INDUSTRIAL CONTROL SYSTEMS

Table of Contents

Page

List of Figures

1.0 SCOPE

This data sheet contains loss prevention recommendations for industrial control systems (ICS), using the systems approach to assess site-wide ICS, including ICS communication networks and cyber hazards. The goal of this document is to provide risk-reduction solutions from a property protection and business continuity perspective.

For the purposes of this document, ICS is defined as the combination of hardware systems and software programs that provide control, protection and monitoring for processes, production, manufacturing and related activities in both industrial and non-industrial facilities. The following list, which is not all inclusive, gives examples of hardware assets that could be connected to the ICS network:

- Supervisory control and data acquisition system (SCADA)
- Distributed control system (DCS), including historian
- Programmable logic controller (PLC)
- Programmable automation controller (PAC)
- Foreign device gateway
- Remote terminal unit (RTU)
- Network devices including switches, firewalls, routers, etc
- Intelligent field devices (e.g., smart meters, valves, relays, and process transmitters)
- Instrument bus
- Human machine interface (HMI)
- Engineering workstation
- Industrial control panels, including equipment and instrumentation cabinets, input/output (I/O) cabinets, etc.
- Building automation/management system
- Intelligent/smart devices or Industrial Internet of Things (IIoT)

This data sheet provides overall guidance for ICS. Where more detailed data sheets exist for specific equipment or processes, they supersede the guidance presented here.

This data sheet does not cover the following:

- Detailed design or operation of ICS equipment or communication/networking
- Performance, compatibility, or functionality of software
- The design, operation, inspection, testing, and maintenance of safety instrumented systems (see Data sheet 7-45, *Safety Controls, Alarms, and Interlocks*)
- Information technology systems used for general business (e.g., systems intended to send and receive email, systems with access to the internet)

1.1 Hazard

If ICS is not properly managed and maintained, minor malfunctions can develop into major failures, resulting in loss of production and/or potentially significant property damage. Many factors can contribute to failure of the control system, including cyber-related acts aimed at disruption, and the lack of incident response and recovery following a cyber incident.

1.2 Changes

July 2024. Interim revision. Editorial changes were made.

2.0 LOSS PREVENTION RECOMMENDATIONS

2.1 Introduction

Every ICS functions differently, depending on the industry in which it is being used; and thus, no two ICSs are the same. ICSs are complex systems of controllers, logic solvers, motors, pumps, actuators, monitoring and sensing equipment, etc., all connected through communication networks.

Ensuring that staff who are responsible for the site-wide ICS have a complete understanding of the overall system, the operational requirements and protection needs, communication networks and software needs is essential to collectively identify risks and exposures related to the site-wide ICS.

2.2 Construction and Location

2.2.1 Locate process control rooms and associated significant equipment rooms outside areas exposed to the effects of explosion hazards. If this cannot be done, provide pressure-resistant construction designed in accordance with Data Sheet 1-44, *Damage-Limiting Construction*, assuming the overpressure is applied on the exterior surface of the control room. Laminated glass meeting ANSI Z97.1 (ASTM E1886 and E1996, or FBC TAS 201 and 203, are acceptable alternatives) for impact resistance, and ASTM E1300 for the required overpressure is recommended for windows.

2.2.2 Locate process control rooms and associated equipment rooms so they are not exposed to damage from corrosive or ignitable liquid, flammable vapor or mechanical equipment such as overhead cranes.

2.2.3 For elevated process control rooms and associated equipment rooms exposed to a fire hazard, provide fireproofing for the structural support steel suitable for the exposure (minimum 1 hour).

2.2.4 Construct process control rooms, control centers and associated industrial control instrumentation equipment rooms (i.e., Input/Output rooms) and/or industrial control panels of noncombustible materials. This construction includes, but is not limited to, suspended ceilings, raised floors, partition walls, furnishings, pipe and HVAC insulation materials, and HVAC filters.

If plastic materials are used, provide FM Approved materials or specification tested materials as appropriate using the following guidelines:

A. FM Approval Standard 4882, *Class 1 Interior Wall and Ceiling Materials or Systems for Smoke Sensitive Occupancies*

B. FM Approval Standard 4884, *Panels Used in Data Processing Center Hot and Cold Aisle Containment Systems*

C. ANSI/FM Approval Standard 4910, *Cleanroom Materials Flammability Test Protocol*

2.2.5 Provide a minimum one-hour, fire-rated separation between process control rooms and adjacent areas, including equipment rooms and low-voltage switchgear rooms. This recommendation is not applicable to stand-alone equipment located outside the process control room.

2.2.6 Where redundant process control systems are provided, locate each system’s controls, equipment and cabling in a separate fire-rated area.

2.2.7 Provide separate areas for locker rooms, lunchrooms, kitchens, meeting rooms, offices, etc.

2.2.8 Seal openings in fire-rated floors and walls through which pipes, wires, and cables pass using an FM Approved or listed penetration seal with a fire-resistance rating equivalent to the rating of the floor or wall.

2.2.9 Route roof drains, domestic water lines, and other liquid lines around process control rooms and associated equipment rooms. In multi-story buildings, seal the floor above to be liquid-tight. When piping cannot be routed away from these areas, provide containment (e.g., concentric piping) or a collection pan; and provide FM Approved leak detection with alarm notification to a constantly attended location. Refer to Data Sheet 1-24, *Protection Against Liquid Damage*, for additional details.

2.2.10 Provide floor drains beneath raised floors if water or other liquids can collect.

2.2.11 Construct industrial control panels, including doors and/or access panels, using noncombustible construction materials. Adhere to recognized international standards.

2.3 Protection

2.3.1 Protect process control rooms, associated equipment rooms and industrial control panels against external fire exposures in accordance with Data Sheet 1-20, *Protection Against Exterior Fire Exposure*.

2.3.2 Provide FM Approved smoke detection for process control rooms, process control centers and associated equipment rooms, arranged to alarm at a constantly attended workstation or location.

2.3.3 Where an enhanced level of detection is desired for business-critical systems and/or safety systems, provide a Very Early Warning Fire Detection (VEWFD) system in the equipment room and/or within the industrial control panel that alarms to a constantly attended location. Use FM Approved air aspirating or intelligent high sensitivity spot detection VEWFD systems, as appropriate, for the enclosure configuration.

2.3.4 Provide FM Approved smoke detection below raised floors and above ceiling areas with cables.

2.3.5 Install smoke detection in accordance with Data Sheet 5-48, *Automatic Fire Detection*.

2.3.6 Provide fire protection for process control rooms, control centers or industrial control instrumentation equipment rooms as follows:

2.3.6.1 Rooms of Combustible Construction

A. Provide a wet or preaction automatic sprinkler system utilizing automatic quick-response (QR) sprinklers. Use design demands, hose demands and duration in accordance with Data Sheet 3-26, *Fire Protection for Nonstorage Occupancies*.

B. Provide an automatic FM Approved water mist system listed specifically for data processing equipment rooms and installed in accordance with Data Sheet 4-2, *Water Mist Systems*, and the manufacturers design, installation, operation and maintenance manual shown in the FM Approval listing. Provide a water supply to water mist system for a 60-minute duration.

For A and B above:

- Use Hazard Category 1 (HC-1) for process control rooms and control centers having ceilings up to 30 ft (9 m)
- Use Hazard Category 2 (HC-2) for industrial control instrumentation equipment rooms or process control rooms and control centers with ceilings in excess of 30 ft (9 m)

2.3.6.2 Rooms of Noncombustible Construction

Provide a halocarbon or inert gas (clean agent) fire extinguishing system designed and installed in accordance with the manufacturer's instructions and Data Sheet 4-9, *Halocarbon and Inert Gas (Clean Agent) Fire Extinguishing Systems*. Wet or preaction automatic sprinkler protection or water mist systems (per Section 2.3.6.1 above) are also acceptable.

