PACSystems™ IPC 6010/7010/8010

SECURE DEPLOYMENT GUIDE

Contents

Warnings and Caution Notes as Used in this Publication

⚠ WARNING

Warning notices are used in this publication to emphasize that hazardous voltages, currents, temperatures, or other conditions that could cause personal injury exist in this equipment or may be associated with its use.

In situations where inattention could cause either personal injury or damage to equipment, a Warning notice is used.

⚠ CAUTION

Caution notices are used where equipment might be damaged if care is not taken.

Note: Notes merely call attention to information that is especially significant to understanding and operating the equipment.

These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and Emerson makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that Emerson may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the Emerson products referenced herein.

Emerson may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

Emerson provides the following document and the information included therein as-is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for a particular purpose.

Section 1: About this Guide

⚠CAUTION

Emerson provides these general recommendations and guidelines to aid the end-user in managing security risks associated with the operation of an Emerson PACSystems IPC 6010/7010/8010 Industrial PC when used with pre-installed software or operating systems, or other user-installed operating systems. These guidelines are not meant to be comprehensive. It is entirely the owner's responsibility to ensure the security of the operating systems, and any associated applications deployed on the platform.

1.1 Applicable Products

This document provides information that can be used to help improve the cybersecurity of the PACSystems IPC 6010/7010/8010 Industrial PC hardware platform with user-installed operating systems, as well as with Emerson's pre-installed software. It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring products.

Table 1: Product Description

Product	Catalog #	Description
IPC 6010	RPB6xxxxxxxx	Raptor Lake U series processors (15-watt class), optional 1 PCIe slot, with optional Windows 10 or PACEdge software package
IPC 7010	RPB7xxxxxxxx	Raptor Lake P series processors (28-watt class), optional 1 – 3 PCIe slots, with optional Windows 10 or PACEdge software package
IPC 8010	RPB8xxxxxxxx	Raptor Lake H series processors (45-watt class), optional 1 – 4 PCIe slots, with optional Windows 10 or PACEdge software package

1.2 Revisions in this Manual

Table 2: Document Revision

Rev	Date	Description
A	May 202	Initial publication

In addition to these manuals, datasheets and product update documents describe individual devices and product revisions. The most recent documentation is available on the Emerson technical support website https://www.emerson.com/Industrial-Automation-Controls/support.

Section 2: Introduction

This document explains what is meant by security, and why it is important to not rely only on a firewall. Readers can expect to learn about the 'Defense in Depth' concept and its general recommendations. An example checklist is also provided, which should help to securely deploy the Emerson product. This checklist is not meant to be comprehensive. Please ensure adequate security measures are in place.

2.1 What is Security?

Security is the process of maintaining the confidentiality, integrity, and availability of a system.

- **Confidentiality**: Ensures that certain confidential information is only seen by authorized personnel.
- **Integrity**: Ensures the data is what it is supposed to be.
- **Availability**: Ensures the system or data is available for use.

Emerson recognizes the importance of building and deploying products with these concepts in mind and encourages customers to take the appropriate care in securing their Emerson products and solutions. As Emerson discovers and fixes product vulnerabilities, security advisories are issued to describe each vulnerability in each product version, as well as detail the corresponding version in which the vulnerability was fixed. Emerson Product Security Advisories can be found at the links provided at the end of this document.

2.2 I have a Firewall. Isn't that enough?

Firewalls and other network security products, including Data Diodes and Intrusion Prevention Devices, can be an important component of any security strategy. However, an effective cybersecurity strategy is made up of multiple layers, and a strategy based solely on any single security mechanism or layer will not be as resilient as one that includes multiple, independent layers of security.

Therefore, Emerson recommends taking a Defense in Depth approach to security.

2.3 What is Defense in Depth?

Defense in Depth is the concept of using multiple, independent layers of security to raise both the cost and the complexity of a successful attack. To carry out a successful attack on a system, an attacker would need to find multiple exploitable vulnerabilities in each layer of defense that protects an asset, rather than only one single exploitable vulnerability.

