and “digital transformation” activities to collect data and bring new capabilities to the plant floor.

These portable devices may not actually be considered part of the industrial process and may, or may not, live co-mingled with OT assets. As these are transient devices, the need for this Safeguard depends on a lot of variables. Having some type of lockout threshold whenever possible helps ensure only authorized people have access.

Safeguard 4.11: Enforce Remote Wipe Capability on Portable End-User Devices

Asset Type: Data	Security Function: Protect	IG2	IG3

Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.

Applicability

These portable devices may not actually be considered part of the industrial process and may, or may not, live co-mingled with OT assets. As these are transient devices, the need for this Safeguard depends on a lot of variables. It may be desirable to have this functionality if the device leaves the facility or is stolen.

Safeguard 4.12: Separate Enterprise Workspaces on Mobile End-User Devices

Asset Type: Data	Security Function: Protect	IG3

Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.

Applicability

For this Safeguard, these devices may not actually be considered part of the industrial process and may or may not live co-mingled with other OT assets. A determination should be made whether a separate workspace or application containerization is most beneficial on these devices. Both options are valid. This need is dependent on the device risk profile.

Bring your own devices (BYOD) in the OT industry are not typical; mobile devices are typically dedicated enterprise owned to help ensure security. However, if an enterprise does allow BYOD devices into the OT environment this Safeguard should be implemented.

CONTROL 5

Account Management

Overview

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

ICS Applicability

Internet of Things (IoT) devices can play a large role in the ICS environment. ICS IoT devices will have a series of accounts already created and in use when the device is purchased and shipped. Account management is applicable to the mobile applications, devices, and cloud platforms all used for IoT. Additionally, enterprises and potentially individual users may also create new accounts. All of these accounts need to be actively managed. It is uncommon for IoT devices to feature dedicated administrative accounts that are separate from user accounts for managing IoT devices. In some situations, especially with enterprise or consumer-grade IoT devices, control or pseudo-administrative access can be obtained through management applications on mobile devices. These devices tend to come out of the box with default settings that should be updated for the functionality for OT environments while ensuring hardening practical for ICS/OT standards.

This CIS Control emphasizes the importance of controlling user access to systems in a typical network environment and ensuring effective account management. A common vulnerability can arise if employee accounts are not closed when employees leave the enterprise or change roles. ICS can be equally, if not more, challenging because they often contain systems from different vendors, each with their own user account directories and often an inconsistent set of individuals that may interact with a system. Additionally, remote and on-premises contractors and OEM technicians often request or require access either locally or remotely. These factors can make managing user accounts difficult for many OT teams, especially over a period of time given competing priorities for systems to be operating in a productive state versus being idle for service and maintenance.

While these factors can make user account control difficult, care must be taken not to inadvertently terminate or prevent a legitimate user from having the appropriate access as this might cause process disruption or delay. Furthermore, a balance must be considered and carefully managed between administrator-only account privileges versus group level privileges. Given the 24x7x365 operation of many ICS systems, incidents can occur at any time, including during a time when there is an absence of those with administrative privileges available to respond, remediate, and recover.

Thorough implementations of CIS Control 5 and Control 6 involve written policies addressing these areas before devices are provided to users.

ICS Challenges

When evaluating IoT components for use in the enterprise, investigate the supported features associated with administrative accounts. This should include the type of authentication credentials and protocols supported by the device and its associated ecosystem. This will most likely include passwords and the strength of the authentication implementation. For administrator accounts, attempt to ensure that at a minimum, strong password requirements are used and account access is audited.

Administrators should be extremely careful when first working with a completely unmanaged device. Some IoT devices are beginning to support some form of Enterprise Mobility Management (EMM) or Unified Endpoint Management (UEM). These technologies allow specific policies and configurations to be sent to an IoT device. General administrative activities can also be performed, such as restarts and diagnosing problems. Administrative accounts can be set up for each device, with credentials managed through that technology portal. Be aware that wireless remote access can be an option that needs to be vetted.

Safeguards related to account expiration, inactivity lockouts, and multi-factor authentication are applicable to ICS systems. Limitations in the firmware and software often prevent complete coverage and the risk(s) created should be tracked.

ICS Additional Discussion

Many IoT devices are deployed in insecure areas (e.g., roadside units, or RSUs, in the transportation sector). These devices are sometimes deployed with shared accounts that are used by technicians to manage the devices. Consider alternative methods for restricting administrative access to these types of devices. For legacy devices without privileged access capability, a compensating control may need be applied, such as additional physical security. Newly designed IoT devices and subsystems should integrate use of this Control.

Attackers may attempt to obtain administrator rights to IoT devices via operating system (OS) or firmware level vulnerabilities so they can hide themselves from the user. This entire Control is difficult to enforce on a rooted device that has its security architecture broken. Although this security architecture bypass may provide a user with root access, they often have default administrator credentials that do not frequently change. To the extent practical in IoT, multi-factor authentication (MFA) should always be used. With that said, the overall goal would be to implement authentication solutions that prevent credential theft. This more abstract goal supports PKI, WebAuthn, and MFA solutions that might only be a password and PIN, which is not preferable to the first two options.

For this CIS Control consider the following additional steps:

- Use shared accounts and passwords only when necessary.
- Establish and follow a process for changing shared account passwords immediately upon termination of any workforce member knowing the credentials.
- Restrict shared operator account permissions to limit system access and changes.
- Where possible, eliminate ICS applications leveraging clear text authentication or basic security authentication. Where not possible, use unique credential sets and monitor for their attempted usage elsewhere.
- Consider access control chain-of-command plans for periods of time when normal personnel with required privileges may not be available.

Consider monitoring the use of all accounts, automatically locking machines that are not used for process monitoring, or control after a standard period of inactivity.

Where possible, implement the CIS Password Policy Guide detailing key recommendations. It is important to require the use of long (14+) passwords or passphrases that are not easily guessed. Length over complexity makes current password cracking methods less effective and allows for users to more easily remember their passwords, reducing the chances of OT members not being able to log in, and the administrative overhead of resetting passwords.

In ICS environments, account access requirements are defined by job duties. Account access should be reviewed when personnel change roles, transfer, or are separated from the enterprise. Enterprises should define a review schedule to verify that staff personnel are matched with the correct system access. Recommend at least annual reviews.

- Establish a process for periodic privilege reviews to validate that the necessary level of access, no less or no more than required, is in place for personnel and that said privileges match required duties, level of trust, and empowerment appropriate for said personnel.

Safeguards

Safeguard 5.1: Establish and Maintain an Inventory of Accounts

Asset Type: Users	Security Function: Identify	IG1 IG2 IG3

Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must at a minimum include user, administrator accounts, and service accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Applicability

For this Safeguard, in the OT environment shared accounts may exist but should be eliminated where possible, and documented specifically as a shared account with rationale if they cannot be eliminated. It is also recommended to maintain a list of individuals with access to any shared accounts, as well as usage logs for potential cross-reference. Document and track all known default and shared accounts as well as who has access to them.

Safeguard 5.2: Use Unique Passwords

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.

Applicability

For this Safeguard, there may be an ICS device that does not support passwords. In this case, a policy/procedure will be needed. Securing physical access to the device may be the preferred option in such cases. If there are differing policies for administrative vs non-administrative accounts, service accounts, etc., those should be documented as well. Risk associated with these policies and procedures should be tracked.

Safeguard 5.3: Disable Dormant Accounts

Asset Type: Users	Security Function: Protect	IG1	IG2	IG3

Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.

Applicability

For this Safeguard, emergency (i.e., break glass) accounts may be exempt.

Use caution on this as there very well could be accounts required that are not used within 45 days, but are used and required thereafter. This will require site specific settings - engineering needs to be engaged here and in some cases ICS/OT vendors. Do Not Disable until engineering staff advise on this.

There may be accounts that only get used during emergency operations or troubleshooting, deleting or disabling the accounts my inhibit restoration / recovery of operations.

Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts

Asset Type: Users	Security Function: Protect	IG1	IG2	IG3

Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

Applicability

For this Safeguard, consider what accounts are in scope for the Safeguard and what account types might be out of scope (i.e., role-based access control (RBAC) may not always be available). It is not common for workstations on an OT network to have internet access. If internet access is required, it should be done from a user's regular workstation outside of the ICS environment.

Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts

Asset Type: Users	Security Function: Identify	IG2 IG3

Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Applicability

For this Safeguard, the OT environment uses a lot of service accounts that likely fall under "shared accounts" as discussed in 5.1. An example would be moving control data between different systems. Consider what accounts are in scope for the Safeguard and what accounts are out of scope. Where possible, service accounts should not be used for any interactive systems access.

Safeguard 5.6: Centralize Account Management

Asset Type: Users	Security Function: Govern	IG2 IG3

Centralize account management through a directory or identity service.

Applicability

For this Safeguard, consider centralization to improve consistency and account management. The enterprise should consider applicable risks of centralization; avoid comingling enterprise and OT accounts. Document and assess decentralized account management processes and systems, such as stand-alone systems which cannot be managed centrally.

CONTROL 6

Access Control Management

Overview

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

ICS Applicability

OT devices may require access management but are often not integrated into traditional directory services for user management. This is due to the fact that software is often used to access a device interface, or there is no user account needed to interact with the device. Access Control Management is meant to manage how a user accesses a device all the way through revoking access credentials and privileges. Thorough implementations of CIS Control 5 and Control 6 involve written policies addressing these areas before devices are provided to users.

ICS Challenges

Realistically, it will not be possible to manage all accounts on a device or manage all accounts on all devices from a singular location. There needs to be a risk-based determination if using the user access control methods on OT devices is feasible, necessary, or useful. The accounts may not be properly documented upon receipt of a device, although obtaining a thorough inventory of identifiable accounts is important.

Safeguards related to the use of multi-factor authentication (MFA) may be possible for crossing boundaries but may not be possible with the internal ICS environment.

Safeguards related to the use of automated tools that alert when new users are added may not be applicable.

Safeguards related to the use of dedicated machines or the use of isolation for administrator machines may not be applicable.

When inventorying all administrative accounts, automated tools are not required and should only be used if known to not impact system availability. Typically account validation is performed by a system owner as opposed to a senior executive.

ICS Additional Discussion

Registering devices within an enterprise directory system such as Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) may be a valid method for restricting access and for effectively monitoring who has authenticated to the devices. However, this is only applicable for those devices that can be configured for AD. Enterprises should ensure that ICS implementation plans include strategies for authentication and monitoring the accounts used to access devices. This data should then be fed back to the SIEM for monitoring and control when ICS devices are incorporated into the enterprise network. Administrators should regularly review user accounts on all systems utilized by the enterprise. Privileges should be adjusted accordingly on a regular basis with over-privileged users addressed and accounts deactivated when necessary.

Legacy ICS systems with stand-alone consolidating or command and control hosts should leverage system tools, augmenting them with manual recording and audit processes as required, to enable this Control. Cloud-based applications supported by the enterprise should be monitored and have their credentials disabled during employee separation. Enterprise ICS applications should be analyzed and reviewed for proper authentication techniques. Special attention should be paid to areas where integration occurs between third-party services and where identities are federated. Logging should be enabled within back-end management services to monitor activity, with the logs regularly reviewed.

Follow the Principle of Least Privilege by minimizing the use of elevated privileges and only using administrative accounts where they are required.

Physical network segmentation has a greater capability to safeguard communications using access control and isolating communications.

Safeguards

Safeguard 6.1: Establish an Access Granting Process

Asset Type: Documentation	Security Function: Govern	IG1	IG2	IG3

Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user.

Applicability

For this Safeguard, many devices may not be tied to a central authentication system and instead use local accounts. This adds an extra layer of effort but should be done. Level of access is all encompassing. This process should also include remote access into the environment.

Safeguard 6.2: Establish an Access Revoking Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

Applicability

For this Safeguard, many devices may not be tied to a central authentication system and instead use local accounts. This adds an extra layer of effort but should be done. Level of access is all encompassing. Any shared accounts will need special consideration such as a password change in lieu of disabling the account. This process should also include remote access into the environment.

Safeguard 6.3: Require MFA for Externally-Exposed Applications

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

Applicability

For this Safeguard, some OT networks have external exposure. However, there are situations for external exposure where MFA may not be possible. Every effort should be made to enable MFA, potentially leveraging multiple tools to add the MFA access layer. An example would be requiring MFA on jump boxes in the OT environment. There is potential for jump box access via externally accessible virtual private networks (VPN). MFA is recommended for VPN. However, accessing a jump box requiring additional credentials over VPN could represent MFA.

Safeguard 6.4: Require MFA for Remote Network Access

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Require MFA for remote network access.

Applicability

For this Safeguard, in OT environments this is a commonly accepted recommendation for accessing the protected environments through something like a VPN. Make use of jump boxes to potentially assist where MFA is not directly supported.

Safeguard 6.5: Require MFA for Administrative Access

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a service provider.

Applicability

For this Safeguard, in OT environments this is commonly accepted. However, more isolated environments may not have or would require a separate MFA instance to operate. For administrative access, follow commonly accepted policies at a minimum. MFA should be leveraged for initial access into the environment where supported, regardless of the level of access granted.

Safeguard 6.6: Establish and Maintain an Inventory of Authentication and Authorization Systems

Asset Type: Software	Security Function: Identify	IG2 IG3

Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.

Applicability

For this Safeguard, in an ICS environment there will be multiple authentication systems (e.g., directory and local) in any given environment. Central management can reduce the number of authentication systems and services needed, and potentially reduce maintenance needs. There could potentially be devices that only support local authentication capabilities. Full understanding and documentation of local versus centralized accounts is valuable.

Safeguard 6.7: Centralize Access Control

Asset Type: Users	Security Function: Protect	IG2 IG3

Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.

Applicability

For this Safeguard, in an OT environment many assets may not support centralized access control. It is not recommended to use combined corporate and industrial access control. Typically, industrial sites have their own directory which may be applicable to a specific network or specific set of assets within a network. There could be multiple directory services within the same plant to manage. If an ICS system can be physically separated, except for centralizing the access control, it might be preferable for the asset to be left physically separated; this removes the risk of compromise via the centralized directory. This should be evaluated on a case-by-case basis and documented.

Safeguard 6.8: Define and Maintain Role-Based Access Control

Asset Type: Users	Security Function: Govern	IG3

Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

Applicability

For this Safeguard, administrator accounts frequently run automated processes in OT environments. Not all systems have RBAC capability. Shared accounts and legacy or "heritage" assets should be considered in this context.

CONTROL 7

Continuous Vulnerability Management

Overview

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

ICS Applicability

This CIS Control addresses the need for continuous vulnerability management, which can be a significant task in most enterprises. Understanding and managing vulnerabilities is just as challenging to an ICS environment as it is to traditional IT systems. One advantage the ICS has in this arena is that these systems typically reside farther into a business's network layers making it harder for external threat actors to reach and exploit new vulnerabilities without first telegraphing some presence inside the system when monitoring is in place.

