PACMotion™ Servo Motion

SECURE DEPLOYMENT GUIDE

EMERSON™

Contents

Section 1: About This Guide

This document provides information that can be used to help improve the cyber security of systems that include the PACMotion Servo systems. It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring the PACMotion Servo products.

The guide points out the unique protocols supported by the PMM345 module. Specifically, the EtherCAT communication protocol. The reader should note that the PMM345 is a module that is a member of the PACSystems RX3i family. Thus, the PACSystem Secure deployment guide (GFK-2830) should be consulted for methods to properly secure the overall RX3i based control system.

Secure deployment information is provided in this manual for the PACMotion Servo product family. An example catalog number is shown below for reference. Refer to *PACMotion Multi-Axis Motion Controller PMM345 User Manual*, GFK-3140 for further product details.

Example: IC830DP00306-NBEC		
Product name	IC830D	PACMotion PSD
Recommended motor power	P	Position
Connection voltage	003	003 = 3 Amps 006 = 6 Amps 012 = 12 Amps 024 = 24 Amps
Interference suppression on the input	06	06 = 120/240 VAC 1Phase/3Phase 07 = 240/480 VAC 3 Phase
Connection type	NB	NB = No Extensions
Design	EC	EC = EtherCAT

1.1 Revisions in this Manual

Rev	Date	Description
A	Aug 2020	• Initial Publication

1.2 Related Documentation

1.2.1 PACSystems Manuals

PACSystems RX3i and RSTi-EP CPU Reference Manual	GFK-2222
PACSystems RX3i and RSTi-EP CPU Programmer's Reference Manual	GFK-2950
PACSystems RX3i and RSTi-EP TCP/IP Ethernet Communications User Manual	GFK-2224
PACSystems TCP/IP Ethernet Communications Station Manager User Manual	GFK-2225
PAC Machine Edition Logic Developer Getting Started	GFK-1918
PAC Productivity Suite Getting Started Guide	GFK-2487
PACSystems RX3i & RSTi-EP PROFINET I/O Controller Manual	GFK-2571
C Programmer's Toolkit for PACSystems User Manual	GFK-2259
PACSystems Memory Xchange Modules User's Manual	GFK-2300
PACSystems Hot Standby CPU Redundancy User Manual	GFK-2308
PACSystems Battery and Energy Pack Manual	GFK-2741
PAC Machine Edition Logic Developer Getting Started	GFK-1918
PAC Process Systems Getting Started Guide	GFK-2487
PACSystems RXi, RX3i, and RSTi-EP Controller Secure Deployment Guide	GFK-2830

1.2.2 RX3i Manuals

PACSystems RX3i System Manual	GFK-2314
PACSystems RX3i PROFINET Scanner Manual	GFK-2737
PACSystems RX3i CEP PROFINET Scanner User Manual	GFK-2883
PACSystems RX3i Serial Communications Modules User's Manual	GFK-2460

1.2.3 PACMotion Manuals

PACMotion PMM335 to PMM345 Migration Guide	GFK-3135
PACMotion Multi-Axis Motion Controller PMM345 User Manual	GFK-3140
PACMotion PSD Installation and User Manual	GFK-3168
PACMotion PSR Installation and User Manual	GFK-3169
PACMotion PSD IMR	GFK-3171
PACMotion PSD Accessories Guide	GFK-3173
PACMotion PSR IMR	GFK-3175

1.2.4 Secure Deployment Guides

PROFINET I/O Devices Secure Deployment Guide	GFK-2904
PACSystems RXi, RX3i and RSTi-EP Controller Secure Deployment Guide	GFK-2830

Section 2: Introduction

This section introduces the fundamentals of security and secure deployment.

2.1 Security

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

Confidentiality: Ensure only the people you want to see information can see it.

Integrity: Ensure the data is what it is supposed to be.

Availability: Ensure 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.

Note: As Emerson product vulnerabilities are discovered and fixed, security advisories are issued to describe each vulnerability in a particular product version as well as the version in which the vulnerability was fixed. Emerson Product Security Advisories can be found at the following location: https://emerson-mas.force.com/communities/CC_Knowledge?q=security%20advisories

2.2 Firewall

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 Defense-in-Depth Strategy

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 just a single exploitable vulnerability, but would need to exploit 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 only needs to circumvent the firewall to gain unauthorized access. However, if there is an additional layer of defense, say a username/password authentication requirement, now the attacker needs 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.

