PACSystems^{TM} IPC 2010 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 IPC 2010 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 2010	UIPCxxxxxxxxx	IPC 2010 Industrial PC with Linux OS and optional PACEdge software packages

1.2 Revisions in this Manual

Table 2: Document Revision

Rev	Date	Description
A	Sep 2023	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 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.
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 U-Boot features that are available.

3.1 Physical Interfaces

IPC 2010 Industrial PC has the following physical data and communication interfaces.

3.1.1 Ethernet Interfaces

	IPC 2010
Number/Type of Ethernet ports	2x 10/100/1000BASE-T

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.

3.1.2 Serial Interfaces

	IPC 2010
Number/Type of Serial ports	1x RS232

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

	IPC 2010
Number/Type of USB ports	2x USB 2.0

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

	IPC 2010
Internal Storage	eMMC SSD, Flash
Externally Accessible Storage	uSD

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

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

	IPC 2010
Number/Type of DP ports	1x DisplayPort

DisplayPort (DP) output is used to attach an external display. The use of the DP output is controlled by Operating System and is a user responsibility.

3.2 U-Boot Level Security Features

IPC 2010 is an open system where the user has full access to U-Boot. Features such as Hardware Root of Trust, signed U-Boot, U-Boot password, Secure Boot and Measured Boot, while available in the default platform, they are not enabled and would require product customization.

3.3 Ubuntu Linux Security Features

IPC 2010 Industrial PCs are available with pre-installed Ubuntu 20.04 LTS Operating System. Security hardening Linux installation, closing unused ports, configuring firewall, etc is outside the scope of this document and responsibility of the user.

3.4 PACEdge Software Security Features

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

3.5 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. The 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 typically used protocols from these three lower layers is summarized in the following tables. Note, for security reasons it is recommended to use secured protocols, such as HTTPS, and disable ports for unsecure protocols, such as FTP or HTTP.

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

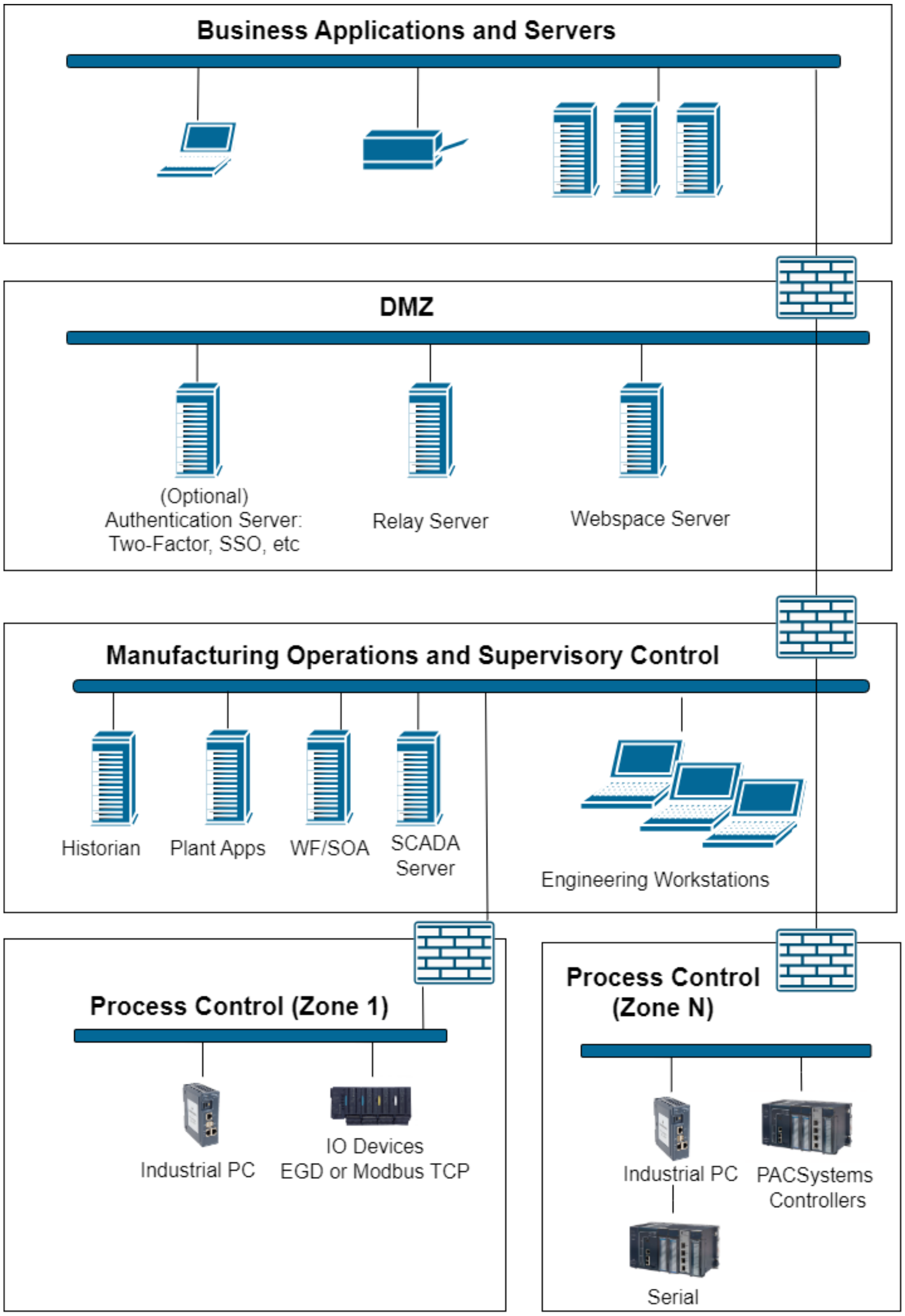
Protocol	Server TCP Port	Dest UDP Port
DCE/RPC	—	34964 on server >1023 on client
DNS	53	53 on server >1023 on client
Control – Warm Standby	12399	—
FTP	21	—
FTPS	990	—
HTTP	80	—
HTTPS	443	—
SNTP	—	123
SNMP	—	—
SSH	22	—

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.

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.