However, the required up-time on ICS means that the service and maintenance windows where updates can be applied are limited and sometimes months (or years) apart. Additionally, differences in ICS life cycle and vendor support can overlap with software obsolescence, causing periods where no updates exist. These scenarios should be identified as part of the vulnerability scanning control and mitigations or upgrade plans should be put into place.

Safeguards(s) related to automated scanning and patching may not be applicable in the ICS environment.

ICS Challenges

Actively scanning a production ICS system without prior testing is risky. As a priority over active scanning, passive analysis of network traffic to help determine software hardware versions, firmware, and related vulnerabilities. Consider taking advantage of maintenance and failover testing periods.

While enterprises might have an IT focused vulnerability management program there needs to be a separate process and considerations when developing an equivalent program for OT.

ICS Additional Discussion

Caution should be exercised if performing active vulnerablity scanning as it can adversely affect ICS network communications and in turn product and system availability. There are several reasons for caution, including network stack sensitivity, limited resources, or other situational factors. When considering an active scanning approach, identify the necessary elements to include in the scan or choose a vulnerability detection platform that is built to operate in an OT environment. Scanning should only take place during process outages such as regularly scheduled maintenance or during planned shutdowns. Furthermore, steps should be taken (example: reboot or restart critical services) to ensure there are no unintended side effects.

Ensure that tools do not automatically deploy software. These tools should report and identify where security updates are needed but allow the appropriate teams to include OT to evaluate and to deploy updates when it is safe to do so.

For this CIS Control consider the following additional steps:

- Utilize passive monitoring tools that identify a specific device and software version and correlate that to known vulnerabilities.
- Ask your OEM for vulnerability notifications relating to the products you utilize and/or have in service.
- Consider using additional information or context from your information sharing and analysis center (ISAC) or information sharing and analysis organization (ISAO) and/or OEM vulnerability reporting service to identify all known vulnerabilities on the enterprise's ICS.
- Operating system and application updates, security patches, and service packs need to be properly regression tested to ensure that availability and reliability of the system will not be adversely affected. Where possible, have any OEM regression test completed prior to OT team testing.

Create a test bed that mimics a production environment for specific patch regression testing prior to implementing in production OT environments.

Safeguards

Safeguard 7.1: Establish and Maintain a Vulnerability Management Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, the enterprise should create an OT focused process. This process should show the vulnerabilities to include the cyber-related impacts to operations and provide the necessary context and prioritization to ensure the correct remediation.

The vulnerability management process should determine the types of testing and amount of information necessary to determine the vulnerabilities.

Develop a risk-based process to determine the importance and priority when determining the need or approach to the remediation. A risk-based, engineering-driven approach — a threat-intel driven approach. Remember threats in ICS are not just 'malware. ICS threat landscape indicate more likely scenario of living off the land — where zero malware, zero vulnerabilities, zero exploits are used to cause impact to safety, reliability and operational downtime, disruption and potential destruction.

Safeguard 7.2: Establish and Maintain a Remediation Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

Applicability

For this Safeguard, vulnerabilities are not necessarily resolved in the same way in the OT environment as they may be firmware related, thus needing additional due diligence to avoid production issues.

When purchasing, review the vendor's commitment to test and implement vulnerability patches in a timely manner. Patch as quickly as possible. Also, consider having remediation and mitigation plans documented. Keep track of any explanations regarding unapplied patches for audit purposes. In OT, patching may not remediate all issues as there will potentially be devices that cannot be patched; track all unpatched systems and assess for enterprise risk. A new device should be considered in such situations. Support team communication with end-users is essential.

Safeguard 7.3: Perform Automated Operating System Patch Management

Asset Type: Software	Security Function: Protect	IG1 IG2 IG3

Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

Applicability

For this Safeguard, the patching/upgrade process should be fully controllable/configurable for the OT environment needs. Patching is an extremely important action and reasonable timelines must be created. Where applicable, test patches to ensure no operational impact. More frequent, shorter patch windows may be a more efficient and easier process, but the specifics of the environment as relates to potential process downtime must be considered. Post patch validation should be conducted. Consider prioritization based on engineering maintenance windows.

Safeguard 7.4: Perform Automated Application Patch Management

Asset Type: Software	Security Function: Protect	IG1 IG2 IG3

Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

Applicability

For this Safeguard, the patching/upgrade process should be fully controllable/configurable for the OT environment needs. Patching is an extremely important action and reasonable timelines must be created. Where applicable, test patches to ensure no operational impact. More frequent, shorter patch windows may be a more efficient and easier process, but the specifics of the environment as relates to potential process downtime must be considered. Post patch validation should be conducted. Consider prioritization based on engineering maintenance windows.

Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets

Asset Type: Software	Security Function: Identify	IG2 IG3

Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans.

Applicability

For this Safeguard, there are a number of systems that might not need to be scanned to determine the likely vulnerabilities. If the firmware revision is known, you can infer potential vulnerabilities based on version and the limited configuration options of the device. However, where practicable, scans are still recommended.

There is additional risk when running scans against an ICS device as some ICS assets can be permanently damaged by these scans. Ideally, a system should be scanned prior to placing it into production to determine what issues scanning could create, and to obtain a baseline. Follow vendor recommendations on when and if an asset can be scanned. The more modern an ICS device is, the more robust it generally is when being scanned. However, scans might be preferable during outages or maintenance windows. Passive vulnerability detection may be less accurate but can potentially provide a safer process. Such scans usually still require active scanning to confirm or refine the results. There are some "lighter weight" active polling approaches that use industrial protocol(s) to solicit information from the assets (e.g., firmware version, attached modules, etc.), and the collection platform does an implied or derived vulnerability assessment based on these basic attributes.

Education and clear communication between enterprise and OT teams is critical to addressing this Safeguard. There is opportunity here to educate and include the enterprise vulnerability management team, if not one and the same, so they fully understand that the OT environment potentially requires a different approach from their expected or preferred methods (i.e., manual version review, passive scanning, etc.). Inferred or derived vulnerability assessments based on collected or provided key system attributes is a common approach that avoids a lot of the traditional scanning pitfalls in an OT environment.

Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets

Asset Type: Software	Security Function: Identify	IG2 IG3

Perform automated vulnerability scans of externally-exposed enterprise assets. Perform scans on a monthly, or more frequent, basis.

Applicability

For this Safeguard, very few, if any OT assets should be exposed externally. Typically, a DMZ or other network segmentation methods are constructed, and any data that needs to be accessed externally is available in such segments. Systems and jump boxes should be designed to endure a scan. However, please assess these devices prior to scanning to determine any impact to the industrial process. If there are other assets that have external communications (e.g., Wi-Fi, cell communication, satellite, modem, wireless, cell, dial-up, etc.), those would be something to start by documenting, so you know who owns them, their criticality, if they have monitor and/or control capabilities within the ICS, etc. These may be more difficult to assess if they are vendor managed. It may be worth adding enterprise deployed tools to manage detection of externally exposed systems (e.g., Shodan, Censys.io, etc.). However, this can prove difficult as it may not be known where on the internet these assets may appear. Also consider assets with wireless connectivity unintentionally connected to the enterprise environment from within the OT environment, thus potentially creating a bridge between the environments.

Safeguard 7.7: Remediate Detected Vulnerabilities

Asset Type: Software	Security Function: Respond	IG2 IG3

Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

Applicability

For this Safeguard, adjustment to the time frame, is not always realistic, but remediation of the vulnerability is important. Have a risk tracking/management plan and tracking to determine what actually poses a threat to the environment with all the other compensating controls that are involved, and then work that into the production operation. Consider a segmentation process to minimize the impact to the overall environment. Disable unnecessary ports and services, set up host and hardware firewalls at strategic points, host segmentation, secure virtual local area networks (VLANs), etc. Consider a long-term obsolesce program plan to replace any vintage or legacy systems potentially vulnerable due to lack of available patches.

CONTROL 8

Audit Log Management

Overview

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

ICS Applicability

This CIS Control offers guidance for the maintenance and monitoring of audit logs. Logging of security events in ICS environments can be a challenge due to the nature of many of the embedded or legacy devices present. Many devices do not support native logging of security events. Those that do often do not inherently support sending those events to an external device such as a central logging server so special action may need to be taken to gain access to such information.

All Safeguards are applicable. However, many systems or devices may not support the level of logging recommended by this Control.

ICS Challenges

Not all ICS devices will be able to log; some that will log are not capable of pushing those logs to remote collectors.

ICS Additional Discussion

If looking to leverage an IT-based SIEM, make sure it supports the ICS environment because many logging analytic and alerting solutions do not support or correctly interpret or correlate ICS specific events.

Safeguards

Safeguard 8.1: Establish and Maintain an Audit Log Management Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a documented audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, not all OT assets support logging. An enterprise should have compensating policies in place if logs are not available; assets lacking logging ability should be documented; and risk associated with lack of logging should be assessed.

Safeguard 8.2: Collect Audit Logs

Asset Type: Data	Security Function: Detect	IG1 IG2 IG3

Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.

Applicability

For this Safeguard, not all OT assets support logging. This can also pose a challenge with shared accounts. Manual collection or other alternate methods should be considered if needed.

Safeguard 8.3: Ensure Adequate Audit Log Storage

Asset Type: Data	Security Function: Protect	IG1	IG2	IG3

Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.

Applicability

For this Safeguard, logging system resources should be assessed for both rate of log data received (i.e., not overwhelming available CPU, memory, or network capacity, etc.) and have adequate permanent storage to comply with policy. An evaluation should be completed before the log system is sized, but it may also be needed after normal production logs begin entering the logging system. Logs can represent a significant volume of information, and this may warrant pruning/limiting the ingested data.

Safeguard 8.4: Standardize Time Synchronization

Asset Type: Data	Security Function: Protect	IG2	IG3

Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.

Applicability

For this Safeguard, proper time synchronization is critical to ensure time stamps for all logged actions can be correlated. Time synchronization is also critical in OT environments due to requirements of associated industrial processes. Isolated network segments may need their own time source. Policies should be in place to ensure such time sources on isolated segments remain in sync with other time sources; this may need to be a manual process.

Safeguard 8.5: Collect Detailed Audit Logs

Asset Type: Data	Security Function: Detect	IG2	IG3

Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

Applicability

For this Safeguard, consider documenting the level of detail desired. Leverage the collection management framework (see Safeguards 8.1 and 8.2) to determine level of granularity available and alternate sources that provide additional context if logging is insufficient or not available. Know relevant capabilities of the available logging system. Alleviate or mitigate any gaps as applicable.

Safeguard 8.6: Collect DNS Query Audit Logs

Asset Type: Data	Security Function: Detect	IG2	IG3

Collect DNS query audit logs on enterprise assets, where appropriate and supported.

Applicability

For this Safeguard, some ICS networks do not have DNS servers and no egress point. For those devices using DNS, this would be useful, especially for devices communicating across zone boundaries as DNS traffic can help identify anomalous, or potentially malicious, communication. This could include an allow-list approach of permissible DNS servers and queries. If an asset begins making unusual DNS queries, an investigation may be needed. Collection options include DNS servers and security appliances with this logging functionality. Generally, all DNS requests outside of the enterprise should be logged; there may be additional situations where internal requests should also be logged, but this will depend on environmental specifics. Often, it is preferable to ensure communication only with an internal DNS server; outside requests can be processed by the internal servers.

Safeguard 8.7: Collect URL Request Audit Logs

Asset Type: Data	Security Function: Detect	IG2 IG3

Collect URL request audit logs on enterprise assets, where appropriate and supported.

Applicability

For this Safeguard, logs will be collected at another point on the network, like a firewall, and not the asset itself. This will not be applicable to many OT due to lack of internet access. Where internet access is available every effort should be made to collect these logs as unusual requests could be reviewed.

Safeguard 8.8: Collect Command-Line Audit Logs

Asset Type: Data	Security Function: Detect	IG2 IG3

Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.

Applicability

For this Safeguard, command line interface (CLI) logging should be enabled where supported. OT environments typically have many CLI driven assets. Risk due to lack of CLI logging ability should be understood and tracked. A strategy to collect logs from isolated assets should be considered. CLI logging is a useful way to review unusual or malicious interactions with an accessed or potentially compromised system.

Safeguard 8.9: Centralize Audit Logs

Asset Type: Data	Security Function: Detect	IG2 IG3

Centralize, to the extent possible, audit log collection and retention across enterprise assets in accordance with the documented audit log management process. Example implementations include leveraging a SIEM tool to centralize multiple log sources.

Applicability

For this Safeguard, there may be multiple log aggregation points due to isolated network segments. A strategy to further centralize these logs should be considered if practical. Typically, the closer to the "field" level an asset sits, the less likely you will be able to get its logs to a centralized log aggregation point. There should be a reasoned and approved plan on where to store such logs, whether remaining local, regional, or centralized. In some OT environments, the same IP address space is used multiple times, typically on unrouteable networks. Every effort should be made to use unique addresses for each asset as it simplifies log collection and review. This may not always be possible due to limitations of vendor supplied equipment or systems. In such circumstances alternatives for identification should be considered (e.g., log MAC address for each entry sent to the log aggregation point).

Safeguard 8.10: Retain Audit Logs

Asset Type: Data	Security Function: Protect	IG2 IG3

Retain audit logs across enterprise assets for a minimum of 90 days.

Applicability

For this Safeguard, retention requirements might be more or less than 90 days or maximum supported by the device, or a process to push the logs of platform if supported, based on specific OT environment needs or regulatory and compliance considerations.

Safeguard 8.11: 8.Conduct Audit Log Reviews

Asset Type: Data	Security Function: Detect	IG2 IG3

Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

Applicability

For this Safeguard, alert configurations based on pre-set conditions can significantly streamline the log review process. There should be regular review to ensure assets are logged and, where applicable, forwarding as expected/needed. Regular confirmation that all expected devices are sending logs to any aggregation point should be done.

Safeguard 8.12: 8.Collect Service Provider Logs

Asset Type: Data	Security Function: Detect	IG3

Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.

Applicability

For this Safeguard, some OT environments have remote vendor access, usually through a demilitarized zone (DMZ)/secure VPN connection. There may be some environments/networks for which this is not applicable.

CONTROL 9

Email and Web Browser Protections

Overview

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

ICS Applicability

This CIS Control focuses on the security of web browsers and email clients, which are very vulnerable to attack vectors. Most ICS environments do not require internet access, and email clients are not needed because they are often isolated from business networks.

Email is utilized in ICS environments but typically only in an outgoing manner. It is common to have systems that monitor critical processes send out alerts or reports via email. These emails are typically accessed from business or corporate assets that are on separate networks and have no access to the ICS environment.

While internet access is not required, often services are provided via internal web servers. Therefore, unlike email clients, web browsers may still be required.

Most of the Safeguards are not applicable to the ICS environment for the reasons stated above. However, Safeguards related to using authorized browsers for business purposes are applicable. The key is restricting internet access.

