White Paper **WP152002EN** Effective July 2024

Cybersecurity considerations for electrical distribution systems

Authors

Max Wandera, BrentJonasson, Jacques Benoit, James Formea, Tim Thompson, Zwicks Tang, DennisGrinberg, Andrew Sowada, Demos Andreou, Thomas Ruchti, Paul Elwell, and Jeff Groat

Purpose

The purpose of this document is to provide high-level guidance to help customers across industries and applications apply Eaton solutions for power management of electrical systems in accordance with current cybersecurity standards. This document is intended to provide an overview of key security features and practices to consider in order to meet industry-recommended standards and best practices.

Table of contents

Powering Business Worldwide

Introduction

Every day, cyber-attacks against government and commercial computer networks number in the millions. According to U.S. Cyber Command, Pentagon systems are probed 250,000 times per hour. Similar attacks are becoming more prevalent on other kinds of information-based smart networks as well, such as those that
operate buildings and utility systems. Whether the objective is to steal intellectual property or halt operations, the tools and the techniques used for unauthorized network access are increasingly sophisticated.

Connectivity—why do we need to address cybersecurity for industrial control systems (ICS)?

There is increasing concern regarding cybersecurity across industries where companies are steadily integrating field devices into enterprise-wide information systems. This occurs in discrete manufacturing and process industrial environments, a wide range of general and specific purpose commercial buildings, and even utility networks. Traditionally, electrical systems were controlled through serial devices connected to computers via dedicated transceivers with proprietary protocols. In contrast, today's control systems are increasingly connected to larger enterprise networks, which can expose these systems to similar vulnerabilities that are typically found in computer systems.

The differences between information technology (IT) and ICS networks can be summarized as follows:

- The main focus of the IT network is to ensure the **confidentiality** and the **integrity** of the data using rigorous access control and data encryption
- The main focus of the ICS network is **safety**, **availability**, and **integrity** of data
- Enterprise security protects the servers' data from attack
- Control system security protects the facility's ability to safely and securely operate, regardless of what may befall the rest of the network

Cybersecurity threat vectors

Cybersecurity threat vectors are paths or tools that an entity can use to gain access to a device or a control network in order to deliver a malicious attack. **Figure 1** shows examples of attack vectors on a network that might otherwise seem secure.

The paths in **Figure 1** include:

- External users accessing the network through the Internet
- Misconfigured firewalls
- Unsecure wireless routers and wired modems
- Infected laptops located elsewhere that can access the network behind the firewall
- Infected USB keys and PLC logic programs
- Unsecure RS-232 serial links

The most common malicious attacks come in the following forms:

- Virus—a software program that spreads from one device to another, affecting operation
- Trojan horse—a malicious device program that hides inside other programs and provides access to that device
- Worm—a device program that spreads without user interaction and affects the stability and performance of the ICS network
- Spyware—a device program that changes the configuration of a device

