Office of the Chief Information Security Officer

Operational technology security guidelines

Effective February 2024

Updated February 2024

UNIVERSITY OF TORONTO

Contents

UNIVERSITY OF TORONTO

Overview

Preamble

There are a number of critical services at the University of Toronto that depend on operational technology (OT).

"OT encompasses a broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment)"[1] that include common systems such as "supervisory control and data acquisition (SCADA), distributed control systems (DCS), programmable logic controllers (PLCs), building automation systems (BAS), physical access control systems (PACS) and the Industrial Internet of Things (IIoT)" and all similar tools and systems deployed at U of T.

These include functions such as controlling access to a power plant and the devices in it, to a building or to a laboratory, controlling fume hoods, access to and devices within animal facilities, controlling the temperature of refrigeration units, maintaining air flow within a laboratory, accessing a laboratory, etc.

Access to many of these control components is achieved through an internet connection to a computing device. All components need to be protected, similarly to IT systems, but with an understanding that in the OT environment**, the focus is usually on safety, availability, integrity and confidentiality,** in that order**.**

Unauthorized changes to OT controls could damage, disable or shut down equipment, create environmental impacts, endanger human and animal life or have other serious negative effects for U of T.

The following are examples of potential consequences[2] of an OT incident, including serious impacts that are possible due to the wide variety of research carried out at U of T. These examples illustrate why it is very important to identify and protect OT systems, detect any changes to a system, respond if there is an incident and recover from the incident.

- Impact on national security – some of the research materials at U of T can potentially be used to facilitate an act of terrorism.
- Injury or death of employees, e.g., unauthorized shutdown of a fume hood, which can lead to potential incident or injury.
- Injury or death of persons in the community, e.g., through release of hazardous material.
- Loss of research animal life if research animal life support systems are compromised, which can lead to serious regulatory consequences, loss of research data and high recovery costs.

[1] NIST SP 800-82r3 (2023, final)
[2] Some impacts are taken from NIST SP 800-82r3 (2023)

- Loss of research material / impact to research material, through unauthorized changes in variables or theft of data. This can mean the loss of many years of work and loss of research reputation for principal investigators and U of T.
- Release, diversion or theft of hazardous materials.
- Environmental damage.
- Damage to equipment.
- Reduction or loss of production at one site or multiple sites simultaneously.
- Violation of regulatory requirements.
- Criminal or civil legal liabilities.

Purpose

The purpose of these guidelines is to provide a curated summary of National Institute of Standards and Technology's guide to operational technology (OT) security (NIST SP 800-82r3)[3] as applicable to U of T, outlining minimal and critical controls applicable to OT systems, plus guidance on approaches to securing OT at U of T.

Audience

As listed in NIST SP 800-82r3 and applicable to U of T:

- Control engineers, integrators and architects who design or implement OT systems.
- System administrators, engineers and other information technology professionals who administer, patch or secure OT systems.
- Managers who are responsible for OT systems.
- Senior management who need to better understand risk for OT systems as they justify and apply an OT cyber security program.
- Vendors that are developing products that will be deployed as part of an OT system at U of T.

Scope and applicability

The guidelines apply to all U of T-managed OT systems that enable and support U of T operations and environments.

The goal of these guidelines is to provide those responsible for OT with guidance to safely deploy and operate OT systems and environments.

[3] NIST SP 800-82r3 (2023, final)

UNIVERSITY OF TORONTO

Guidelines

Applicable controls for OT systems from the Information Security Control Standard

OT systems at U of T must be protected in accordance with the University's Information Security Control Standard.

The table below highlights priority controls for OT, as per NIST's guide to OT security. These priority controls are an incomplete set of all the controls in the U of T standard. Given the possible impact of misuse of OT, it is recommended that additional controls in the Information Security Control Standard be reviewed by units managing OT, and compensating controls be applied where necessary.

