INDUSTRIAL CONTROL SYSTEMS

Table of Contents

Page

List of Figures

List of Tables

1.0 SCOPE

1.1 Overview

This data sheet provides loss prevention recommendations for Industrial Control Systems (ICS), applying a threat-based approach, combined with our engineering expertise, to evaluate site-wide ICS infrastructure, including communication networks and potential cyber hazards. The objective is to build resilience against cyber attacks that may lead to physical damage to equipment or work in process/loss of production, and business interruption.

1.2 Definition of ICS

For the purposes of this document, ICS refers to the integrated hardware and software systems used to control, monitor and protect industrial and non-industrial processes. These systems are critical for managing operations in sectors such as manufacturing, energy, utilities and building automation.

1.3 Examples of ICS-Connected Devices

The following list includes core components that may be connected to an ICS network. It is not intended to be comprehensive or definitive:

- Supervisory Control and Data Acquisition (SCADA) Systems
  Centralized systems used to monitor and control industrial processes across large geographic areas
- Distributed Control Systems (DCS)
  Used for continuous process control in industries like oil and gas, chemicals, and power generation
- Programmable Logic Controllers (PLC)
  Industrial computers that control machinery and processes in real time, often using specialized programming language like ladder logic or structured text
- Remote Terminal Units (RTU)
  Field devices that collect data and communicate with SCADA systems, especially in remote or distributed environments
- Human-Machine Interfaces (HMI)
  Interfaces that allow operators to interact with control systems and visualize process data.
- Engineering Workstations
  Used to configure, program, and maintain control systems like PLCs, DCS and SCADA
- Network Infrastructure Devices (e.g., switches, firewalls, routers)Critical for secure and reliable communication between OT components.
- Safety Instrumented Systems (SIS)
  Instrumented systems used to implement one or more safety functions.
  SIS are composed of sensors, logic solvers and final control elements designed to take the process to a safe state when predetermined conditions are violated. Other commonly used terms include emergency shutdown system (ESD, ESS), safety shutdown system (SSD), safety system and safety interlock system.

The purpose of this data sheet is to support FM Clients and asset owners in identifying vulnerabilities within their ICS, and to recommend practical steps for reducing associated risks and exposures. The guidance in this document is not all-inclusive or exclusive and may not apply to all locations.

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
- Information technology (IT) systems used for general business (e.g., systems intended to browse the web or send and receive emails, systems with access to the internet—except devices within the shop floor level with internet connectivity)

1.4 Hazard

If ICS are not properly protected, managed and maintained, loss of production and/or potentially significant property damage can result. 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.

1.5 Changes

June 2026. This data sheet was completely reorganized with minor editorial changes.

2.0 LOSS PREVENTION RECOMMENDATIONS

2.1 Introduction

An ICS system is a complex system of controllers, logic solvers, motor starters, drives, monitoring and sensing equipment, and other components, all interconnected through communication networks.

To identify risks and exposures related to the site-wide ICS, the system management team and operators should have a complete understanding of the overall system, including its operational, security, communication and software requirements.

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

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

C. ANSI/Examinationll 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 For rooms of combustible construction do the following:

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 manufacturer's design, installation, operation and maintenance manual shown in the FM Approval's 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 exceeding 30 ft (9 m)

2.3.6.2 For 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:

A. 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.

1. 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.
2. 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.

B. 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.

C. Equipment enclosures are constructed of metal.

D. Minimal use of paper and other combustible materials in the room.

E. No storage of packing materials or plastic cassettes within the room. Note: This requirement includes all combustible media (e.g., tape reels).

F. 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. Halocarbon or inert gas (clean agent) fire extinguishing system

1. In the room, provided the cabinets are ventilated

2. Arranged to discharge the halocarbon or inert gas directly inside the cabinets

Follow the guidance in Section 2.3.6.2 above.

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

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.

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 suitable type or combination type.

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

2.3.14.1 Verify electrical personnel can respond 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.

2.3.14.2.1 These individuals must be capable of diagnosing the fire/smoke condition in the affected area and implementing the pre-incident plan for local, regional or complete manual power isolation.

2.4 Human Factor

2.4.1 OT Boundary Architecture

This section outlines the framework and design principles used for managing and controlling industrial processes and physical devices. It focuses on clear communication and coordination among system components.

2.4.1.1 To enhance OT network security and resilience against cyber threats, apply the following principles when designing the OT boundary architecture:

A. Implement an industrial firewall at the OT network boundary to create separation between IT and OT networks. For outbound-only communication, a one-way diode may be used as an alternative to a firewall. See Figure C.2 in Appendix C for an example.

B. To manage communications into the OT network boundary (such as Remote Access, enterprise resource planning [ERP], manufacturing execution systems [MES], or historian data exchange), implement an Industrial Demilitarized Zone (iDMZ) between IT and OT networks. An iDMZ is required whenever the OT environment receives inbound communication, uses outbound-only communication through a firewall, or allows remote access.

C. Credentials for accessing ICS should not rely on corporate Active Directory accounts. Instead, ICS credentials should be managed in a dedicated user repository separate from IT systems. Alternatively, using non-networked or local accounts is considered acceptable.

D. The use of dual-homed devices to bridge the IT/OT boundary or multiple OT networks is strictly prohibited. See Figure C.4 in Appendix C for an example.

E. Prohibit OT personnel from accessing any internet services, such as web browsing or email, from any OT device.

2.4.2 Remote Access

Operational Technology (OT) Remote Access enables secure connectivity and management of OT systems (including Engineering Workstations, Programmable Logic Controllers [PLC], Distributed Control Systems [DCS], and Industrial Automation and Control Systems [IACS]) from anywhere outside the OT network (including the corporate IT network).

Implementing a secure OT remote access solution is crucial for safeguarding industrial systems and ensuring uninterrupted operations. It enables authorized personnel to access and manage OT environments remotely while protecting against cyber threats.

2.4.2.1 Securely manage remote access to the OT environment by implementing a jump server (or equivalent solution) in an Industrial Demilitarized Zone (iDMZ). This intermediary device acts as a secure gateway between different security zones (such as IT and OT networks). It provides controlled access to OT systems. Figure C.3 in Appendix C shows an example of an OT Jump Server.

The main reason for using an iDMZ and a jump server is to restrict direct access from IT and external networks to OT systems. Since most cyber attacks start in IT, this setup adds a secure layer that protects OT by allowing only controlled and monitored access.

A Jump Server (or equivalent solution) should incorporate key security measures to ensure secure access between different networks (e.g., IT, OT, internet/Cloud, etc.).

Mandatory Security Requirements for Jump Server Equivalent Solution:

- Access Control Lists (ACLs)
  Define which users, devices or IP addresses are allowed to access specific resources in the OT environment, helping enforce strict access boundaries.
- Network Segmentatio
  nLimits the impact of a cyber incident by containing it within a specific network segment, preventing threats from spreading to critical OT systems.
- Role-based Inbound and Outbound Access
  Role-based access controls ensure remote users can only access the specific OT assets needed for their duties via the OT jump server. This control ensures they only reach approved assets, preventing unauthorized access to other systems and reducing the risk of threat propagation. Additionally, clearly defined roles and responsibilities guarantee that only authorized personnel interact with sensitive OT systems, minimizing the likelihood of unauthorized or accidental actions.
- Logging and Monitoring
  Implement logging and monitoring for unauthorized access or potentially malicious events within the OT environment, including OT devices accessed and failed login attempts. These actions help

detect issues early, track system activity and respond quickly to potential threats. Logs should be retained for a minimum of 180 days to support investigations.

- Application Whitelisting
  Only approved applications can run on the jump server equivalent solution. This method blocks unknown or harmful software, helping protect against malware and unauthorized changes.

2.4.2.2 Protect remote access to the OT environment by enforcing multifactor authentication (MFA) at the OT network boundary (including from the corporate IT network). MFA should be required upon every login.

2.4.3 System Security

This topic refers to the practices, technologies, and measures specifically designed to protect the integrity and availability of systems that monitor and control industrial processes and physical devices.

2.4.3.1 Account Security

2.4.3.1.1 To enhance the system security for the ICS environment (including laptops, desktops, PLCs, DCS, HMIs, servers, etc.) implement robust measures focusing on preventing unauthorized access, misuse, modification or destruction by applying the following security measures:

A. Engineering workstations require a unique, user-specific login and password to gain access to the system.

B. Change the default factory username and password on all systems, hardware, and software.

C. Enforce strong password requirements for engineering workstations by implementing the following controls, aligned with the organization's risk tolerance:

1. Minimum length and complexity
2. Password expiration or rotation
3. Lockout after failed attempts

2.4.3.2. Network Monitoring

Network monitoring for OT systems is essential for ensuring security and operational continuity. It provides real-time visibility into system performance, detects and responds to cyber threats, and supports proactive maintenance to prevent disruptions.

2.4.3.2.1 Implement continuous monitoring of the OT network to detect anomalous activity, such as unauthorized changes. This proactive approach helps identify potential cyber threats and unusual behavior in real-time, allowing for quick response and mitigation. Key OT monitoring aspects include:

A. **Detecting New Devices:** Actively identify and log new devices on the network to ensure they are authorized and properly configured.

B. **Monitoring Traffic in and out of the OT boundary:** Continuously analyze communication between IT and OT systems to detect unusual patterns or unauthorized access attempts.

C. **Identifying Attack Patterns:** Leverage advanced tools such as Security Information and Event Management (SIEM), Intrusion Detection Systems (IDS), Endpoint Detection and Response (EDR) and threat detection tools to recognize and respond to common attack patterns on the network, including malware, ransomware and other cyber threats.

2.4.3.3 General System Security

2.4.3.3.1 Use the following precautions for portable devices (e.g., laptops, tablets, mobile phones and external storage devices, etc.) connecting to the ICS:

A. **Device Security Measures:** For portable devices, ensure wireless connections are disabled. Regularly update security patches and antivirus software to maintain device security.

B. **External Storage Security:** Perform thorough antivirus/malware scans on memory cards, USB thumb drives, portable hard drives and other external storage devices before connecting them to the ICS. Before granting site access, ensure contractors and temporary visitors are informed about organizational internal

security requirements, particularly regarding portable OT devices. This awareness helps maintain site security by preventing unauthorized access and potential data breaches. For further details, refer to Section 2.4.4.2, Training.

2.4.3.3.2 Disable unused ports (USB and RJ45) logically/electronically (e.g., BIOS, group policy or other software utilities) or using physical lockable inserts for all equipment connected to the ICS.

2.4.3.3.3 Limit unnecessary features and functions (such as unused protocols and services) on OT/ICS systems, including servers, workstations, DCSs, PLCs and HMIs, wherever possible, as part of system hardening process. OEMs typically provide hardening guides for their products to ensure secure configuration and best practices.

2.4.3.3.4 Antivirus protection software (or equivalent EDR/XDR/MDR tools) should be employed on ICS and in the OT environment, including SCADA systems, when possible. Clients should work with the ICS vendor or service provider to determine which protection software is certified within their ICS.

2.4.3.4 Patch Management Program

2.4.3.4.1 Patch management for OT is essential to maintain cybersecurity, ensure system reliability, support compliance and mitigate risks:

A. Establish and execute a comprehensive patch management program for OT, covering all relevant equipment and devices (e.g., Remote Access Solutions, PLC, HMI, DCS, Network devices, MES, Historian, engineering workstations, etc.). Furthermore, regularly validate patches with the OEM to ensure compatibility and enhance system security and efficiency.

A comprehensive patch management program includes:

- Monitor bulletins and alerts of cyber-IT and OT security vulnerabilities from system and device manufacturers, ICS integrators, government agencies and others; and ensure approval is obtained from vendors before implementing any patches in OT environments.
- Upon learning of a cybersecurity notification, the ICS oversight team determines the actions required to protect the site's ICS, based on the criticality of the ICS and the associated cybersecurity risk. Additional temporary protection measures against system vulnerabilities may be necessary until a software patch can be installed.
- 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.
- Provide additional protection measures against cybersecurity vulnerabilities for obsolete equipment and/or software due to the lack of support from the OEM.