ICS Challenges

The policies around requiring email and web access to occur outside ICS and to ensure there is a lock down.

For ICS environments, the main challenge would be policies that require email and internet access to occur outside the environment.

ICS Additional Discussion

In cases where certain Safeguards are not applicable, the following additional requirements should be enforced:

- Ensure that all systems are segmented such that there is no internet access.
- Ensure that no email clients are installed or present on any systems. Where a device or system has the capability to send email-based alerts or reports, ensure that it is limited to outbound only.

Safeguards

Safeguard 9.1: Ensure Use of Only Fully Supported Browsers and Email Clients

Asset Type: Software	Security Function: Protect	IG1	IG2	IG3

Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.

Applicability

For this Safeguard, there are situations where a vendor may not have approved an up-to-date browser, leaving an enterprise supporting/using an obsolete version. In such a case it is suggested to limit use of such browsers only to required workflows. Additionally, most browsers are updated frequently, which could be challenging in an OT environment. Long-term support (LTS) browser versions should be considered if available.

Safeguard 9.2: Use DNS Filtering Services

Asset Type: Devices	Security Function: Protect	IG1	IG2	IG3

Use DNS filtering services on all end-user devices, including remote and on-premises assets, to block access to known malicious domains.

Applicability

For this Safeguard, DNS is typically controlled at a firewall, network tap, or proxy. Many OT assets will not use public DNS. Ensure DNS queries from the OT environment do not utilize public DNS servers.

Safeguard 9.3: Maintain and Enforce Network-Based URL Filters

Asset Type: Network	Security Function: Protect	IG2 IG3

Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.

Applicability

For this Safeguard, it is recommended to set "deny by default" and explicitly allow only necessary access. Web browser traffic should not be allowed to egress from the OT environment to the internet; browsers should be limited to internal resources only.

Safeguard 9.4: Restrict Unnecessary or Unauthorized Browser and Email Client Extensions

Asset Type: Software	Security Function: Protect	IG2 IG3

Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.

Applicability

For this Safeguard, it is recommended to set "deny by default" and explicitly allow only necessary plugins/extensions.

Safeguard 9.5: Implement DMARC

Asset Type: Network	Security Function: Protect	IG2 IG3

To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

Applicability

For this Safeguard, email clients should be restricted in the OT environment. Email access typically should only be available in the enterprise environment.

Safeguard 9.6: Block Unnecessary File Types

Asset Type: Network	Security Function: Protect	IG2 IG3

Block unnecessary file types attempting to enter the enterprise's email gateway.

Applicability

For this Safeguard, email clients should be restricted in the OT environment. Email access typically should only be available in the enterprise environment.

Safeguard 9.7: Deploy and Maintain Email Server Anti-Malware Protections

Asset Type: Network	Security Function: Protect	IG3

Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.

Applicability

For this Safeguard, email clients should be restricted in the OT environment. Email access typically should only be available in the enterprise environment.

CONTROL 10

Malware Defenses

Overview

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

ICS Applicability

This CIS Control addresses the steps needed to ensure a strong defense against malware intrusions. Malicious code is a very real threat to ICS. It has been crafted to target the devices or processes unique to these industries. While proper network segmentation and defense-in-depth strategies help to mitigate this risk by making it difficult for threat actors to deliver malware to their intended locations, malware defense still needs tools and processes in place to detect incidents.

Unfortunately, the sensitivity and critical nature of these environments make it difficult to regularly update antivirus definitions for fear the update process might impact the reliability of critical systems.

Additionally, many devices do not support endpoint software, thus making on-device malware monitoring difficult.

All Safeguards are applicable.

ICS Challenges

Fear exists that updating antivirus definitions might impact the reliability of critical systems.

Additionally, many devices do not support endpoint protection, thus making on-device malware monitoring difficult.

ICS Additional Discussion

For this CIS Control consider the following additional steps:

- Anti-malware tools need to be properly regression-tested to ensure that availability and reliability of the system will not be adversely affected. This testing should take place whenever a change is made to the anti-malware software such as a configuration change, software hotfix, or repository update.
- Ensure anti-malware tools are configured such that false positive detection will not negatively impact the availability or reliability of any critical processes.

Some OT teams may not want to incur the risk of updating antivirus definitions while critical processes are running. Consider, at a minimum, performing software updates to scanning engines and signature databases during scheduled maintenance or outages, or possibly test scanning with the action set to log what it would have done. Scan and log is preferable to scan and remediate if the remediation will have a negative effect.

When scanning removable media, it is recommended that the content be scanned before it can be accessed, but not upon insertion. By scanning on insertion, larger portable storage devices can take a significant time to finish scanning and impede productivity. However, by scanning prior to access, content can be scanned on demand and has less of an impact on productivity. An enhanced method to reduce the likelihood of introducing malware could include copying data from an untrusted device, scanning for malware, and then copying to a trusted portable storage media.

Anti-exploitation features can be very challenging to implement. Much of the industry's proprietary software has not been designed to leverage operating systems' memory protection features. Other devices simply cannot support these technologies. Some third-party packages can enable anti-exploitation functionality to supported devices. However, they can often create resource overhead that may impact the real-time requirements of these systems. While anti-exploitation technologies are valuable, they should only be applied where they are innately supported or do not impact the performance of ICS.

Safeguards

Safeguard 10.1: Deploy and Maintain Anti-Malware Software

Asset Type: Devices	Security Function: Detect	IG1 IG2 IG3

Deploy and maintain anti-malware software on all enterprise assets.

Applicability

For this Safeguard, there may be OT assets that do not support this Control. Consider mitigating any such gaps with network and firewall-based malware detection. Place tight procedural controls on removable media and portable devices to assist in protection of assets.

It is recommended to document assets not directly supporting anti-malware software and any associated mitigations. Document any anti-malware coverage gaps.

Any anti-malware solution should be tested prior to entering production to ensure no disruptions to ICS processes. Baselines should be established to assist in identifying indicators of compromise (IOCs).

Safeguard 10.2: Configure Automatic Anti-Malware Signature Updates

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Configure automatic updates for anti-malware signature files on all enterprise assets.

Applicability

For this Safeguard, the update cadence and coverage may vary. If reliant on an enterprise-side solution, there should be an OT separation of management, signature updates, and monitoring.

Testing of any anti-malware solution should occur prior to full production rollout to ensure there are no negative effects on the industrial process. Consider a centrally managed solution.

For situations where it is not possible or recommended to do automated updates, there should be compensating policies to address such gaps.

Safeguard 10.3: Disable Autorun and Autoplay for Removable Media

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Disable autorun and autoplay auto-execute functionality for removable media.

Applicability

For this Safeguard, this is very important in an OT environment as infected media is often an easier attack vector than penetrating security layers that typically protect OT environments.

Where supported, disable any autoplay, auto-execute, or similar features. Document and track any exceptions.

Safeguard 10.4: Configure Automatic Anti-Malware Scanning of Removable Media

Asset Type: Devices	Security Function: Detect	IG2 IG3

Configure anti-malware software to automatically scan removable media.

Applicability

For this Safeguard, this is very important in an OT environment as infected media is often an easier attack vector than penetrating security layers that typically protect OT environments. While not all assets will support this Safeguard, where it is supported, automated scanning should be configured.

Where it is not supported, consider implementing a process where removable media is first plugged in and scanned by a system with updated signatures/definitions that does support it. Consider physically blocking or otherwise disabling any unneeded ports on OT assets.

There continue to be legitimate use cases for removable media in the OT space, and removing such devices entirely is not generally feasible.

Safeguard 10.5: Enable Anti-Exploitation Features

Asset Type: Devices	Security Function: Protect	IG2 IG3

Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

Applicability

For this Safeguard, anti-exploitation features should be enabled where supported; however, many OT assets may not support such features. Vendor provided assets also may not support these features. Anti-exploitation features should be subject to testing prior to entering production to ensure there is no ICS or SCADA impact.

As vendors advance their security posture, additional features may be made available. It is important to know the default state of these new features. Advanced functionality makes it more difficult to run in their default state and enablement of a new feature could impact the OT environment.

Safeguard 10.6: Centrally Manage Anti-Malware Software

Asset Type: Devices	Security Function: Protect	IG2 IG3

Centrally manage anti-malware software.

Applicability

For this Safeguard, as much consistency as possible across the OT environment is crucial. Settings or baselines should be considered for OT assets in addition to general settings or baselines for traditional computing systems (servers, laptops, etc.). Develop a policy/standard/procedure for how OT assets are managed in the central management solution.

Often, the anti-malware software chosen will be dependent on vendor support. This software may not have the ability to be centrally managed, but every effort should be made to implement centralized management. Commonly accepted OT architecture principles typically have this management as separate from the enterprise.

If the centralized anti-malware system can also correlate telemetry or supply information to the centralized log management solution, it can provide additional data for analysis.

Safeguard 10.7: Use Behavior-Based Anti-Malware Software

Asset Type: Devices	Security Function: Detect	IG2 IG3

Use behavior-based anti-malware software.

Applicability

For this Safeguard, the primary concern is whether the asset is compatible with such software. This feature is present in many host-based anti-malware solutions, and any software with these features should be preferentially considered.

This software may only be available for traditional server and desktop operating systems. Vendor provided assets may, however, be incompatible with such software even if leveraging standard server or desktop operating systems due to incompatibility with other hardware or software elements. Where such software is not feasible, it may be possible to increase protection by using network traffic scanning tools. Consider leveraging a network-based malware detection tool as part of the CIS Control 13 implementation.

CONTROL 11

Data Recovery

Overview

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

ICS Applicability

This CIS Control references the need for performing system backups for data recovery capability. It requires different approaches within individual ICS environments. Different components support various backup methods. While some support full system backups, the majority offer only configuration exports. Still others may offer no capability to export configurations.

All the Safeguards are applicable.

ICS Challenges

There may be difficulty maintaining backups of critical remote systems that do not have centralized capabilities or which may be segmented or isolated from the network.

Depending on the ICS vertical, a quarterly time frame of testing backup and recovery may be difficult.

ICS Additional Discussion

For this CIS Control consider the following additional steps:

- Ensure that system backups and recovery procedures are documented and tested.

Most ICS systems do not support complete automatic backups, and scheduling of backups may cause ICS performance problems. Where this is the case, ensure backups are taken as appropriate.

Additionally, some device configurations remain static and rarely change. In these situations, backups may only need to be performed when configurations or data changes are made.

Regardless, it remains important to evaluate configurations that are expected to remain unchanged. This could allow for the detection of any alterations including accidental/unintentional alteration, tampering, or malicious intent.

In cases where devices are not capable of complete backups, all software, settings, and configurations should be captured such that all information necessary to perform a restoration is known and available.

Safeguards

Safeguard 11.1: Establish and Maintain a Data Recovery Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a documented data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

Consider using a responsible, accountable, consulted, and informed (RACI) chart to establish responsibilities for backups. A common strategy for backups is the 3-2-1 backup policy, which involves having three copies of data (production data and two backup data copies) on at least two different media (backup disk, tape, etc.) with one copy off-site for disaster recovery (DR) (off-site physical media and/or off-site cloud storage).

Many backup services are now cloud based and may be suitable to satisfy this Safeguard. When assessing risk for backup storage, consider such things as the security of the location for on-premises or cloud storage. Additional considerations related to cloud storage could include available network/internet bandwidth. For off-site, offline storage, physical distance could be a factor.

At least one offline backup should be considered to additionally protect data. Consider the scope of any potential disasters (local, regional, national, etc.) that any offline or off-site copies may be impacted by. DR as a Service is becoming more common, although it would not likely be as useful in the OT space.

Safeguard 11.2: Perform Automated Backups

Asset Type: Data	Security Function: Recover	IG1	IG2	IG3

Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.

Applicability

What can be done automatically needs to be determined and documented; this will vary based on the backup software chosen. Some items may be feasible through scripting, while others may require manual intervention in accordance with the affected ICS process. Consideration should be given to modification of suggested backup timelines due to differing rates of data change that would be typical in the enterprise environment. Any such policies should be documented.

Safeguard 11.3: Protect Recovery Data

Asset Type: Data	Security Function: Protect	IG1	IG2	IG3

Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.

Applicability

For this Safeguard, network-bound backup should have secure controls applied to it. Keeping physical, offline configuration backups in a secure location (i.e., portable storage device in a safe or other secure location) may be a viable option as well. These requirements should be part of the overall process with specifics documented within standards or other codified methods.

Some backup methods may provide in-app encryption; some may rely on disk-based encryption. Access control should be in-place to ensure minimal access to the backups. Manual backups may require additional steps such as ensuring adequate storage, the number of copies, schedule compliance, and access to them. Ensure that any super-administrative accounts are protected to prevent unauthorized backup access, and that the data is not available in an unauthenticated manner.

Safeguard 11.4: Establish and Maintain an Isolated Instance of Recovery Data

Asset Type: Data	Security Function: Recover	IG1 IG2 IG3

Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.

Applicability

For this Safeguard, this can be complicated due to network segmentation or isolation. Backups should not be stored in the same physical location unless secured and additional copies are stored elsewhere.

Data in OT environments sometimes does not change for long periods of time, which makes storing an offline backup easier. For configuration-based backups, a snapshot may be a good option.

Backup retention policies are needed to determine how long backups are retained.

Safeguard 11.5: Test Data Recovery

Asset Type: Data	Security Function: Recover	IG2 IG3

Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

Applicability

Backups need to be periodically tested and validated. A backup that cannot be restored provides a false sense of security and can be a single point of failure in the disaster recovery process.

Depending on the OT vertical, a quarterly time frame may be difficult. An internal determination of the time frame will be needed with a plan. Quarterly, or more frequent, may be possible with a lab environment but needs to match the enterprise's requirements. As it is a "sampling," it should include different types of OT assets, not just commodity operating system (OS) servers. Depending on the specific needs of the OT vertical, validation of all backups may be warranted as opposed to validating a sampling. Automated tools may assist with this.

It may be helpful to perform a tabletop exercise prior to an actual recovery as a way to strengthen the recovery process that would apply to a broader set of devices.

CONTROL 12

Network Infrastructure Management

Overview

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

ICS Applicability

This CIS Control addresses the need to manage the configuration of all network devices using a change control process. The network infrastructure of an ICS network typically carries additional requirements when compared to traditional IT systems. Usually, these networks focus on availability and are architected with safety, resiliency requirements, and real-time performance requirements in mind.

Common attack vectors to ICS network infrastructure remain the same as traditional IT networks. Unsecure services, poor firewall configurations, firmware, end of life (EoL), OS, software, and default credentials remain issues.

The need to control access to systems based on the need to know is critically important. When following proper network layering best practices (e.g., see the Purdue reference model), some degree of physical and logical segmentation will be in place. Devices that directly measure or control physical processes are typically segmented from general purpose workstations. However, segmentation within layers should also be considered. Consider adding security such as SANS ICS is a Target for adding security to the Purdue Levels.