Control area	Controls from the U of T set that are specifically mentioned in the NIST OT document	Notes
Access control	AC-1 AC-3 AC-5 AC-8 AC-14 AC-16 AC-17	RBAC (Role-Based Access Control) can be used to manage access to OT devices/components
Awareness & training	AT-1	
Audit & accountability	AA-1 AA-3	The controls under audit should be reviewed and more than the minimum implemented. It is necessary to determine that the OT systems are performing as intended.
Configuration management	CM-1 CM-2 CM-3 CM-4 CM-5 CM-7 CM-9	Asset management (CM-1) is essential. For CM-7, **it is critical to test changes to assure this will not impact OT system operation.**

Identification & authentication	IA-1 IA-7 IA-8	Ensure identification meets required controls. If not possible, provide mitigations through access controls. 800-82r3 recommends OT network accounts should not use corporate network accounts.
Incident response	IR-1	Should an incident occur, it is critical to also have plans in place to manage evacuation of people and containment of the physical effects of an event.
Maintenance	M-1 M-2 M-3	
Media protection	MP-1 MP-4 MP-7 MP-8	Protect media on which configurations of OT systems are recorded.
Personnel security	PS-2	
Physical protection	PP-1 PP-2 PP-3	OT systems should be protected from physical access by unauthorized personnel. Restrict physical access to the OT network and components. See guidance.
Risk assessment	RA-1 RA-3	Include misuse of OT systems in the risk assessment.
Security assessment	SA-1 SA-3	
System & communications protection	SCP-1 SCP-2 SCP-5 SCP-6 SCP-7	See network controls below for more detail.
System & information integrity	SII-1 SII-3 SII-5 SII-6 SII-7	

Highlighted controls are in the approval process and are recommended at this time.

Additional network control recommendations and guidance

The University's Information Security Control Standard controls SCP-1, SCP-2, SCP-5, SCP-6 and SCP-7 do not provide sufficient detail for needed controls for OT systems. Since network management is critical for OT systems, C1 is recommended. Specific guidance is provided for C1. Also consult NIST 800-82r3 figure 16, which is a high-level example of the Purdue model and IIoT model for network segmentation with DMZ segments.

C1:

The OT network should be logically separated from the corporate network, or be on physically separated network devices, to prevent any interconnectivity of traffic between the two networks.

Guidance for C1:

Logical separation of networks can be achieved in different ways. Two well-known techniques that are used to create logical separation are virtual local networks (VLANs) and virtual route forwarding instances (VRFs). The former operates at layer 2 and the latter at layer 3. The OT network should employ logical network separation by leveraging VLANs and/or VRFs and, at minimum, by placing control devices on a separate logical network from other OT components.

Physically separated networks can achieve full or partial isolation of the OT network from the corporate network. Full isolation is accomplished when network equipment between the corporate network and the OT network is never shared. Partial isolation occurs when there is one or more entry/exit point(s) between the two networks. Physical network separation may be a suitable approach for high security equipment, e.g. electrical high-voltage switchgear.

See guidance under number two, "Protect" for further detail.

Data Classification Standard as applied to OT systems

The U of T Information Security Control Standard is dependent on the Data Classification Standard (level 1 to 4). The possible impact of malicious or accidental misuse of OT systems should guide whether the control should be applied at level 1, 2, 3 or 4, and not the data involved. In the OT environment, the focus is usually on safety, availability, integrity and confidentiality, in that order. In many cases, the control for OT systems should be based on requirements for level 3 or 4.

Guidance

Consistent with existing IT cyber security programs and practices, U of T departments and divisions (units) should develop and deploy an OT cyber security program. However, the lifespan of an OT system can exceed 20 years. As a result, many legacy systems may contain hardware and software that are no longer supported by the vendors and cannot be patched or updated to protect against known vulnerabilities. Legacy systems also may not provide desired features such as error logging, password protection or encryption capabilities. In that case, the security program should tailor compensating controls. Such compensating/mitigating controls should be documented, added as exceptions to a risk register and time limited. Refer to additional recommendations in the NIST guide as needed.

Overall, the effectiveness of an OT cyber security program is enhanced through coordination or integration with a unit's and U of T's processes and information security program.

Given the possible impacts, in addition to the Information Security Control Standard controls, the following guidance (best practices) can help protect OT and electronic systems and ultimately improve and strengthen the overall cyber and physical security of U of T's assets and facilities. The guidance can also reduce the vulnerability of components/systems and data to malicious attacks, equipment failures and other threats. OT security measures are designed to reduce the likelihood of accidental or deliberate loss or damage to University assets and the surrounding environment.

1. Identify

1.1 Inventory

The first step is to understand what needs to be protected in order to manage the risk, by each unit completing a comprehensive, accurate inventory of the OT components/systems (i.e., assets) under their control.