Examples of additional protection measures may include:

- Placing legacy devices in a separate network with a firewall (not connected to plant control network)
- Restricting physical and logical access to the legacy control system
- Providing additional logging and monitoring (Refer to Section 2.4.3.2. for further information.)

2.4.4 OT Incident Response and Safety Systems

OT Incident Response and Safety Systems prepare and enable organizations to detect, quickly respond to and mitigate the impact of incidents such as cyber attacks, natural disasters and other crises.

Incident Response is the structured approach an organization takes to identify, manage and recover from a cybersecurity incident. Organizations should document and implement a robust OT Incident Response Plan to quickly detect, contain and recover from incidents impacting their ICS.

2.4.4.1 OT Incident Response Planning

2.4.4.1.1 Apply the following key topics when documenting an OT IRP:

A. Ensure the OT IRP includes guidance on how to shut down the system and/or process (i.e., bring the system to a safe state) when the ICS behaves suspiciously or ceases to function. This guidance should include the following known or suspected cyber incidents (not a comprehensive list):

1. Detection of malware by antivirus or EDR solution (when in place)
2. Black screen/HMI screen freeze-up
3. Unexplained unit trip
4. Ransomware messages appearing on workstations
5. Cursors moving unexpectedly on workstations without operator input
6. Unrecognized configuration change

Ensure the OT IRP identifies key personnel who should be involved in the organization's response. Organizations should consider whether their staff have the required skills or whether they should engage third-party consultants or specialists with the expertise required to respond to a cybersecurity incident.

B. Conduct regular ICS tabletop exercises to verify incident response plan effectiveness. These simulations reveal security gaps, improve situational awareness, and reinforce team coordination. They validate response plans, train staff and clarify roles during cyber incidents.

These tabletop exercises are also applicable to SCADA systems, where appropriate.

C. Ensure the OT IRP includes processes to mitigate the impact to the ICS and production from the loss of an ERP system or MES.

2.4.4.2 Training

2.4.4.2.1 Cybersecurity training is the educational process of teaching employees how to protect their systems, networks and data from cyber threats. Apply the following measures when designing cybersecurity training for OT employees, contractors and vendors:

A. Ensure that OT employees, contractors, and vendors receive regular cybersecurity training, focusing on ICS/OT risks. This training should be in addition to IT-focused cybersecurity awareness training.

Contractors and vendors can leverage previous training, if they provide evidence showing they have received similar cybersecurity training content from their respective companies.

By implementing ICS/OT cybersecurity training programs, organizations can significantly enhance their resilience against cyber threats and ensure the security of their ICS/OT systems. A cybersecurity training program should include, but is not limited to:

- Overview of Key OT Cybersecurity Topics: Provide an understanding of the critical aspects of OT cybersecurity.
- Internal Policies for Mobile and Portable OT Device Usage: Establish guidelines regarding the use of portable OT devices to maintain security standards. Highlight the increased risk associated with connecting devices to both IT and OT and connecting devices from outside vendors/contractors.
- Internal Policies for the Use of USBs and Other Media: Establish guidelines regarding the use of USBs, portable hard drives and other storage media.
- Recognizing and Avoiding Security Risks in OT Environments: Educate employees, contractors and vendors on common OT threats and best practices for mitigating them.
- How to initiate the OT IRP: Make sure employees are trained on how to activate the OT IRP and conduct initial containment, so that cyber incidents are handled correctly, preserving forensic evidence.

2.4.4.3 Backup

2.4.4.3.1 Making backups refers to the process of systematically copying and storing data so it can be recovered in case of data loss, corruption or disaster. Backups for OT are essential to ensure business continuity, protect against cyber threats, comply with regulations, manage risks and support incident response. Apply the following measures when defining a backup plan:

A. Maintain current offline or immutable backups for critical OT/ICS systems to ensure operational resilience and quick recovery in case of cyber incidents.

1. Periodically update these backups to include the latest configuration files and system images.
2. Periodically test backup recovery processes to ensure they are working as intended.

B. Ensure that redundant systems or manual overrides are in place for critical OT processes to mitigate the impact of cyber-induced failures.

Redundant systems provide backup capabilities, allowing operations to continue seamlessly in the event of a primary system failure. Examples include:

- Dual or triple-redundant PLCs
- Redundant power supplies to ICS equipment
- Hot/Cold standby OT servers
- Network redundancy (e.g., dual network paths, redundant switches, or ring topology to maintain connectivity during link or device failures)

2.4.4.4 Safety Systems

Safety Systems are specialized systems designed to ensure the safe operation of industrial processes, even in the presence of faults, failures or cyber threats. Safety systems are integral components in industrial settings. They are designed to protect people, equipment and the environment from hazardous conditions and potential accidents. These systems include basic safety functionality in PLCs and DCSs such as overspeed/vibration, Safety Instrumented Systems (SIS), emergency shutdown systems, and fire and gas detection systems.

2.4.4.4.1 Apply the following measures when implementing and securing Safety Systems, as applicable:

A. Ensure that Safety Systems in ICS environments are not accessible remotely. This practice mitigates the risk of cyber threats and unauthorized access, which can compromise the integrity and safety of critical operations.

B. Ensure the security and reliability of the SIS by segregating them from process control networks. The separation of SIS from process control networks prevents common-cause failures and ensures safety functions remain uncompromised by issues within the control network. Implement dedicated communication channels and hardware for SIS, and regularly review and update the network architecture to maintain robust segregation and compliance with industry standards.

C. Ensure that SIS are set to ″run mode″ and protected by a physical key switch or digital password before enabling the system and operating the ICS. The use of “run mode,” physical key switches and digital passwords protect against unauthorized changes to, tampering or misconfiguration of the SIS, which could jeopardize safety in the OT environment. Additionally, integrate changes to the operating mode into the system monitoring protocols to maintain continuous oversight and security.

2.4.5 Governance and Third-Party Risk Management

Governance in OT refers to the framework of policies, procedures and accountability structures that guide how security and operational decisions are made and enforced. It ensures that cybersecurity and operational integrity are embedded into every layer of the organization, from executive leadership to plant-floor operations.

Third-party risk management (TPRM) focuses on identifying, assessing and mitigating risks introduced by external entities that interact with OT systems. Third-parties may include equipment suppliers, maintenance contractors, software vendors and managed service providers. Each third party represents a potential entry point for cyber threats or operational disruptions.

2.4.5.1 Governance

2.4.5.1.1 Apply the following key practices when managing a cybersecurity Governance program:

A. Organizations should create an ICS oversight team composed of individuals from the corporate and local facility levels that are responsible for overseeing the implementation of cybersecurity policies related to the ICS. The roles and responsibilities of individuals from the corporate and local facility levels should be clearly defined.

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

Ensure comprehensive inclusion of all ICS assets, such as PLCs, HMIs, DCSs, network devices, industrial robots, SCADA systems, Building Management Systems (BMS) and Energy Management Systems (EMS), among others.

2.4.5.2 Third-Party Risk Management

TPRM (also referred to as vendor risk management, supplier risk management or outsourced risk management) involves the systematic process of managing and overseeing relationships with suppliers and service providers. This process includes selecting vendors, negotiating contracts, monitoring performance, and ensuring compliance with agreed-upon terms.

2.4.5.2.1 Apply the following key practices when providing vendors or suppliers with access to the ICS:

A. Vendors or suppliers should ideally only access the ICS physically while on site or through an organizationally approved remote access solution.

B. In cases where the vendor will not utilize the approved corporate remote access solution, any persistent third-party connections should be routed through a firewall or dedicated security device. Additionally, consider the following criteria:

1. Create dedicated network segments specifically for vendor access, limiting vendor access to only the OT devices they support.
2. Leverage physically controlling network access through network switch boxes.

C. Ensure that the organization's cybersecurity team has reviewed and approved all remote access solutions used by vendors.

D. Assess the cybersecurity posture of OT hardware and software vendors to safeguard organizational infrastructure. This assessment involves verifying compliance with industry standards, practicing proper change management, conducting risk assessments, monitoring performance, ensuring robust incident response planning, and encouraging continuous improvement in security practices.

This approach helps to mitigate risks associated with external access and protects critical infrastructure from potential cyber threats.

Vendors often establish persistent connections to monitor and maintain OT systems remotely. These connections allow them to perform diagnostics, updates and troubleshooting without the need to be physically present (e.g., predictive maintenance, supply chain integration and energy management services). Figure A.7 in Appendix C shows an example of a persistent vendor connection.

3.0 SUPPORT FOR RECOMMENDATIONS

3.1 Industrial Control Systems

3.1.1 OT Boundary Architecture

In today's industrial environments, connecting IT and OT is key to enabling real-time insights, predictive maintenance and better decision-making. But this integration also brings new cybersecurity and operational risks that must be managed with a well-designed OT boundary architecture.

Unlike traditional IT systems, OT systems focus on availability, safety and real-time performance. That's why the OT boundary architecture must be carefully built to protect operations, while allowing secure data sharing and visibility.

A strong OT boundary architecture should clearly separate enterprise and control networks leveraging zones (Network Segments) and conduits (secure communication paths), firewalls, iDMZs, and secure gateways. This layered setup helps prevent threats from spreading and supports a defense-in-depth approach.

To keep the architecture secure and resilient, asset owners should follow best practices such as using an iDMZ, limiting IT–OT communication, and managing OT credentials separately.

A well-structured OT boundary architecture not only improves cybersecurity but also ensures safe, efficient and reliable industrial operations.

3.1.1.1 Key Security Controls for OT Boundary Architecture

Table 3.1.1.1. Key Security Controls for OT Boundary Architecture

Control	*What It Does*	*Why It's Important*
Industrial Firewall	Creates a secure boundary between IT and OT networks.	Prevents unauthorized access and limits the spread of threats between IT and OT environments.
Industrial DMZ (iDMZ)	Manages and filters communication between IT systems (e.g., Remote Access, ERP, MES) and OT systems (e.g., Jump Server).	Enables a controlled data exchange and reduces the risk of direct exposure of OT systems to IT or external networks.
Separate OT Credentials	Requires OT credentials to be managed independently from IT credentials, ideally within the OT environment.	Reduces the risk of credential compromise spreading across domains and supports RBAC specific to OT needs.
Enforce Single Network Pathways	Ensures all OT communication flows through the Industrial Firewall at the OT network boundary or unidirectional devices; prohibits dual-homed devices and port forwarding.	Maintains network segmentation and prevents unauthorized cross-network communication, which could be exploited by attackers.
Restrict Internet Access for OT Devices	Prohibits OT users from accessing the internet (e.g., web browsing, email) from OT systems.	Minimizes exposure to internet-based threats such as phishing, malware and drive-by downloads that could compromise critical OT systems.

3.1.2 Remote Access

As ICS become more connected to company IT networks and remote support tools, remote access is now a helpful tool — but also a growing cybersecurity risk. Remote access makes it easier to conduct maintenance, fix problems and work with vendors; but it also creates new ways for attackers to reach OT systems.

To reduce these risks, asset owners or responsible staff need to create a clear cybersecurity plan when setting up and managing remote access. This plan should cover both internal users (like employees on the company network) and external users (like vendors or equipment suppliers). The plan must make sure all remote access is secure, monitored and follows industry best practices to keep ICS systems safe and running smoothly.

