SECURE DEPLOYMENT GUIDE
GFK-3200A
Oct 2020

RXi2-BP 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 particular purpose.

Section 1: About this Guide

⚠CAUTION

Emerson provides these general recommendations and guidelines to aid the end-user in managing security risk associated with the operation of an Emerson RXi2-BP Industrial PC when used with pre-installed Windows or other, user-installed, operating systems. 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-BP Industrial PC hardware platform with the user-installed operating system, as well as RXi2-BP with Emerson pre-installed Windows OS. 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-BP no OS	R2B0NxNxxxxxx	RXi2-BP Core Software Installer
RXi2-BP with Windows	R2B0NxAxxxxxx	RXi2-BP, 1GHz/2C/AMD, 4GB RAM, 32GB SSD, 2xRJ45, Ubuntu Server 20.04 LTS w/ RXi2-BP, DIN mount

1.2 Related Documentation

This chapter provides information on related documents. These documents include product landing pages and related documents that contain additional information.

1.3 Product Landing Pages

Table 2: Landing Page Reference

Product	URL
RXi2-BP Landing Page	https://emerson-mas.force.com/communities/en_US/Article/RXi2-BP-Industrial-PC-Landing-Page

1.4 Other Documentation

Document ID	Document Title
00813-0100-0134	RXi2-BP Datasheet
GFK-3199	RXi2-BP Quick Start Guide
GFK-3187	RXi2-BP User's Manual

1.5 Revisions in this Manual

Table 3: Document Revision

Rev	Date	Description
A	Sep 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

Section 2 is intended to demonstrate?? Illustrate?? why it is important to cyber? secure Emerson products. It 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.

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 it 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 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 detailthe 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, a strategy based solely on any single security mechanism 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 the cost and complexity of a successful attack. To carry out a successful attack on a system, an attacker would need to find not only a single exploitable vulnerability but also multiple exploitable vulnerabilities in each layer of defense that protects an asset.

For example, if a system is protected because it is on a network protected by a firewall, the attacker would only 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.

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 on. Customers purchasing Industrial PC will typically be adding their operating system of choice and then application software. With this in mind, the main burden of cybersecurity hardening will fall in the customer's purview. Nevertheless, without a strong cybersecurity foundation that starts with 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 further chapters within this document will provide guidance on how to enable and use hardware and UEFI features that are available.

3.1 Physical Interfaces

RXi2-BP has the following physical data and communication interfaces.

3.1.1 Ethernet Interfaces

Four Ethernet ports, each supporting standard 10/100/1000BASE-T interfaces. Ethernet ports are fully accessible by the operating system and can be used for most standard OSI stack link 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.

DASH remote management functionality is currently not implemented.

3.1.2 Serial Interfaces

One RS232 and one RS422 serial interfaces are available. Serial port redirection is not implemented on these two ports. 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.

3.1.3 USB Interfaces

Four USB interfaces are available. 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 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.

3.1.4 microSD Storage

One microSD slot is available. Operating system and applications control access to it and what cybersecurity restrictions do apply

The user is responsible for configuring and restricting the use of this port.

3.1.5 M.2 SATA Storage

One M.2 SATA storage slot is available. This is the main storage medium for the RXi2-BP. Operating system and applications control access to it and what cybersecurity restrictions do apply

The user is responsible for configuring and restricting the use of this port.

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, which initializes and configures the hardware components of an IPC. The UEFI offers menus to modify hardware and firmware options. Since settings directly influence the 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 password., This password protection is not activated by default. Emerson strongly recommends taking advantage of an enabled password. You can change/activate the UEFI password by hitting the F2 button of an attached keyboard during boot and then select the Security menu and the Password Change entry.

3.2.2 Secure Boot

Secure Boot is an option 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 with the intention of loading compromised operating systems. If activated, UEFI validates a signature attached to a bootloader using public keys embedded into UEFI. Customers can add their own 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.

3.2.3 Measured Boot

Measured Boot is a technology that performs measurements of 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 software elements that were executed. Protective actions, such as sealing secrets and attestation, need to be additionally implemented to benefit the Measured Boot technology. For this product, it is the user's responsibility to consider, choose, and implement protective measures that are based on the Measured Boot.

RXi2-BP uses a CPU integrated TPM version 2. Measured Boot can be activated in the Security menu of the UEFI settings.

3.2.4 Secure Flash and UEFI Updates

To protect against UEFI modifications or tampered UEFI images, the UEFI image is signed and its signature is checked. Therefore, UEFI firmware update can only be done using Emerson authorized, and properly signed UEFI images.