- There will be a large number of components/systems. It is recommended that the inventory of assets be prioritized based on the possible consequences of failure of an asset (the impact). Subject matter experts responsible for managing the components/systems are best placed to decide prioritization. Divisional staff and Information Security staff are available to provide input. Please see table 1 in the appendix for examples of impact.
- In the longer term, inventory all OT assets under control of the unit. Include both those accessible through the network and those accessible only through physical access.
- Include OT systems within U of T's laboratories and research enclaves.
- Do not include systems owned and operated by others, e.g., Toronto Hydro, unless such systems are using U of T's network resources.

1.2 Data to collect per asset

Per asset, collect as much of the following data as possible/relevant and store this information in a secure unit asset inventory system. Collect:

- Criticality information to judge the importance of the asset.
- Location information to enable rapid physical discovery of assets.
- Make, model, serial number, relevant technical specifications such as the device's memory and storage capacity and, where applicable, its MAC address, hostname, IP address, BACNet instance numbers and communication protocols used.
- Comprehensive software inventory including operating system, firmware, application software, etc.
- User credentials.
- Network connections and possible paths, as well as network protections in place.
- Configuration settings to determine whether the asset is securely configured for ports, services, passwords, etc.
- Antivirus and other protection software status, such as whether they've been updated.
- Backup status.
- The inventory should be treated as highly sensitive information and be protected accordingly. Current and accurate inventory information should be maintained.

1.3 Identify supporting infrastructure and people

As part of the process, identify:

- Network devices, such as routers, switches and firewalls, that support the OT network. Identify parties responsible for managing them and support contracts if available. Unmanaged and third-party managed devices should also be highlighted.
- The people, including third parties, needed to maintain the availability of assets under usual working circumstances.
- The people, including third parties, that need to be called on to recover from a mechanical or accidental outage or a malicious incident.
- Maintenance schedules.

1.4 Identify supply chain risk

Before purchasing any equipment, identify supply chain risk. As per the NIST guidance, "Cyber security risks can arise from the products or services acquired to support OT needs. These risks can be introduced anywhere in the supply chain and at any stage in the life cycle."

- Work with Procurement, even when the cost of the desired solution is below the threshold for purchasing through Procurement.

    - Procurement should follow institutional practices that include requesting cyber security assessments and following applicable standards and guidelines.
    - Procurement has knowledge of many other systems in use across U of T.
- As part of the procurement process, request the Hardware Bill of Materials (HBOM), and Software Bill of Materials (SBOM) from the vendor, and use these to update your inventory.
- Evaluate the risk of vendor access to the equipment supplied. Limit vendors/third-party access as described in the section above.
- Ensure that the solution being proposed adheres to the University's Information Security standards and best practices.

2. Protect

Below is a list of suggested additional protective controls. The recommendation for the "Identify" section (above) is to prioritize the inventory based on the possible consequences of failure of an asset. Using the prioritized inventory as a basis, choose protective controls that apply to the identified asset.

2.1 Network devices, such as routers, switches and firewalls.

- Apply permit-by-exception policy to IP addresses and domains to/from connections (allow-listing).
- Apply port isolation and unidirectional gateways (data diodes) wherever possible.
- Allow only one IP device connected to one switch port. This allows easy device isolation at the switch port. It provides isolation of network traffic to other devices. It allows easier detection of unauthorized devices. In addition, ensure the ports are set to allow only one MAC address to connect to a single port, or that there is a mechanism to identify and alert if more than one MAC address is connected to a single port.
- Apply logical separation between the corporate and OT networks by leveraging layer 2 (e.g., VLANs), layer 3 (e.g., VRFs) and layer 4 (e.g., stateful inspection firewall) technologies.
- Use privileged access credentials for users of the OT network.
- Only allow protocols that are absolutely required and block all others. Use secure protocols when possible (e.g., HTTPS, SSH, SCP, SFTP), and use compensating controls for insecure/legacy protocols (e.g., BACNet). Refer to the "Guidance" section above.
- Remote sessions, if required, should be encrypted over remote desktop protocol and leverage University VPN access. They should be time-bound and access granted only during the working session.
- Wireless devices must support WPA2-Enterprise with AES and 802.1X authentication. New devices must support the latest WPA3 security standards

in addition to WPA2-Enterprise with AES and 802.1X authentication. Role-based access control is available in the backend to provide access control mechanisms defined around roles and privileges.