There are different approaches to network segmentation. For example, private VLANs or secure VLANs are utilized heavily in IT and retail spaces. This approach may be applicable for ICS systems. However, consideration needs to be given to ACLs to control access and other routing requirements when provisions for remote configuration and monitoring are requirements in highly segmented systems. Segmenting by subnets is typically an acceptable approach. VLANs or dedicated switches can be used depending on availability and cost requirements.

There are many references to sensitive data through this Control. These references should align with Control 3: Data Protection. This may remove applicability for parts of this Control depending on the ICS environment.

Network level authentication via 802.1x does not work on many of the devices found in ICS that do not support supplicant software. Network level authentication can cause reliability issues if not strictly maintained. Instead, consider a non-802.1x network access approach that is more ICS device-friendly and can at a minimum alert of new devices detected on the network.

- Safeguards related to network level authentication may not be applicable to ICS environments.
- Safeguards related to client-based certificates may not be applicable to ICS environments.

Certificate-based authentications in public key infrastructure (PKI) environments can be complex and expensive.

ICS Challenges

Below is a list of challenges that the ICS environment may face:

- There may not be centralized management available
- Vision for air-gapped systems may be lacking
- Having a full picture of the environment
- Lack of remote access and distance can create challenges in response time
- The age of the system may make it difficult to update or upgrade with existing systems
- Lack of standardized maintenance windows
- Systems may not be designed or built with native security built-in
- Lack of test environments
- Systems may be proprietary
- Mergers and acquisitions of vendors
- MFA can be complex to implement and can limit the use of vendor supplied network monitoring solutions

ICS Additional Discussion

For this CIS Control consider the following additional steps:

- Ensure firewalls are configured to deny by default
- Where available, configure transport layer security (TLS) or secure sockets layer (SSL) communication, decryption, and inspection
- If a location is unmanned or if critical process data flows through a perimeter device, ensure redundancy exists, or device failure won't prevent this data from being received by its intended destination

Safeguards

Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date

Asset Type: Network	Security Function: Protect	IG1 IG2 IG3

Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network as a service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.

Applicability

For this Safeguard, in an ICS environment it is important to develop a plan for evaluating updates to determine applicability, necessity, and frequency. A review of release notes should be done to identify any change in default behaviors and identify any end-of-life concerns. Coordination efforts are needed between the enterprise IT and OT staff.

Safeguard 12.2: Establish and Maintain a Secure Network Architecture

Asset Type: Network	Security Function: Protect	IG2 IG3

Design and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. Example implementations may include documentation, policy, and design components.

Applicability

For this Safeguard, this may be easier in an OT environment than a traditional IT environment. The standards for OT environment segmentation should include minimal to no connectivity between OT/IT networks. Document any weaknesses.

Consider referencing the Purdue model, NIST SP 800-82 Rev. 3, ISA/IEC 62443, CISA Critical Infrastructure Sectors guidance, or similar frameworks.

Only intentionally internet accessible equipment should be in the DMZ. No internet accessible equipment should be in a non-DMZ segment. Ensure your environment is as segmented as possible. An intermediate host such as a jump box is suggested.

Systems should be air gapped where possible. Traffic traversing the environment should use encrypted and secure channels where possible. This ensures no cross contamination, as well as preventing leaks of any sensitive clear-text data.

Separation of duties is important for preventing insider threats.

Safeguard 12.3: Securely Manage Network Infrastructure

Asset Type: Network	Security Function: Protect	IG2 IG3

Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.

Applicability

For this Safeguard, only intentionally internet accessible equipment should be in the DMZ. No internet accessible equipment should be in a non-DMZ segment.

An intermediate host such as a jump box is suggested.

Use different protocols so that your OT environment is totally segmented. Systems should be air gapped and using encrypted and secure channels where possible, to ensure no cross-contamination. Log collection should also be reviewed to ensure no unencrypted credentials are stored in the logs.

Separation of duties is important for preventing insider threats.

Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, OT architecture diagrams are typically critical and are usually already available. Ensure that documentation is up to date and published.

Safeguard 12.5: Centralize Network Authentication, Authorization, and Auditing (AAA)

Asset Type: Network	Security Function: Protect	IG2 IG3

Centralize network AAA.

Applicability

For this Safeguard, implement where feasible and applicable. For those unable to use centralized authentication, authorization, and accounting (AAA), having processes/procedures, adequate logging and auditing, and standard configurations can help compensate.

Safeguard 12.6: Use of Secure Network Management and Communication Protocols

Asset Type: Network	Security Function: Protect	IG2 IG3

Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).

Applicability

For this Safeguard, an ICS environment is not a good candidate for wireless network access.

If utilizing Wi-Fi, apply recommended security best practices in accordance with available OT specific frameworks and guidance (e.g., Purdue model, NIST SP 800-82 Rev. 3, ISA/IEC 62443, CISA Critical Infrastructure Sectors guidance).

Consider at a minimum WiFi Protected Access 2 (WPA2) or higher; WiFi Protected Access 3 (WPA3) is recommended. Older standards are insufficient.

Safeguard 12.7: Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure

Asset Type: Devices	Security Function: Protect	IG2 IG3

Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.

Applicability

For this Safeguard, it is recommended that no VPN connection to the OT environment exists.

If remote access is required, all VPN connections should occur from the enterprise side through the DMZ with access to a jump host which allows access to the OT environment.

Safeguard 12.8: Establish and Maintain Dedicated Computing Resources for All Administrative Work

Asset Type: Devices	Security Function: Protect	IG3

Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.

Applicability

For this Safeguard, if a connection between the OT and enterprise environments is required, a jump box or intermediate host from a privileged system in the enterprise environment to a privileged system in the OT environment is required.

CONTROL 13

Network Monitoring and Defense

Overview

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

ICS Applicability

The network infrastructure of an ICS network typically carries additional requirements when compared to traditional IT systems. Usually, these networks focus on availability and are architected with real-time performance and redundancy requirements.

We cannot rely on network defenses to be perfect. Adversaries continue to evolve and mature, as they share, or sell, information among their community on exploits and bypasses to security controls. Even if security tools work "as advertised," it takes an understanding of the enterprise risk posture to configure, tune, and log them to be effective. Often, misconfigurations due to human error or lack of knowledge of tool capabilities give enterprises a false sense of security.

Security tools can only be effective if they are supporting a process of continuous monitoring that allows staff the ability to be alerted and respond to security incidents quickly. A Computer Emergency Response Team (CERT) should be formalized, with appropriate policies and procedures, to respond to incidents. Enterprises that adopt a purely technology-driven approach will also experience more false positives, due to their over-reliance on alerts from tools. Identifying and responding to these threats requires visibility into all threat vectors of the infrastructure and leveraging humans in the process of detection, analysis, and response. It is critical for large or heavily targeted enterprises to have a security operations capability to prevent, detect, and quickly respond to cyber threats before they can impact the enterprise. This process will generate activity reports and metrics that will help enhance security policies and support regulatory compliance for many enterprises.

As we have seen many times in the press, enterprises have been compromised for weeks, months, or years before discovery. The primary benefit of having comprehensive situational awareness is to increase the speed of detection and response. It is critical to respond quickly when any compromised systems or malware are discovered, credentials are stolen, or when sensitive data is compromised to reduce impact to the enterprise.

Through good situational awareness (i.e., security operations), enterprises will identify and catalog Tactics, Techniques, and Procedures (TTPs) of attackers, including indicators of compromise (IOC) that will help the enterprise become more proactive in identifying future threats or incidents. Recovery can be achieved faster when the response has access to complete information about the environment and enterprise structure to develop efficient response strategies.

ICS Challenges

Below is a list of challenges that the ICS environment may face:

- The potentially critical nature of many ICS systems deserves special consideration when establishing enterprise risk posture.
- Enterprises may not have adequate internal resources to fully implement this Control.
- If managed services are required, a traditional managed service provider (MSP) may not have the necessary expertise; a managed security service provider (MSSP) should be considered.
- Third-party vendors and vendor services may not have a robust security posture. Vendors should be vetted for policies that match the enterprise risk posture.
- Logging of security events in ICS environments can be a challenge due to the nature of many of the embedded or legacy devices present. Many devices do not support native logging of security events, or do not inherently support sending events to an external device.
- Many logging analytics and alerting solutions do not support or correctly interpret or correlate ICS specific events.

ICS Additional Discussion

Most enterprises do not need to stand up a Security Operations Center (SOC) to gain situational awareness; however, depending on enterprise risk posture a SOC may be necessary. SOC as a service should always be considered for applicability when an internal SOC is not feasible. This starts with first understanding critical business functions, ICS, network and server architectures, data and data flows, vendor service and business partner connections, and end-user devices and accounts. This informs the development of a security architecture, technical controls, logging, monitoring, and response procedures.

At the core of this process is a trained and organized team that implements processes for incident detection, analysis, and mitigation. These capabilities could be conducted internally, or through consultants, or through a MSSP. Enterprises should consider network, enterprise asset, user credential, and data access activities. Technology will play a crucial role in collecting and analyzing all of the data, monitoring networks and enterprise assets internally and externally to the enterprise. Enterprises should include visibility to cloud platforms that might not be in line with on-premises security technology.

Forwarding all important logs to analytical programs, such as SIEM solutions, can provide value; however, they do not provide a complete picture. Weekly or more frequently scheduled log reviews are necessary to tune thresholds and identify abnormal events. Correlation tools can make audit logs more useful for subsequent manual inspection. These tools are not a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand attacks. Requirements for the SOC would be people who have the following to be effective: IT security knowledge, ICS/engineering security knowledge and an understanding of the control system devices (PLCs, HMIs, RTUs, IEDs, and their purpose and consequence if they are unavailable), with a prioritization of safety, first above all.

As this process matures, enterprises will create, maintain, and evolve a knowledge base that will help to understand and assess the business risks, developing an internal threat intelligence capability. Threat intelligence is the collection of TTPs from incidents and adversaries. To accomplish this, a situational awareness program will define and evaluate which information sources are relevant to detect, report, and handle attacks. Most mature enterprises can evolve to threat hunting, where trained staff manually review system and user logs, data flows, and traffic patterns to find anomalies.

Safeguards

Safeguard 13.1: Centralize Security Event Alerting

Asset Type: Network	Security Function: Detect	IG2 IG3

Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

Applicability

For this Safeguard, where possible, it is recommended to have a full understanding of data sources, availability, and usefulness of said sources.

Each information source should be documented. Where potential gaps in alerting are discovered, and centralization is not possible, correlation may need to be done manually.

This may require additional due diligence and planning to acquire the data from desired systems within the OT environment.

Safeguard 13.2: Deploy a Host-Based Intrusion Detection Solution

Asset Type: Devices	Security Function: Detect	IG2 IG3

Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

Applicability

For this Safeguard, where appropriate and/or supported, if not feasible consider using network intrusion detection systems (NIDS) as a complementary control. Focus first on identifying and validating baseline communications, then detecting deviations from those.

Consider commonly accepted practices for host-based intrusion detection systems (HIDs) management. See CIS Control 8 where management and log collection are covered.

Safeguard 13.3: Deploy a Network Intrusion Detection Solution

Asset Type: Network	Security Function: Detect	IG2 IG3

Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.

Applicability

For this Safeguard, a NIDS should be implemented in one or more locations, where possible. Consider adding requirements to the network that focus on OT-related aspects.

Inspection at zone boundaries are a good place to monitor traffic. The architecture should be designed to provide and encourage inspection points deeper into the OT environment (i.e., being able to see OT devices on network) in the field.

The IDS should not preclude the use of a HIDS. Where possible, both should be leveraged. If your firewalls are capable of intrusion detection, application filtering, and deep packet inspection, these should play a role if practical.

Safeguard 13.4: Perform Traffic Filtering Between Network Segments

Asset Type: Network	Security Function: Protect	IG2 IG3

Perform traffic filtering between network segments, where appropriate.

Applicability

For this Safeguard, traffic filtering should be implemented for traffic flowing from and to the data center (north-south traffic) as well as within the data center (east-west traffic). Also consider, north-south and east-west traffic for intra-network vs inter-network. Specifically, must be ICS protocol aware.

Additional traffic filtering between network zones within OT environments should be implemented where practical.

A determination should be made as to what system(s) will perform the filtering, including logging. This may be done by a dedicated appliance (i.e., firewall) or a more general-purpose device such as a server, depending on environmental architecture. Some options provide more manageable solutions than others.

Safeguard 13.5: Manage Access Control for Remote Assets

Asset Type: Devices	Security Function: Protect	IG2 IG3

Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.

Applicability

For this Safeguard, if remote access is used in the OT environment, where integration occurs will be important. Where remote access originates, the path, intermediate hops, and the destination will be important to understand (i.e., DMZ, jump box, network device traversal, etc.).

Various access control methods provide additional options on the levels and types of access rather than immediate, full access to the environment. Anti-malware technology with managed detection and response (MDR) should be implemented to scan any remote connections where available.

Safeguard 13.6: Collect Network Traffic Flow Logs

Asset Type: Network	Security Function: Detect	IG2 IG3

Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

Applicability

For this Safeguard, network flow data can be useful for a variety of functions and should be collected where feasible.

There are solutions that turn full packet capture (PCAP) data into flow data. There are many caveats with deploying a full PCAP, but it remains an option for generating the flow data if already deployed and managed.

Safeguard 13.7: Deploy a Host-Based Intrusion Prevention Solution

Asset Type: Devices	Security Function: Protect	IG3

Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

Applicability

For this Safeguard, the deployment of an IPS is a critical component of OT security.

However, IPS technologies used in traditional IT infrastructure may not be easily transferable to the OT environment; thus, security experts should strive to build IDS specifically for this OT infrastructure.

Detection, prevention, and mitigation should be as comprehensive as possible; where available, extended detection and response (XDR) should be implemented.

Safeguard 13.8: Deploy a Network Intrusion Prevention Solution

Asset Type: Network	Security Function: Protect	IG3

Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.

Applicability

For this Safeguard, NIPS requires more testing and validation. Detection, prevention, and mitigation should be as comprehensive as possible; where available, XDR should be implemented.

Depending on deployment location, this can be more effective at zone and segment boundaries as opposed to intra-network and inter-network boundaries (i.e., north-south and east-west traffic boundaries).

Safeguard 13.9: Deploy Port-Level Access Control

Asset Type: Network	Security Function: Protect	IG3

Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.

Applicability

For this Safeguard, where supported, port-level access control should be implemented.

Legacy OT devices may have to rely on 802.1x authentication methods (e.g., MAC authentication), as many of those devices do not support 802.1x and/or certificates, which should be used where available.

Some vendors allow including other attributes that provide additional context for profiling and then assigning policy to connecting devices. These additional methods should be investigated for applicability to the environment.

There are many considerations when deploying 802.1x on an OT environment, including re-authorization times, failure modes, default connectivity, testing and validation, delayed network connection impacts, exception process, enrollment, etc. These additional considerations should be investigated for applicability to the environment.