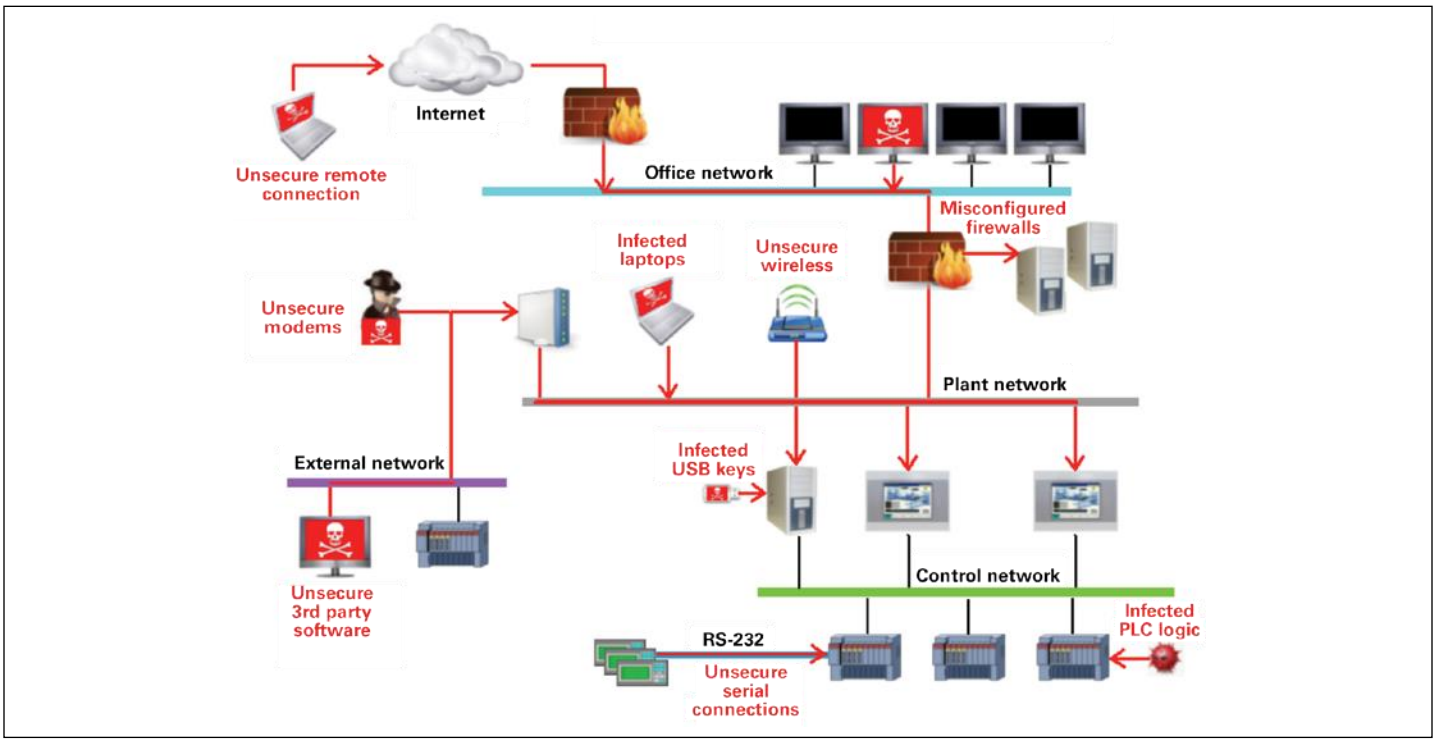

Figure 1. Paths to the control network

Defense in depth

While there are differences between traditional IT systems and ICS, the fundamental concept of "defense in depth" is applicable to both. Defense in depth is a strategy of integrating technology, people, and operations capabilities to establish variable barriers across multiple layers of an organization. These barriers include electronic countermeasures such as firewalls, intrusion detection software/components, and antivirus software, coupled with physical protection policies and training. Fundamentally, the barriers are intended to reduce the probability of attacks on the network and provide mechanisms to detect "intruders."

Designing for the threat vectors

Firewalls

Firewalls provide the capability to add stringent and multifaceted rules for communication between various network segments and zones in an ICS network. They can be configured to block data from certain segments, while allowing the relevant and necessary data through. A thorough understanding of the devices, applications, and services that are in a network will guide the appropriate deployment and configuration of firewalls in a network. Typical types of firewalls that can be deployed in a network include:

- **Packet filter or boundary firewalls that work on the network layer**
  These firewalls mainly operate at the network layer, using pre-established rules based on port numbers and protocols to analyze the packets going into or out of a separated network. These firewalls either permit or deny passage based on these rules.
- **Host firewalls**
  These firewalls are software firewall solutions that protect ports and services on devices. Host firewalls can apply rules that track, allow, or deny incoming and outgoing traffic on the device and are mainly found on mobile devices, laptops, and desktops that can be easily connected to an ICS.
- **Application-level proxy firewalls**
  These firewalls are highly secure firewall protection methods that hide and protect individual devices and computers in a control network. These firewalls communicate at the application layer and can provide better inspection capabilities. Because they collect extensive log data, application-level proxy firewalls can negatively impact the performance of an ICS network.
- **Stateful inspection firewalls**
  These firewalls work at the network, session, and application layers of the open system interconnection (OSI). Stateful inspection firewalls are more secure than packet filter firewalls because they only allow packets belonging to allowed sessions. These firewalls can authenticate users when a session is established and analyze a packet to determine whether they contain the expected payload type or enforce constraints at the application layer.
- **SCADA hardware firewalls**
  These are hardware-based firewalls that provide defense for an ICS based on observing abnormal behavior on a device within the control network. For example, if an operator station computer suddenly attempts to program a PLC, this activity could be blocked, and an alarm could be raised to prevent serious risk to the system.

Demilitarized zones (DMZ)

Network segmentation is a key consideration in establishing secure control networks. Firewalls should be used to create DMZ by grouping critical components and isolating them from the traditional business IT network. A three-tier architecture should be employed at a minimum, with a DMZ between the organization's core network and an isolated control system's network as shown in **Figure 2**.

