SECURE DEPLOYMENT GUIDE

GFK-3200B

Oct 2021

PACSystems™ RXi2 Industrial PC

SECURE DEPLOYMENT GUIDE

EMERSON™

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 RXi2 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 RXi2 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
RXi2-LP	R2L0Nxxxx	RXi2-LP: 0 PCIe slot, with optional Windows 10 or PACEdge software packages
RXi2-BP	R2Bxxxxxxxxxx	RXi2-BP: 0-1 PCIe slot, with optional Windows 10, Movicon.NExT or PACEdge software packages
RXi2-XP	R2Xxxxxxxxxxx	RXi2-XP: 0-4 PCIe slot(s), with optional Windows 10 software package
RXi2-UP	R2Uxxxxxxxxxx	RXi2-UP: 0-4 PCIe slot(s), with optional Windows 10 or Movicon.NExT software packages

1.2 Product Landing Pages

Table 2: Landing Page Reference

Product	URL
RXi2-LP Landing Page	https://emerson-mas.force.com/communities/en_US/Article/RXi2-LP-Industrial-PC-Landing-Page
RXi2-BP Landing Page	https://emerson-mas.force.com/communities/en_US/Article/RXi2-BP-Industrial-PC-Landing-Page
RXi2-XP Landing Page	https://emerson-mas.force.com/communities/en_US/Documentation/RXi2-XP-Industrial-PC-IPC-Hardware-Reference-Manual-GFK-3022
RXi2-UP Landing Page	https://emerson-mas.force.com/communities/en_US/Article/RXi2-UP-Industrial-PC-Landing-Page

1.3 Revisions in this Manual

Table 3: Document Revision

Rev	Date	Description
B	Oct 2021	Adds support for PACEdge 2.1
A	Oct 2020	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 following location: https://www.emerson.com/Industrial-Automation-Controls/support.

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 protect 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.
7. On each Emerson product, change every supported password to something other than its default value.
8. Harden the configuration of each Emerson product, disabling unneeded features, protocols, and ports.
9. Test/qualify the system.
10. 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

In typical use cases, an Industrial PC is not a final product, but rather a platform for the final product to be built upon. Customers purchasing an Industrial PC will typically be adding their operating system of choice and then some application software on top of the operating system. With this in mind, the main burden of cybersecurity hardening will fall in the user's purview. Nevertheless, the software is only a part of the solution. Without a strong cybersecurity foundation that starts with the hardware and UEFI design, it is virtually impossible to build a solid security product. Emerson Industrial PCs have been designed from the ground up with cybersecurity in mind, and subsequent chapters within this document will guide how to enable and use the hardware and UEFI features that are available.

3.1 Physical Interfaces

All RXi2 Industrial PCs have the following physical data and communication interfaces.

3.1.1 Ethernet Interfaces

	RXi2-LP	RXi2-BP	RXi2-XP / RXi2-UP
Number/Type of Ethernet ports	2x 10/100/1000BASE-T	4x 10/100/1000BASE-T	5x 10/100/1000BASE-T
Support for remote management (Intel AMT or AMD Dash)	Not Available	Available, but disabled by default in UEFI	Available, but disabled by default in UEFI

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 control what protocols are enabled and what cybersecurity restrictions do apply.

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

Remote management functionality, such as Intel's AMT or AMD's DASH, allows access to the IPC via a dedicated Ethernet port **even when the IPC is in S5 power downstate**. Furthermore, this access path goes through a separate (from Operating System) TCP/IP protocol stack and needs to be carefully considered within the scope of cybersecurity. Please refer to section 4.3 Remote Management (DASH, Intel AMT) of this document for best practices.

This functionality is disabled in UEFI by default and can be enabled by the user after purchase. For details on how to enable the remote management functionality (DASH), please refer to GFK-3187, RXi2-BP Hardware Reference Manual.

3.1.2 Serial Interfaces

	RXi2-LP	RXi2-BP	RXi2-XP / RXi2-UP
Number/Type of Serial ports	1x RS232 1x RS422	1x RS232 1x RS422	2x – 4x mix of RS232, RS422

Operating systems and applications control which protocols are enabled and which cybersecurity restrictions apply.

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

3.1.3 USB Interfaces

	RXi2-LP	RXi2-BP	RXi2-XP / RXi2-UP
Number/Type of USB ports	2x USB	4x USB	4x USB

USB interfaces can be used for both communications, such as USB-Ethernet adapters, as well as for storage, such as a USB stick. Operating systems and applications control which protocols are enabled and which cybersecurity restrictions apply.

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

3.1.4 Non-Volatile Storage

	RXi2-LP	RXi2-BP	RXi2-XP / RXi2-UP
Internal Storage	1x 2.5’’ short form factor SSD	1x M.2 SSD	1x M.2 SSD
Externally Accessible Storage	uSD	uSD	CFast 2x RAID (on selected models)

Internal SSD is by default the main storage medium where the operating system and applications are installed. UEFI 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 apply.