3.1.2.1 Key Security Controls for OT Remote Access

Table 3.1.2.1. Key Security Controls for OT Remote Access

Security Control	*What It Does*	*Why It's Important*
Jump Server in iDMZ	Acts as a secure gateway	Ensure the authenticity of remote sessions, and limit the attack surface
Multi-Factor Authentication (MFA)	Strengthens user access by verifying something a user has (e.g., token, code) or something a user is (e.g., biometrics)	Stops attackers even if they steal a password
Role-Based Access Control (RBAC)	Limits access based on job role	Prevents unnecessary access
Audit Logging	Records who did what and when	Helps detect and investigate issues
Access Control Lists (ACLs)	Defines who can connect	Blocks unauthorized devices
Network Segmentation	Separates systems into zones	Limits the spread of attacks
Restricted Outbound Access	Explicitly authorizes OT assets for the remote session	Reduces internal exposure/threats
Routine Patching & Whitelisting	Keeps systems secure and clean	Protects against known vulnerabilities and restricts unapproved software

3.1.3 System Security

In OT environments, system security is essential to ensuring the safety, reliability, and continuity of industrial operations. Unlike traditional IT systems, OT systems are designed to operate in real time, manage physical processes, and must meet strict availability and safety requirements. As a result, securing OT systems requires a nuanced approach that balances cybersecurity best practices with operational constraints.

OT system security involves safeguarding the hardware, software and firmware that control and monitor industrial processes, including PLCs and RTUs, engineering workstations, and HMIs.

To effectively secure these systems, asset owners or designated personnel should implement the best industry-recognized practices aimed at enhancing cyber resilience and reducing the risk exposure within the ICS environment. These practices include adopting a defense-in-depth strategy, maintaining secure configurations, and ensuring continuous monitoring and access control tailored to the unique demands of OT systems.

3.1.3.1 Key Security Controls for System Security

Table 3.1.3.1. Key Security Controls for System Security

Control Area	*What It Does*	*Why It's Important*
Account Security		
OT-Specific User Repositories	Separates OT and IT user repositories	Reduces the risk of lateral movement into OT in cyber attacks.
Unique User Credentials	Requires user-specific login and password for engineering workstations.	Prevents unauthorized access and ensures accountability.
Credential Review	Periodically reviews and updates user credentials.	Reduces risk from outdated or orphaned accounts, especially after personnel changes.
Default Credential Change	Replaces factory default usernames and passwords.	Prevents exploitation of known OT default credentials by attackers.
Password Policy	Enforces minimum password length and complexity.	Enhances resistance to brute-force and dictionary attacks.
Vendor Validation	Validates that the vendor can support security features (e.g., password complexity requirements).	Ensures compatibility and effectiveness of security controls.
Network Monitoring		
Continuous Monitoring	Detects anomalous activity and unauthorized changes in real time.	Enables rapid threat detection and response, reducing potential damage.
Device Detection	Identifies and logs new devices on the network.	Prevents rogue device connections and ensures proper configuration.
IT/OT Traffic Monitoring	Analyzes communication between IT and OT systems.	Detects lateral movement and unauthorized access attempts.
Attack Pattern Detection	Uses SIEM, IDS, EDR, etc., to identify threats.	Recognizes and mitigates malware, ransomware and other cyber threats.
Physical Parameter Monitoring	Tracks real-time process values like pressure and temperature.	Detects cyber-physical anomalies that could indicate sabotage or malfunction.
General System Security		
Wireless Encryption	Applies encryption (WPA2/WPA3, etc.) to wireless communications.	Protects data in transit from interception and tampering.
Portable OT Device Security	Disables wireless, updates patches, scans external storage.	Prevents malware introduction and unauthorized access via mobile devices.
Visitor Awareness	Informs contractors and visitors of security policies.	Reduces the risk of accidental or intentional breaches by third parties.
Malware Scanning Levels	Implements tiered scanning solutions for portable OT devices.	Ensures devices are clean before connecting to ICS, reducing infection risk.
Port & Feature Limiting	Disables unused USB/RJ45 ports and unnecessary services.	Minimizes attack surface and prevents unauthorized access.
Antivirus Deployment	Uses antivirus software where feasible in OT/ICS.	Detects and removes known malware threats.
Patch Management		
Patch Program Establishment	Covers all OT assets and validates patches with OEMs.	Ensures timely and compatible updates to fix vulnerabilities.
Vulnerability Monitoring	Tracks alerts from vendors and agencies.	Keeps systems protected against emerging threats.
Risk-Based Response	Determines protective actions based on system criticality.	Prioritizes resources and responses to safeguard essential operations.
Vendor Consultation	Coordinates patching with ICS vendors and tests in simulation.	Prevents system instability and ensures safe deployment.
Legacy System Protection	Applies compensating controls for unsupported systems.	Maintains security, even when patching is not possible.

3.1.4 OT Incident Response & Safety Systems

In OT environments, effective incident response and the deployment of safety devices are critical to protecting human life, maintaining operational continuity, and minimizing the impact of cyber-physical threats.

Incident response in OT involves a structured approach to detecting, analyzing, and responding to security events that may affect ICS. This includes not only cyber incidents but also physical malfunctions and safety breaches. Given the unique characteristics of each OT operation, response plans must be tailored to the specific processes, equipment and safety requirements of the environment.

Safety devices, such as emergency shutdown systems and SIS play a vital role in mitigating the consequences of incidents. These systems are designed to operate independently of standard control systems, ensuring that critical safety functions are preserved even during a cyber attack or system failure.

3.1.4.1 Key Security Controls for OT Incident Response & Safety Systems

Table 3.1.4.1. Key Security Controls for OT Incident Response & Safety Systems

Security Control	*What It Does*	*Why It's Important*
Incident Response		
OT Incident Response Plans (OT IRP)	Documents the organization's approach to detecting, responding to and recovering from cybersecurity incidents.	Supports a swift, coordinated and effective response to cybersecurity incidents, minimizing damage and restoring operations quickly.
Audit Logging	Records who did what and when.	Helps detect and investigate issues
Continuous Monitoring	Detects anomalous activity and unauthorized changes in real time.	Enables rapid threat detection and response, reducing potential damage.
Attack Pattern Detection	Uses SIEM, IDS, EDR, etc., to identify threats.	Recognizes and mitigates malware, ransomware and other cyber threats.
CS Tabletop Exercises	Simulates cyber incidents in ICS environments to test IRPs and improve response strategies.	Helps identify gaps in preparedness, and enhances coordination among teams before a real-world attack occurs.
Training		
Cybersecurity training focusing on ICS/OT risks	Educates employees on recognizing and responding to cyber threats in ICS/OT environments and following security best practices.	Reduces human error risks by fostering a security-aware culture.
Internal Policies	Establishes rules and guidelines for secure behavior, system use and data handling within an organization.	Clear policies enforce consistency, accountability and compliance with organizational cybersecurity requirements.
Backup		
Offline Backups	Stores copies of data in a disconnected environment, isolated from the main network.	Protects data from ransomware and other threats that target online systems, supporting the efficient restoration of operations.
Immutable Backups	Creates copies of data that cannot be altered or deleted once written.	Guarantees data integrity and availability even if attackers gain access to backup systems.
Backup Testing	Verifies that backup systems can successfully restore data and systems as intended.	Ensures data recovery processes are reliable and effective in the event of data loss or cyber incidents.
Redundant Systems	Provides duplicate hardware or software components to maintain operations if the primary system fails.	Enhances system availability and resilience by minimizing downtime during failures or attacks.
Safety Systems		
Physical Parameter Monitoring	Tracks real-time process values like pressure and temperature.	Detects cyber-physical anomalies that could indicate sabotage or malfunction.
Segregation of Safety Systems	Isolates safety-critical systems from non-safety systems to prevent interference or compromise.	Protects essential safety functions from cyber threats and operational errors, preserving human and environmental safety.
Run Mode in PLCs	Restricts control system changes by operating in a mode that prevents unauthorized modifications.	Reduces the risk of accidental or malicious changes to critical system configurations during normal operations.
Physical Key Switch on SIS	Requires a physical key to change the operational mode of SIS, adding a manual layer of control.	Prevents unauthorized or accidental changes to safety-critical settings, enhancing operational integrity.
Digital Password on SIS	Uses password authentication to control access to SIS configuration and control functions.	Adds a layer of cybersecurity to prevent unauthorized digital access to safety systems.

3.1.5 Governance and Third-Party Risk Management

In OT environments, strong governance and effective Third-Party Risk Management (TPRM) are foundational to maintaining secure, resilient and compliant industrial operations. As OT systems become increasingly interconnected with external vendors, service providers and cloud platforms, the risk landscape expands, making governance and oversight more critical than ever.

By integrating governance and TPRM into the broader OT security strategy, organizations can better safeguard critical infrastructure, ensure regulatory compliance and build trust across the supply chain.

3.1.5.1 Key Security Controls for Governance and Third-Party Risk Management

Table 3.1.5.1. Key Security Controls for Governance and Third-Party Risk Management

Control Area	*What It Does*	*Why It's Important*
Governance		
Roles and Responsibilities Definition	Establishes clear accountability by assigning specific cybersecurity duties across teams and individuals at the corporate and local facility levels.	Prevents gaps or overlaps in security coverage and ensures coordinated response to threats.
Internal Policies	Establishes rules and guidelines for secure behavior, system use and data handling within an organization.	Clear policies enforce consistency, accountability, and compliance with organizational cybersecurity requirements.
Asset Inventory	Maintains a comprehensive list of all OT assets, including hardware, software and communication links.	Enables effective risk management, patching and incident response by knowing what needs protection.
Third-Party Risk Management		
Review of Vendor Remote Access Solutions	Evaluates and validates the security of remote access methods used by third-party vendors.	Ensures external connections do not introduce vulnerabilities or bypass internal security controls.
Third-Party/Vendor Assurance Program	Assesses and monitors the cybersecurity posture of vendors and service providers.	Mitigates supply chain risks by ensuring partners meet security requirements and do not compromise OT environments.

3.2 Illustrative Losses

3.2.1 German Steel Mill

Cybersecurity Analysis of the 2014 German Steel Mill Cyber Attack

In 2014, a major cyber attack targeted a German steel mill, resulting in significant physical damage. It was one of the first publicly-known incidents where a cyber intrusion caused real-world industrial harm. The attack was detailed in a report by Germany's Federal Office for Information Security (BSI), highlighting the growing convergence of cyber threats and OT vulnerabilities.

Attack Vector and Capabilities

The attackers reportedly gained access to the steel mill's corporate IT network through a spear phishing campaign, which allowed them to pivot into the plant's production network. Once inside the OT environment, they manipulated control systems responsible for managing industrial processes.

Key capabilities and tactics included:

- Compromising administrative systems to escalate privileges and move laterally
- Disrupting control components within the production network
- Preventing proper shutdown of a blast furnace, leading to mechanical damage
- The attackers demonstrated a high level of technical knowledge about both IT and OT systems, suggesting a well-resourced and highly skilled threat actor.

Incident Outcome and System Impact

The most severe consequence of the attack was the inability to shut down a blast furnace in a controlled manner, which led to extensive physical damage to the facility. While specific technical details were not disclosed, the incident marked a turning point in the understanding of how cyber attacks can directly impact industrial safety and reliability.

Vulnerabilities and Contributing Factors

The attack exploited several systemic weaknesses:

- Lack of network segmentation between IT and OT environments
- Insufficient monitoring and detection of lateral movement within the network
- Inadequate access controls and user awareness, enabling phishing success
- Legacy systems with limited cybersecurity protections

Broader Implications for Industrial Cybersecurity

This incident was a wake-up call for critical infrastructure operators worldwide. It demonstrated that cyber attacks can cause physical destruction, not just data loss or downtime. The German steel mill attack underscored the importance of integrating cybersecurity into industrial risk management.

This attack highlights the need for:

- Robust network segmentation between corporate IT and industrial OT systems
- Advanced threat detection and monitoring across both environments
- Employee training to recognize and respond to phishing and social engineering
- Strict access controls and MFA for critical systems
- Regular security assessments of legacy control systems and protocols
- Incident response planning that includes both cyber and physical contingencies

3.2.2 Ukraine Power Grid

Crash Override Malware: Ukraine Power Grid Cyber Attack (December 2015)

On 23 December 2015, Ukraine experienced one of the most significant cyber attacks on ICS to date. The attack caused widespread power outages, affecting approximately 225,000 customers across three regional electric power distribution companies. While power was eventually restored, the affected companies were forced to operate under constrained conditions during the recovery process.