For example, if a system is only protected because it is on a network protected by a firewall, the attacker would simply need to circumvent the firewall to gain unauthorized access. However, if there is an additional layer of defense, such as a username/password authentication requirement, the attacker would need to find a way to circumvent both the firewall and the username/password authentication, providing an additional layer of defense. Multiple such layers are recommended to mitigate the vulnerability.

2.4 General Recommendations

Adopting the following security best practices should be considered when using Emerson products and solutions.

- Edge devices span both, control networks and wide area networks (WAN), potentially extending to include access to the Internet as a whole. Network segmentation and firewall rules must be carefully considered to reduce the allowed traffic to the bare minimum needed for operation. Care must be taken to control, limit, and monitor all access, using, for example, Virtual Private Networks (VPN) or Demilitarized Zone (DMZ) architectures. All communication endpoints should be considered individually, and if a specific protocol or the device as a whole does not require wide area network access, it is strongly recommended that the relevant protocols be restricted to the most limited network possible.
- Harden system configurations by enabling/using the available security features, and by disabling unnecessary ports, services, functionality, and network file shares.
- Apply the latest Emerson product security updates, SIMs, and other recommendations.
- Apply the latest operating system security patches to control systems PCs.
- Use anti-virus software on control systems PCs and keep the associated anti-virus signatures up-to-date.
- Use whitelisting software on control systems PCs and keep the whitelist up-to-date.

2.5 Checklist

This section provides a sample checklist to help guide the process of securely deploying Emerson products.

1. Create or locate a network diagram.
2. Identify and record the required communication paths between nodes.
3. Identify and record the protocols required along each path, including the role of each node.
4. Revise the network as needed to ensure appropriate partitioning, adding firewalls or other network security devices as appropriate. Update the network diagram.
5. Configure firewalls & other network security devices.
6. Enable and/or configure the appropriate security features on each Emerson product.
1. On each Emerson product, change every supported password to something other than its default value.
7. Harden the configuration of each Emerson product, disabling unneeded features, protocols, and ports.
8. Test/qualify the system.
9. Create an update/maintenance plan.

Note: *Secure deployment is only one part of a robust security program. This document, including the checklist above, is limited to only providing secure deployment guidance.*

Section 3: Cybersecurity Features and Hardening

An Industrial PC is typically not a final product, but a platform for building the final product. Customers who purchase an Industrial PC usually add their preferred operating system and application software on top. The responsibility or cybersecurity hardening primarily falls on the user. The software alone is not enough. Without a strong cybersecurity foundation to start with, the hardware and UEFI Firmware design is virtually impossible to build a solid security product. Emerson Industrial PCs have been designed from the ground up with cybersecurity in mind. The subsequent chapters within this document will guide how to enable and use the hardware and UEFI Firmware features that are available.

3.1 Physical Interfaces

All PACSystems IPC 6010/7010/8010 Industrial PCs have the following physical data and communication interfaces.

3.1.1 Ethernet Interfaces

	IPC 6010/7010/8010
Number/Type of Ethernet ports	5 x 10/100/1000/2500 BASE-T
Support for remote management (Intel AMT)	Available at RJ45 port 1 (maintenance port), but disabled by default in UEFI Firmware

Ethernet ports are fully accessible by the operating system and can be used for most standard OSI stack links through application layer protocols. Operating systems and applications determine which protocols are enabled and which cybersecurity restrictions are enforced.

The user is responsible for configuring and limiting protocols to the minimum settings required for a specific application.

Remote management features, such as Intel's AMT, provide access to the IPC via a dedicated Ethernet port **even when the IPC is in S5 power-down state**. Furthermore, this access path goes through a separate TCP/IP protocol stack, distinct from the operating system, and must be carefully considered in the context of cybersecurity. For best practices, please refer to section 4.3 Remote Management (Intel AMT) of this document.