For a halocarbon or inert gas (clean agent) fire extinguishing system, ensure the following conditions are met:

1. VEWFD or automatic power-down to the room and equipment (except emergency lighting) upon smoke detection, provided a process hazard analysis or equivalent evaluation proves an automatic power-down will not damage the controlled equipment (i.e., process equipment) and/or create a hazardous condition.
   a. When an automatic power-down is provided, install in accordance with power isolation of data processing equipment and HVAC systems, per Data Sheet 5-32.
   b. Adjust the delay time for power-down to not exceed the hold time of the halocarbon or inert gas (clean agent) fire extinguishing system with a safety factor of two in order to bring the process to a safe state.
2. Very early warning fire detection (VEWFD) with a supervisory alert/signal is provided to allow sufficient time for an investigation by the operator or responders prior to discharge of the clean agent system.
3. Equipment enclosures are constructed of metal.
4. Minimal use of paper and other combustible materials in the room.
5. No storage of packing materials or plastic cassettes within the room. **Note:** This requirement includes all combustible media (e.g., tape reels).

6. Shutdown and/or damper of ventilation systems that use return or make-up air is provided.

2.3.7 Provide protection of the facilities process control equipment. Base this protection on the criticality of the physical process and impact if the process control system is lost due to a fire. See Section 3.1, Fire Protection for Industrial Control Equipment. Provide either of the following (A or B):

A. Noncombustible cabinets with subdivisions to limit damage to the smallest possible configuration

B. A halocarbon or inert gas (clean agent) fire extinguishing system in the room, provided the cabinets are ventilated and/or arranged to discharge directly inside the cabinets. Follow guidance in Section 2.3.6.2 above.

2.3.8 Provide automatic sprinkler protection in accordance with Data Sheet 3-26, *Fire Protection for Nonstorage Occupancies*, throughout building spaces adjacent to the control rooms and centers (including but not limited to offices, break areas, file rooms, permit areas, conference rooms, training rooms, bathrooms, etc.) for the appropriate hazard classification associated with this occupancy.

2.3.9 Install fire protection systems in accordance with Data Sheet 2-0, *Installation Guidelines for Automatic Sprinklers*, and the applicable special protection system data sheet.

2.3.10 Protect data centers associated with process control rooms in accordance with Data Sheet 5-32, *Data Centers and Related Facilities*. Perform a process hazard analysis (PHA) for controls before allowing automatic shutdown.

2.3.11 Protect emergency generators in accordance with Data Sheet 5-23, *Design and Protection for Emergency and Standby Power Systems*.

2.3.12 Protect grouped cables and cable trays in accordance with Data Sheet 5-31, *Cables and Bus Bars*.

2.3.13 Provide carbon dioxide or clean agent portable (Class C) fire extinguishers listed for energized electrical hazards to protect electronic equipment in accordance with Data Sheet 4-5, *Portable Extinguishers*.

2.3.13.1 Do not use dry chemical fire extinguishers in areas containing electronic equipment.

2.3.13.2 For ordinary combustible materials, provide portable fire extinguishers of the type or combination type that are suitable per Data Sheet 4-5, *Portable Extinguishers*.

2.3.14 Develop a pre-incident plan for fire and electrical response to process control rooms, control centers, associated industrial control instrumentation equipment rooms and/or industrial control panels.

2.3.14.1 Verify electrical personnel are capable of responding at the same time as firefighting personnel and are trained to safely de-energize or isolate the affected process control panels and initiate firefighting activities.

2.3.14.2 When de-energizing all electrical equipment in the industrial control instrumentation equipment rooms and panels is not practical, ensure the response to the fire alarm notification includes trained personnel capable of diagnosing the fire/smoke condition in the affected area and implementing the pre-incident plan of either local, regional or complete manual power isolation.

2.4 Human Factor

2.4.1 Management of Change Program

2.4.1.1 Administer the ICS management and ICS security programs in conjunction with the management of change program.

2.4.2 ICS Management

Management commitment is the cornerstone of successful ICS oversight and management programs. Strong management commitment helps ensures that all areas of the ICS receive the necessary attention, funding and staffing.

2.4.2.1 ICS Oversight Team

2.4.2.1.1 Organizations should create an ICS oversight team composed of individuals from the corporate and local facility levels that is responsible for overseeing the implementation of cyber security policies related to the ICS.

2.4.2.2 Asset Management Program

2.4.2.2.1 Establish and implement an ICS inspection, testing, and maintenance program. See Data Sheet 9-0, *Asset Integrity*, for guidance on developing an asset integrity program. Include the following elements in an asset management program as applicable:

A. Maintain an inventory of hardware connected to the ICS network, including manufacturer, model number, and installed firmware, software, and applications with version numbers.

B. Ensure the inventory list includes a criticality rating of ICS assets to prioritize security efforts and to maintain applicable security updates.

C. Retain drawings and documentation for the ICS (e.g., electrical/control schematics, networking drawings, and (where relevant) Piping and Instrumentation Diagrams (P&ID)). Keep these documents up to date as changes are made to the ICS.

D. Store asset inventory, drawings and documentation that detail the design and functionality of the ICS in a controlled and restricted location. Grant access only on an as-needed basis. If these documents are digital, password protect them; and maintain backup copies stored on a trusted network. Encrypt these files where possible. All networks outside of the ICS/OT environment should be considered untrusted networks, including the local IT network.

2.4.2.3 Supply Chain Management Program

2.4.2.3.1 Include the following elements in a supply chain management program as applicable:

A. Include cyber security requirements for systems/applications or devices as part of the bid documentation to the supplier. Reevaluate site-approved suppliers, including third-party service providers, regarding their security policies and procedures before signing/renewing any contracts.

2.4.3 ICS Security

With any process, the availability of ICS is critical. An effective ICS security strategy can play a key role in maintaining that availability.

2.4.3.1 Access Management Program

2.4.3.1.1 Include the following elements in an access management program as applicable:

A. Use ICS credentials to control access to the ICS (i.e., role-based access to HMI/operator workstation and engineering workstations). Additionally, limit access to engineering workstations to those who have authority to change the process. To support controlled access to ICS, adhere to the following:

1. HMI/operator workstations (with no ability to change safety device alarm and interlock setpoints) may use shared login credentials.
2. Engineering workstations require a unique, user-specific login and password to gain access to the system every time and have automatic lockout when the workstation is idle for a period of approximately 30 minutes or less.
3. Credentials used to access the ICS are managed independently from the credentials used to access IT systems. Maintain ICS user credentials in an up-to-date user repository in the OT environment, periodically review access permissions and remove access from people who no longer need it. Alternatively, non-networked local logins may be acceptable.

B. Change the default factory username and password on all systems, hardware, and software. Update passwords on a routine basis or when significant and/or key personnel or vendor changes occur. Avoid using general usernames and weak passwords.

C. Protect wireless communications by using authentication and encryption.

D. Use the following precautions for portable devices connecting to the ICS:

1. Before granting site access, provide ICS cyber security training for contractors and other visitors who enter the site on temporary basis. This training should include familiarization with site rules and procedures per Section 2.4.3.1.1, part D.2 through D.5.

2. For devices used in ICS environment such as laptops (including third-party laptops, tablets, etc.), disable wireless connections, maintain/check for current security patches and antivirus software, and perform virus scanning every time prior to connecting to the ICS.

3. For memory cards, USB thumb drives, portable hard drives, etc., perform security scanning every time prior to connecting to the ICS.