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

3.1.5 DisplayPort Output

	RXi2-LP	RXi2-BP	RXi2-XP / RXi2-UP
Number/Type of DP ports	1x	1x	2x

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 Level Security Features

3.2.1 UEFI 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 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 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 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 (see above), which allows only trusted/signed Bootloaders to be executed by the UEFI. This prevents attackers from modifying or replacing bootloaders to load compromised operating systems. If activated, UEFI validates the signature attached to a bootloader using public keys embedded into UEFI. Customers can add their public keys to the UEFI key database and sign their bootloaders (e.g. Grub2) with the appropriate private key. As the Windows bootloader is already signed by Microsoft, the UEFI 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 settings.

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

Note: To protect against an attacker changing the Secure Boot settings in UEFI, the UEFI 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. 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.

RXi2 Industrial PC uses a CPU integrated TPM version 2.0. Measured Boot can be activated in the Security menu of the UEFI settings.

	RXi2-LP	RXi2-BP	RXi2-XP / RXi2-UP
TPM Implementation	TPM v2 Infineon Device	TPM v2 CPU-internal	TPM v2 Infineon Device

3.2.4 Secure Flash and UEFI Updates

To protect against UEFI modifications or tampered UEFI images, the UEFI 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 images.

It is recommended to periodically visit the RXi2 Industrial PC landing page to check for available security-related UEFI firmware updates. It is recommended to install the updates as soon as feasible.

3.2.5 UEFI Security Features Default States

Feature	Default State
UEFI Password	Not set
Secure Boot	Disabled
Measured Boot	Enabled
Secure Flash	Enabled
TPM v2 Device	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 key database. By default, the Microsoft key is already stored in the UEFI 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 key database.

3.3.2 Securing Operating Systems

Regarding Microsoft Windows, the Windows Boot Manager is responsible for checking windows NTOS 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 cybersecurity features.

3.4 Windows 10 Security Features

RXi2 Industrial PCs arrive with Windows 10 pre-installed from Emerson. Each IPC is pre-installed with Windows 10 IoT Enterprise 2019 LTSC that is updated with a Servicing Stack Update and a Cumulative Update.

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	Enabled	-
Remote Desktop Device Redirector Bus	Disabled	-
Autoplay for USB	Enabled	-
DEP (Data Execution Prevention)	Enabled	-
Windows Defender Firewall	Enabled	Incoming connections: block all incoming connections to apps that are not on the list of allowed apps

3.5 Movicon NExT Software Security Features

RXi2 Industrial PCs are optionally available with pre-installed Movicon.NExT software packages. The Movicon.NExT software is installed in the Windows operating system environment; therefore, please refer to the Windows 10 Security Features section in this document.

Movicon.NExT Software has undergone a formal cybersecurity evaluation, based on the IEC62443-3-3 specification. For details, please follow this link to the specification.

3.6 PACEdge Software Security Features

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

3.7 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. User is 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 4: Link Layer Protocols

Protocol	Ethernet Type
ARP	0x0806
LLDP	0x88cc

Table 5: Internet Layer Protocols

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

Table 6: 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	—

Depending on the remote management solution implemented by the system (AMD DASH vs. Intel AMT), different network ports are used by the remote management network interface.

Please note that both, AMD DASH and Intel AMT implement 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.

4.1.2.1 DASH Network Protocols

Protocol	TCP Port	UDP Port
DASH over HTTP [1] [2]	623	-
DASH over HTTPS [1] [3]	664	-
DASH Console Redirection over Telnet [1] [2] [4]	87	-
DASH Console Redirection over SSH [1] [3] [4]	57	-
DASH Mass Storage Redirection [1] [2] [4]	59	-

[1] TCP Port number refers to out-of-band DASH network interface on managed target system.