> By default, this functionality is disabled in UEFI Firmware, but users can enable it after purchase. For instructions on how to enable the remote management, please refer to GFK-3306, IPC XX10 User Manual.

3.1.2 Serial Interfaces

	IPC 6010/7010/8010
Number/Type of Serial ports	2 x RS232 2 x RS422/RS485 (configurable)

Operating systems and applications determine which protocols are enabled and which cybersecurity restrictions are enforced.

The user is responsible for configuring and limiting protocols to the minimum required settings for a specific application.

3.1.3 USB Interfaces

	IPC 6010/7010/8010
Number/Type of USB ports	4 x USB3.2 (Type A connector) 2 x UCB-C 1 x M.2 E-Key USB Part

The USB3.2 interfaces can be used for communications, such as USB-Ethernet adapters, as well as for storage, such as a USB thumb drive. The USB-C type interfaces are also capable of running Thunderbolt (TBT4) and DisplayPort. Operating systems and applications determine which protocols are enabled and which cybersecurity restrictions are enforced.

The user is responsible for configuring and limiting protocols to the minimum required settings for a specific application.

Thunderbolt

With USB-C connector-based computer ports that provide PCI Express (PCIe) protocol, users can connect PCIe devices to the computer just as if they were installed internally. Such devices include portable and desktop storage, external graphics, memory card readers, ethernet adapters and other PCIe-based devices.

PCIe devices are unique because they are capable of Direct Memory Access (DMA), which enables fast and efficient access to the system memory without involving the processor. However, shared memory between all the different devices in the system including those that are externally connected via the USB-C port may present a security risk if not properly protected.

Thunderbolt port security is hardware-based, relying on Intel's Virtualization Technology for Directed I/O (Intel VT-d). The operating system further enhances protection during runtime. To defend against DMA attacks before the system boots and until the transition to the operating system, UEFI Firmware (BIOS) includes support that helps block devices from unauthorized access to system memory.

Although physical attacks may be challenging to perform and require that an attacker possess your PC, it is still recommended to follow standard security practices to minimize risk. Such practices include using only trusted peripherals and preventing

unauthorized physical access to computers. Hard disk drive encryption and a BIOS password can provide additional protection.

3.1.4 Non-Volatile Storage

	IPC 6010/7010/8010
Internal Storage	M.2 SSD (NVMe) MRAM (optional feature) NVSRAM mPCIe module (optional feature)
Externally Accessible Storage	1 x µSD card slot (SDHC and SDXC)

Internal SSD is by default the main storage medium where the operating system and applications are installed. UEFI Firmware controls access to different storage devices and can be used to enable/disable booting from those devices.

Once OS has booted the operating system and applications will control access to these storage devices and configure which cybersecurity restrictions are enforced.

The user is responsible for configuring and limiting the use of these storage devices.

3.1.5 DisplayPort Output

	IPC 6010/7010/8010
Number/Type of DP ports	2 x DisplayPort 2 x USB-C DisplayPort

DisplayPort (DP) outputs are used to attach external displays. The use of DP outputs is controlled by Operating System and is a user responsibility.

3.2 UEFI Firmware Level Security Features

3.2.1 UEFI Firmware Password

Unified Extensible Firmware Interface (UEFI) is the interface between the operating system and the IPC's firmware that initializes and configures the hardware components of an IPC. The UEFI Firmware offers menus to modify hardware and firmware options. Since these settings directly influence hardware behavior (e.g. the device the IPC boots from), they pose a security risk. To avoid unauthorized changes in UEFI Firmware settings, access to the menus can be restricted by a password. **This password protection is not activated by default**. Emerson strongly recommends taking advantage of this feature and enabling the password. You can change/activate the UEFI Firmware password by hitting the F2 button of an attached keyboard during the boot sequence and then select the Security menu and the Password Change entry.