4. Do not allow cell phones or any other mobile network enabled devices to connect to the ICS.

5. Disable unused ports (USB, RJ45, serial, etc.) on equipment connected to the ICS, where possible.

2.4.3.2 Configuration Management Program

2.4.3.2.1 Include the following elements in a configuration management program as applicable:

A. Limit the features/functions for all digital devices connected to the ICS to only those features/functions that are required to support the operation of the ICS. This includes field devices that have multiple settings and communicate digitally; controllers that perform both basic process control and safety control; supervisory devices, HMI and engineering workstations; historians; servers; networking equipment such as gateways, switches and routers; and network protection equipment such as firewalls, including all the devices installed within an ICS demilitarized zone (DMZ).

B. Verify that the ICS oversight team is analyzing, validating, and approving all changes to any digital device connected to the ICS for security impacts prior to deployment, as part of the management of change program.

C. Use system monitoring to check for any unauthorized changes to basic control equipment, safety control equipment and the OT networking equipment.

D. Ensure logic solvers, PLCs, or controllers used as part of the basic process control system and the safety system have the operating mode selection (i.e., run/program/remote etc.) set to the OEMs recommended setting prior to enabling the system and operating the ICS. Include changes to the operating mode in the system monitoring recommendation above.

2.4.3.3 Patch Management Program

2.4.3.3.1 Include the following elements in a patch management program as applicable:

A. Ensure the patch management program includes support and communication equipment such as, but not limited to, remote access servers, jump servers, historians, virus protection, virtual private networks and other networking components, including firewalls, etc. Also include any equipment used for servicing the ICS such as laptops or handheld devices, and scanning equipment used to check portable devices such as USB kiosks, etc.

B. Monitor for bulletins and alerts of cyber security vulnerabilities from system and device manufacturers, ICS integrators, government agencies and others.

C. Upon learning of a cyber security notification, have the ICS oversight team determine the actions required to protect the site's ICS, based on its criticality and the exposure. Additional protection measures against system vulnerabilities may be necessary until a software patch can be installed.

D. Verify the ICS oversight team consults with the ICS vendor prior to patch deployment. Where possible, test in a simulation or virtual system prior to installation.

E. Provide additional protection measures for obsolete equipment and/or software against cyber security vulnerabilities due to the lack of support from the OEM.

2.4.3.4 Networking Safeguards

2.4.3.4.1 Implement secure remote access to the ICS/operational technology (OT) environment. All networks outside of the ICS/OT environment should be considered untrusted networks, including the local IT network. Use the following precautions as applicable:

A. Verify remote access to the ICS is as follows:

1. From an internal network (connection originates on-corporate network) such as the local IT network, use multifactor authentication (MFA) through a jump server located in an industrial DMZ (refer to Section 2.4.3.4.2 B).
2. From any external network (connection originates off-corporate network), use a secure virtual private network (VPN) and multifactor authentication (MFA) through a dedicated path, using corporate systems to an intermediate system (jump host in the industrial DMZ) before gaining access to the ICS/OT environment.
3. Personal computers or any other personal external devices are not used for remote access to the ICS/OT environment.

B. Do not allow remote connections to dedicated safety systems.

C. Do not allow persistent remote connections into the ICS/OT environment. Remote monitoring, data collection, and diagnostics with restricted data flow in one direction are suitable and require no time limits on the connection to the ICS.

D. Replace dial-up modems with secure modern communication methods. If this is not possible, do the following:

1. Turn off and/or unplug dial-up modems when not in use.
2. Provide additional protection measures for active dial-up modems (e.g., call back setting to a designated phone number, caller ID filtering, disabling auto answer).

2.4.3.4.2 Implement the following networking safeguards as applicable:

A. Provide separation between ICS/OT networks and IT or other business networks with an industrial demilitarized zone (DMZ), and direct all communications to and from the ICS through the DMZ.

B. Provide separation between basic process control system (BPCS) network and safety networks by segregation (air-gapped or interfaced architecture) or by segmentation (integrated or common architecture). For additional guidance on safety systems, see Data Sheet 7-45, *Safety Controls, Alarms, and Interlocks (SCAI)*.

C. Verify the firewall rules (opened ports, protocols allowed, etc.) are reviewed on a periodic basis by staff with networking and cyber security experience. Changes to the firewall rules are implemented from the ICS/OT environment and managed through an MOC under the direction of the ICS oversight team.

D. Use application ″allowlisting″ in the ICS environment where possible. Use caution in implementation of this solution.

E. Employ network monitoring and logging of activities of the ICS network (also referred to as intrusion detection system or IDS), along with security information event and management (SIEM) software where possible to detect unauthorized activity. Where possible, monitor the OT environment from a Security Operations Center (SOC).

F. Employ antivirus protection software on ICS and in the OT environment, including SCADA systems. Work with the ICS vendor or service provider and use caution in the selection and implementation of antivirus solutions.

2.5 Operation and Maintenance

Confidence that an ICS is operating as intended is critical to preventing significant damage to equipment and/or property that may result in long-term outages. The possibility of ICS-related failures and long-term outages can be minimized by monitoring and notification procedures, viable emergency response/recovery and ICS contingency planning, and adequately trained, knowledgeable operators following documented standard and emergency operating procedures.

2.5.1 ICS Operations

2.5.1.1 Alarm Management Program

2.5.1.1.1 Include system monitoring of the ICS equipment and OT networking equipment if determined to be an available option under the configuration management recommendation 2.4.3.2.1 C:

A. Using system monitoring, arrange for an alert to trigger when an unauthorized change to configuration settings in the ICS equipment has been made, including safety systems, and OT networking equipment.

Note: The alerts noted above are not intended to be addressed by process operators. Rather, these alerts are to be escalated to personnel responsible for monitoring the OT networking equipment and the ICS equipment.

For additional guidance on alarm management refer to Data Sheet 10-8, *Operators*.

2.5.1.2 Emergency Operating Procedures (EOP)

2.5.1.2.1 Planning and preparation are vital for a successful cyber/ICS EOP, including identifying staff and, if needed, third-party consultants or other specialists with the required skills to respond to a cyber intrusion event.

A. Verify roles and responsibilities for handling cyber incidents are established.

B. Maintain information on vendors who are authorized/contractually obligated to provide support during a cyber event.

2.5.1.2.2 Include the following elements in the cyber/ICS EOPs as applicable:

A. Ensure a procedure exists to mitigate the impact to the ICS and production from the loss of an enterprise resource planning (ERP) system or manufacturing execution system (MES).

B. Ensure guidance is provided on how to shut down the system and/or process (i.e., bring the system to a safe state) when control of the ICS behaves suspiciously or ceases to function. This guidance should include known or suspected cyber incidents including, but not limited to, the following:

- Black screen/HMI screen freeze-up
- Unexplained unit trip
- Ransomware messages appearing on workstations
- Cursors moving unexpectedly on workstations without operator input
- Unrecognized configuration change
- Problem configuring or calibrating some portion of the ICS

C. Verify procedures exist for operating critical equipment in manual mode.

D. Verify EOPs are practiced (at a minimum) in tabletop exercises on a routine basis.

2.5.1.3 Contingency Planning

2.5.1.3.1 Equipment Contingency Planning

Develop and maintain a documented ICS contingency plan per Data Sheet 9-0, *Asset Integrity*. See Appendix C of that data sheet for guidance on the process of developing and maintaining a viable ICS contingency plan. Also refer to sparing, rental, and redundant equipment mitigation strategy guidance in that data sheet.

In addition, include the following elements in the contingency planning process specific to ICS:

A. Address the actions needed to manage unintended shutdowns and to recover from the ICS outage scenario(s) as part of the incident response and recovery program (see Section 2.5.1.4).