Safeguard 13.10: Perform Application Layer Filtering

Asset Type: Network	Security Function: Protect	IG3

Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.

Applicability

For this Safeguard, implement where possible in OT environments.

If internet access is necessary for the filtering process, this would be recommended for placement in the DMZ to serve as an enforcement point and a protocol break.

Safeguard 13.11: Tune Security Event Alerting Thresholds

Asset Type: Network	Security Function: Detect	IG3

Tune security event alerting thresholds monthly, or more frequently.

Applicability

For this Safeguard, tuning is necessary to minimize overwhelming the SOC/CERT/etc. while ensuring adequate visibility into what is going on within the environment.

Enabling detection and alerting is the simplest part. Tuning those to what is effective and manageable is the goal and will require concerted effort. Conducting the tuning requires involvement from multiple teams to understand what input on how detections become alerts, who triages, and who responds to them safely and effectively.

As OT environments are typically less dynamic than the enterprise, monthly may not be realistic and/or useful cadence. Where necessary, an alternate cadence that is realistic and useful can be set.

CONTROL 14

Security Awareness and Skills Training

Overview

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

ICS Applicability

This CIS Control focuses on educating and training based on job-role in a range of security practices that span basic to advanced skills, and to security awareness and vigilance. Human error, oversights, and negligence are leading causes of security weakness, and the consequences of untrained or inadequately or infrequently trained personnel in an ICS environment and adjacent and interdependent systems can have a range of effects from disruption to damage, to destruction of both a digital and physical nature, etc. It is essential for OT teams to be thoroughly versed in security best practices so that they can ensure the security readiness of the ICS environment. These same skills should be nurtured and expanded over time to reinforce best practices and to evolve as new risks are identified and new threats emerge.

Additionally, many OT teams rely on contractors or vendors who need access to critical parts of the network to service specialized equipment, but they may not be aware of security threats. For these reasons, the experience and pedigree of these third-party resources should be carefully evaluated, including evaluation and validation of purported knowledge, skills, and abilities (KSAs) prior to allowing said third parties access to critical components and systems.

ICS Challenges

Users themselves, both intentionally and unintentionally, can cause incidents as a result of mishandling sensitive data (e.g., sending an email to the wrong recipient, misplacing a portable device, reusing passwords, using weak passwords) in these areas:

- Identifying, developing, and implementing appropriate training for various job roles across the entire enterprise
- Identifying, developing, and implementing appropriate training for vendors, contractors, subcontractors, and visitors prior to accessing sensitive areas or granting remote access
- Keeping training up to date and relevant
- Production schedules may create difficulties in scheduling necessary training

ICS Additional Discussion

An appropriate security awareness program, with consideration for the specialized needs of an OT environment, must be implemented in congruence with the challenges listed above. Consider advanced, immersive cybersecurity security education and training for personnel expected to perform high-risk activities, advanced processes, or those who are making decisions relating to architecture, implementation, operation, and maintenance of the OT environment. Regular capability assessments in line with this training should be considered, as well as relevant industry certifications. Training must be reviewed regularly for appropriateness to the current OT environment, current risk factors, and the emergence of new threats. This will help ensure that the enterprise risk posture evolves as new threats emerge and help ensure adherence to industry best practices.

Additionally, many OT teams rely on contractors or vendors who need access to critical parts of the network to service specialized equipment, but they may not be aware of security threats. For these reasons, the experience and qualifications of these third-party resources should be carefully evaluated, including evaluation and validation of purported KSAs prior to allowing said third parties access to critical components and systems.

Safeguards

Safeguard 14.1: Establish and Maintain a Security Awareness Program

Asset Type: Documentation	Security Function: Govern	IG1	IG2	IG3

Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, it must be tailored to the OT environment. OT applicable content should be included for operator and OT support/administration training. Vendors should also be included in this program.

Consider ICS specific content for those that use, interact with, and support the business - the ICS/OT — at Leadership, End-User and Practitioners roles.

- How ICS Cybersecurity Supports Safety & Reliability
- Differences in Security Controls for IT vs. ICS/OT
- Overview of ICS Attacks History
- ICS Attack Surfaces

- ICS Network Visibility
- ICS specific Incident Handling Steps

Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members to recognize social engineering attacks, such as phishing, business email compromise (BEC), pretexting, and tailgating.

Applicability

For this Safeguard, OT assets typically do not have access to email. Targeted phishing campaigns are likely to occur against OT engineers. Training and recognition for the traditional IT side translates directly into the OT side. Operators are not immune to social engineering and should receive relevant training as well. Tailgating is a valid concern.

It is important that training provides an understanding of why this is important and relevant to their roles.

Safeguard 14.3: Train Workforce Members on Authentication Best Practices

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.

Applicability

For this Safeguard, there may be different authentication practices for different assets (due to supported features), and these should be tailored as needed. There may be less authentication options on certain types of OT systems.

It is important that training provides an understanding of why this is important and relevant to their roles.

Safeguard 14.4: Train Workforce on Data Handling Best Practices

Asset Type: Users	Security Function: Protect	IG1	IG2	IG3

Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.

Applicability

For this Safeguard, this is relevant for many industries, as there are numerous vendor-managed/controlled systems. These may be needed for support/administrative/integration, or specific to a piece of equipment. In some cases, the vendor may be supporting their own products. In others, it could be a vendor who provides support for other vendors' products. Other information to collect would include remote and/or local access requirements, criticality, availability impacts, roles and responsibilities, etc. Third-party organizational risk must be understood.

Safeguard 14.5: Train Workforce Members on Causes of Unintentional Data Exposure

Asset Type: Users	Security Function: Protect	IG1	IG2	IG3

Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

Applicability

For this Safeguard tailoring is needed based on workforce role and for vendors with access. Tailoring is also required based on the level of access granted.

Safeguard 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members to be able to recognize a potential incident and be able to report such an incident.

Applicability

For this Safeguard, it is as relevant in OT as any other industry.

Safeguard 14.7: Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.

Applicability

For this Safeguard, patching cycles may be longer on OT assets.

Safeguard 14.8: Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.

Applicability

For this Safeguard, consider adding training regarding inappropriate use of OT assets, since there is usually a separation of functions between OT and IT assets. Recent movement toward more permanent teleworking arrangements have made such training even more relevant and important.

Safeguard 14.9: Conduct Role-Specific Security Awareness and Skills Training

Asset Type: Users	Security Function: Protect	IG2	IG3

Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.

Applicability

For this Safeguard, in OT the roles/topics would likely be different from typical examples given in enterprise environments. Role specific SANS and CISA training and resources are available for managers and specialists. This role-specific training should be considered.

General workforce training in OT security is integral to the enterprise security posture.

Consider ICS specific content for those that use, interact with, and support the business — the ICS/OT — at Leadership, End-User and Practitioners roles.

- How ICS Cybersecurity Supports Safety & Reliability
- Differences in Security Controls for IT vs. ICS/OT
- Overview of ICS Attacks History
- ICS Attack Surfaces
- ICS Network Visibility
- ICS specific Incident Handling Steps

CONTROL 15

Service Provider Management

Overview

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

ICS Applicability

In our modern, connected world, enterprises rely on service providers to help manage their data or rely on third-party infrastructure for core applications or functions. This Control covers actions that should be taken to ensure that third-party service providers are properly securing their customers' data, and their own systems. The recommended measures for this Control include understanding which service providers are in use, what types of data they store, and monitoring their performance. There have been numerous examples where third-party breaches have significantly impacted an enterprise, disrupting the ability to continue normal business operations. Third-party trust is a core Governance Risk and Compliance (GRC) function, as risks that are not managed within the enterprise are transferred to entities outside the enterprise.

ICS Challenges

A major challenge is ensuring that the vendor has the same understanding of security as your enterprise; e.g., the level of security needed for a system that is not internet facing.

While reviewing the security of third parties has been a task performed for decades, there is not a universal standard for assessing security, and many service providers are being audited by their customers frequently, causing impacts to their own productivity. This is because every enterprise has a different "checklist" or set of standards to grade the service provider, often affecting these functions:

- Updates to the regulatory frameworks and the ability to pass audits
- Shared responsibility matrixes with cloud service providers
- Providing a false sense of security because compliance is not security

ICS Additional Discussion

This Control revolves around obtaining assurances from service providers as to their cybersecurity practices. Not all service providers will protect an enterprise's data in the same manner. Accordingly, a service provider's cybersecurity posture affects their ability to secure enterprise data entrusted to them. Obtaining ongoing information about a service provider's security posture will be difficult. If they have audits or other security assessments done, the outcome of those can be useful. General research on the vendor is also useful. If a negative event occurred in the past, they are not likely to announce it to you.

Most enterprises have traditionally used standard checklists, such as ones from ISO 27001 or the CIS Controls. Often, this process is managed through spreadsheets; however, there are online platforms now that allow central management of this process. The focus of this CIS Control though is not on the checklist; instead, it is on the fundamentals of the program. Make sure to revisit annually, as relationships and data may change. No matter what the enterprise's size, there should be a policy about reviewing service providers, an inventory of these vendors, and a risk rating associated with their potential impact to the business in case of an incident. There should also be language in the contracts to hold service providers accountable if there is an incident that impacts the enterprise.

When performing reviews, focus on the services or departments of the provider that are supporting the enterprise. A third party that has a managed security service contract, or retainer, and holds cybersecurity insurance, can also help with risk reduction. It is critical to securely decommission service providers when contracts are completed or terminated. Decommission activities may include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

Safeguards

Safeguard 15.1: Establish and Maintain an Inventory of Service Providers

Asset Type: Users	Security Function: Identify	IG1	IG2	IG3

Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, this is relevant for ICS/OT, as there are numerous vendor-managed/ controlled systems.

In the ICS OT space, there are commonly service providers that offer comprehensive solutions for a specific purpose and systems integrators that offer a wide range of available system builds and integrations into the existing control system.

These may be needed for support/administrative /integration, or specific to a piece of equipment.

In some cases, the vendor may be supporting their own products. In others, it could be a vendor who provides support for other vendors' products.

Other information to collect would include remote and/or local access requirements, criticality, availability impacts, roles and responsibilities, etc. Where feasible, it is good to understand the potential third-party organizational risk posed as well.

Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, ensure ICS OT stakeholders are involved in the policy management life cycle.

Safeguard 15.3: Classify Service Providers

Asset Type: Users	Security Function: Govern	IG2 IG3

Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, data and systems need to be classified. Identifying where sensitive data exists is important. Understand that a follow-on phase or later enhancement can change the classification of the data and therefore the system. If these are known during the design phase, they can be accounted for. When unknown during design, the enhancements may not be known by the appropriate parties, resulting in the appropriate controls possibly not being implemented.

Safeguard 15.4: Ensure Service Provider Contracts Include Security Requirements

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.

Applicability

For this Safeguard, sometimes an enterprise will be dependent on what their service provider (vendor) will support or provide. Be aware of mergers and acquisitions of service providers, as it can have direct impacts on the service provided. The contract should have provisions for mergers and acquisitions. Should a merger or acquisition occur, how it impacts on the enterprise should be addressed, including considerations of data ownership, access, retention, destruction, SLAs, incident response plan, etc.

Safeguard 15.5: Assess Service Providers

Asset Type: Users	Security Function: Govern	IG3

Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.

Applicability

For this Safeguard, there may be additional considerations whether required by regulation (e.g., NERC CIP) or possibly added from other more specific OT guidance (e.g., Purdue model, NIST SP 800-82 Rev. 3, ISA/IEC 62443, CISA Critical Infrastructure Sectors guidance).

Safeguard 15.6: Monitor Service Providers

Asset Type: Data	Security Function: Govern	IG3

Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.

Applicability

For this Safeguard, the monitoring categories should be tailored to ICS OT. Depending on if monitoring is organizational or technical, it can change the monitoring requirements and processes.

Mailing lists for the vendors, products, press releases, etc., often provide insight into the enterprise. CISA has an optional subscription for notifications specifically for ICS vulnerabilities. There are also websites dedicated to current ICS vulnerabilities. Dark web monitoring may be the most difficult portion of this Safeguard to integrate, but some threat monitoring subscription services may include this type of monitoring. At a minimum, an evaluation of available services should be performed to determine if any effective dark web monitoring is available.

General IT Security websites provide a good source of information as well. These sources may provide a perspective that includes the enterprise IT side. They may report on what the enterprise is doing, planning, or considering. This can provide advanced warning of both technical and non-technical events that can impact your contract, such as a merger, acquisition, takeover, spin-off, mass layoffs, or moving/closing of offices. Major changes in technology, the decommissioning of a technology, adding or removing new partnerships with their vendors, subcontractors, etc., can have an indirect impact.

If an enterprise has a security department, it may be worth the effort for the ICS operators/maintainers to initiate and develop a relationship with them to understand what vision the security department has into the ICS world, and what assistance they can provide.

Safeguard 15.7: Securely Decommission Service Providers

Asset Type: Data	Security Function: Protect	IG3

Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

Applicability

For this Safeguard, often times the service provider and equipment vendor will be the same. If the enterprise data resides with the provider, understanding how that will be handled is important, and should be in the contract. Sometimes the decommissioning can be for negative reasons.

As ICS systems are engineered systems, all pieces should be known and be documented. Ensure that all remote access is accounted for and removed. The identity and access management (IAM) deactivation should cover most of it, but the vendor (or you) may also have alternative methods that do not use the primary IAM process/technology. It may be under termination of data flow, but removing any applicable firewall rules, identity provider (IDP), application programming interfaces (APIs), etc., may require additional processes to ensure embedded devices are properly wiped prior to disposal.

CONTROL 16

Application Software Security

Overview

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

ICS Applicability

This Control focuses on application security in the OT environment, where countless off-the-shelf, web-based, and proprietary applications can be running on a network. This can be a big task for system administrators. It is not uncommon for ICS environments to contain some custom-engineered, in-house built web-based or other application software that is specialized for the given system. Such applications and services may not always follow a disciplined engineering development, test, and maintenance process. This can lead to application vulnerabilities that can be exploited by an attacker to aid in gaining access to or pivoting through ICS systems and network architectures. If an environment does contain this software, then this entire Control can be applied with minor modifications. This CIS Control is relevant to ICS environments if they contain web-based or other application software built by OT teams, and aspects of this Control even apply to commercial off-the-shelf (COTS) software sourced from product and solution vendors.

The first step in developing an application security program is implementing a vulnerability management process. This process must integrate into the development life cycle and should be lightweight to insert into the standard bug-fixing progress. The process should include root cause analysis to fix underlying flaws so as to reduce future vulnerabilities, and a severity rating to prioritize remediation efforts. Applications are rarely created from scratch, and are often "assembled" from a complex mix of development frameworks, libraries, existing code, and new code. A software bill of materials (SBOM) should be collected for each application; third-party application providers should be evaluated for compliance with SBOM best practices. These factors make traditional approaches to security, like control (of processes, code sources, run-time environment, etc.), inspection, and testing, much more challenging. Also, the risk that an application vulnerability introduces might not be understood, except in a specific operational setting or context.