It is recommended to periodically visit the RXI2-BP landing page to check whether security-related UEFI firmware updates are available, and to install the upgrades 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 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

The bootloader in its turn will start an operating system and is responsible for passing off the cybersecurity protection process to it. In the case of Microsoft Windows, Windows Boot Manager is responsible for checking windows NTOS kernel and drivers. Once Windows has booted, it loads 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 existing UEFI cybersecurity features.

3.4 Windows 10 Security Features

In the case of RXi2-BP with Emerson pre-installed Windows 10 IoT 2019 LTSC operating system, the following security-relevant features should be considered.

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 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, security hardening the RXi2-BP Industrial PC is only part of the overall Cybersecurity implementation strategy. The following information is deemed to be useful for further hardening the RXi2-BP device, 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 layer are 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

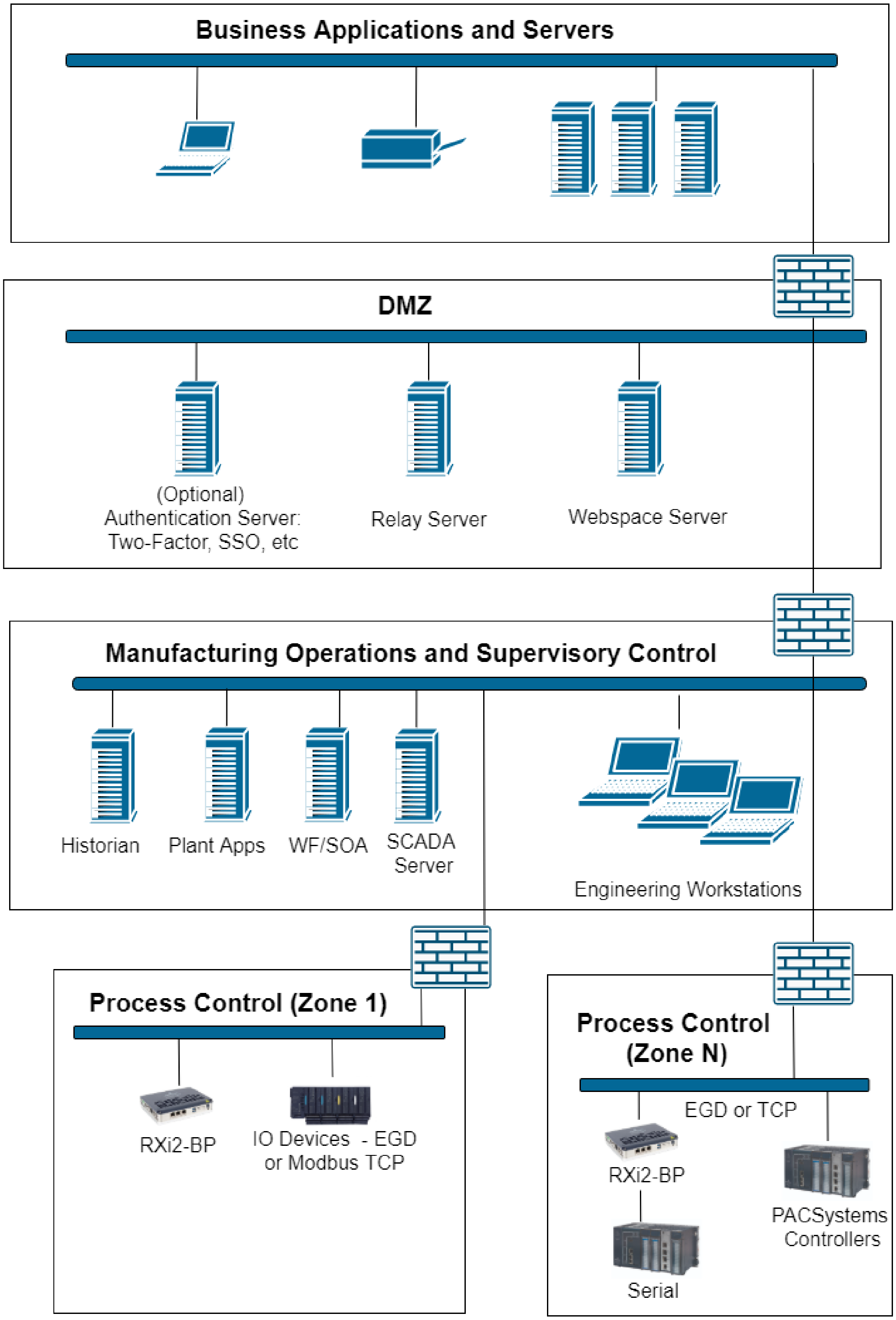
Protocol	Server TCP Port	Dest UDP Port
DCE/RPC	—	34964 on server >1023 on client
DNS	53	53 on server >1023 on client
Control – Warm Standby	12399	—
FTP	21	—
HTTP	80	—
SNTP	—	123
SNMP	—	—
SSH	22	—

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.