B. Test and exercise the plan at a frequency determined by the asset owner and commensurate with the exposures.

C. Based on the inventory of hardware (see Section 2.4.2.2.1), including criticality of the component and lifecycle management plans, evaluate the need for and scope of ICS component breakdown sparing.

2.5.1.3.2 ICS contingency plans are reviewed annually.

2.5.1.4 Incident Recovery Program

2.5.1.4.1 Include the following elements in an incident response and recovery program as part of ICS contingency planning as applicable:

A. Determine the root cause for any unintended shutdown before attempting to restart the ICS.

B. Maintain electronic records when unintended shutdown occurs for forensic evaluation, to the extent possible.

C. Maintain an up-to-date, viable copy of all ICS configuration files (e.g., last known reliable configuration, baseline configuration) and documentation required for a fully functional system. Maintain a history of back-up files in a physically secure location.

1. If backup files are immutable (e.g., write once/read many, cannot be overwritten), then:
    a. Store immutable backup files on a trusted network drive separate from the network where the data originated.
    b. Create new backup files when changes to the system occur and after any system update.
    c. Create new backup files prior to the end of the retention period for the last immutable file.
2. If backup files are not immutable (e.g., can be overwritten), then:
    a. At least one copy of all the backup files should be stored offline in a physically secure location.
    b. Create new backup files when changes to the system occur and after any system update.

D. Review service contracts with OEMs and/or vendors to identify the duration for delivery of components to determine the optimum recovery and equipment breakdown spare part strategy.

E. Review the incident response and recovery program on a routine basis at a frequency commensurate with the exposures, but at least annually. Update the program as needed to maintain its efficacy.

For additional guidance on pre-incident planning and recovery response, see Data Sheet 9-1, *Supervision of Property*, Data Sheet 10-1, *Pre-Incident and Emergency Response Planning*, and Data Sheet 10-5, *Disaster Recovery Planning*.

For additional guidance on incident investigations, refer to Data Sheet 10-8, *Operators*, and Data Sheet 7-43, *Process Safety*.

2.6 Training

2.6.1 As part of the site's operator training program, implement an ICS security training and awareness program for security policies and procedures. This program should include industry cyber security standards and best practices.

2.6.2 Provide focused training for operators and key site personnel who interact with the ICS before they are provided access to the ICS. Provide additional training to system administrators or personnel who have privileged/increased access levels (i.e., role-based training) to perform job duties.

2.6.3 Conduct initial and refresher ICS cyber security training for all ICS personnel on an ongoing, annual basis.

2.6.4 Conduct training for fire emergency response personal on fighting process control fires. Refer to Data Sheet 5-32, *Data Centers and Related Facilities*, Section 2.7.1.

For additional guidance on operators, refer to Data Sheet 10-8, *Operators*.

2.7 Utilities

2.7.1 Provide uninterruptible power supplies (UPS) and emergency power systems to permit operation of the ICS until a safe power-down can be accomplished. Include UPS power for any support systems, such as instrument air (where used) and HVAC, that may be required for the duration of a safe power-down.

2.7.2 Perform inspection and maintenance activities for utilities and support systems provided for ICS (e.g., batteries, uninterruptible power supplies [UPS], generators, and climate control) as part of the asset integrity program. For additional guidance, see Data Sheet 5-28, *DC Battery Systems*, and Data Sheet 5-23, *Design and Protection for Emergency and Standby Power Systems*.

2.7.3 Provide a reliable instrument air system where pneumatic air controls are used (e.g., an independent instrument air compressor with N+1 backup or suitably designed air receiver).

2.7.4 Provide a reliable heating, ventilation, and air conditioning (HVAC) system to maintain the ICS equipment space environmental conditions required for normal operations. This recommendation is focused on ICS equipment considered critical to operations.

3.0 SUPPORT FOR RECOMMENDATIONS

3.1 Fire Protection for Industrial Control Equipment

Recognize that provision of automatic sprinkler protection is largely designed to protect the room structure and neighboring occupancy. In a small room, all equipment may be lost even in a sprinkler or water mist system-controlled fire. As such, a halocarbon or inert gas (clean agent) fire extinguishing system may be a better choice if the goal is to protect the equipment itself.

A fire in well-subdivided process control equipment cabinets will likely cause fire damage to the cabinet where the fire originated and limited damaged to adjacent cabinets. Conversely, a fire in process control equipment cabinet that lacks subdivision is expected to travel the length of the enclosure. The impact for loss of process control equipment depends on the extent of fire damage and the critically of the process, availability of replacement parts, etc.

3.2 ICS Management

The asset owner or identified individual should have a cybersecurity strategy to protect the site-wide ICS.

3.2.1 ICS Oversight

With the complexity of automation, the interconnection of different systems and networks, and data acquisition for analytical business purposes, a new peril has been introduced to ICS: cyber hazards. To keep the site's process running, ICS needs an identified individual with the ability to protect the ICS from cyber hazards and to understand how cyber security methods, products, and systems might affect the performance of the ICS.

3.2.2 Asset Management Program

To maintain a cyber-resilient ICS, organizations should know what is connected to the ICS network. Without this knowledge, they cannot begin to identify devices that expose the ICS to cyber hazards.

The assets that need to be included in the asset management program are the digital devices that are connected to the ICS network. Consider HMI/operator workstations, engineering workstations, network switches, modems, routers, firewalls, application servers, printers, DCS, PLC and other logic controllers, and network-connected smart field devices. Operating systems (e.g., equipment employed on Purdue model level 3 of an OT network) should also be included in the asset tracking. Items typically found in this level include plant aggregate historians, operation scheduling systems, alarm and other application servers, operations-specific IT services such as DHCP, LDAP, DNS, and file servers. Additionally, consider the Industrial Internet of Things (IIoT) and even basic Internet of Things (IoT) devices that might incorrectly be connected to the ICS network.

Good asset management programs identify devices connected to the ICS network. Devices include but are not limited to HMIs, PLCs, engineering workstations, networking equipment, servers, etc. Identifying the firmware, software, and applications for each device is also critical. Without this additional information, the features, and services available for each device cannot be ascertained, leaving the ICS vulnerable.

Many vendors in the marketplace provide automated active and passive asset discovery/network mapping solutions. Where possible, employment of passive asset discovery solutions is preferred over manual asset management techniques.

3.2.3 Supply Chain Management Program

A good supply chain management program helps ensure procured equipment and software are securely configured by vendors to meet the organization's security requirements.

Before installing any new digital controller or other digital device, or software and/or application to the ICS, the organization needs to have confidence that the device is from a trusted chain of custody through the developer, manufacturer, supplier, shipping and storage, and through commissioning and acceptance testing.

3.3 ICS Security

3.3.1 Access Management Program

Unsecure access points are one of the most vulnerable attack vectors into the ICS. These access points are vulnerable to both deliberate and unintentional cyber intrusion. Cybercriminals know the ICS must support remote access and will look for easy access points to compromise the system. Worst case would be that an access point is compromised for an extended period, allowing unapproved third parties access to the ICS where they can gain valuable insight about the site's ICS and process, leaving them time to plan and launch a cyberattack.

3.3.2 Configuration Management Program

Digital/electronic devices are provided with many options and features for performance and/or communications within their firmware and/or software. To reduce the potential cyber-attack surface, "hardening" of this equipment is used (for example, based on asset criticality or a cyber PHA) to limit options and features for digital/electronic devices to only those required for the ICS to operate.