Coordinated and Sophisticated Intrusion

The cyber attack was highly coordinated and synchronized, reportedly involving as much as six months of reconnaissance. The intrusions at each company occurred within a 30-minute window, targeting multiple facilities simultaneously. Attackers remotely operated circuit breakers without authorization, using either existing remote administration tools at the operating system level or ICS client software accessed via VPN connections.

Crucially, the attackers had obtained legitimate user credentials in advance, enabling them to bypass many security controls and gain direct access to critical systems.

Malware Deployment and System Sabotage

At the conclusion of the attack, the adversaries deployed KillDisk malware, which:

- Erased selected files and corrupted the Master Boot Record (MBR), rendering systems unbootable
- Overwrote Windows-based HMIs embedded in RTUs
- Corrupted firmware in Serial-to-Ethernet devices at substations, disabling communication
- Disconnected Uninterruptible Power Supplies (UPS) via remote management interfaces, complicating restoration efforts

- Significantly delayed recovery and increased the operational impact of the attack

Initial Access via BlackEnergy Malware

All three companies reported prior infections with BlackEnergy malware, believed to have been delivered through spear phishing emails containing malicious attachments. Whether BlackEnergy directly facilitated the attack remains unclear; it may have been used to harvest credentials. However, any remote access Trojan (RAT) could have served this purpose.

Operational Impact and Recovery

Due to the sabotage of remote-control systems, the companies were unable to remotely reset circuit breakers. Field personnel had to be dispatched to perform manual switching, resulting in power outages lasting between four and six hours. Importantly, no damage was reported to power generation facilities.

This incident underscores the urgent need for:

- Enhanced ICS Security Posture: Strengthening the cybersecurity of ICS, including segmentation from corporate networks, and minimizing remote access points
- Credential Management and Monitoring: Implementing robust identity and access management (IAM) practices, including MFA and continuous monitoring for credential misuse
- Advanced Threat Detection: Deploying intrusion detection systems (IDS) and behavioral analytics tailored to ICS environments to detect anomalies early
- Incident Response Preparedness: Developing and regularly testing incident response and recovery plans specific to OT environments
- Employee Awareness and Training: Educating staff on phishing and social engineering tactics to reduce the risk of initial compromise
- Firmware and Device Hardening: Ensuring that embedded devices and firmware are secure, monitored, and capable of being restored quickly in the event of compromise.

For further guidance on enhancing cybersecurity resilience in ICS environments, please refer to Section 2.4, Human Factor.

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 4-9, *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

EU Cybersecurity Act: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, repealing Regulation (EU) No 526/2013. - Establishes a European cybersecurity certification framework and strengthens ENISA's mandate. Regulation - 2019/881 - EN - EUR-Lex

NIS2 Directive: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148. - Enhances cybersecurity across essential and important entities in the EU, replacing the original NIS Directive. EUR-Lex – Directive (EU) 2022/2555

EU Cyber Resilience Act: Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements, amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828. - Introduces mandatory cybersecurity requirements for hardware and software products with digital elements, promoting secure-by-design principles. EUR-Lex – Regulation (EU) 2024/2847

KRITIS Regulation (BSI-Kritisverordnung) or Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) – German regulation that defines critical infrastructure sectors and sets thresholds for mandatory cybersecurity measures under the BSI Act. https://www.gesetze-im-internet.de/bsi-kritisv/

Australian Cyber Security Centre (ACSC). *Protecting industrial control systems*. https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure/protecting-industrial-control-systems

Canadian Centre for Cyber Security. *Security considerations for industrial control systems* (ITSAP.00.050). https://www.cyber.gc.ca/en/guidance/security-considerations-industrial-control-systems-itsap00050

Canadian Centre for Cyber Security. *Security considerations for critical infrastructure* (ITSAP.10.100). https://www.cyber.gc.ca/en/guidance/security-considerations-critical-infrastructure-itsap10100

Cybersecurity & Infrastructure Security Agency (CISA). *Industrial Control Systems*. https://www.cisa.gov/topics/industrial-control-systems

Cybersecurity & Infrastructure Security Agency (CISA). *Primary Mitigations to Reduce Cyber Threats to Operational Technology*. https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology

Electric Power Research Institute (EPRI), *Generation Cyber Security*. International Society for Automation (ISA). ISA/IEC 62443 standards and technical reports series.

The MITRE Corporation, *ATTA&CK ICS Techniques*. https://attack.mitre.org/techniques/ics/.

National Institute of Standards and Technology (NIST). *Security and Privacy Controls for Information Systems and Organizations*. NIST SP 800-53, Revision 5.

National Institute of Standards and Technology (NIST). *Guide to Industrial Control Systems (ICS) Security*. NIST SP 800-82, Revision 3.

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

SANS Institute. ICS Cybersecurity Field Manual Series. https://www.sans.org/mlp/ics-field-manual

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

E-Cyber Strategy - Brazil's national cybersecurity strategy, established by Decree No. 10.222/2020, focused on protection of critical infrastructure and promotion of cyber resilience and risk management. https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber

Cybersecurity Framework Law (2024) – Chile's national cybersecurity agency (ANCI), focused on protection of critical infrastructure and coordination across defense for public and private sectors.

Second National Cybersecurity Strategy (2023). Argentina - Focused on Digital sovereignty and protection of critical infrastructure.

APPENDIX A GLOSSARY OF TERMS

Term	Definition	Related Terms
Access control	The ability and means to communicate with or otherwise interact with a system 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).	**Access Control List (ALC), Role-Based Access Control (RBAC)**
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	Any component (hardware, software, data, or network resource) that has value to an organization and plays a role in delivering services within the IT or OT environment. Assets need to be tracked, managed and protected.	
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 process of confirming that someone or something is who or what they claim to be. It usually follows identification (e.g., entering a username) and involves verifying that identity using a method such as a password, security token or biometric data. For example, entering a password to access a system is a basic form of authentication.	
Baseline	A specification or product that has been formally reviewed and agreed upon, thereafter serving as the basis for further development, and that can be changed only through formal change control procedures.	**Configuration Management, Hardening**
Cloud-Based Zero Trust	Cloud-Based Zero Trust is an implementation of the Zero Trust security model designed specifically for cloud environments. It enforces strict identity verification, continuous monitoring and least-privilege access across cloud services, applications and workloads, regardless of user location or device.	
Control network	Time-critical network, 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 Control, Authentication**
Data diode/ unidirectional gateways	A data diode is a hardware-based cybersecurity device that enforces one-way data flow between two networks. It allows data to travel in only one direction (typically from a secure internal network to a less secure external network) while physically preventing any return traffic.	**One-way communication**
Defense in depth	The practice of layering multiple overlapping security controls to secure IT or OT environments.	
Distributed control system (DCS)	A DCS is an automated 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.	
Dual-homed device	A networked device that has two separate network interfaces, allowing it to connect to two different networks simultaneously. This configuration is often used to enhance redundancy or performance by isolating traffic between networks or providing alternative communication paths. Common examples of dual-homed devices include printers and historians/servers, which may connect to both IT and OT networks.	
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 plain text into ciphertext conceals the data's original meaning to prevent it from being known or used.	

Term	Definition	Related Terms
Endpoint Detection and Response (EDR)	Endpoint Detection and Response (EDR) is a cybersecurity technology focused on continuously monitoring and analyzing endpoint activities to detect, investigate and respond to threats in real time. It provides visibility into endpoint behavior, uses advanced analytics to identify suspicious patterns, and enables rapid containment and remediation of security incidents.	**Threat Detection and Incident Response**
Engineering workstation	The engineering workstation is usually a reliable, high-performance computing platform designed for configuration, maintenance and diagnostics of control system applications and other control system equipment. It typically contains the vendor-specific software and the project files needed to program devices, including PLCs and HMIs.	**Operator Workstation**
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.	**Manufacturing execution system (MES)**
Factory-default usernames and passwords	The standard username and password provided on a system when first delivered or installed. Users should always immediately change the factory-default password.	**Access control, Authentication, Credentials**
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**
Gateway	A gateway is a network device or software that acts as a bridge between different systems, networks or protocols, enabling communication and data exchange. It often connects internal to external networks or networks of different criticality.	**Firewall**
Hardening	A security measure that includes removing or disabling unnecessary features, functions, ports and services, and applying cybersecurity controls to prevent unauthorized use. Two types of hardening include: A. Physical hardening: Disabling through physical means; removing unneeded communication ports, blocking access to the ports and drives, etc. B. Logical hardening: Disabling unused network and communication protocols, drivers for unused peripherals, web servers, etc., and applying cybersecurity 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 whitelisting 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)	A. 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. B. Software and hardware that allows authorized users to monitor and control processes and/or equipment, such as status or historic trend display, control setting modifications, and manual override in the event of emergency.	
ICS Oversight Team	The group responsible for managing and protecting Industrial Control Systems (ICS). They make sure these systems are secure, working properly and follow company policies. Their tasks include checking for risks, ensuring compliance, and helping respond to any problems or incidents.	
Immutable backup files	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.	**Write-once-read-many (WORM) storage**

Term	Definition	Related Terms
Industrial Control System (ICS)	An ICS is a broad term encompassing various types of control systems used to monitor and manage industrial processes, such as manufacturing, power generation and water treatment. These systems include hardware and software components like SCADA systems, PLCs and DCSs, which work together to ensure safe, efficient and automated operation of critical infrastructure.	**Basic process control system (BPCS), Operational technology network (OT)**
Industrial Demilitarized Zone (iDMZ)	An iDMZ is a secure buffer zone that protects internal networks from external threats. It sits between trusted and untrusted environments, often separating IT systems from OT systems. A. Firewall Interface: Implemented as a dedicated firewall interface, filtering traffic and applying security policies. B. Neutral Network Segment: Acts as a middle layer between private networks and external networks (like the internet). C. Perimeter Security Layer: Enforces rules for external data exchange, limiting access to sensitive systems while allowing controlled communication.	
Industrial firewall	An industrial firewall is a specialized network security device designed to safeguard industrial control systems (ICS) and operational technology (OT) environments. It enables secure and reliable data exchange within critical infrastructure. It should be located at the OT network boundary.	**IT-OT Separation**
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	The quality of a system, reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that provide the protection mechanisms, and the consistency of the data structures and stored data.	
Intrusion detection system (IDS)	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.	
Jump server	An ICS jump server (also called a jump host, jump box or bastion server) is a secure, intermediary system used to centralize, control and monitor remote access to Industrial Control Systems (ICS) or Operational Technology (OT) environments. It acts as a gateway between external networks, including the corporate IT network and third-party users (e.g., vendors and contractors).	**Remote access servers**
Local area network (LAN)	Communications network designed to connect computers and other intelligent devices in a limited geographic area (typically less than 10 kilometers).	**Wide Area Network (WAN)**
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 for transformation of raw materials to finished goods).	**Enterprise Resource Planning (ERP) system**
Managed Detection and Response (MDR)	A managed service, providing 24/7 threat monitoring, detection and response by security experts.	**Threat detection and Incident Response**

Term	Definition	Related Terms
Multi-Factor Authentication (MFA)	MFA adds an extra layer of security by requiring users to provide two or more types of verification before gaining access. These factors include: A. Something you know (e.g., a password) B. Something you have (e.g., a phone or security token) C. Something you are (e.g., a fingerprint or face scan)	**Authentication**
Non-networked accounts	Non-networked or local accounts only work on an individual machine or workstation. They do not rely on a central user repository (such as Active Directory) for authentication.	**Local Accounts**
One-way communication	Strategies used to ensure secure one-way communications from devices or across different networks/protection zones include: A. Sending only an analog signal (an amperage or voltage) to/from a device instead of digital data B. Use of a one-way data-diode/ unidirectional gateway C. Use of rules in a firewall or a iDMZ to pass data across networks	**Data diode/ unidirectional gateways**
Operating system (OS)	The underlying software that enables interaction with a computer. The operating system controls computer storage, communications and task management functions.	
Operational technology network (OT)	Systems and infrastructure that manage industrial operations, including ICS and Process Control Networks (PCNs), distinct from business IT networks.	**Basic process control system (BPCS), Industrial Control System (ICS)**
Operator workstation	An operator workstation provides a dynamic view of plant processes needed to operate control systems. It presents control graphics, diagnostics, trends, alarms and status displays.	
Operational technology network (OT)	Systems and infrastructure that manage industrial operations, including ICS and Process Control Networks (PCNs), distinct from business IT networks.	**Basic process control system (BPCS), Industrial Control System (ICS)**
Operator workstation	An operator workstation provides a dynamic view of plant processes needed to operate control systems. It presents control graphics, diagnostics, trends, alarms and status displays.	
Original Equipment Manufacturer (OEM)	An Original Equipment Manufacturer (OEM) is a company that produces parts or equipment used in another company's product.	**Vendor, Supplier**
OT devices	OT devices are units designed to support the ICS by providing specific functionality. Types of OT devices include remote terminal units (RTUs), programmable logic controllers (PLCs), actuators, sensors and associated communications.	**Field device, Programmable logic controller (PLC), Remote Terminal Unit (RTU), Sensor**
OT WAN	Operational Technology Wide Area Network is a network infrastructure that connects industrial control systems and devices across multiple sites or geographic locations, enabling secure communication and management of OT environments. In addition to physical site-to-site connectivity, an OT WAN can include cloud-based services that facilitate remote monitoring, data exchange and centralized management of operational technology systems.	