Figure 2 shows that the control networks are divided into layers or zones based on control functions, which are then connected by conduits (connections between the zones) that provide security controls to:

- Control access to zones
- Resist denial of services (DOS) attacks or the transfer of malware
- Shield other network systems
- Protect the integrity and the confidentiality of network traffic

Beyond network segmentation, access control (both physical and logical) should be defined and implemented.

The key consideration when designing access control is defining the **required** interactions both within a given zone and between zones. These interactions should be mapped out clearly and prioritized based on need. It is important to realize that every hole poked in a firewall and each non-essential functionality that provides access or creates additional connectivity increases potential exposure to attacks. A system then becomes only as secure as the devices connecting to it.

If mapped correctly, the potential adverse impact to control system reliability and functionality should be negligible. However, this element introduces additional costs (in terms of firewall and other network infrastructure) and complexity to the environment.

Intrusion detection and prevention systems (IDPS)

These are systems that are primarily focused on identifying possible incidents in an ICS network, logging the information about them, attempting to stop them, and reporting them to ICS security administrators. Because these systems are critical in an ICS network, they are regular targets for attacks and securing them is extremely important.

The type of IDPS technology deployed will vary with the type of events that need to be monitored. There are four classes of IDPS technology:

- Network-based IDPS monitors network traffic for particular ICS network segments or devices and analyzes the network and application protocol activity to identify suspicious activity
- Wireless IDPS monitors and analyzes wireless network traffic to identify suspicious activity involving the ICS wireless network protocol
- Network behavior analysis IDPS examines ICS network traffic to identify threats that generate unusual traffic flows such as DOS attacks
- Host-based IDPS monitors the characteristics and the events occurring within a single ICS network host for suspicious activity