Once the desired configuration has been set and the system works properly, these setting should be saved as the baseline or the last known reliable configuration. This baseline would be used in efforts to reestablish the system in the event of a disruption, either by physical damage or corruption of firmware/software.

Once the configuration of safety PLCs or other controllers has been set, the PLCs or controllers should be placed in the mode of operation recommended by the manufacturer (run, program, remote, etc.). This configuration, including the settings and mode of operation, would be locked in place by removing the physical key or setting the digital key. This method supports the access management program by allowing access to only those who have the authority to adjust the safety settings.

Monitoring the configuration settings will identify when unauthorized changes are made to the ICS. This monitoring is useful for identifying and possibly preventing internal or external threats to the ICS.

3.3.3 Patch Management Program

Patch management is the process of applying updates to software, drivers and firmware to protect against vulnerabilities. Patches should be evaluated to determine how a patch may affect the process.

Prior to installing any patch, authenticate and verify the integrity of the software to ensure it is in its original form and hasn't been altered. The source of the software is also critical; prior to downloading any software, the trustworthiness of the source must be confirmed.

If a patch offers no benefit from a cyber security or performance perspective, it may not be needed. The asset owner should work with the ICS vendor on deploying patches in the ICS/OT environment.

3.3.4 Networking Safeguards

With advancements in technology, such as Industry 4.0, ICS/OT environments are more connected than ever before. This increased connectivity exposes ICS/OT environments to cyber threats that historically did not exist.

Remote access has become a common method for off-site vendor support and provides a convenient way for employees to access the ICS/OT environment. Communications that originate externally and desire access to the ICS/OT environment should be made through a secure VPN, with MFA through a DMZ, landing on a remote access server/jump server with access to the ICS/OT environment. Communications that originate within the corporate environment and desire access to the ICS/OT environment should use MFA through a DMZ, landing on a remote access server/jump server with access to the ICS/OT environment.

An Industrial DMZ (demilitarized zone) is a perimeter network that adds an extra layer of security to an organization's internal OT network from untrusted traffic. A demilitarized zone (DMZ) is an area defined at the limits of a trusted network that provides resources accessible to untrusted networks such as the internet. In this way, the resources that must be consumed by users from untrusted areas will not have access to the network considered safe. An industrial DMZ provides services that require connectivity to both IT and OT such as remote access, patching, antivirus, historian, Manufacturing Execution System (MES) and file transfers.

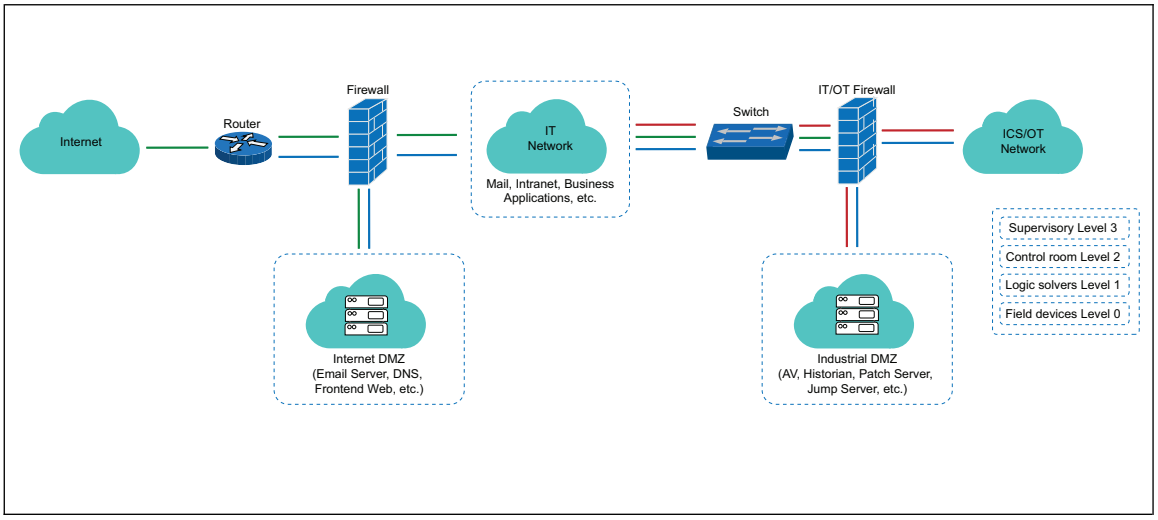

Fig. 3.3.4. Example communication path showing the Corporate/Internet DMZ and the ICS/Industrial DMZ

Intrusion detection systems (IDS) are a network security tool that monitors network traffic and devices for malicious activity. Alerts from the ICS should be relayed to a Security Operations Center (SOC) for further investigation.

Signature-based IDS focuses on searching for signatures (i.e., patterns) to detect an intrusion. These signatures need to be updated regularly to be able to identify the latest attack patterns.

Anomaly-based IDS focuses on unexpected patterns of activity to detect an intrusion such as a spike in network activity, multiple failed logon attempts, unusual network port activities that are flagged as suspicious activities, etc. These alerts are relayed to the security operations center (SOC) regularly.

3.4 Illustrative Losses

3.4.1 Ukraine Power Grid

Crash Override Malware. One of the most notable incidents of an unauthorized ICS breach occurred in the Ukraine on 23 December 2015 when several unscheduled power outages affected approximately 225,000 customers. The outages were caused by remote cyber intrusions at three regional electric power distribution companies. While power was being restored, the companies involved continued to run under constrained operations.

The cyber-attack was reportedly synchronized and coordinated following extensive reconnaissance of the affected networks. Some reports suggest that this attack took place over a six-month period. Reports state that the cyber-attacks at each company occurred within 30 minutes of each other and impacted multiple facilities. During the event, several circuit breakers were operated remotely and without authorization by multiple external bodies, using either existing remote administration tools at the operating system level or remote industrial control system (ICS) client software via virtual private network (VPN) connections. The external bodies reportedly acquired legitimate credentials prior to the cyber-attack to facilitate remote access.

The three power companies have reported that several systems were wiped at the conclusion of the cyber-attack by using Kill Disk malware. The malware erases selected files on systems and corrupts master boot record, thereby rendering systems inoperable. Additionally, Windows based HMIs embedded in remote terminal units were also overwritten by Kill Disk. Several Serial-to-Ethernet devices at substations were rendered inoperable by corrupting their firmware. The Uninterruptable Power Supplies (UPS) were disconnected via the UPS remote management interface which interfered with expected restoration efforts.

The three companies reported that they had been infected with Black Energy malware, but whether this played a role in the cyber-attack is uncertain. The malware was reportedly delivered via spear phishing emails with malicious attachments. Although not confirmed, Black Energy may have been used to gain legitimate credentials. However, any remote access Trojan could have been used.

Following the attacks, the companies could not remotely reset the breakers. Therefore, operations personnel had to be dispatched to complete manual switching. This situation resulted in an outage which lasted between four and six hours. Note that no damage to any power generation facilities was reported because of this incident.

3.4.2 TRISIS

In December 2017, security researchers identified a malware attack on Safety Instrumented Systems (SIS) and Distributed Control Systems (DCS) at a large industrial facility in the Middle East. This malware has been referred to as both TRITON and TRISIS by cyber security organizations, and as HATMAN by the Department of Homeland Security's ICS-CERT team. The malware affected Schneider Electric's Triconex Tricon safety controllers and HMI and allowed an attacker to read/modify controller memory contents (i.e., overwrite existing programs via a remote network connection).