Term	Definition	Related Terms
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 govern how certain procedures are handled.	
Portable OT device/ Transient device	Portable OT devices are portable devices that can be connected to the ICS. They include laptops, tablets, mobile phones and external storage devices. These devices may be capable of connecting to both the IT and OT networks.	**Laptops, tablets, mobile phones, external storage devices**
Procedure	Steps taken to perform a certain task.	
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 equipment functions. 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.	**Control center, Operator workstation, Process control center**
Programmable logic controller (PLC)	PLCs are automation controllers with the capability of controlling complex processes. 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 set of rules that enables devices to exchange and interpret data. ICS protocols are often vendor-specific, prioritize functionality over security, and usually transmit unencrypted, making OT/IT separation important. Examples include Modbus RTU/ TCP, Profibus, Profinet, DNP3, and ControlNet. Common IT protocols include FTP, DNS, HTTP and HTTPS.	
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	Allows users or systems to connect to an internal network from outside its security perimeter with the same privileges as on-site users or systems. Common tools include modems (signal conversion), routers (data routing), and remote access servers (“jump” hosts for managing external connections).	
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 (RBAC)	A form of identity-based access control where system entities that are identified and controlled are functional positions in an organization or process.	**Access control**
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 instrumented systems (SIS)	Systems used to implement one or more safety-instrumented functions. They are composed of any combination of sensors, logic solvers and actuators.	**Safety system, Safety network**
Safety network	A network that connects SIS for the communication of safety-related information.	
Security information and event management (SIEM)	An application that provides the ability to gather security data from information system components. It normalizes audit trails and logs tests against a set of correlation rules. When triggered, these rules create events for analysis and present that data as actionable information via a single interface.	

Term	Definition	Related Terms
Security operations center (SOC)	Solution that encompasses the people, processes and technology, including SIEM, 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 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.	**Separation**
Segregation	Disconnecting a network from other networks completely (air-gapped). SIS at large facilities are segregated, because they are not controlled by the ICS network handling the basic process control system (BPCS).	
Separation	Proper partitioning of different networks that are considered untrusted to each other. Separation is usually achieved using firewalls (and ideally a formal iDMZ) or unidirectional gateway. Separation from IT is key for ICS networks.	**Segmentation**
Supervisory control and data acquisition (SCADA)	Supervisory Control and Data Acquisition (SCADA) systems are centralized systems used to monitor and control industrial processes across large geographic areas.	
Third-Party Risk Management (TPRM)	Third-party risk management (TPRM) focuses on identifying, assessing and mitigating risks introduced by external entities that interact with OT systems. These entities may include equipment suppliers, maintenance contractors, software vendors and managed service providers. Each third party represents a potential entry point for cyber threats or operational disruptions.	**Contractor, Supplier risk management, Outsourced risk management, Vendor risk management**
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.	**Attacker**
Threat-based approach	A method used in risk management, cybersecurity, defense and related fields that focuses on identifying, analyzing and mitigating specific threats to an organization, system or asset. Rather than starting with vulnerabilities or general risks, this approach begins by understanding the intentions, capabilities and actions of potential adversaries or hazards.	
User repository	A system that stores information about users/members for a particular domain, using a centralized approach to ensure authentication and authorization. Microsoft Active Directory is a common example of a user repository commonly seen in IT and OT networks.	**Active Directory**
Virtual Local Area Network (VLAN)	A grouping of devices on a network that can communicate as if they were on the same physical connection, even if they are not. A VLAN creates separate, isolated sections within a wider network, helping to improve security, reduce congestion and simplify network management.	**Local Access Network (LAN), Segmentation**
Virtual private network (VPN)	A secure connection between a public network (usually the internet) and a private network.	
Virtual server	A software-based version of a physical server that shares hardware resources, while acting like an independent server.	
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.	
Whitelist	A list of discrete entities, such as hosts or applications, which 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 computer as part of its hardening.**

Term	Definition	Related Terms
Wide Area Network (WAN)	A network that connects smaller networks across large regions, countries or globally, using various technologies. Common wired options include MPLS, T1 lines and virtual circuits, while wireless options include 4G, 5G, Wi-Fi and satellite.	**Local Area Network (LAN)**
XDR (Extended Detection and Response)	A platform that unifies threat detection and response across multiple security layers like endpoints, network and cloud.	**Threat detection and Incident response**
Zero Trust	A security model that assumes no user or device is inherently trusted. It requires continuous verification of identity, device health and context for every access request, applying least privilege and strict access controls.	

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).

June 2026. This data sheet was completely reorganized with minor editorial changes.

August 2025. Significant changes have been made, shifting the strategy from a system-based to a threat-based approach. Leveraging our cyber and engineering expertise, the updated guidance prioritizes the most critical elements driving cyber-related losses and business interruption.

July 2025. Interim revision. Editorial changes were made.

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.