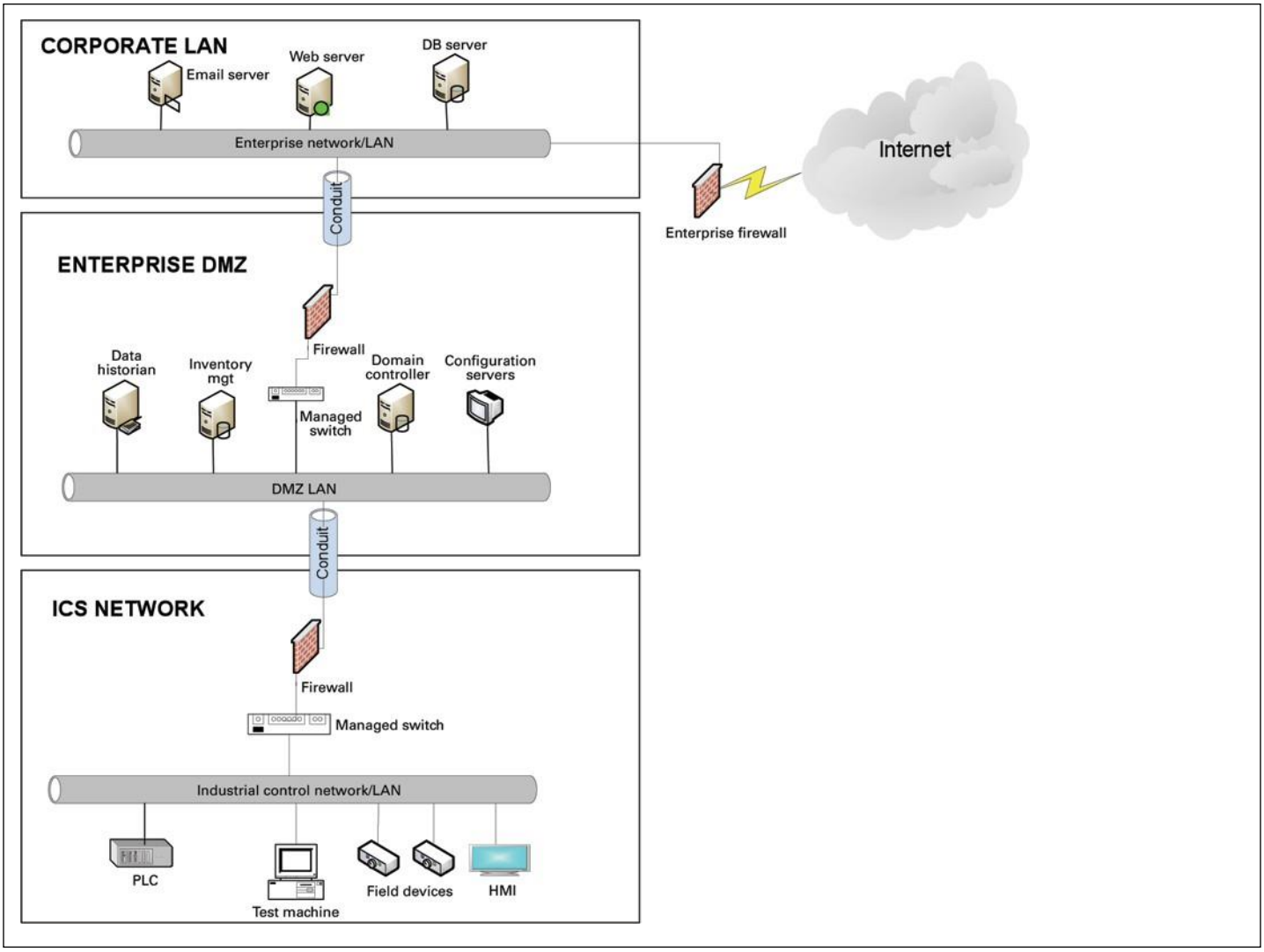

Figure 2. Three-tier architecture for a secure control network

Policies, procedures, standards, and guidelines

For the defense in depth strategy to succeed, there must be well-documented and continuously reviewed policies, procedures, standards, and guidelines.

- **Policies** provide procedures or actions that must be carried out to meet objectives and to address the who, what, and why
- **Procedures** provide detailed steps to follow for operations and to address the how, where, and when
- **Standards** typically refer to specific hardware and software, and specify uniform use and implementation of specific technologies or parameters
- **Guidelines** provide recommendations on a method to implement the policies, procedures, and standards

Understanding an ICS network

Creating an inventory of all the devices, applications, and services that are hosted in a network can establish an initial baseline for what to monitor. Once those components are identified and understood, control, ownership, and operational consideration can be developed.

Log and event management

It is important to understand what is happening within the network from both a performance and security perspective. This is especially true in a control systems environment.

Log and event management entails monitoring infrastructure components such as routers, firewalls, and IDS/IPS, as well as host assets. Security Information and Event Management (SIEM) systems can collect events from various sources and provide correlation and alerts.

Generating and collecting events, or even implementing a SIEM is not sufficient by itself. Many organizations have SIEM solutions, but alerts go unwatched or unnoticed.

Monitoring includes both the capability to monitor environments and the capacity to perform the monitoring. Capability relates to the design and the architecture of the environment. Has it been built in a manner that takes into consideration the ability to monitor? Capacity speaks to the resources (personnel, tools, expertise) needed to perform meaningful interpretation of the information and initiate timely and appropriate action.

Through monitoring, the organization can identify issues such as suspicious or malicious activities. Awareness can be raised when new (potentially unauthorized) devices appear in the environment. Careful consideration should be taken into account to ensure that log and event management does not adversely impact the functionality or the reliability of the control system devices.

Security policy and procedures

It is important to identify “asset owners,” and to develop policies and procedures for a cybersecurity program. These policies need to be practical and enforceable in order to be effective. Policies should also address access related issues, such as physical access, contractors, and vendors.

Existing (traditional) IT standards and policies may not apply (or have not been considered) for control systems. A gap analysis should be performed to determine which components are not covered (or not adequately covered) by existing policies. Relationships with existing policies and standards should be explicitly identified and new or supporting policies should be developed. It is important that industrial control system administrators have proper authorizations and full support of their management to implement policies that will help secure the ICS network.

ICS hardening

The goal for system hardening is to reduce as many security risks as possible by securely configuring ICS networks. The idea is to establish configurations based on what is required and eliminate unnecessary services and applications that could potentially provide another possible entry point to an intruder.

Minimum security baselines should be established for the various platforms and products deployed (operating system, application, and infrastructure elements such as drives, meters, HMI devices). The following actions should be implemented where applicable:

- Disable unnecessary services
- Disable anonymous FTP
- Do not use clear text protocols (e.g., use SSH v2 instead of Telnet)
- Install only required packages/applications/features
- Deploy antivirus solutions (where possible)
- Disable or otherwise control use of USB devices
- Establish a warning banner
- Change default passwords (e.g., SNMP)

It may be easier to implement these actions on devices for which you control the base operating system platform. However, several of the items listed above can be configured from the product specific configuration options.