Based on the available information, attackers gained remote access to an SIS engineering workstation and deployed the malware: a Windows PC-based executable file to communicate with the safety controller (Triconex), and a malicious binary component that was downloaded to the controller. Mandiant, a FireEye cyber security firm who was called to investigate the incident stated in their report [1] that "the malware could read and write programs and query the state of the controller. It also had the capability to communicate with the controller using TriStation protocol, a proprietary protocol that the TriStation software (Tricon programming software) uses to communicate with Triconex safety systems. It appears the attacker is familiar with the Triconex system and had tested the malware prior to the attack."

Based on Mandiant's analysis, evidence exists that the attackers had gained access to the plant DCS as well but decided to compromise the safety system. The attackers accidently caused a system shutdown while attempting to reprogram the controllers to cause physical damage. The system entered a fail-safe state due to a failed validation check between the processors, which shut down the system and alerted the owner. As stated by Mandiant, "taking control of both DCS and SIS would have enabled the attacker to potentially create major impact."

ICS-CERT and Dragos have stated that the TriStation protocol used in older controllers, such as the one attacked in this event, lacks an authentication or encryption mechanism for backdoor accounts, which are vital to ensure administrator-level access and control over the device in an emergency. However, the newer versions of Triconex systems contain an authentication factor for these accounts and are less susceptible to such attacks. A security notification from Schneider Electric confirmed this vulnerability and they developed a tool to detect and remove the malware in a Tricon controller. They also stated that the hardware key switch that provides physical operation control was left in the "Program" mode, which is not considered an acceptable practice when not programming the controller.

Triconex systems are highly rated safety systems available in the market. Tricon is based on Triple Modular Redundant (TMR) technology. TMR employs three isolated, parallel control systems and extensive diagnostics integrated into one system. The Tricon system provides high-integrity, error-free, uninterrupted process operation with no single point of failure. TMR applies to inputs, outputs and logic. Due to the footprint and cost of the system, they are mainly used for critical applications such as turbine controls (overspeed control) and sometimes as DCS. Even though this malware was designed specifically for Triconex systems, cyber security organizations believe the malware's capability and methodology can be tailored by adversaries to target a different vendor's safety system. The belief that even if the process control system is compromised the safety system will prevent damage has been challenged by this incident.

4.0 REFERENCES

4.1 FM

Data Sheet 1-20, *Protection Against Exterior Fire Exposure*
Data Sheet 1-44, *Damage-Limiting Construction*
Data Sheet 2-0, *Installation Guidelines for Automatic Sprinklers*
Data Sheet 3-26, *Fire Protection for Nonstorage Occupancies*
Data Sheet 4-5, *Portable Extinguishers*
Data Sheet 4-9, *Halocarbon and Inert Gas (Clean Agent) Fire Extinguishing Systems*
Data Sheet 5-11, *Lightning and Surge Protection for Electrical Systems*
Data Sheet 5-23, *Design and Protection for Emergency and Standby Power Systems*
Data Sheet 5-28, *DC Battery Systems*

Data Sheet 5-31, *Cables and Bus Bars*
Data Sheet 5-32, *Data Centers and Related Facilities*
Data Sheet 7-43, *Process Safety*
Data Sheet 7-45, *Safety Controls, Alarms, and Interlocks (SCAI)*
Data Sheet 9-0, *Asset Integrity*
Data Sheet 9-1, *Supervision of Property*
Data Sheet 10-1, *Pre-Incident and Emergency Response Planning*
Data Sheet 10-5, *Disaster Recovery Planning*
Data Sheet 10-8, *Operators*

4.2 Other

International Society for Automation (ISA). ISA/IEC 62443 standards and technical reports series.

National Institute of Standards and Technology (NIST). *Guide to Industrial Control Systems (ICS) Security*. NIST SP 800-82, Revision 2.

North American Electric Reliability Corporation (NERC). CIP Reliability Standards.

Electric Power Research Institute (EPRI), *Generation Cyber Security*.

US Department of Homeland Security, National Cybersecurity and Communications Integration Center's (NCCIC), ICS-CERT.

APPENDIX A GLOSSARY OF TERMS

Access: The ability and means to communicate with or otherwise interact with a system in order to use system resources. Access may involve physical access (authorization to be physically allowed in an area, possession of a physical key lock, PIN code, access card or biometric attributes that allow access) or logical access (authorization to log into a system and application through a combination of logical and physical means).

Allowlist: A list of discrete entities, such as hosts or applications, that are known to be benign and are approved for use within an organization and/or information system. Example: Allowing only certain applications and services to run on a host as part of its hardening.

Antivirus software: Software that protects a computer against viruses and malware. Once the presence of malicious code is detected, the antivirus software attempts to clean, delete or quarantine any affected files, directories, or disks.

Asset: Physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization.

Asset discovery solutions:

1. Passive monitoring: A silent, nonintrusive monitoring technique used to capture traffic from a network by copying traffic, often from a span port or mirror port or via a network tap. OT-based IDS solutions use this technique for asset discovery as well as to detect unauthorized activity.
2. Active monitoring: An intrusive monitoring technique, performing queries which vary slightly depending on the manufacturer, in the relevant controller's native language (protocol). An active monitoring approach involves asking a controller for detailed information (IP and MAC address, firmware version, backplane configuration, etc.).

Attacker: A person who creates and/or modifies computer software and hardware to commit crimes or for financial gain. Attackers generally try to gain access to computer systems to obtain usernames and passwords.

Attack vector: A method or means by which a threat actor gains access to or harms an organization's data or computer network. Examples of attack vectors include denial of service (DoS), malware, physical access, ransomware and social engineering.

Authentication: The act of proving an assertion, such as the identity of a computer system user. In contrast with identification, the act of indicating a person or thing's identity, authentication is the process of verifying that identity. A typical means of authentication is a password provided by a user to login.

Baseline: A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures.

Basic process control system (BPCS): The basic process control system (BPCS) is the system that manages equipment, production, and processes at a facility. Based on a preset condition or conditions, the BPCS uses feedback from control loops to automate and maintain a desired condition, output or process. BPCSs are customized to match any process need - from very large and complex systems such as power generation systems or chemical processors to very simple systems with only one input and output such as motion detectors or lighting systems.

Configuration management (CM): Policies and procedures for controlling modifications to hardware, firmware, software and documentation to ensure the information system is protected against improper modifications prior to, during and after system implementation.

Control center: See Process control room.

Control network: Time-critical network that is typically connected to equipment that controls physical processes. The control network can be subdivided into zones, and multiple, separate control networks can exist within one enterprise and site.

Credentials: At a minimum, credentials would include a username and password; but they could also be a physical or human biometric element such as a fingerprint. Credentials are used to authenticate a user when they log into the ICS. Access permissions may be tied to the user's credentials. A user's credentials may only grant them access to an operator's workstation, whereas a higher level of access for a different user could grant access to an engineering workstation.

Data diode/unidirectional gateways: See One-way data diode below.

Default password: The standard password provided on a system when it is first delivered or installed. Users should always change the default password immediately.

Defense in depth: The practice of layering multiple overlapping security controls to secure information technology or operational technology environments.

Demilitarized zone (Industrial DMZ):

1. An interface on a routing firewall like the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied.
2. A host or network segment inserted as a "neutral zone" between an organization's private network and the internet. Most Industrial DMZs are between and organization's IT and OT environments.
3. A perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Distributed control system (DCS): A DCS is an automated control system that controls processes by distributing control functions across multiple interconnected components. It uses distributed components rather than a centrally-located, single unit. Note that the term "DCS Controller" applies to the physical controller component, whereas the term "DCS" applies to the entire system, including application servers, HMI, etc.

Encryption: The scrambling of data so that it becomes unreadable to anyone not in possession of the "key" used to unscramble it. Cryptographic transformation of plaintext into ciphertext conceals the data's original meaning to prevent it from being known or used.