- Maintain a list of OT devices connected to the network and monitor their activity periodically, preferably via a SIEM solution. Devices using wireless technologies such as Bluetooth, ZigBee, LoRa and LTE must be identified, and appropriate security controls applied.
- BACNet considerations: every device on a BACNet network must have a unique BACNet instance number. When connecting BACNet networks, Broadcast Management Devices (BBMDs) must be used to allow BACNet broadcast traffic to traverse a routed network; appropriate planning for BBMD configuration is required.
- For more detailed security controls on how to protect and improve network devices, refer to NIST SP 800-82r3 best practices.

2.2 Environmental control systems

Examples: Air conditioners, temperature and humidity control systems, vents, air quality systems, air handlers, measurement tools, etc., and process controls (e.g., services serving processes, such as chilled water, steam, compressed air and reverse osmosis water).

- Critical heating, ventilation and air conditioning (HVAC) systems, which could include the release of toxic substances:
  - Ensure that these systems are configured with backup operating measures to enable a secure shutdown in the event of a compromised controller or system failure. This can include the use of wired interlocks.
  - Ensure that the controller is powered by an uninterruptible power supply (UPS) with an adequate power supply to facilitate system shutdown in case of a power failure, especially when alternative operating measures like spring return valves or battery packs are utilized.
  - Develop a comprehensive list of scenarios (cases) in which manual intervention might become necessary, and clearly designate the personnel responsible for these interventions.
  - Implement detection systems and establish management procedures for monitoring and responding to potential issues within these systems.
  - Ensure these measures are tested and recorded at a frequency that is reflective of the risk.
- Fire prevention:
  - Confirm that the HVAC systems sequences and hardwired safety features align with fire prevention strategies.
  - Verify that these safety measures are regularly tested and documented at intervals that correspond to the level of risk involved.

2.3 Biometric and fob/electronic keys

- Define electronic systems where these data should be stored. These are identity stores and must be managed in accordance with the control standard for the classification level of that data.
- Develop access management procedures to these systems.
- Correlate the HR system with the identity management system (for timely removal/provisioning of access rights). Access should be automatically revoked when an employee's record is terminated in the HR system.

2.4 Personal devices

- Develop controls, rules and restriction for individuals who bring in their own devices (web cameras, phones, tablets, etc.) applicable to the area. For example, a control may be that devices must be left outside of the secure area, or individuals are required to sign an acceptable use agreement.

2.5 Power supply systems

- Ensure backup power availability to critical and essential loads, where electrical failure would pose a serious threat to human safety (e.g., animal and high-containment laboratories, power stations, etc.)
- Regularly inspect generators and/or UPS devices to check if they have enough capacity to support the orderly shutdown of the systems.
- Recommend all new builds include UPS for B-BC building controllers, as per ASHRE-135, to protect the hardware from power spikes.

2.6 Protect telecommunications cabling from interception or damage

- Consider alternate or shielded cabling that provides suitable protection against environmental effects. Examples:
    - Install thin wall EMT conduit or better, or armored fibre cable in publicly accessible locations.
    - Use optical fibre cabling where technically possible.
    - Use electromagnetic shielding in areas with heavy EMI.
- Use alternative routings and/or transmission media rather than one pathway where technically possible.
- Use redundant links.
- Lock rooms or boxes at inspection and termination points.
- Conduct regular technical sweeps and physical inspections for unauthorized devices being attached to the cables.

2.7 Physical access to the facilities

Physical security controls are any physical measures that limit physical access to assets. These measures are employed to prevent many types of undesirable effects including unauthorized physical access to sensitive locations, unauthorized introduction of new systems, infrastructure, communications interfaces or

removable media and unauthorized disruption of the physical process. Physical access controls include controls for managing and monitoring physical access, maintaining logs and handling visitors.