Changes such as these could potentially impact the functionality of a control system device. Extensive testing needs to be conducted before deployment to minimize this impact.

Continuous assessment and security training

It is critical that ICS network administrators and regular users be properly trained to ensure the security of the ICS and the safety of the people who operate and depend on it.

Ongoing vulnerability assessments are critical to identify issues and understand the effectiveness of other defensible network elements. Assessments should include testing and validating the following:

- Monitoring capabilities and alerts are triggered and responded to as expected
- Device configuration of services and applications
- Expected connectivity within and between zones
- Existence of previously unknown vulnerabilities in the environment
- Effectiveness of patching

A program should be established for performing assessments. The actual assessment should be performed by a qualified resource, which can be an in-house or third-party organization. Regardless of who performs the assessments, in-house resources need to be involved in the planning, scoping, and supporting of assessment activities and must be appropriately trained to do so.

Assessments should be conducted according to a methodology that is clearly defined to address:

- Physical security
- People and processes
- Network security
- Host security
- Applications security (both internally developed and commercially off-the-shelf (COTS))

Patch management planning and procedures

A patching and vulnerability management process should be established based on the timely awareness of issues and appropriate action. This process should take all of the elements that make up the control system environment into consideration.

Information resources should be identified for vulnerability and advisory information for the various components in the environment. These should include vendor-specific sources as well as other public or commercial services that provide vulnerability advisory information. For example, the National Vulnerability Database (NVD) provides information related to vulnerabilities identified in general IT components, while the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) publishes advisories specific to control systems.

A regular patch deployment schedule should be established for each component in the environment. Depending on the component, this could range from a monthly schedule to an as-needed deployment, depending on the historical frequency of patch or vulnerability related issues for the component or the vendor. Additionally, out-of-band or emergency patch management needs to be considered and qualifications need to be defined.

Vulnerability information and advisories should be reviewed regularly, and assessments should be performed to determine the relative severity and urgency of issues.

Elements of the process should also include the preparation, scheduling, and change controls; testing and rollback procedures; and pre-deployment notification to stakeholders that includes scope, expectations, and reporting. Testing is a significant element, as the effect of the patch application needs to be clearly understood; unintended or unexpected impacts to a control system component influence the decision to deploy a patch. In the event that it is determined that a patch cannot be safely deployed but the severity of the issue represents a significant concern, compensating controls should be investigated.

Conclusion

To protect important assets, all organizations must take cybersecurity threats seriously and meet them proactively with a system-wide defensive approach specific to organizational needs.

There is no protection method that is completely secure. A defense mechanism that is effective today may not be effective tomorrow– the ways and means of cyber-attacks constantly change. It is critical ICS administrators remain aware of changes in cybersecurity and continue to work to prevent any potential vulnerabilities in the systems they manage.

Terms and definitions

DMZ	A demilitarized zone is a logical or physical sub network that interfaces an organization's external services to a larger, untrusted network and providing an additional layer of security.
Encryption	The process of transforming plain or clear text using an algorithm to make it unreadable to anyone except those possessing special knowledge.
ICS	A device or set of devices that manage, command, direct, or regulate the behavior of other devices or systems.
Protocol	A set of standard rules for data representation, signaling, authentication, and error detection required to send information over a communications channel

Acronyms

COTS	Commercially Off-the-Shelf
DMZ	Demilitarized Zone
DOS	Denial of Service
FTP	File Transfer Protocol
HMI	Human Machine Interface
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDPS	Intrusion Detection and Prevention Systems IDS Intrusion Detection Systems
IPS	Intrusion Prevention Systems IT Information Technology
NVD	National VulnerabilityDatabase
OSI	Open System Interconnection PLC Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SNMP	Simple Network Management Protocol SSH Secure Shell
SIEM	Security Information and Event Management
USB	Universal Serial Bus

References

[1] Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, October 2009 http://ics-cert.uscert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

[2] NIST.SP.800-82 Guide to Industrial Control Systems (ICS) Security, June 2011
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[3] NIST.SP.800-94 Guide to Intrusion Detection and Prevention Systems (IDPS), Feb 2007
http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[4] Common Cybersecurity Vulnerabilities in Industrial Control Systems, May 2011
http://ics-cert.uscert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

[5] The Tao of Network Security Monitoring, 2005 Richard Bejtlich

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States Eaton.com

Printed in USA
Publication No. WP152002EN / Z18871
July 2024