Engineering workstation: The engineering workstation is usually a reliable, high-performance computing platform designed for configuration, maintenance and diagnostics of the control system applications and other control system equipment. It typically contains the vendor specific software needed to program devices and the project files used to program devices, including PLCs and HMIs.

Enterprise resource planning (ERP) system: Software used in business environments. Examples are SAP and Oracle/PeopleSoft, systems that drive production orders, warehousing and transportation information for completed orders.

Field device: Equipment that is connected to the field side on an ICS. Types of field devices include remote terminal units (RTUs), programmable logic controllers (PLCs), actuators, sensors, human/machine interfaces (HMIs) and associated communications.

Firewall: A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Gateway: A relay mechanism that attaches two or more computer networks that have similar functions but dissimilar implementations and that enables host computers on one network to communicate with hosts on the other.

Hardening: A security measure that includes removing or disabling unnecessary features, functions, ports, and services, and applying cyber security controls to prevent unauthorized use. Two types of hardening include:

1. Physical hardening: Disabling through physical means; removing unneeded communication ports, blocking access to the ports and drives, etc.
2. Logical hardening: Disabling unused network and communication protocols, drivers for unused peripherals, web servers, etc., and then applying cyber security controls such as enabling password protection to update firmware and load programs, enabling logs and alerts, and enabling any security technologies such as antivirus or allowlisting that came with the device.

Historian: An ICS historian is a specialized software system that collects point values, alarm events, batch records and other information from industrial devices and systems and stores them in a purpose-built database (i.e., a centralized database supporting data analysis using statistical process control techniques).

Human/machine interface (HMI):

1. The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software.
2. Software and hardware that allows authorized users to monitor and control processes and/or equipment such as status or historic trend display, control setting modification, and manual override in the event of emergency.

Immutable backup files: Immutable backup files are files that cannot be altered or changed in any way (write once, read many) and cannot be deleted until the retention period has ended. (This retention period end-date needs to be configured at the time of the immutable file creation.) Because immutable files cannot be altered or deleted, version control is crucial.

Industrial control equipment: See Industrial control panels.

Industrial control instrumentation equipment rooms: Rooms where the process control equipment is located, which typically include several industrial control panels and the networking equipment needed for the physical process to function.

Industrial control panels (ICP): An assembly that comprises two or more control-circuit and power-circuit components. Control circuit components include Programmable Logic Controllers (PLCs), input and output modules, motor drives and communication modules. Power circuit components include power sources, Uninterrupted Power Supply (UPS) devices, relays, electrical transformers and voltage/current converters. Typically, ICPs work with 600 volt or less power, although UL 508A and IEC standards allow for 1,000 volts or less.

Industrial control system (ICS):

1. 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 (PLCs), safety logic solvers often found in the industrial sectors

and critical infrastructures. An ICS consists of various control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, generating and transportation of matter or energy).

2. Collection of personnel, hardware and software that can affect or influence the safe, secure and reliable operation of an industrial process.

Information technology network (IT): A network typically used to conduct business where computers are used to create, manipulate, store, retrieve and transmit data.

Input/output (I/O) device: A general term for the equipment used to communicate with a computer or a control system.

Insider threat: Threats (both malicious and unintentional) from people within the organization, such as disgruntled employees, former employees, contractors and business associates who have inside information concerning the organization's security practices, data and computer systems.

Integrity: Quality of a system, reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data.

1. Intelligent electronic device (IED): Any device incorporating one or more processors with the capability to receive, send and control data from/to an external source (e.g., electronic multifunction meters, digital relays, controllers).

Intrusion detection system: A security service that monitors and analyzes network or system events to find and provide real-time or near real-time warning of attempts to access system resources in an unauthorized manner. An intrusion detection system can detect and alert, but not block or reject, bad traffic.

Local area network (LAN): Communications network designed to connect computers and other intelligent devices in a limited geographic area (typically less than 10 kilometers).

Malware: A generic term used to describe malicious software such as viruses, Trojan horses, spyware and malicious active content.

Manufacturing execution system (MES): A computerized system, including software, used in production and manufacturing environments to help track inventory and other production information. Similar to ERP but with a more specialized focus on manufacturing (e.g., tracking and documentation of the transformation of raw materials to finished goods).

Multi-factor authentication (MFA): Multi-factor authentication involves two or more authentication factors (i.e., something you know such as a password, something you have such as a time-based token/static token, or something you are such as a fingerprint). Two-factor authentication is a special case of multi-factor authentication involving exactly two factors.

One-way communication: Strategies used to ensure secure one-way communications from devices or across different networks/protection zones include:

1. Sending only an analog signal (an amperage or voltage) to/from a device instead of digital data.
2. Use of a one-way data-diode/ unidirectional gateway.
3. Use of rules in a firewall or a DMZ to pass data across networks.

One-way data diodes and unidirectional gateways: Hardware-based devices with two nodes or circuits (one sends only, and one receives only) that allow the flow of data in one direction only, from a source to a destination. They use an LED as a data transmitter on one side and a photo-receiver on the other, making it physically impossible for data to pass in the other direction. Some may refer to a software solution (e.g., through a firewall setting) or even a switch or router configuration as a unidirectional gateway, but a "true" unidirectional gateway utilizes one-way data diode(s) as a component to create the unidirectional gateway. As per NIST 800-82: Unidirectional gateways are a combination of hardware and software. The hardware permits data to flow from one network to another but is physically unable to send any information at all back into the source network. The software replicates databases and emulates protocol servers and devices.

Operating system (OS): The underlying software that enables interaction with a computer. The OS controls computer storage, communications and task management functions.

Operational technology network (OT): The term OT is often used interchangeably with industrial control system (ICS) or process control network (PCN). The term is meant to distinguish between the business information technology network (IT) and the network controlling operational assets (OT). ICS comprise various controllers and instruments to monitor and control a physical process, whereas OT includes the computing systems and infrastructure that manage industrial operations (including the ICS).

Operator workstation: An operator workstation provides a dynamic view of all plant processes needed to operate control systems. It presents control graphics, diagnostics, trends, alarms and status displays.

Patch: A software add-on designed to fix bugs and security issues in operating systems or applications. Security risks can be minimized by keeping software current with patches.

Phishing: Type of security attack that persuades victims to reveal information by presenting a forged email to lure the recipient to a web site that looks like it is associated with a legitimate source.

Physical access: On-site, hands-on access to computer and network hardware or other parts of a network installation.

Policy: A set of rules that governs how certain procedures are handled.

Procedure: Steps taken to perform a certain task.

Process control center: See Process control room.

Process control room: A cutoff and/or isolated room in which personnel monitor and control processes from a central or remote location. The process control room is typically separate from, but integrated with, industrial control equipment rooms to control the function of equipment. Process control is extensively used in industry. It commonly enables mass production of continuous processes such as paper, pharmaceuticals, chemicals and electric power, as well as other industrial processes. In some scenarios, process control rooms/technical spaces may be unattended and operated remotely.

Programmable logic controller (PLC): PLCs are automation controllers with the capability of controlling complex processes, and they are used substantially in supervisory control and data acquisition (SCADA) systems and distributed control systems (DCSs). PLCs are also used as the primary controller in smaller system configurations. PLCs are used extensively in almost all industrial processes.

Protocol: A protocol is a system of rules used by two components sharing data to understand the data being shared. A protocol is not a “language” but can more appropriately be described as the grammar and syntax for communicating that language. In the ICS world, many of these protocols are unique by vendor and have been designed for functionality and reliability rather than security. They are typically transmitted in clear text (not encrypted). This enhances the need to separate OT environments from IT. A few examples of ICS protocols common in industry are Modbus RTU, Modbus TCP, Profibus, Profinet, DNP3 and ControlNet. On the IT side, protocols based on TCP/IP (such as FTP, DNS, HTTP, HTTPS) are common.