APPENDIX C DIAGRAMS

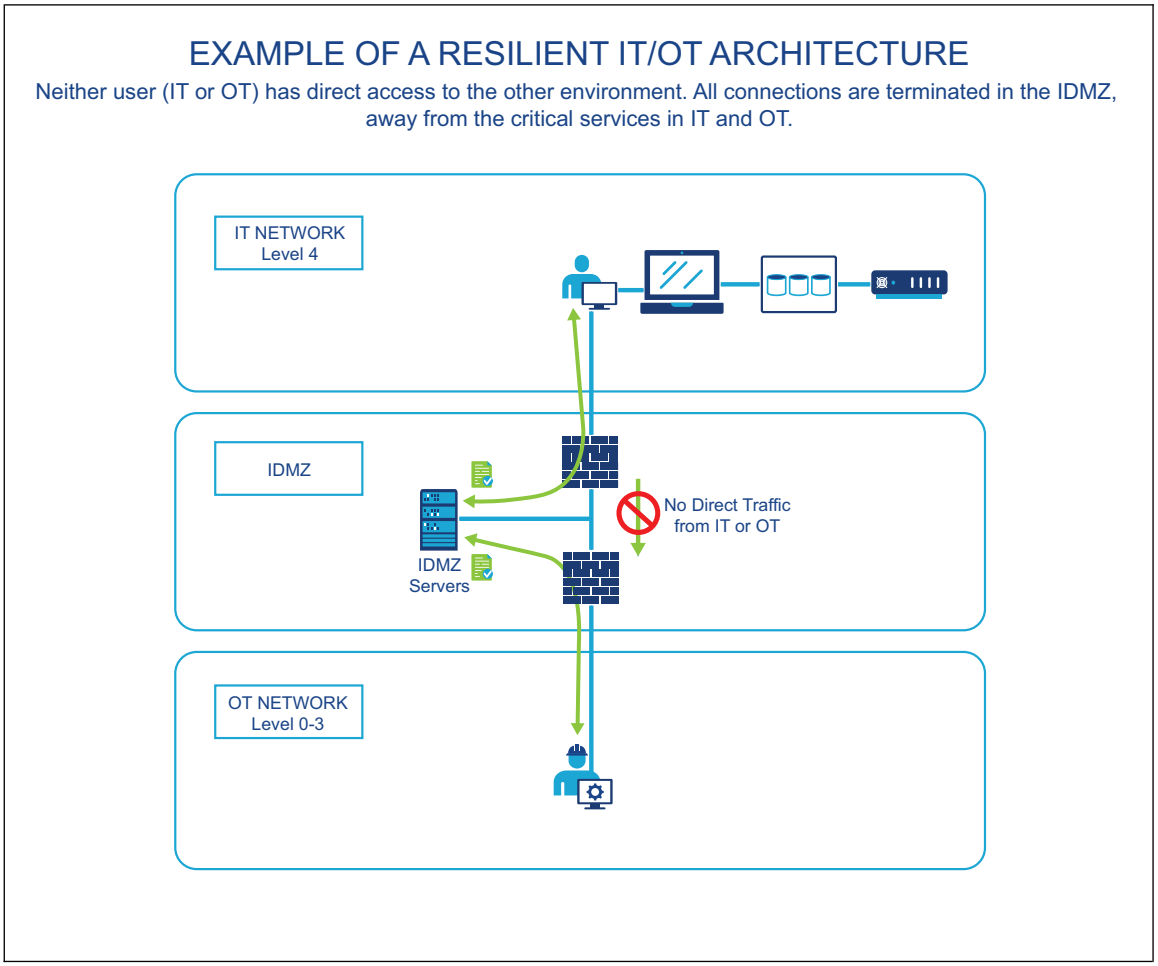

Fig. C.1. Example of a resilient IT/OT architecture

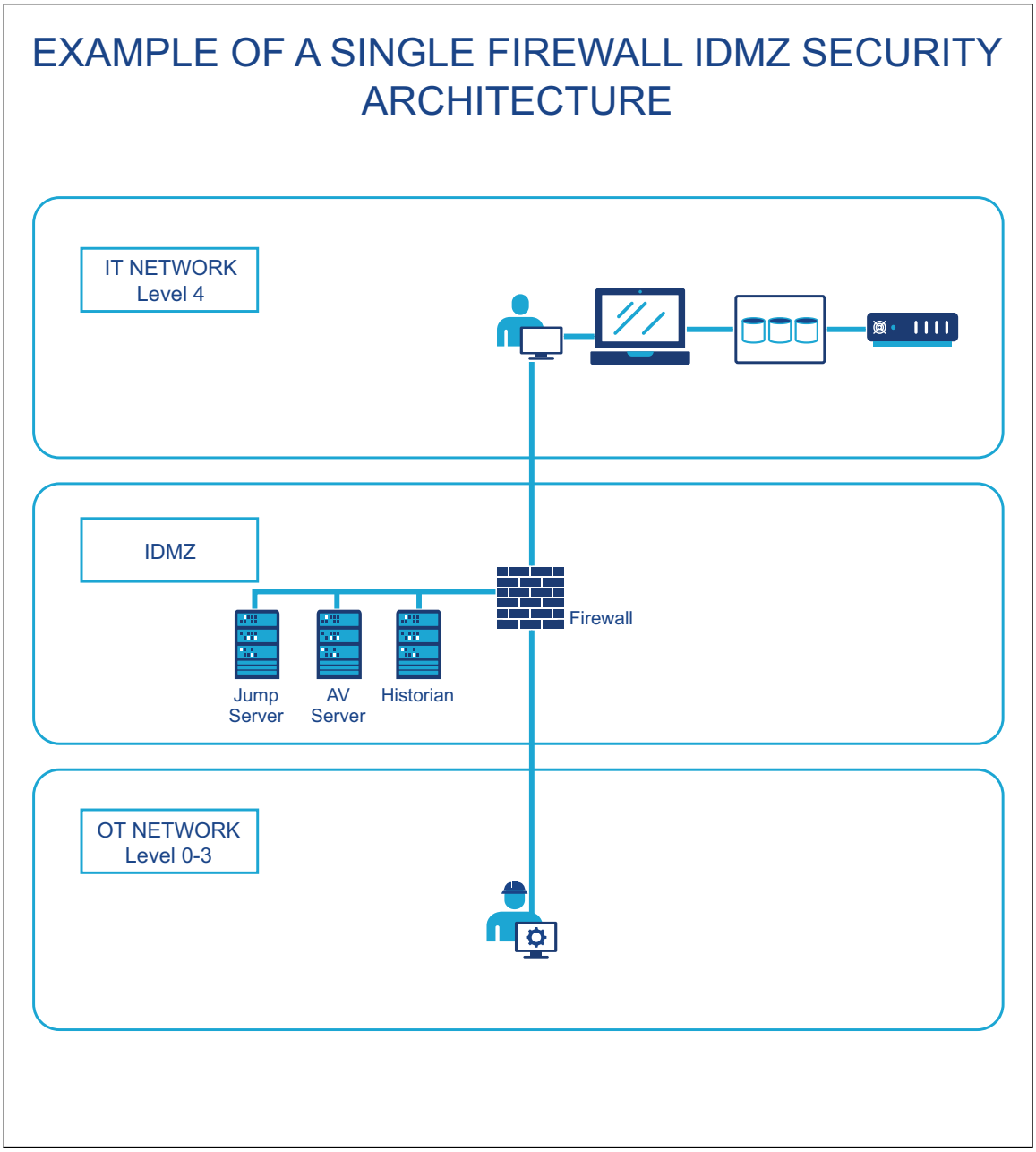

Fig. C.2. Example of a single firewall with iDMZ

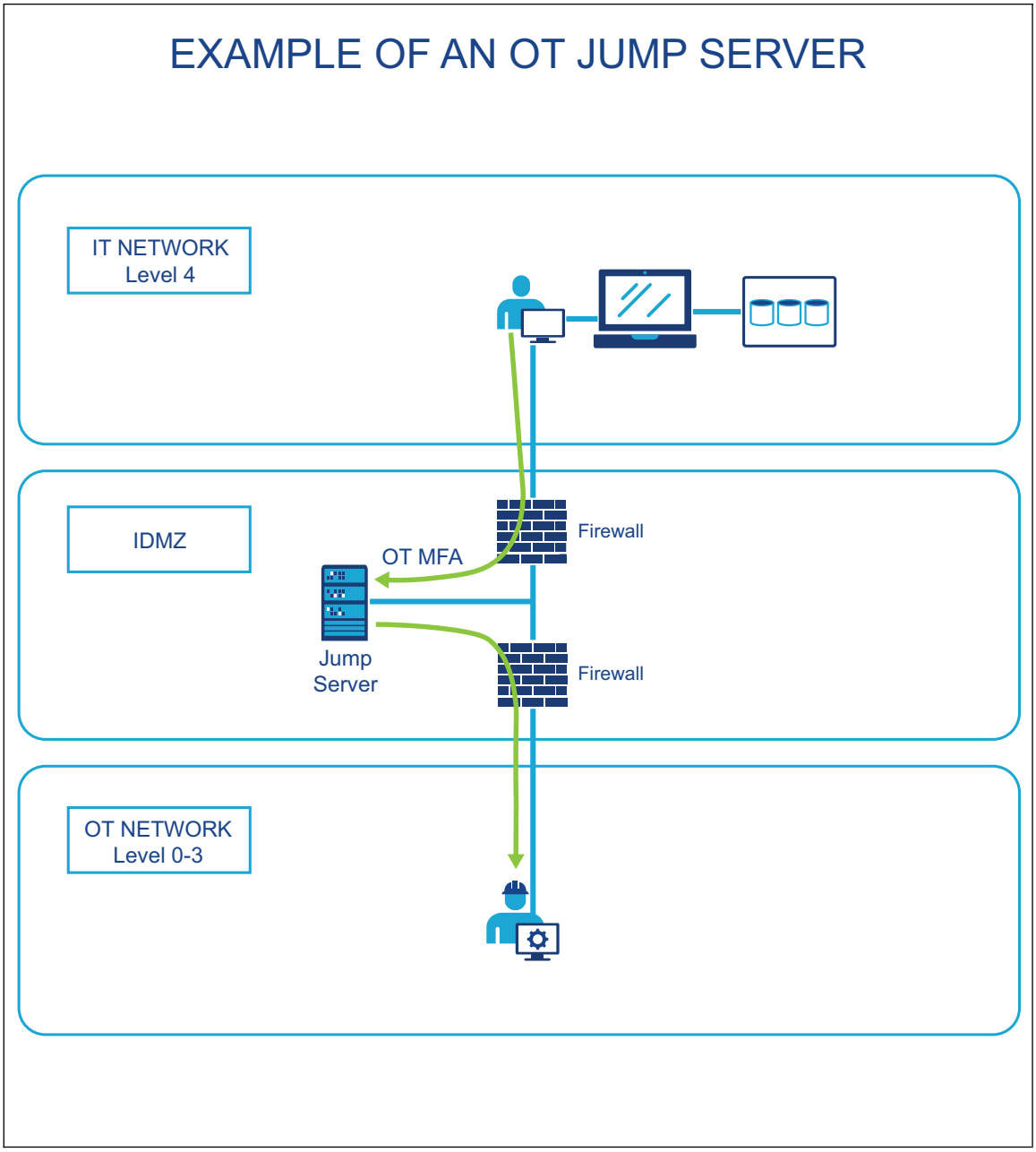

Fig. C.3. Example of an OT jump server

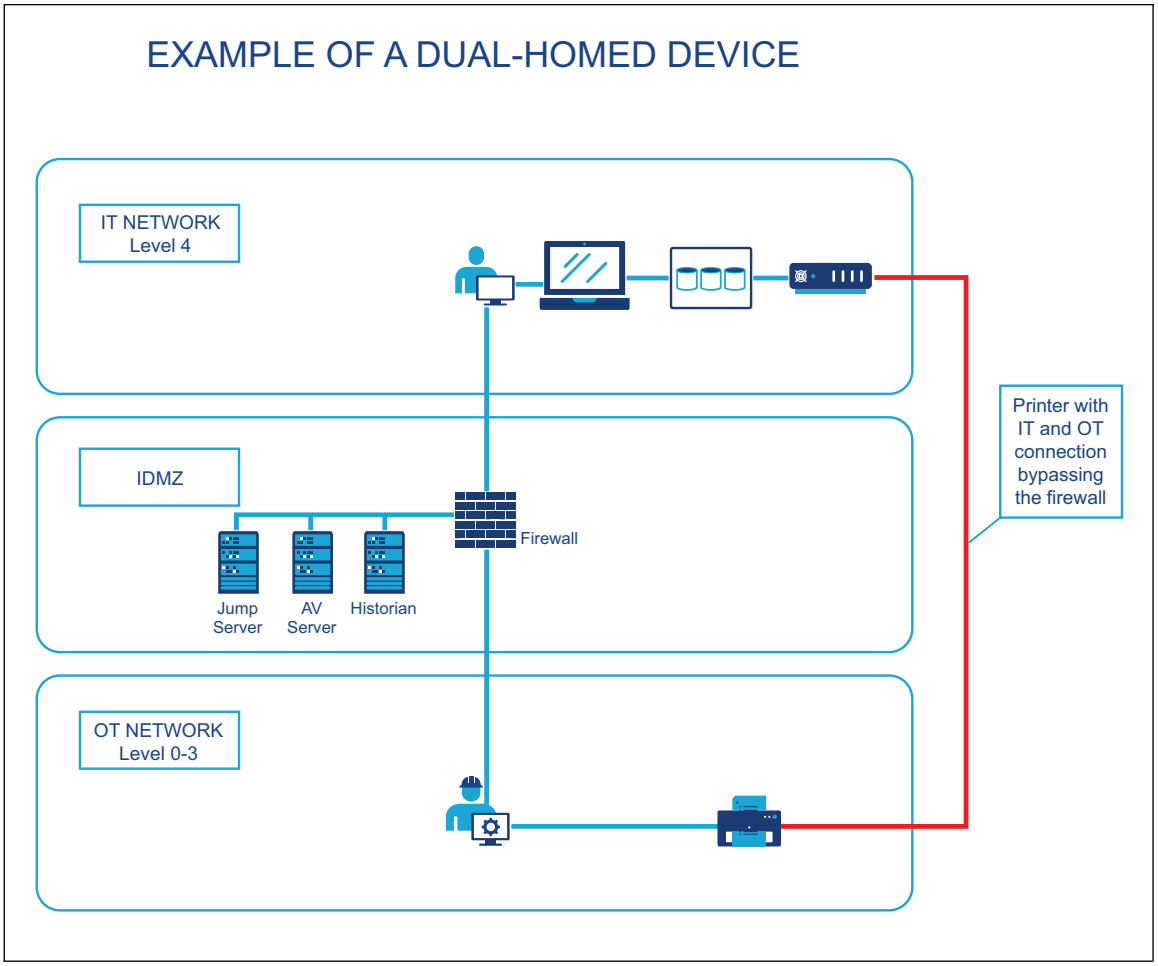