ICS Challenges

There are legacy programming languages that may not support secure coding.

ICS are used to monitor and control physical processes and are considered cyber physical systems. They have a connection to robots, sensors, PLCs, etc., that allow interaction with the physical world. Therefore, security vulnerabilities and issues in general can have a safety impact and impact on health and life.

COTS developed software does not necessarily take security into consideration when being developed.

Understanding the shared responsibility matrix can be difficult.

All the Safeguards are applicable although Safeguards related to automated scanning may not be appropriate.

ICS Additional Discussion

The ideal application security program is one that introduces security as early into the software development life cycle as possible. The management of security problems should be consistent and integrated with standard software flaw/bug management, as opposed to a separate process that competes for development resources. Larger or more mature development teams should consider the practice of threat modeling in the design phase. Design-level vulnerabilities are less common than code-level vulnerabilities; however, they often are very severe and much harder to fix quickly. Threat modeling is the process of identifying and addressing application security design flaws before code is created. Threat modeling requires specific training, technical knowledge, and business knowledge. It is best conducted through internal "security champions" in each development team, to lead threat modeling practices for that team's software. It also provides valuable context to downstream activities, such as root cause analysis and security testing.

Application vulnerabilities can be present for many reasons: insecure design, insecure infrastructure, coding mistakes, weak authentication, and failure to test for unusual or unexpected conditions. Attackers can exploit specific vulnerabilities as a launching point for further attacks.

It is now more common to acquire Software as a Service (SaaS) platforms, where software is developed and managed entirely through a third party. These might be hosted anywhere in the world. This brings challenges to OT enterprises that need to know what risks they are accepting with using these platforms, and they often do not have visibility into the development and application security practices of these platforms. Some of these SaaS platforms allow for customizing of their interfaces and databases. Enterprises that extend these applications should follow this CIS Control, similar to if they were doing ground-up development.

Finally, in 2020 NIST® published its Secure Software Development Framework (SSDF), which brought together what the industry has learned about software security over the past two decades and created a secure software development framework for planning, evaluating, and communicating about software security activities. Enterprises acquiring software or services can use this framework to build their security requirements and understand whether a software provider's development process follows best practices. These are some application security resources:

- **SAFECode Application Security Addendum:** https://safecode.org/cis-controls/
- **NIST® SSDF:** https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf
- **The Software Alliance:** https://www.bsa.org/reports/updated-bsa-framework-for-secure-software
- **OWASP®:** https://owasp.org

Be sure to test in-house developed and third-party procured web applications for common security weaknesses using automated application scanners during scheduled maintenance when performance of these applications won't negatively affect the process. Monitoring for the release of software security patches and general product upgrades is an important aspect of maintaining software security. However, retesting after the application of said patches and upgrades is critical since it is not uncommon for new services, capabilities, or features to be introduced or enabled, or configuration changes or resets to result from applying these patches and upgrades.

Obtaining software patches and upgrades from only the most reputable sources and taking care in the secure transfer of these files is necessary to ensure software assurance, and product and system security. Verifying file hashes, or more ideally making use of digitally signed software, and using only vendor-approved methods and tools to apply updates, helps with this assurance. Ensuring that the most current and relevant patch or software version is used, and avoiding older versions that may contain known or unknown vulnerabilities, also help with software assurance.

Safeguards

Safeguard 16.1: Establish and Maintain a Secure Application Development Process

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, many ICS systems will be built from vendor products with little software development required of the end-user enterprise. However, to the extent that the end-user enterprise is required to create application software or scripts to control the ICS system, secure development of that software is critically important. The enterprise should rely on published best practices, lessons learned from root cause analysis of its own and other organizations' reported vulnerabilities (see CIS Safeguard 16.3), industry standards, and public advisories from organizations such as CISA to create and update its secure development process. The IEC 62443-4-1 standard defines secure product development life cycle requirements for Industrial Automation Control Systems (IACS) and their components, such as PLCs.

Safeguard 16.2: Establish and Maintain a Process to Accept and Address Software Vulnerabilities

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.

Applicability

For this Safeguard, consider a fresh perspective of "Where are we today and where is the technology in this space heading?" This process may need frequent re-evaluation as the OT space is rapidly evolving due to changes in technology.

Some mitigations may not be addressable through upgrades or patching alone. Ensure proper internal processes exist to find and address software vulnerabilities, versus relying on being informed by a vendor or other entity.

Tracking and reporting will likely be more involved unless a system is deployed capable of tracking activity and compliance for both IT and OT environments.

Safeguard 16.3: Perform Root Cause Analysis on Security Vulnerabilities

Asset Type: Software	Security Function: Protect	IG2	IG3

Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.

Applicability

For this Safeguard, the enterprise should perform root cause analysis and identify any actions that it should take to remediate vulnerabilities in current software. These lessons should be applied to any other software in the OT environment which may be similarly vulnerable. These "lessons learned" should be documented and reviewed to prevent similar vulnerabilities from being introduced in the future.

Safeguard 16.4: Establish and Manage an Inventory of Third-Party Software Components

Asset Type: Software	Security Function: Identify	IG2 IG3

Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.

Applicability

For this Safeguard, SBOM is an emerging approach. While not all vendors currently can or will provide this information, it is still best practice to request this information from the vendor. This information, if available, should be captured and reviewed. If an SBOM is not available, there should be a process to check with applicable vendors if a third-party software vulnerability occurs (e.g., Log4j). This process could be added to an existing OT vulnerability management process. If the enterprise is internally developing software that involves the use of externally produced components, then the enterprise should create and maintain its own SBOM to enable faster and more complete response to discovered vulnerabilities.

Safeguard 16.5: Use Up-to-Date and Trusted Third-Party Software Components

Asset Type: Software	Security Function: Protect	IG2 IG3

Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.

Applicability

For this Safeguard, applicability will depend on vendor sophistication and information availability for purchased or open-source application components. All effort should be made to properly validate all components of an internally developed application.

In the OT space, up to date may not be most current due to application/system incompatibilities. This "maximum viable version" may be many revisions behind. Any such situation should be documented and addressed as part of the vulnerability management and risk assessment process to ensure that any risk this may, or does, pose to the OT environment is understood and tracked.

As for procuring and downloading software, firmware, etc., there should be a process to get it only from trusted sources; software packages should be properly validated once downloaded.

Safeguard 16.6: Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.

Applicability

For this Safeguard, a contextualized evaluation and prioritization mechanism must be in place regardless of the device type (traditional desktop and servers OS, embedded device, etc.) that will help determine when and what vulnerabilities to address. Tracking and reporting will likely be more involved unless a system is deployed capable of tracking activity and compliance for both IT and OT environments. As vulnerability severity ratings may not be comparable between various sources, it is important to define a process which can accurately track the severity of any vulnerabilities with respect to the particulars of the IT and OT environments.

Safeguard 16.7: Use Standard Hardening Configuration Templates for Application Infrastructure

Asset Type: Software	Security Function: Protect	IG2 IG3

Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.

Applicability

For this Safeguard, while templates may not exist, some OT vendors provide hardening guides for their applications/systems. Common/base hardening (e.g., operating system and commodity applications) is also applicable but requires scoping, testing, and validation to ensure there are no negative impacts to the OT environment. If there are cloud-based systems the same basic concepts and caveats apply, though they may be applied differently than in a privately hosted environment. There also should be a mechanism to test adherence to the hardening standards and ongoing compliance. There may be circumstances where this Safeguard is not feasible, but every effort should be made to comply.

Updated CIS hardening guides and compliance suites would be a great resource assuming that ICS software is common enough for common guides to be practical.

Safeguard 16.8: Separate Production and Non-Production Systems

Asset Type: Network	Security Function: Protect	IG2 IG3

Maintain separate environments for production and non-production systems.

Applicability

For this Safeguard, to the extent possible a separated dev/QA environment is recommended. However, it is likely not feasible to have a full dev/QA environment in OT. If possible, the enterprise should have logically separated, representative systems that are available for testing configuration changes, etc. This helps minimize negative impacts resulting from testing on production equipment. Non-production interactions will likely occur during downtime windows.

Safeguard 16.9: Train Developers in Application Security Concepts and Secure Coding

Asset Type: Users	Security Function: Protect	IG2 IG3

Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.

Applicability

For this Safeguard, this may have some overlap in the OT space (i.e., devs may need to create applications providing front-end interfaces for various processes, to be accessed via web browser, etc.). There are more resources beginning to become available to assist with this Safeguard. OT code development is usually much different from traditional IT-related programming, making this less applicable unless the enterprise writes their own software or a vendor provides software.

The closest developer guidance within ICS is the Top 20 PLC Secure Coding Practices.

Safeguard 16.10: Apply Secure Design Principles in Application Architectures

Asset Type: Software	Security Function: Protect	IG2 IG3

Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.

Applicability

For this Safeguard, as the IT and OT worlds continue to grow closer together, where these things are possible implementing this Safeguard would be a good practice. There are some elements of this in HMI design (i.e., limiting the upper and lower bounds of certain set points, some PLCs validate the requests/responses they receive when updating a set point or getting an instruction, etc.). As for the hardening elements, there are some things that will be helpful in reducing the attack surface of the OT applications.

Safeguard 16.11: Leverage Vetted Modules or Services for Application Security Components

Asset Type: Software	Security Function: Identify	IG2 IG3

Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.

Applicability

For this Safeguard, many of these things are lacking within existing OT offerings, most specifically on embedded devices, but this may be more feasible on solutions based on a commodity OS (e.g., Windows, Linux).

This is an opportunity to evaluate current platform functionality to see what is available and to what extent. Gaps can be documented to align on risk acceptance where this is not feasible, and it will also provide a guide for areas of improvement internally, or to work with vendors to improve.

Safeguard 16.12: Implement Code-Level Security Checks

Asset Type: Software	Security Function: Protect	IG3

Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.

Applicability

For this Safeguard, this should be implemented where feasible. If it cannot be done, code review by peers should be done at minimum. Top 20 PLC Secure Coding Practices provide some more applicable options, though not through automated testing at this point.

Safeguard 16.13: Conduct Application Penetration Testing

Asset Type: Software	Security Function: Detect	IG3

Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

Applicability

For this Safeguard, any vulnerability assessment or penetration testing occurring within the ICS OT environment requires an approach focused on safety and is highly likely to require downtime. This should be done by enterprises with specific expertise in assessing OT environments.

The scoping, approach/methods, goals, etc., will require augmentation beyond traditional approaches to ensure the correct goals are achieved and they are realistic to the threats encountered.

Safeguard 16.14: Conduct Threat Modeling

Asset Type: Software	Security Function: Protect	IG3

Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.

Applicability

For this Safeguard, while not necessarily application specific, threat modeling is useful in the OT space and should be realistic to potential attacker capabilities, organization, critical infrastructure vertical, etc. Threat modeling, as referred to in this Safeguard, is a structured search for design-level vulnerabilities and for areas to focus a search for potential coding errors. Threat modeling should enable enterprises to identify where security mitigations are required, and whether they take the form of software coding changes, hardware or software configuration changes, or operational procedures.

CONTROL 17

Incident Response Management

Safeguards: 9	IG1: 3/9	IG2: 8/9	IG3: 9/9

Overview

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

ICS Applicability

This CIS Control addresses the processes and steps required to prepare for an incident. Well-defined and implemented incident response plans can allow an enterprise to identify, contain, reduce impacts, and more quickly recover from a cyber incident. This is especially important for enterprises where ICS downtime can lead to safety, health, or profitability impacts affecting the company, employees, customers, supply chain partners, community, and other constituents depending on the safe, reliable operation of an enterprise.

Most OT teams are accustomed to performing some aspects of backups of critical systems to mitigate risks of failed components, loss of services, accidental employee actions, or even aspects of natural disasters. There is often a gap in the other areas of incident response, such as efficient coordination, chain of command, decision-making authority, impact isolation, reporting, data collection, management responsibility, legal protocols, and communications strategy. Furthermore, it is not unusual for such processes to not be adequately or periodically tested, let alone evolve over time as new variables emerge, risks are identified, and threats evolve.

All of the Safeguards are applicable.

ICS Challenges

For this CIS Controls consider the following challenges:

- The time it takes to properly prepare for a tabletop exercise
- Getting all of the right people together at the same time for the tabletop exercise
- Keeping an incident response plan update today
- The unknowns and those unknown needs
- Obtaining and maintaining the cost of cyber insurance. Be aware of the stipulations with cyber insurance should there be an incident so as to not violate the terms of the insurance policy.

ICS Additional Discussion

For this CIS Control consider the following additional steps:

- If extending an IT Incident Response Plan, ensure the Plan has been reviewed and approved by ICS Operational Leadership and covers all aspects of the OT environment.
- Response teams should be thoroughly familiar with the risks inherent to the ICS environment and the mitigations to prevent secondary damage that may impact operational safety and protection of personnel, equipment, information, and a myriad of other dependent and interdependent factors.

Aspects of this CIS Control can mimic plans and procedures from non-ICS environments. However, it is not uncommon for these plans to require an augmentation of IT plans and procedures already in place for an enterprise's information technology system in order to be relevant, applicable, and complete for OT.

One other area that is often overlooked is the loss of life due to the event. The "aspects of natural disasters" are often overlooked parts of the process. Be prepared for situations where a key resource may not be available. Keep in mind taking people out of their comfort zone that the assumptions may not be correct.

Tabletop exercises are invaluable for enterprises to work through possible scenarios. Removing a person could reinforce the importance of understanding the loss of life possibility. An example would be to scramble the roles of the participants to make them interpret and react to the event from another perspective. Roles should broadly match skill set, if possible, for best results in a published Incident Response Plan. This can broaden the vision and understanding of everyone involved.

SANS has identified a top 5 ICS controls and where there is alignment with the CIS Controls, they prioritize in this manner and focus on those areas.

For ICS OT environments, it is possible that an enterprise may find that reordering the Safeguards would better meet their needs, and consideration of reordering the Safeguards for this CIS Control may be warranted.

- **Safeguard 17.1:** *Designate Personnel to Manage Incident Handling.* This could remain as 17.1 because people need to be designated in order to manage the remaining Safeguards.
- **Safeguard 17.9:** *Establish and Maintain Security Incident Thresholds.* This Safeguard is about incident response, so defining upfront what an incident is will help the rest flow.
- **Safeguard 17.3:** *Establish and Maintain an Enterprise Process for Reporting Incidents.* Now that incidents are defined, reporting them can be covered.
- **Safeguard 17.4:** *Establish and Maintain an Incident Response Process.* This Safeguard closely resembles 17.3, and they might possibly be able to be combined.
- **Safeguard 17.5:** *Assign Key Roles and Responsibilities.* This Safeguard is part of the process from Safeguards 17.3 and 17.4.
- **Safeguard 17.6:** *Define Mechanisms for Communicating During Incident Response.* This Safeguard now appears ahead of "Establish and Maintain Contact Information for Reporting Security Incidents" (currently 17.2) since 17.2 may be dependent on the mechanisms that are in use being defined.
- **Safeguard 17.2:** *Establish and Maintain Contact Information for Reporting Security Incidents.* After roles and responsibilities are assigned, and mechanisms of contact are determined, "who contacts whom" when reporting can be established.
- **Safeguard 17.8:** *Conduct Post-Incident Reviews.* This Safeguard is part of an actual incident review, and now appears ahead of the Safeguard for ongoing exercises.
- **Safeguard 17.7:** *Conduct Routine Incident Response Exercises.* This Safeguard covers the routine follow-on exercises used to test and train for handling an actual incident.