- Install intruder detection systems on external doors and windows.
- Ensure wiring closets (telecom rooms) are protected and they must be locked at all times. Wiring closets (telecom rooms) should be alarmed and should be covered by security cameras. Cabinets with locked doors are preferred to open racks even within the rooms. Cabinets located in multi-use areas must be locked and should have the doors alarmed.
- Restrict access for personnel to limited areas.
- Develop processes and procedures for access to and review of logical and physical access logs (records), including regular review of those who have access to the logs and procedures to report anomalies.
- Security cameras should be part of the entry/exit of all building and critical areas. Where security cameras are installed, follow the Campus Safety requirements for your campus, including delegating management of the cameras to them.
- Every physical access (entry and exit) should be logged, monitored and information-retained according to retention schedules.
- Where entry/exit recording is not functioning correctly (e.g., as part of construction), record as a problem in a risk register and use security cameras and/or security guards as part of a stop-gap to view entries.
- Correlate information gained from logical (entry logs, operations conducted, etc.) and physical (CCTV, journals, etc.) monitoring systems to enhance security on an as-needed basis. Ensure access to the correlated logs respects privacy principles, and that the logs are protected according to the U of T's Information Security Control Standard and Data Classification Standard.
- Develop storing and backup procedures for the logs.
- Define retention periods for the logs, which should be based on the risk level of the facilities.

2.8 Highly sensitive facilities

- Permit physical access for specific, authorized purposes only.
- Require visitors to be accompanied at all times.
- Record visitors' arrival and departure times.
- Require visitors to wear visitor badges at all times.
- Make visitors aware of behaviour or actions that are prohibited (e.g., filming/photography) in case they are not required to leave all electronic devices outside.
- Secure entrances to high-risk areas with devices that sound alarms to initiate an incident response if the door is forced or held open.
- Control physical access to high-risk areas using multi-factor authentication mechanisms.

2.9 Access to the facilities

Access for third-party (visitors, vendors, news media, delegations, etc.) should be requested by approved U of T employees/staff, who must apply for third-party access and provide a valid business justification. These requests should be granted only to the areas specified in the request and be time limited. These requests should be approved by authorized personnel, and access is revoked after request time expires. Anyone granted visitor badge access must present identification when arriving on site and they must be signed in and escorted by authorized staff.

2.10 Protect people from entering a potentially dangerous area

In the case of an incident, follow documented incident response plans to protect people from entering a potentially dangerous area.

2.11 Redundancy

Design OT systems so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the OT or other networks, or does not cause another problem elsewhere such as a cascading event.

3. Detect

Below is a list of suggested additional detection controls. The criticality of the asset, as decided under “Identify”, helps prioritize the order to apply recommended detection controls to the assets.

3.1 Unsafe conditions

Overall, “Systems must be able to detect unsafe conditions and trigger actions to reduce unsafe conditions to safe ones. In most safety-critical operations, human oversight and control of a potentially dangerous process are essential.[4]” Documented response plans (“Response” section) should be prepared and tested to protect people and systems.

3.2 Detection systems

Use detection systems to monitor, detect and automatically alert appropriate personnel of security or equipment malfunctioning incidents.

3.3 Ingress and egress points

Secure ingress and egress points to server rooms and the facilities with devices that track back to an identity before granting entry or exit. The devices should sound alarms if the door is forced open without authentication or held open.

[4] Under OT System Design Considerations

3.4 High-risk areas

For high-risk areas, devices that require multi-factor authentication for entry are preferred.

3.5 Regular inspection

Conduct regular inspections of U of T's facilities (laboratories, server rooms and other restricted areas), as well as inspections and tests of OT systems, environmental control systems, backup electricity systems and infrastructure (secondary/redundant cables, generator, UPS devices).

4. Respond

As with protect and detect, the criticality of the asset as decided under "Identify" helps prioritize the order to apply the recommendations below.

4.1 Cyber incident

Develop and implement appropriate activities regarding a detected cyber incident, as per U of T's Incident Response Plan. Responding rapidly and as planned supports the ability to contain the impact of a potential incident.

4.2 Prepare plans to respond to incidents

Responses in the event of an incident range from doing nothing to full system shutdown. The response taken will depend on the type of incident and its effect on the OT and/or electronic systems and the physical process being controlled. Effective and adequate response should be based on a written plan documenting the types of incidents and the response to each type. The plan should include step-by-step actions to be taken in case of an incident.

4.3 Business continuity and disaster recovery plans

Prepare business continuity and disaster recovery plans to implement your recovery process. The plans should be tested regularly (at least annually), which includes simulations of different scenarios, tabletop exercises, etc.