3.2.2 Secure Boot

Secure Boot is a security feature in the UEFI Firmware (see above), which allows only trusted/signed Bootloaders to be executed by the UEFI Firmware. This prevents attackers from modifying or replacing bootloaders to load compromised operating systems. If activated, UEFI Firmware validates the signature attached to a bootloader using public keys embedded into UEFI Firmware or allows only those images which have a known image hash. Customers can add their public keys to the UEFI Firmware key database and sign their bootloaders (e.g. Grub2) with the appropriate private key or add known image hashes. As the Windows bootloader is already signed by Microsoft, the UEFI Firmware Key database already includes Microsoft public keys to ensure that Windows can be booted with secure boot enabled.

Secure Boot can be activated in the Security menu of the UEFI Firmware settings.

The UEFI Firmware Key database also can be extended/modified via the Security Menu in the UEFI Firmware settings.

Note: To protect against an attacker changing the Secure Boot settings in UEFI Firmware, the UEFI Firmware password needs to be configured and enabled.

3.2.3 Measured Boot

Measured Boot is a technology that measures different software and configuration settings before the software is executed and extends those measurements to Trusted Platform Module (TPM). For this technology to be efficient, measurements need to be started very early in the boot process, typically in UEFI Firmware. To be effective, bootloaders, and later, operating systems, need to continue the process of measurements. It is important to understand that Measured Boot by itself does not take any protective actions from a cybersecurity perspective, but rather collects and safely stores the record of the software elements that were executed for retroactive analysis. Protective actions such as sealing secrets and attestation need to be additionally implemented to benefit the Measured Boot technology. It is the user's responsibility to consider, choose, and implement protective measures that are based on the Measured Boot.

PACSystems IPC 6010/7010/8010 Industrial PCs use a firmware TPM version 2.0 integrated in chipset.

	IPC 6010/7010/8010
TPM Implementation	Intel TPM v2 (integrated in chipset)

3.2.4 Secure Flash and UEFI Firmware Updates

To protect against UEFI Firmware modifications or tampered UEFI Firmware images, the UEFI Firmware image is signed by Emerson and its signature is checked. Therefore, UEFI Firmware update can only be carried out using Emerson-authorized and properly signed UEFI Firmware images.

3.2.5 UEFI Firmware Security Features Default States

The following table shows the most important security features. Note that the UEFI Firmware configuration menu has a separate configuration option for some, but not all, features.

Feature	Default State
UEFI Firmware Password	Not set
Secure Boot	Disabled
Measured Boot	Active
Secure Flash	Active
TPM 2.0 Support	Enabled

3.3 Boot Loader and OS Security Features

3.3.1 Securing Boot Loader

Following the Secure boot protection scheme, a next-level boot loader needs to be signed by the key that is stored in the UEFI Firmware key database. By default, the Microsoft key is already stored in the UEFI Firmware key database, allowing to use of Microsoft boot loader. If the user wishes to use GRUB or a similar boot loader in conjunction with Secure Boot technology, then such a boot loader needs to be signed and the appropriate key needs to be stored in the UEFI Firmware key database or the boot loader hash needs to be added to the known hash database.

3.3.2 Securing Operating Systems

Regarding Microsoft Windows, the Windows Boot Manager is responsible for checking Windows kernel and drivers. Once Windows has booted, it will load the remaining kernel drivers and user-mode processes. In the case of other operating systems, it is the customer's responsibility to analyze and understand the secure boot process and how it can be coupled with the existing UEFI Firmware cybersecurity features.

3.4 Windows Security Features

PACSystems IPC 6010/7010/8010 Industrial PCs are available with Windows IoT Enterprise pre-installed. At time of writing, the pre-installed version is Windows 10 IoT Enterprise 2021 LTSC that is updated with a Servicing Stack Update and a Cumulative Update. Newer Windows versions and patches will be used as they become available.

Regarding Windows OS, the following security-relevant features among the others should be considered by the user and configured as required.