SANS has identified a top 5 ICS controls and where there is alignment with the CIS Controls, they prioritize in this manner and focus on those areas.

Safeguards

Safeguard 17.1: Designate Personnel to Manage Incident Handling

Asset Type: Users	Security Function: Respond	IG1 IG2 IG3

Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, service providers, or a hybrid approach. If using a service provider, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard when there are specific OT incident response personnel or combined with enterprise incident response, there must be additional training on ICS/OT specific threats, a solid understanding of engineering device operations and related consequences if unavailable, while prioritizing safety above all else, and effectively, engaging ICS incident response with operational staff leading the charge, etc. Cross training helps cover potential gaps and helps avoid single points of failure.

Safeguard 17.2: Establish and Maintain Contact Information for Reporting Security Incidents

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service providers, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.

Applicability

For this Safeguard, the contact information should be published and socialized as part of the incident reporting process, whether through traditional service/help desk or specific SOC.

Safeguard 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents

Asset Type: Documentation	Security Function: Govern	IG1	IG2	IG3

Establish and maintain an documented enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, establish and maintain an enterprise process for incident reporting that includes the specifics for the OT workforce to report security incidents.

Safeguard 17.4: Establish and Maintain an Incident Response Process

Asset Type: Documentation	Security Function: Govern	IG2	IG3

Establish and maintain a documented incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, OT incidents would represent one or more playbooks in the incident response plan.

Safeguard 17.5: Assign Key Roles and Responsibilities

Asset Type: Users	Security Function: Respond	IG2 IG3

Assign key roles and responsibilities for incident response, including staff from incident responders, analysts, and relevant third parties. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, ensure proper identification of local site (plant/site) resources. Ensure workforce members who are assigned roles know and understand their responsibilities. A primary and a backup should be designated for each role to allow for coverage in an absence. Cross-training may assist in covering gaps. Depending on the criticality of the role a tertiary backup may be considered.

Safeguard 17.6: Define Mechanisms for Communicating During Incident Response

Asset Type: Users	Security Function: Respond	IG2 IG3

Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, secure chat, or notification letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, communication methods need to work for local sites as well (i.e., being in an industrial environment can create additional challenges). These methods should be communicated and practiced. Sufficient alternatives should be available in case certain methods fail or are insufficient. In some cases, there may be more than one communication mechanism used simultaneously. In these cases, consistent messaging is important. It also needs to be clear who can communicate what with whom. For example, who can communicate with the media? A “tree type” communications link layout could be helpful, so that inheritance can be understood. Succession needs to be considered, as the loss of personnel is often overlooked. Having one or more backups to the primary contact helps address this concern.

Safeguard 17.7: Conduct Routine Incident Response Exercises

Asset Type: Users	Security Function: Recover	IG2 IG3

Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.

Applicability

For this Safeguard, the exercises should include the plant/site personnel. These should be applicable/relevant to OT, using a variety of methods (e.g., tabletop exercises, etc.), and have varied depths for the exercise to target the appropriate personnel. Start small and build. Be sure to conduct "lessons learned" reviews to improve the exercise process and operations.

One possible way to enhance the exercises is to put individuals in positions they would not normally be in; this allows participation from a different perspective. The performance of the individual in the unfamiliar role can be evaluated by those more familiar with the role. Any lessons learned from this process could better inform the incident response plan and lead to improvement.

Safeguard 17.8: Conduct Post-Incident Reviews

Asset Type: Users	Security Function: Recover	IG2 IG3

Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

Applicability

For this Safeguard, post-incident reviews (e.g., after action report, root cause analysis, lessons learned, etc.) are a necessary element of responding to incidents and exercises, including what went well and identifying areas where improvements can be made. It is helpful to have a template to guide these discussions to ensure coverage for the needed areas, and ensure that all relevant teams provide input. A review should be a timely, flexible, and inclusive engagement for local site personnel which may have varying availability based on work type, schedule/shift, etc. When complete, the information needs to be shared so that everyone can improve. All effort should be made to avoid placing undue blame on an individual/team/etc. Fault, if any, should be noted for full recordkeeping, but the primary goal is to improve the incident response process, identify and fill training gaps, etc.

Safeguard 17.9: Establish and Maintain Security Incident Thresholds

Asset Type: Documentation	Security Function: Recover	IG3

Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Applicability

For this Safeguard, this should be part of any incident response process. Be sure to allow adequate time, as it will be a complex process. Depending on one's perspective, definitions are not always clear. There should be specific conversations on how/where OT thresholds may need to be different from the traditional enterprise. Ensure that local site personnel have input into and understand these thresholds. Consider pipeline security directives, CIP-008, NRC, DOE, etc.

CONTROL 18

Penetration Testing

Safeguards: 5	IG1: 0/5	IG2: 3/5	IG3: 5/5

Overview

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

ICS Applicability

This CIS Control is focused on designing and conducting controlled penetration testing in an operational technology environment, including connected devices and systems that may not be normally viewed as a constituent component, service, or system for an ICS. The goal is to test both employee responsiveness and the resiliency of internal controls. It refers to conducting tests on connected products, systems, and other interconnected products and systems in a real-time manner to identify, isolate, and demonstrate exploitability of a weakness or vulnerability in the security posture of the ICS.

Processes controlled by ICS environments are easily disrupted by penetration testing, red team exercises, or other similar activities. Performing these activities on production systems, even during scheduled outages, can lead to downtime, destruction, injury, or introduce lingering artifacts that reduce the safety, efficiency, or performance of the tested system.

For these reasons, it is highly recommended to only perform penetration testing and red team exercises on non-production systems, such as lab equipment, during scheduled downtime or during factory acceptance testing with proper oversights and precautions before a system is installed. However, such testing should be conducted periodically since system configurations change, new vulnerabilities are discovered, new threats emerge, and tools and testing methodologies evolve.

When analyzing production systems, it is recommended to use security assessments that are nonintrusive. These assessments can be paper-based, and can used passive enumeration of system and network details or any other activity that does not impact the safety, availability and performance of the ICS environment.

ICS Challenges

Well-planned and coordinated penetration tests can be useful for related Safeguards. Alternatively, an architecture and vulnerability assessment can be an option. Safeguards relating to penetration tests on production systems may not apply. These Safeguards do apply when testing on test beds or non-production systems.

ICS Additional Discussion

Instead of exclusively relying on an internal OT team, also consider conducting regular nonintrusive security assessments with the assistance of third parties to identify a greater diversity of vulnerabilities and attack vectors that can be used to breach security of ICS systems.

Ensure that personnel conducting vulnerability assessments are skilled in working within ICS environments to reduce the possibility of inadvertent negative impact to operations. Careful consideration should be given to the training, experience level, and pedigree of those performing such assessments.

Include tests for the presence of unprotected system information, data leakage, and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, documents containing passwords, or other information critical to system operation.

Consider using results from vulnerability scans and security assessments in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus security testing efforts. Furthermore, these results should operate as a guide for developing and applying corrective measures and other compensating controls to mitigate risks and better safeguard systems from threats.

Human and functional safety, as well as protecting digital and physical assets, throughout the testing process is paramount. Testing an ICS environment's security posture is important, but not as important as ensuring the safety of personnel and systems that are critical to continued operations.

Safeguards

Safeguard 18.1: Establish and Maintain a Penetration Testing Program

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain a penetration testing program appropriate to the size, complexity, industry, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

Applicability

For this Safeguard, to the extent possible, careful scoping of the pen testing program should be done with a focus on safety and potential for production impact. A test environment, if available, provides a good starting point for testing without impacting production; this allows for better understanding of the potential impact of pen testing in the production environment. Apply the appropriate type and scope of assessment to the need.

Safeguard 18.2: Perform Periodic External Penetration Tests

Asset Type: Network	Security Function: Detect	IG2 IG3

Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.

Applicability

For this Safeguard, the assessor must be capable of safely and effectively performing these types of activities against OT environments. This testing needs to be applicable and realistic to the enterprise. In the OT context, consider for example:

- Attempting to access the OT environment from the enterprise network, potentially performed against a jump host after first compromising the enterprise network, credentials, systems, etc.
- If there are known internet-driven and/or internet-bound connections, this is a potential attack vector.
- Any remote access for employees and/or vendors should be considered a potential attack vector.
- Other attack vectors may exist depending on the specific OT environment.

Safeguard 18.3: Remediate Penetration Test Findings

Asset Type: Network	Security Function: Protect	IG2 IG3

Remediate penetration test findings based on the enterprise's documented vulnerability remediation process. This should include determining a timeline and level of effort based on the impact and prioritization of each identified finding.

Applicability

For this Safeguard, having a prioritized, detailed data-based remediation plan generated from findings is needed. The prioritization should also take into account actual risk reduction benefit, resources necessary, financial implications, etc.

Safeguard 18.4: Validate Security Measures

Asset Type: Network	Security Function: Protect	IG3

Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.

Applicability

For this Safeguard, this could also be an opportunity to improve detections across zone boundaries if the enterprise has this capability. The ease of building out the validations may also depend on the type of test defined and executed.

A purple team exercise may be the more advantageous approach here as the testers and defenders work through different scenarios together to see what was prevented and/or detected, and what was not, and why. However, a red team exercise need not be excluded if the environment is ready for it.

Safeguard 18.5: Perform Periodic Internal Penetration Tests

Asset Type: Network	Security Function: Detect	IG3

Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.

Applicability

For this Safeguard, it is important to focus on safety and effectiveness. Enterprises may not have sufficient internal capabilities to conduct this level of testing. There are risk and landscape visualization solutions (i.e., attack surface management) that can provide some of this information on an ongoing basis, but these solutions are not a cure-all, nor do they replace human assessors.

Closing Notes

In this document, we provide guidance on how to apply the security best practices found in CIS Controls Version 8.1 to ICS environments. By walking through CIS Controls Version 8.1 with this Companion guide, the reader should be able to tailor the CIS Controls in the context of a specific IT/OT enterprise as an essential starting point for a security improvement assessment and roadmap. The newest version of the CIS Controls and other complementary documents may be found at www.cisecurity.org.

As a nonprofit organization driven by its volunteers, we are always in the process of looking for new topics and assistance in creating cybersecurity guidance. If you are interested in volunteering and/or have questions, comments, or have identified ways to improve this guide, please write us at: controlsinfo@cisecurity.org.

All references to tools or other products in this document are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Contact Information

CIS
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlsinfo@cisecurity.org

Appendix

Acronyms and Abbreviations

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AD	Active Directory
API	Application Programming Interface
ARP	Address Resolution Protocol
BYOD	Bring Your Own Device
CERT	Computer Emergency Response Team
CIS	Center for Internet Security
CLI	Command Line Interface
COTP	Connection Oriented Transport Protocol
COTS	Commercial Off the Shelf
DCS	Distributed Control Systems
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
DR	Disaster Recovery
EMM	Enterprise Mobility Management
EoL	End of Life
EoS	End of Support
FAT	Factory Acceptance Test
GRC	Governance Risk and Compliance
HIDS	Host-based Intrusion Detection System
HMI	Human Machine Interface
IACS	Industrial Automation Controls Systems
IAM	Identity and Access Management
ICS	Industrial Controls Systems
IDP	Identity Provider
IOC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Protection System
ISAC	Information Sharing and Analysis Centers
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
KSA	Knowledge, Skills, and Abilities
LDAP	Lightweight Directory Access Protocol
LTS	Long-Term Support
MAC	Media Access Control
MDM	Mobile Device Management
MDR	Managed Detection and Response
MFA	Multi-Factor Authentication
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
NaaS	Network as a Service
NAC	Network Access Control
NGFW	Next Generation Firewall
NIDS	Network Intrusion Detection Systems
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OS	Operating System
OT	Operational Technology
PCAP	Packet Capture

PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PoLF	Principle of Least Privilege
RACI	Responsible, Accountable, Consulted, and Informed
RBAC	Role-Based Access Control
RSU	Roadside Unit
RTOS	Real-Time Operating Systems
SaaS	Software as a Service
SAT	Site Acceptance Test
SBOM	Software Bill of Materials
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SOC	Security Operations Center
SSDF	Secure Software Development Framework
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPKT	ThroughPacket
TTPs	Tactics, Techniques, and Procedures
UEM	Unified Endpoint Management
VLANS	Virtual Local Area Networks
VPN	Virtual Private Network
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
XDR	Extended Detection and Response

Glossary

3-2-1 Backup policy

The 3-2-1 backup strategy is a popular rule of thumb for protecting data by making multiple copies.

Access control

The process of granting or denying specific requests for obtaining and using information and related information processing services; and to enter specific physical facilities (e.g., federal buildings, military establishments, and border crossing entrances).

Adequate security

Security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

Administrator accounts

Dedicated accounts with escalated privileges and used for managing aspects of a computer, domain, or the whole enterprise information technology infrastructure. Common administrator account subtypes include root accounts, local administrator and domain administrator accounts, and network or security appliance administrator accounts.

Application

A program, or group of programs, hosted on enterprise assets and designed for end-users. Applications are considered a software asset in this guide. Examples include web, database, cloud-based, and mobile applications.

Application

A software program hosted by an information system.

Assessment

See control assessment or risk assessment.

Assessor

The individual, group, or organization responsible for conducting a security or privacy control assessment.

Assurance

Grounds for justified confidence that a [security or privacy] claim has been or will be achieved.
Note 1: Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g., security claims, safety claims) and the claims themselves may be interrelated. Note 2: Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims.

Attack surface

The set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from that system, component, or environment.

Audit

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures

Audit log

A chronological record of system activities, including records of system accesses and operations performed in a given period.

Audit trail

A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to result.

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

Authentication systems

A system or mechanism used to identify a user through associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system, user directory service, or within an authentication server. Examples of authentication systems can include active directory, Multi-Factor Authentication (MFA), biometrics, and tokens.

Authenticator

Something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. This was previously referred to as a token.

Authorization

Access privileges granted to a user, program, or process or the act of granting those privileges.

Authorization systems

A system or mechanism used to determine access levels or user/client privileges related to system resources including files, services, computer programs, data, and application features. An authorization system grants or denies access to a resource based on the user's identity. Examples of authorization systems can include active directory, access control lists, and role-based access control lists.