4.4 Biological labs

Incorporate response policies and procedures into the disaster recovery planning that prepare personnel to rapidly respond to the release of infectious disease material or other types of outbreak threats. These outbreaks can be caused by the failure of OT systems.

4.5 Mitigation strategies in the case of a failure

Include mitigation strategies with alternative staffing models to transfer critical processes or materials to out-of-location resources if needed, and strategies that activate a crisis management plan to support critical operations.

5. Recover

The recover function supports timely recovery to normal operations to reduce the impact from an incident. Based on the prioritization of assets dependent on the impact of an incident, as per “Identify”:

5.1 Recovery planning

Document step-by-step recovery actions (recovery planning) so that a system can be returned to normal operations as quickly and safely as possible after an incident. A disaster recovery plan is essential to continued availability of OT systems.

5.2 Maintenance of plans

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to an incident.

5.3 Risk analysis

Conduct regular risk analysis to determine the sensitivity of the OT systems.

UNIVERSITY OF TORONTO

Appendix

Tables

Table 1[5]**:** Possible definitions for OT impact levels based on product produced, industry and security concerns

This table is directly copied from NIST SP 800-82r3, table 3. It provides some guidance in deciding criticality of particular OT, based on the impact.

U of T staff managing OT in specific areas are best placed to decide impact for the systems under their care.

Category	High	Moderate	Low
Outage at multiple sites	Significant disruption to operations at multiple sites with restoration expected to require one or more days	Operational disruptions at multiple sites, with restoration expecting to require more than one hour	Partially disrupted operations at multiple sites, with restoration to full capability requiring less than one hour
National infrastructure and services	Impacts multiple sectors or disrupts community services in a major way	Potential to impact sector at a level beyond the company	Little to no impact to sectors beyond the individual company; little to no impact on community
Cost (% of revenue)	> 25%	> 5%	< 5%
Legal	Felony criminal offense or compliance violation affecting license to operate	Misdemeanor criminal offense or compliance violation resulting in fines	None
Public confidence	Loss of brand image	Loss of customer confidence	None
People onsite	Fatality	Loss of workday or major injury	First aid or recordable injury
People offsite	Fatality or major community incident	Complaints or local community impact	No complaints
Environment	Citation by regional agency or long-term significant damage over large area	Citation by local agency	Small, contained release below reportable limits

[5] Table copied from NIST SP 800-82r3, page 46

UNIVERSITY OF TORONTO

Glossary

Keywords as defined in NIST SP 800-r3 glossary

Control system	A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include SCADA, DCS, PLCs, BAS and other types of OT measurement and control systems.
Distributed control system (DCS)	In a control system, it refers to control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit.
Industrial control system (ICS)	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) often found in the industrial sectors and critical infrastructures. An ICS 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).
Operational technology	A broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems and devices detect or cause a direct change through monitoring and/or control of devices, processes and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems and physical environment measurement systems.
Programmable Logic Controller (PLC)	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.

Risk management	The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations and the nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Security controls	The management, operational and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information.
Supervisory control and data acquisition (SCADA)	A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave and satellite. Usually shared rather than dedicated.

Keywords as defined in NIST SP 800-r3 document

Physical access control systems (PACS) See page 24 of the NIST guide.	A type of physical security system designed to control access to an area. Unlike standard physical barriers, physical access control can control who is granted access, when the access is granted, and how long the access should last. An access point is the entrance/barrier where access control is required. Some common physical access control examples of access points are doors and locks, security gates, turnstiles and vehicular gate arms. Depending on the type of facility there can be a single access point (e.g., for high-security areas) or many (e.g., for a large office building).

	An identification (ID) or personal credential is used to identify the authorized user trying to gain access to the area or facility. A PACS often requires a user to have credentials to gain entrance to a facility or access sensitive data. Examples of identification credentials include simple controls (e.g., PIN codes, passwords, key fobs, key cards) and more advanced credentials (e.g., encrypted badges, mobile credentials). Identification credentials allow the system to know who is attempting to gain access and to maintain access logs. Readers and/or keypads are typically located at the access point. If a keypad or biometric reader is also required (i.e., for multi-factor authentication), the user will enter their PIN or perform the biometric scan following their credential scan.

References

1. Information Security Control Standard
2. NIST SP 800-82r3 from NIST Computer Security Resource Centre: Guide to OT security
3. NIST cyber security framework v.1.1