Fig. C.4. Example of a dual-homed device

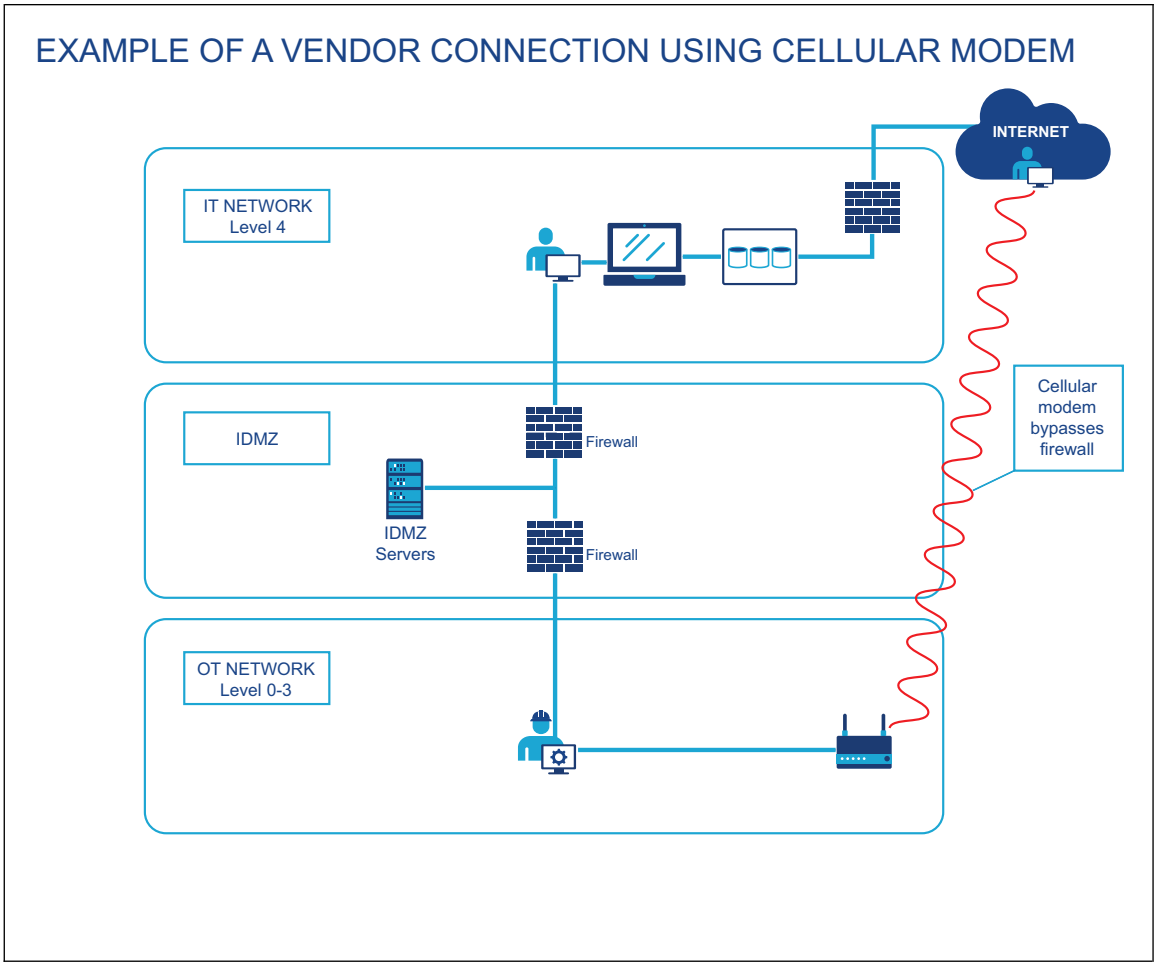

Fig. C.5. Example of a vendor connection using cellular modem

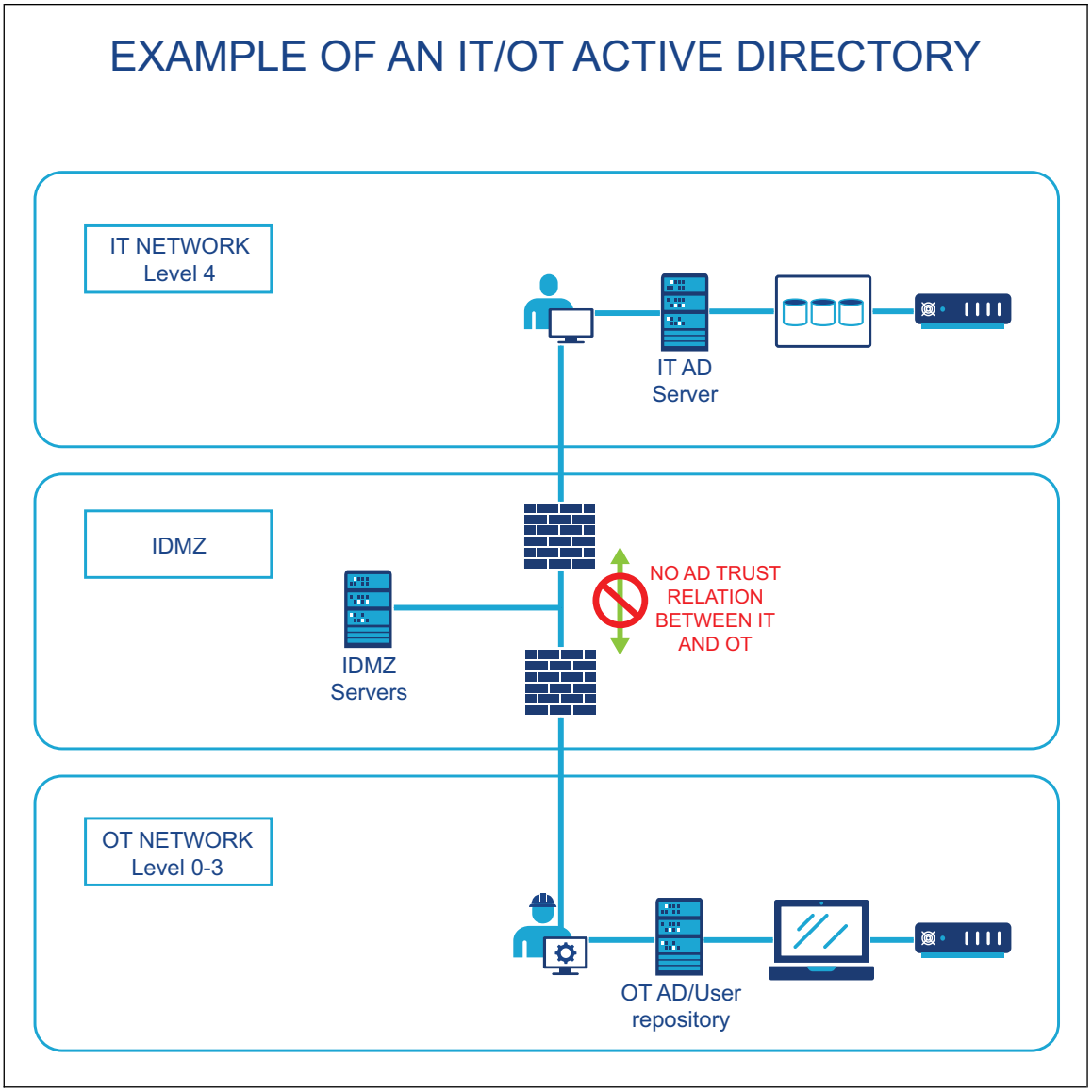

Fig. C.6. Example of an IT/OT active directory

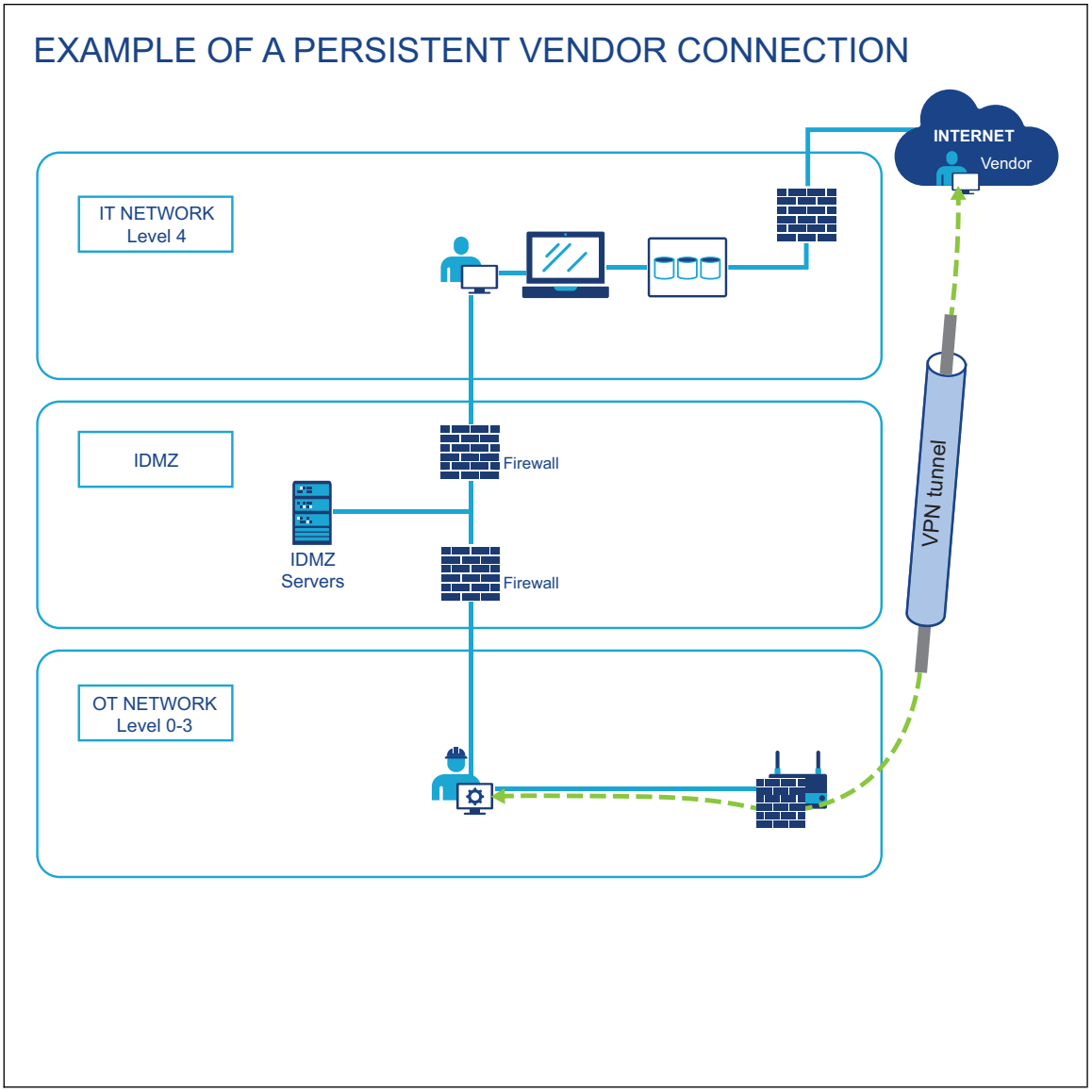

Fig. C.7. Example of a persistent vendor connection

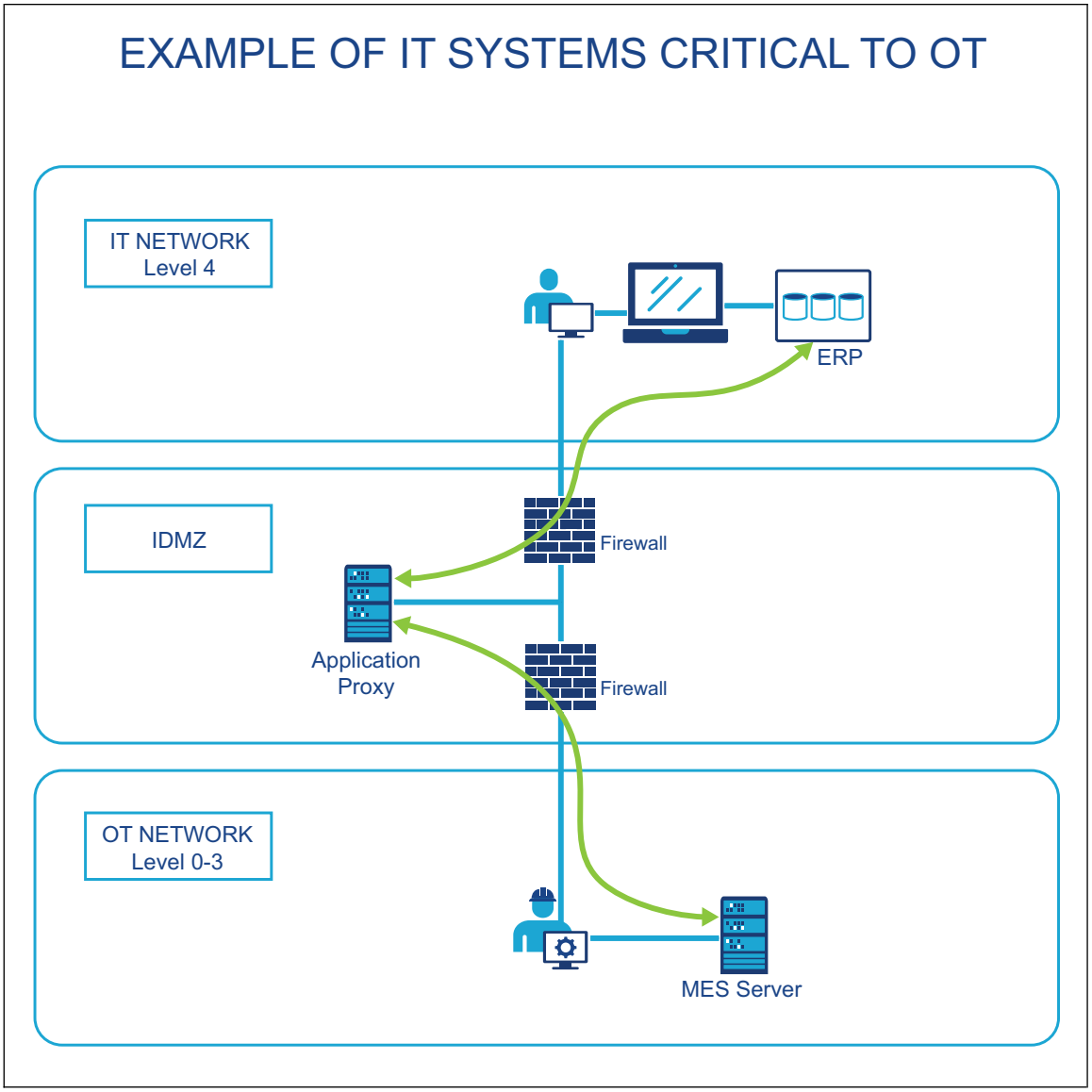