Availability

Ensuring timely and reliable access to and use of information.

Baseline

See control baseline.

Boundary

Physical or logical perimeter of a system. See also authorization boundary and interface.

Breach

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for an unauthorized purpose.

Breadth

An attribute associated with an assessment method that addresses the scope or coverage of the assessment objects included with the assessment.

Capability

A combination of mutually reinforcing security and/or privacy controls implemented by technical, physical, and procedural means. Such controls are typically selected to achieve a common information security or privacy-related purpose.

Category

The subdivision of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.

Central management

The organization-wide management and implementation of selected security and privacy controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security and privacy controls and processes.

CIA triad

Represents the three pillars of information security: confidentiality, integrity, and availability

Cloud environment

A virtualized environment that provides convenient, on-demand network access to a shared pool of configurable resources such as network, computing, storage, applications, and services. There are five essential characteristics to a cloud environment: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Some services offered through cloud environments include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Compensating controls

The security and privacy controls employed in lieu of the controls in the baselines described in NIST Special Publication 800-53B that provide equivalent or comparable protection for a system or organization.

Component

See system component.

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration item

An aggregation of system components that is designated for configuration management and treated as a single entity in the configuration management process.

Continuous monitoring

Maintaining ongoing awareness to support organizational risk decisions.

Control

See security control or privacy control.

Credential

An object or data structure that authoritatively binds an identity, via an identifier or identifiers, and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.

Critical infrastructure

Essential services and related assets that underpin American society and serve as the backbone of the nation's economy, security, and health. [DHS]

Critical infrastructure

Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Critical services

The subset of mission-essential services required to conduct manufacturing operations. Function or capability that is required to maintain health, safety, the environment, and availability for the equipment under control. [62443]

Cybersecurity

The process of protecting information by preventing, detecting, and responding to attacks. [CSF]

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Cyberspace

The interdependent network of information technology infrastructures that includes the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

Data historian

A data historian is a software program that records the data of processes running in a computer system. Organizations use data historians to gather information about the operation of programs to diagnose failures when reliability and up-time are critical.

Database

Organized collection of data, generally stored and accessed electronically from a computer system. Databases can reside remotely or on-site. Database Management Systems (DMSs) are used to administer databases, and are not considered part of a database for this guide.

Defense-in-depth

The application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another. [62443 1-1]

Depth

An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method.

Developer

A general term that includes developers or manufacturers of systems, system components, or system services; systems integrators; vendors; and product resellers. The development of systems, components, or services can occur internally within organizations or through external entities.

Domain

An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See security domain.

End-user devices

Information technology (IT) assets used among members of an enterprise during work, off-hours, or for any other purpose. End-user devices include mobile and portable devices such as laptops, smartphones and tablets, as well as desktops and workstations. For the purpose of this guide, end-user devices are a subset of enterprise assets.

Enterprise

An organization with a defined mission/goal and a defined boundary, using systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, human resources, financial management, security and systems, information, and mission management. See also organization.

Enterprise assets

Assets with the potential to store or process data. For the purpose of this guide, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers, in virtual, cloud-based, and physical environments.

Event

Any observable occurrence on a manufacturing system. Events can include cybersecurity changes that may have an impact on manufacturing operations (including mission, capabilities, or reputation). [CSF]

Event

Any observable occurrence in a system.

Executive agency

An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

Externally-exposed enterprise assets

This refers to enterprise assets that are public facing and discoverable through domain name system reconnaissance and network scanning from the public internet outside of the enterprise's network.

Failover

The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby system upon the failure or abnormal termination of the previously active system.

Firmware

Software program or set of instructions programmed on the flash ROM of a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware. [Techterms.com]

Firmware

Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs. See also hardware and software.

Framework

The Cybersecurity Framework developed for defining protection of critical infrastructure. It provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. Includes activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes.

Function

Primary unit within the Cybersecurity Framework. Exhibits basic cybersecurity activities at their highest level.

Hardware

The material physical components of a system. See also software and firmware

Identifier

Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. A unique label used by a system to indicate a specific entity, object, or group.

Impact

The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system.

Incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [CSF]

Incident

An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Industrial control system

General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) found in the industrial sectors and critical infrastructures. An industrial control system consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

Information

Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.

Information security

The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information technology

Any services, equipment, or interconnected system(s) or subsystem(s) of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires its use or, to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.

Insider threat

The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of organizational operations and assets, individuals, other organizations, and the Nation. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of organizational resources or capabilities.

Integrator

A value-added engineering organization that focuses on industrial control and information systems, manufacturing execution systems, and plant automation, that has application knowledge and technical expertise, and provides an integrated solution to an engineering problem. This solution includes final project engineering, documentation, procurement of hardware, development of custom software, installation, testing, and commissioning. [CSIA.com] NISTIR 8183 CYBERSECURITY FRAMEWORK MANUFACTURING PROFILE 48. This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8183

Integrity

Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.

Interface

Common boundary between independent systems or modules where interactions take place.

Internal enterprise assets

Refers to non-public facing enterprise assets that can only be identified through network scans and reconnaissance from within an enterprise's network through authorized authenticated or unauthenticated access.

Least privilege

The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Local access

Access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

Malicious code

Software or firmware intended to perform an unauthorized process that will have adverse impacts on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Manufacturing operations

Activities concerning the facility operation, system processes, materials input/output, maintenance, supply and distribution, health, and safety, emergency response, human resources, security, information technology and other contributing measures to the manufacturing enterprise.

Media

Physical devices or writing surfaces including magnetic tapes, optical disks, magnetic disks, Large-Scale Integration memory chips, and printouts (but excluding display media) onto which information is recorded, stored, or printed within a system.

Mobile device

A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable data storage; and is powered on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, tablets, and e-readers.

Mobile end-user devices

Small enterprise-issued end-user devices with intrinsic wireless capability, such as smartphones and tablets. Mobile end-user devices are a subset of portable end-user devices, including laptops, which may require external hardware for connectivity. For the purpose of this guide, mobile end-user devices are a subset of end-user devices.

Multi-factor authentication

An authentication system or an authenticator that requires more than one authentication factor for successful authentication. Multi-factor authentication can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors.

Network

A system implemented with a collection of connected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Network access

Any access across a network connection in lieu of local access (i.e., user being physically present at the device).

Network access

Access to a system by a user (or a process acting on behalf of a user) communicating through a network, including a local area network, a wide area network, and the internet.

Network devices

Electronic devices required for communication and interaction between devices on a computer network. Network devices include wireless access points, firewalls, physical/virtual gateways, routers, and switches. These devices consist of physical hardware, as well as virtual and cloud-based devices. For the purpose of this guide, network devices are a subset of enterprise assets.

Network infrastructure

Refers to all of the resources of a network that make network or internet connectivity, management, business operations, and communication possible. It consists of hardware and software, systems and devices, and it enables computing and communication between users, services, applications, and processes. Network infrastructure can be cloud, physical, or virtual.

Non-computing/internet of things (iot) devices

Devices embedded with sensors, software, and other technologies for the purpose of connecting, storing, and exchanging data with other devices and systems over the internet. While these devices are not used for computational processes, they support an enterprise's ability to conduct business processes. Examples of these devices include printers, smart screens, physical security sensors, industrial control systems, and information technology sensors. For the purpose of this guide, non-computing/IoT devices are a subset of enterprise assets.

Object

Passive system-related entity, including devices, files, records, tables, processes, programs, and domains that contain or receive information. Access to an object (by a subject) implies access to the information it contains. See also subject.

Operating system

System software on enterprise assets that manages computer hardware and software resources, and provides common services for programs. Operating systems are considered a software asset and can be single- and multi-tasking, single- and multi-user, distributed, templated, embedded, real-time, and library.

Operational technology

Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. [Gartner.com]

Operational Technology Teams

OT Teams maintain critical infrastructure and industrial environments. OT teams often rely heavily on vendor technologies, products, systems, and services.

Organization

An entity of any size, complexity, or positioning within an organizational structure, including federal agencies, private enterprises, academic institutions, state, local, or tribal governments, or, as appropriate, any of their operational elements.

Penetration testing

A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system.

Portable end-user devices

Transportable end-user devices that have the capability to wirelessly connect to a network. For the purpose of this guide, portable end-user devices can include laptops and mobile devices such as smartphones and tablets, all of which are a subset of enterprise assets.

Portable storage device

A system component that can communicate with and be added to or removed from a system or network and that is limited to data storage—including text, video, audio or image data—as its primary function (e.g., optical disks, external or removable hard drives, external or removable solid-state disk drives, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks).

Potential impact

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (FIPS Publication 199 low); a serious adverse effect (FIPS Publication 199 moderate); or a severe or catastrophic adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.

Privileged user

A user that is authorized (and therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Programmable logic controller

A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three-mode (PID) control, communication, arithmetic, and data and file processing. [800-82]

Protocol

A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. [800-82]

Public key infrastructure

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates.

Records

All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

Red team exercise

An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions or business processes and to provide a comprehensive assessment of the security capabilities of an organization and its systems.

Remote access

Access by users (or information systems) communicating externally to an information system security perimeter. Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). [800-53]

Remote access

Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network.

Remote devices

Any enterprise asset capable of connecting to a network remotely, usually from public internet. This can include enterprise assets such as end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers.

Remote file systems

These enable an application that runs on an enterprise asset to access files stored on a different asset. Remote file systems often make other resources, such as remote non-computing devices, accessible from an asset. The remote file access takes place using some form of local area network, wide area network, point-to-point link, or other communication mechanism. These file systems are often referred to as network file systems or distributed file systems.

Removable media

Any type of storage device that can be removed from a computer while the system is running and allows data to be moved from one system to another. Examples of removable media include compact discs (CDs), digital versatile discs (DVDs) and Blu-ray discs, tape backups, as well as diskettes and universal serial bus (USB) drives.

Resilience

The ability of an information system to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities, and to recover to an effective operational posture in a time frame consistent with mission needs.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk assessment

The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. NISTIR 8183 CYBERSECURITY FRAMEWORK MANUFACTURING PROFILE 49. This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8183 Part of risk management, synonymous with risk analysis. Incorporates threat and vulnerability analyses. [800-82]

Risk management

The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

Role-based access control

Access control based on user roles (i.e., a collection of access authorizations that a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Security

A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach.

Security control

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system, its components, processes, and data. [800-82]

Security control

The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

Security requirement

A requirement levied on an information system or an organization that is derived from applicable laws, executive orders, directives, regulations, policies, standards, procedures, or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. Note: Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.

Security service

A security capability or function provided by an entity that supports one or more security objectives.

Servers

A device or system that provides resources, data, services, or programs to other devices on either a local area network or wide area network. Servers can provide resources and use them from another system at the same time. Examples include web servers, application servers, mail servers, and file servers.

Service accounts

A dedicated account with escalated privileges used for running applications and other processes. Service accounts may also be created just to own data and configuration files. They are not intended to be used by people, except for performing administrative operations.

Services

Refers to a software functionality or a set of software functionalities, such as the retrieval of specified information or the execution of a set of operations. Services provide a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and based on the identity of the requestor per the enterprise's usage policies.

Social engineering

Refers to a broad range of malicious activities accomplished through human interactions on various platforms, such as email or phone. It relies on psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Software

Computer programs and associated data that may be dynamically written or modified during execution.

Software assets

Also referred to as software in this document, they are the programs and other operating information used within an enterprise asset. Software assets include operating systems and applications.

Subject

An individual, process, or device that causes information to flow among objects or change to the system state. Also see object.

Subsystem

A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.

Supplier

Organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain; developers or manufacturers of systems, system components, or system services; systems integrators; vendors; product resellers; and third-party partners.

Supply chain

Linked set of resources and processes between and among multiple tiers of organizations (each of which is an acquirer) that begins with the sourcing of products and services and extends through their life cycle.

Switch

A device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. [Whatis.com]

System

Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. Note: Systems also include specialized systems such as industrial control systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems. Combination of interacting elements organized to achieve one or more stated purposes.

Note 1: There are many types of systems. Examples include: general and special-purpose information systems; command, control, and communication systems; crypto modules; central processing unit and graphics processor boards; industrial control systems; flight control systems; weapons, targeting, and fire control systems; medical devices and treatment systems; financial, banking, and merchandising transaction systems; and social networking systems. Note 2: The interacting elements in the definition of system include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities. Note 3: System-of-systems is included in the definition of system.

Tailoring

The process by which security control baselines are modified by: identifying and designating common controls, applying scoping considerations on the applicability and implementation of baseline controls, selecting compensating security controls, assigning specific values to organization-defined security control parameters, supplementing baselines with additional security controls or control enhancements, and providing additional specification information for control implementation.

Tampering

An intentional but unauthorized act resulting in the modification of a system or components of systems, its intended behavior, or data.

Third-party providers

Service providers, integrators, vendors, telecommunications, and infrastructure support that are external to the organization that operates the manufacturing system.

Third-party relationships

Relationships with external entities. External entities may include, for example, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums, and investors, and may include both contractual and non-contractual parties. [DHS]

Threat

Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

Threat modeling

A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment.

Thresholds

Values used to establish concrete decision points and operational control limits to trigger management action and response escalation.

User

An individual, or (system) process acting on behalf of an individual, authorized to access a system.

User accounts

An identity created for a person in a computer or computing system. For the purpose of this guide, user accounts refer to “standard” or “interactive” user accounts with limited privileges and are used for general tasks such as reading email and surfing the web. User accounts with escalated privileges are covered under administrator accounts.

Virtual environment

Simulates hardware to allow a software environment to run without the need to use a lot of actual hardware. Virtualized environments are used to make a small number of resources act as many with plenty of processing, memory, storage, and network capacity. Virtualization is a fundamental technology that allows cloud computing to work.

Virtual private network

Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability assessment

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Links and Resources

CIS Controls: https://www.cisecurity.org/controls/

SANS Institute: https://www.sans.org//

ICS ISAC: http://ics-isac.org/blog/

ICS Cert: https://ics-cert.us-cert.gov/

ICS Security Resources and Tools: http://www.chemicalcybersecurity.org/RESOURCES-And-TOOLS

CIS Password Policy Guide: https://www.cisecurity.org/white-papers/cis-password-policy-guide/

NIST 800-82 v2: Component Lifeline: https://csrc.nist.gov/pubs/sp/800/82/r2/final

Industry 4.0: https://www.sap.com/products/scm/industry-4-0/what-is-industry-4-0.html

NERC CIP 007-6.32: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-6.pdf

NIST SP 800-82 Rev 3: https://csrc.nist.gov/pubs/sp/800/82/r3/ipd

ISA/IEC 62443: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

CISA Critical Infrastructure Sectors: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

ISO 27001: https://www.iso.org/standard/27001

Top 20 Secure PLC Coding Practices: https://plc-security.com/

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

CIS® Center for Internet Security®

www.cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
CenterforIntSec
@CISecurity
TheCISecurity
cisecurity