[2] Unencrypted and decodable network traffic

[3] Encrypted network traffic

[4] Non-standard port for this protocol

4.1.2.2 Intel AMT Network Protocols

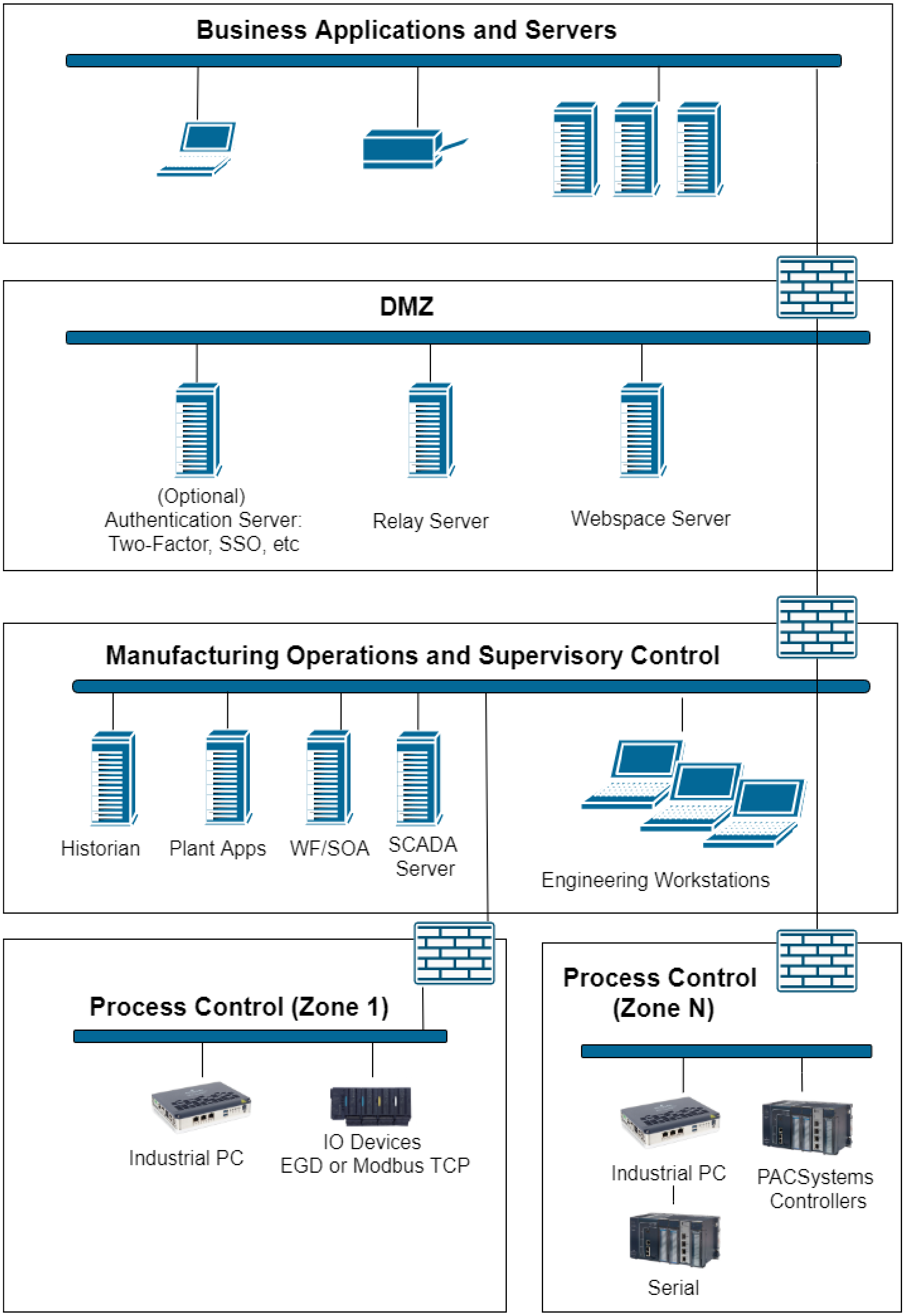
Protocol	TCP Port	UDP Port
Intel(R) AMT HTTP	16992	16992
Intel(R) AMT HTTPS	16993	16993
Intel(R) AMT Redirection/TCP	16994	16994
Intel(R) AMT Redirection/TLS	16995	16995
ASF Remote Management and Control Protocol (ASF-RMCP)	-	623
• TCP: DMTF out-of-band secure web services management protocol • UDP: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

Remote management enables a remote operator to perform actions like powering a system on/off, changing UEFI 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 sections 4.1.2.1 DASH Network Protocols for 4.1.2.2 Intel AMT Network Protocols 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

General Contact Information

Home link: http://www.emerson.com/industrial-automation-controls

Knowledge Base: https://www.emerson.com/industrial-automation-controls/support

Technical Support

Americas
Phone: 1-888-565-4155
1-434-214-8532 (If toll free option is unavailable)

Customer Care (Quotes/Orders/Returns): customercare.mas@emerson.com
Technical Support: support.mas@emerson.com

Europe
Phone: +800-4444-8001
+420-225-379-328 (If toll free option is unavailable)

Customer Care (Quotes/Orders/Returns): customercare.emea.mas@emerson.com
Technical Support: support.mas.emea@emerson.com

Asia
Phone: +86-400-842-8599
+65-6955-9413 (All other Countries)

Customer Care (Quotes/Orders/Returns): customercare.cn.mas@emerson.com
Technical Support: support.mas.apac@emerson.com

Any escalation request should be sent to mas.sfdcescalation@emerson.com

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.