Fig. C.8. Example of IT systems critical to OT

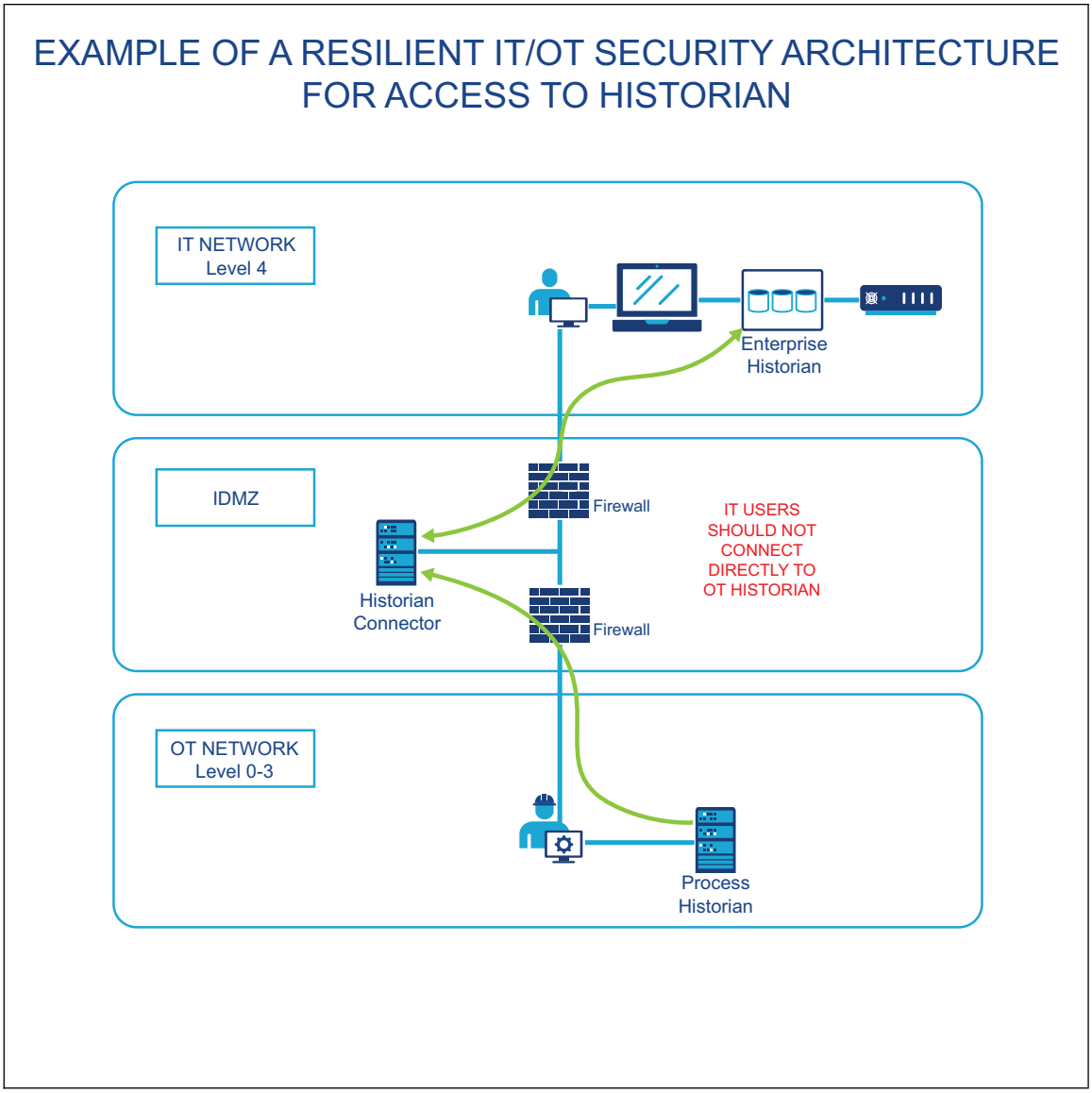

Fig. C.9. Example of a resilient architecture for access to historian

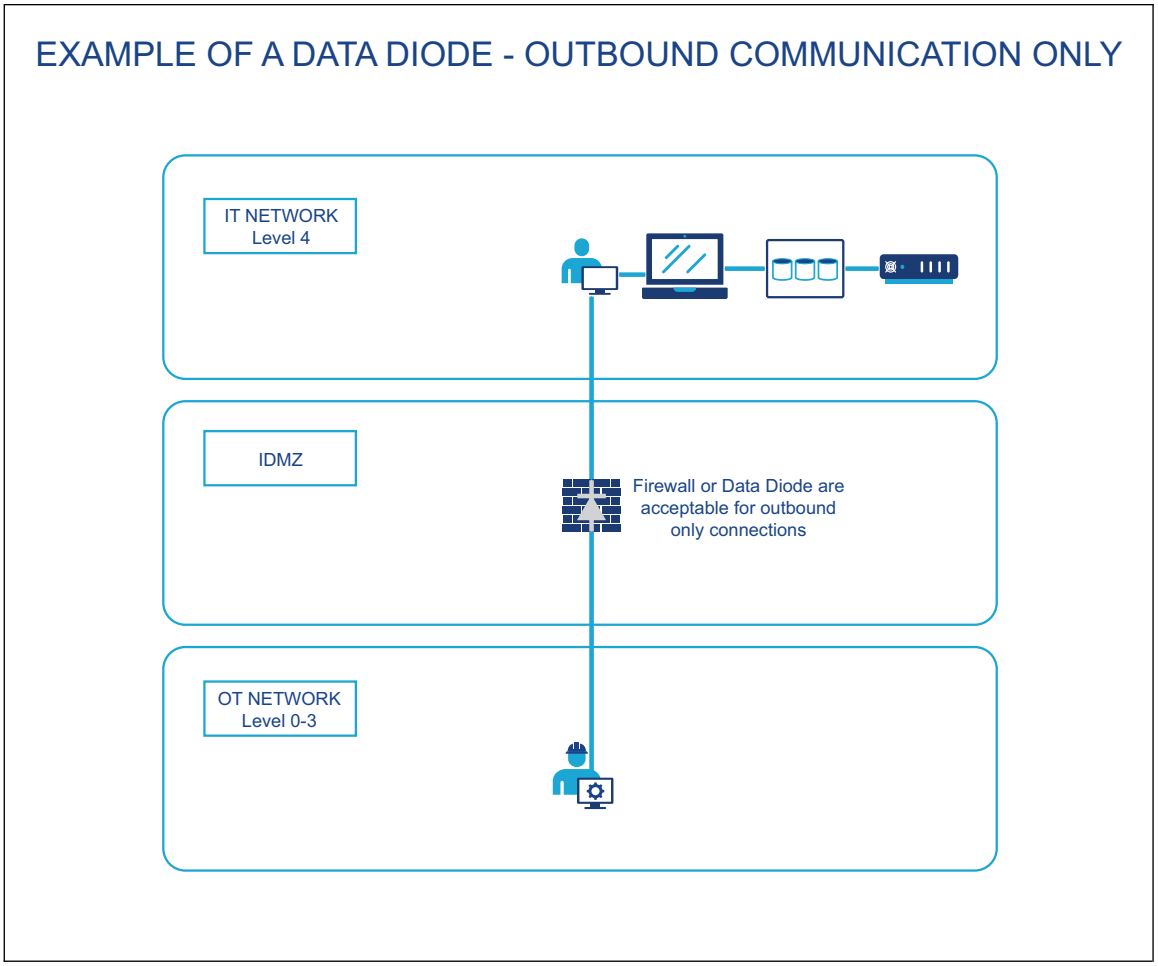

Fig. C.10. Example of a data diode connection

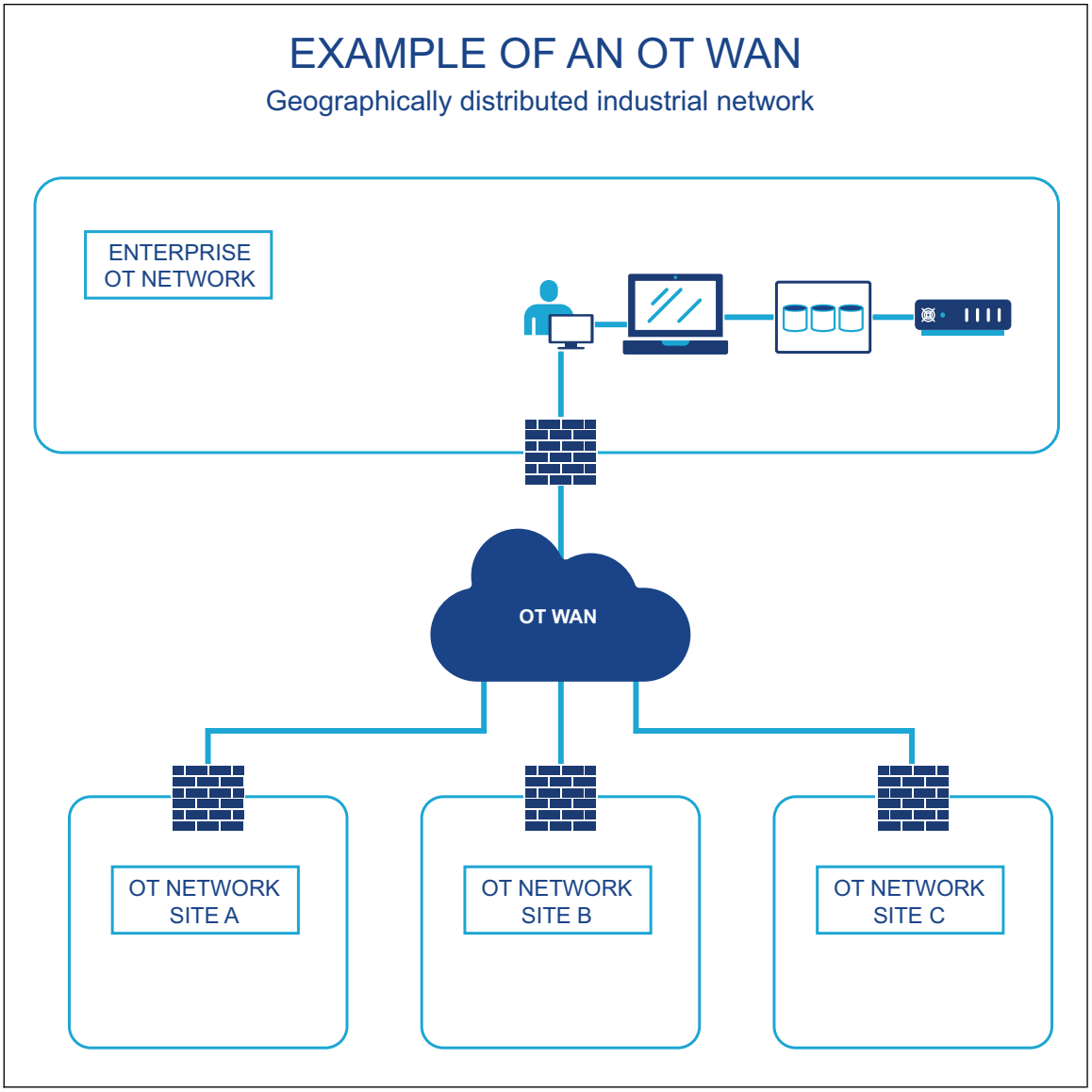

Fig. C.11. Example of an OT WAN