Feature	Default State	Notes
FTP Server	Disabled	-
DNS Client Service (dnscache)	Enabled	The DNS Client service caches Domain Name System (DNS) names and registers the full computer name for this computer
Remote Desktop	Disabled	-
Autoplay for USB	Enabled	-
DEP (Data Execution Prevention)	Enabled	DEP for essential Windows programs and services only
Windows Defender Firewall	Enabled	Incoming connections: block all incoming connections to apps that are not on the list of allowed apps

3.5 PACEdge Software Security Features

For the PACEdge software package please consult a PACEdge Cybersecurity Deployment Guide, GFK-3197.

3.6 Security Updates and Patches

A strategy for applying security fixes, including patches, firmware updates, and configuration changes, should be included in a facility's security plan. Users are strongly encouraged to continuously monitor the availability of cybersecurity updates and patches and apply them as soon as feasible.

Section 4: Additional Cybersecurity Information

Following a Defense in Depth Cybersecurity concept and security-hardening, the Industrial PC is only part of an overall Cybersecurity implementation strategy. The following information is deemed to be useful for further hardening of the Industrial PC, as well as for establishing system-level cybersecurity mechanisms.

4.1 Firewall Configuration

Network-based and host-based firewalls should be configured to only allow expected and required network traffic. This section identifies the Ether Types and the TCP/UDP ports that are typically used.

This information should be used to help configure network firewalls, to support only the required communications paths for any particular installation.

4.1.1 Lower-level Protocols

Ethernet communication is typically described using four layers, each with its own set of protocols. At the top of that hierarchy is the Application layer. Below the Application, the layer is the Transport, Internet, and Link layers.

Information on the supported protocols from these three lower layers is summarized in the following tables.

Table 3: Link Layer Protocols

Protocol	Ethernet Type
ARP	0x0806
LLDP	0x88cc

Table 4: Internet Layer Protocols

Protocol	Ethernet Type	IP Protocol
IPv4	0x0800	N/A
ICMP		1
IGMP		2

Table 5: Transport Layer Protocols

Protocol	Ethernet Type	IP Protocol
TCP	0x0800	6
UDP		17

4.1.2 Application Layer Protocols

Protocol	Server TCP Port	Dest UDP Port
DCE/RPC	—	34964 on server >1023 on client
DNS	53	53 on server >1023 on client
Control – Warm Standby	12399	—
FTP	21	—
HTTP	80	—
SNTP	—	123
SNMP	—	—
SSH	22	—

Please note that Intel AMT implements private network interfaces which are invisible to an operating system running on a system. Also, from a network perspective, these network interfaces appear as separate hosts with a separate network configuration.