Ransomware: A type of malicious software (malware) that disables operation or blocks access to data until the owner or operator responds to a demand for payment.

Reliability: Ability of a system to perform a required function under stated conditions for a specified period.

Remote access: Access by users (or information systems) communicating externally to an information system security perimeter. (Source: NIST SP 800-53.) Use of systems that are inside the perimeter of the security zone from a different geographical location but with the same rights as when physically present at the location. Examples of equipment used in remote access:

1. Modems modulate and demodulate data in and out of the box. Essentially, they convert analog electrical signals from outside the network into digital 1s and 0s to be handled by the router, and vice versa.
2. Routers are downstream of the modem. They connect to a WAN or to the internet with a public IP address. They guide and direct network data, while prioritizing the data and choosing the best route to use for each transmission.
3. Remote access servers provide services that manage remote connections from outside the LAN. Commonly referred to as “jump” servers/hosts.

Remote access servers: A type of server that provides services to manage a remote connection from outside the LAN. Commonly referred to as “jump” servers.

Remote terminal unit (RTU): Unit designed to support distributed control system (DCS) and supervisory control and data acquisition (SCADA) remote stations. RTUs are field devices used for monitoring parameters. They communicate with a supervisory controller using remote communication capabilities, which can include modem, cellular, radio interfaces or any wide area communication technology. Sometimes, PLCs are implemented as field devices to serve as RTUs. In this case, the PLC is often referred to as an RTU. They are often installed in locations with no easy access to electricity and can be supplied with solar power.

Rogue device: A rogue device is an unauthorized device that does not have permission to access and operate on the network. Such devices may be malicious in nature and could be used to bypass security.

Role-based access control: Form of identity-based access control where the system entities that are identified and controlled are functional positions in an organization or process.

Router: A gateway between two networks at open systems interconnection (OSI) layer 3 that relays and directs data packets through that inter-network. The most common form of router operates on internet protocol (IP) packets.

Safety network: Network that connects safety instrumented systems for the communication of safety-related information.

Safety system: System used to implement one or more safety-instrumented functions. It is composed of any combination of sensors, logic solvers and actuators.

Security information and event management (SIEM): Application that provides the ability to gather security data from information system components, normalizes audit trails and logs tests against a set of correlation rules that when triggered, creates events for analysis and presents that data as actionable information via a single interface.

Security operations center (SOC): Solution that encompasses the people, processes and technology, including SIEM solution, involved in protectively monitoring digital environments (i.e., IT and OT), responding to events that translate into incidents, researching for known/unknown threats, incident response and information sharing, among other things.

Segmentation: Splitting up a network into smaller, compartmented sections that are still part of the same overall network. Within ICS, segmentation is typically achieved through virtual local area networks (VLANs) or hardware firewalls. Segmentation helps slow the spread of malware or impede an attacker. However, use of VLANs is not an acceptable means to separate IT from OT.

Segregation: Disconnecting a network from other networks completely (air-gapped). Safety instrumented systems (SIS) at large facilities are segregated because they are not controlled by the ICS network handling the basic process control system (BPCS).

Sensor:

1. A device that produces a voltage or current output that is representative of some physical property being measured (e.g., speed, temperature, flow)
2. A device that measures a physical quantity and converts it into a signal that can be read by an observer or an instrument
3. A device that responds to an input quantity by generating a functionally related output, usually in the form of an electrical or optical signal

Separation: Proper partitioning of different networks that are considered untrusted to each other. Separation is usually achieved using firewalls (and ideally a formal DMZ) or unidirectional gateway. Separation from IT is key for ICS networks.

Supervisory control and data acquisition (SCADA): Used to control dispersed assets where centralized data acquisition is as important as control. SCADA systems are used in distribution systems such as the following:

1. Water distribution and wastewater collection systems
2. Oil and natural gas pipelines
3. Electrical utility transmission and distribution systems
4. Rail and other public transportation systems

SCADA systems integrate data acquisition systems with data transmission systems and human/machine interface (HMI) software to provide a centralized monitoring and control system for numerous process inputs and outputs. SCADA systems are designed to collect field information, transfer it to a central computer facility and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in near real time. Based on the sophistication and setup of the system, control of any system, operation or task can be automatic or can be performed by operator commands.

SCADA Control Center: A control center using computers with SCADA software to monitor and operate equipment at one or more locations that are geographically remote from the control center. SCADA Control Centers are typically located in a building that does not have local process controls like DCS or PLCs. These SCADA control centers have two-way data traffic and can make operating changes to the geographically remote equipment.

Threat actor: An entity that is partially or wholly responsible for an incident that impacts an organization's security. Examples of threat actors include Hacktivists, Insider threat, Nation state and Organized crime.

User repository: A system that stores information about users/members for a particular domain, with the intent of ensuring authentication and authorization capabilities using a centralized approach. Microsoft Active Directory is a common example of a user repository commonly seen in IT and OT networks.

Virtual private network (VPN): A secure connection between a public network (usually the internet) to a private network.

Vulnerability: Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy.

WAN solutions: A wide area network (WAN) is a computer network spanning large regions, countries or even the world. Data is transferred between networks that span a geographical location in various ways, using different types of connections to create these WANs. Wired solutions include: MPLS, T1 and persistent virtual circuits. Wireless communication services include 4G and 5G, Wi-Fi and satellite networks.

War dialing: A war dialer is a computer program used to identify the phone numbers that can successfully make a connection with a computer modem. The program automatically dials a defined range of phone numbers, and logs and enters into a database those numbers that successfully connect to the modem. Some programs can also identify the particular operating system running in the computer and may also conduct automated penetration testing. In such cases, the war dialer runs through a predetermined list of common usernames and passwords in an attempt to gain access to the system.

APPENDIX B DOCUMENT REVISION HISTORY

The purpose of this appendix is to capture the changes that were made to this document each time it was published. Please note that section numbers refer specifically to those in the version published on the date shown (i.e., the section numbers are not always the same from version to version).

July 2024. Interim revision. Editorial changes were made.

January 2024. Interim revision. Minor editorial changes were made.

July 2023. Interim revision. The following significant changes were made:

A. Improved and clarified fire protection recommendations.

1. Improved guidance on occupancy fire protection and equipment fire protection.

B. Updated ICS Security recommendations.

1. Provided guidance on connections to remote SCADA control centers.

C. Added terms to Appendix A Glossary of Terms.

January 2023. Interim revision. The following changes were made:

A. Clarified fire protection recommendations.

B. Clarified ICS management recommendations.

C. Clarified and modified ICS security recommendations, including:

1. Modified configuration and system monitoring recommendations for ICS and OT networking equipment including safety systems.
2. Clarified patch management recommendations.
3. Clarified networking safeguard recommendations.

D. Clarified and modified ICS operations recommendations, including:

1. Clarified alarm management recommendations.
2. Modified incident recovery program — specifically, the types of acceptable backup files.

E. Added terms to Appendix A Glossary of Terms.

July 2022. Interim revision. Minor editorial changes were made.

October 2021. Interim revision. Updated reference to battery testing (Section 2.7).

July 2021. Interim revision. Updated and clarified the following:

A. ICS Security

i. Access Management
ii. Configuration Management
iii. Patch Management
iv. Networking Safeguards

B. ICS Operations

i. Emergency Operating Procedures

C. Construction and Fire recommendation.

July 2020. Interim revision. Updated contingency planning and sparing guidance.

October 2019. This is the first publication of this document.