Intel AMT Network Protocols

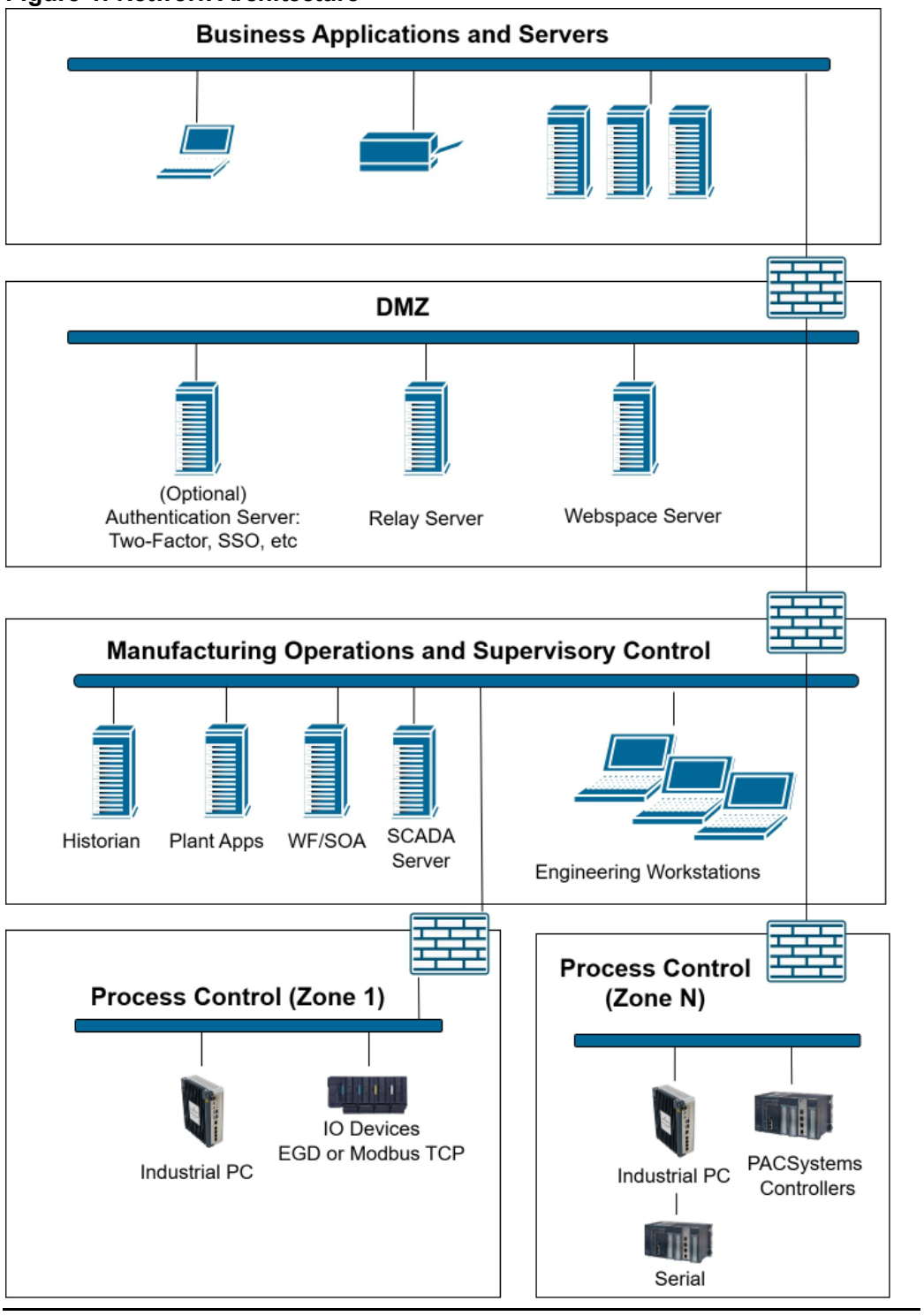
Protocol	TCP Port	UDP Port
Intel(R) AMT HTTP	16992	16992
Intel(R) AMT HTTPS	16993	16993
Intel(R) AMT Redirection/TCP	16994	16994
Intel(R) AMT Redirection/TLS	16995	16995
ASF Remote Management and Control Protocol (ASF-RMCP)	-	623
• TCP: DMTF out-of-band secure web services management protocol • UDP: ASF Secure Remote Management and Control Protocol (ASF-RMCP)	664	664
Virtual Network Computing (VNC)	5900	5900

4.2 Network Architecture and Secure Deployment

This chapter provides security recommendations for deploying the IPC in the context of a larger network.

The Manufacturing Zone networks (which include the Manufacturing Operations, Supervisory Control, and Process Control networks) are segregated from other untrusted networks such as the enterprise network (also referred to as the business network, corporate network, or intranet) and the internet using Demilitarized Zone (DMZ) architecture. The Process Control networks have limited exposure to traffic from higher-level networks, including other networks in the Manufacturing Zone, and other Process Control networks.

Figure 1: Network Architecture



4.2.1 Remote Access and Demilitarized Zones (DMZ)

A DMZ architecture uses two firewalls to isolate servers that are accessible from untrusted networks. The DMZ should be deployed such that only specific (restricted) communication is allowed between the business network and the DMZ, and between the control network and the DMZ. The business network and the control networks should ideally not communicate directly with each other.

If direct communication with a control network is required from the business network or the internet, carefully control the limit, and monitor all access. For example, require two-factor authentication for a user to obtain access to the control network using Virtual Private Networking (VPN) and even then, restrict the allowed protocols/ports to only the minimum set required. Further, every access attempt (successful or not) and all blocked traffic should be recorded in a security log that is regularly audited.

4.2.2 Access to Process Control Networks

Ethernet traffic from the Supervisory Control network to the Process Control networks should be restricted to support only the functionality that is required. If a particular protocol (such as Modbus TCP) doesn't need to be used between those regions, then the firewall should be configured to block that protocol. Additionally, if a controller has no other reason to use that particular protocol, then – in addition to blocking it at the firewall – the controller itself should be configured to disable support for the protocol.

Note:

Network Address Translation (NAT) firewalls typically do not expose all the devices on the trusted side of the firewall to devices on the untrusted side of the firewall. Further, NAT firewalls rely on mapping the IP address/port on the trusted side of the firewall to a different IP address/port on the untrusted side of the firewall.

4.3 Remote Management (Intel AMT)

Remote management enables a remote operator to perform actions like powering a system on/off, changing UEFI Firmware settings and booting a system from a remotely emulated mass storage device. Since these functions are accessible over network, enabling them creates a potential attack surface that should be considered when analyzing the cybersecurity of a network or an environment (see section 2.5 Checklist).

Besides the general recommendations in section 2.4 General Recommendations, the following guidelines must be met when using remote management. Implementing these guidelines to ensure secure operation is the responsibility of the customer.

- Protection from internet exposure: Remote management functions are not designed to be exposed directly to the internet.
  Systems with active remote management must be protected by a firewall!

Please refer to section 4.2 Network Architecture and Secure Deployment for recommendations on network architecture.

- Secure network protocols: Use a firewall to allow only secure network protocols for remote management (see section 4.1.2 Application Layer Protocols) such as HTTPS, SSH and TLS secured protocols.
  See section 0 Intel AMT Network Protocols for lists of protocols used by the respective remote management solution.
- Strong passwords: Only use unique passwords with sufficient length and complexity to protect remotely manageable systems.
- Verified management applications: Only use management applications from verified and trustable sources.
- User authentication: Use standard authentication mechanisms to identify users of remote management administration PCs.

Section 5: Other Considerations

5.1 Government Agencies & Standards Organizations

Government agencies and international standards organizations may guide on creating and maintaining a robust security program, including how to securely deploy and use industrial control systems and related equipment. Below is a list of common standards and regulations to consider when designing a system's security policy and architecture. Such documentation, when appropriate, should be considered in addition to this document.

- ISA/IEC 62443 (formerly ISA99) for critical infrastructure
- T 800-53 for federal information systems
- ISO 27001 for information security management
- ISO 27002 for information security management
- ISO 27019 for information security management of electric systems
- NERC CIP V5 for critical infrastructure specific to electric systems
- NIST Cybersecurity Framework for critical infrastructure

Contact Information and Support Guide

Questions? We are here to help.

Try searching the Knowledge Base system on our Customer Center website before starting a case or picking up the phone.

Search our Knowledge Base	Open a Support Ticket	Register for a Customer Account
pacsystems.co/knowledge	pacsystems.co/support	pacsystems.co/signup

Customer Center Home Page	Commercial Website	Contact Information
pacsystems.co/customercenter	pacsystems.co/commercial	pacsystems.co/contactus

Note: If the product is purchased through an Authorized Channel Partner, please contact the seller directly for any support.

Emerson reserves the right to modify or improve the designs or specifications of the products mentioned in this manual at any time without notice. Emerson does not assume responsibility for the selection, use or maintenance of any product. Responsibility for proper selection, use and maintenance of any Emerson product remains solely with the purchaser.