- The devices covered in this document are not designed for or intended to be connected directly to any wide area network, including but not limited to a corporate network or the internet at large.
- Deploy and configure firewalls to limit the exposure of control system networks to other networks, including internal business networks and the Internet. If a control system requires external connectivity, care must be taken to control, limit and monitor all access, using, for example, virtual private networks (VPN) or Demilitarized Zone (DMZ) architectures.
- Harden system configurations by enabling/using the available security features, and by disabling unnecessary ports, services, functionality, and network file shares.
- Apply all of the latest Emerson product security updates, SIMs, and other recommendations.
- Apply all of 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 the PACMotion Servo 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 value.
5. Configure firewalls and other network security devices
6. Only utilize the PACMotion Workbench tool to PACMotion Servo Drive during commissioning and/or when making parameter changes. It is recommended to directly connect the PC to the PSD. Do not leave Workbench/Servo Drive connected once these activities complete.
7. When drive commissioning is complete, it is recommended to set the Servo Drive parameter FBUS.PROTECTION = 1. The parameter blocks Workbench/Service Port commands that would interfere with motion. Gain and I/O configuration changes are allowed with this parameter enabled.
8. Secure the PACMotion Servo Drive using mechanical means such as a control cabinet with limited access.
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. For more information about security programs in general, see section 6.5 Additional Guidance.

Section 3: Communication Requirements

Communication between different parts of a control system is, and must be, supported.

However, the security of a control system may be enhanced by limiting the protocols allowed and the paths across with which they are allowed, to only what is needed. This can be accomplished by disabling every communication protocol that is not needed on a particular device, and by using appropriately configured and deployed network security devices (for example, firewalls and routers) to block every protocol (whether disabled or not) that does not need to pass data from one network/segment to another.

Emerson recommends limiting the protocols allowed by the network infrastructure to the minimum set required for the intended application. Successfully limiting protocols requires knowing which protocol is needed for each system-level interaction.

This section describes how the supported serial and Ethernet application protocols are used with PACMotion Servo System and indicates the role of each participant in the communication. Lower-level Ethernet protocols are not discussed here, but are instead assumed to be supported when needed by the application protocol.

Note: This information is intended to be used to guide the specification of the network architecture and to help configure firewalls internal to that network, in order to support only the required communications paths for any particular installation.

3.1 Supported Protocols

3.1.1 Ethernet Protocols

	Protocol	PACMotion		
		PMM345	Servo Drive EtherCAT Port	Servo Drive Service Interface
Link	ARP			✓
	LLDP			✓
Internet	IPv4			✓
	ICMP			✓
Transport	TCP			✓
	UDP			
Application Layer	DHCP			✓
	EtherCAT Master	✓		
	EtherCAT Slave		✓	
	Telnet Server			✓

3.1.2 Serial Protocols

This section indicates which serial protocols are supported. Note that some of the supported protocols may not be required in a given system, since the installation may only be using a subset of the available protocols.

The PACMotion PSD and PMM345 module do not support any serial protocols.

Section 4: Secure Capabilities

This section describes the capabilities of the PACMotion Servo products and security features that can be used as part of a defense-in-depth strategy to secure your control system.

4.1 Capabilities by Product

This section provides a summary view of the security capabilities supported on each PACMotion PSD only. The PACSystems Controller provides extensive features in this area and the PACSystems™ RXi, RX3i and RSTi-EP Controller Secure Deployment Guide should be consulted (GFK-2830) for details.

Security Capability	Servo Drive
Encoded Login	No
Secure Login (SRP-6a)	No
Access Control List	No
Firmware Signatures	Yes

4.2 Access Control and Authorization

This section describes the Access Control capabilities supported by PSD network options which includes its Authorization capabilities.

The Access Control process can be divided into two phases:

1. Definition – Specifying the access rights for each subject (referred to as *Authorization*), and
2. Enforcement – Approving or rejecting access requests

4.2.1 Authorization Framework

Defining the access rights for each subject implies that the system must have some means to identify each subject. The usual way this is achieved is by assigning a unique User ID to each person who will access the system.

4.3 Authentication

Physical access should be used to protect a PACMotion Servo. For example, a locking control cabinet can be used to both limit access and provide a point of authorization. Note: PSD products currently do not support password locking servo drive parameters.

4.3.1 Summary

This section summarizes the authentication mechanisms supported by PACMotion Servo Drive (PSD) and the supported communications adapters.

Mode	Functionality	Application Protocol	Subjects Available
PSD Service Port	Firmware Update	TCP/IP	Access to Service Port via TCP/IP
	Parameter Update	TCP/IP	Access to Service Port via TCP/IP

4.4 Confidentiality and Integrity

PACMotion Servo firmware updates are signed and validated when loaded into the drive. PMM345 Firmware is signed with validation occurring when loaded via the RX3i CPU Controller.

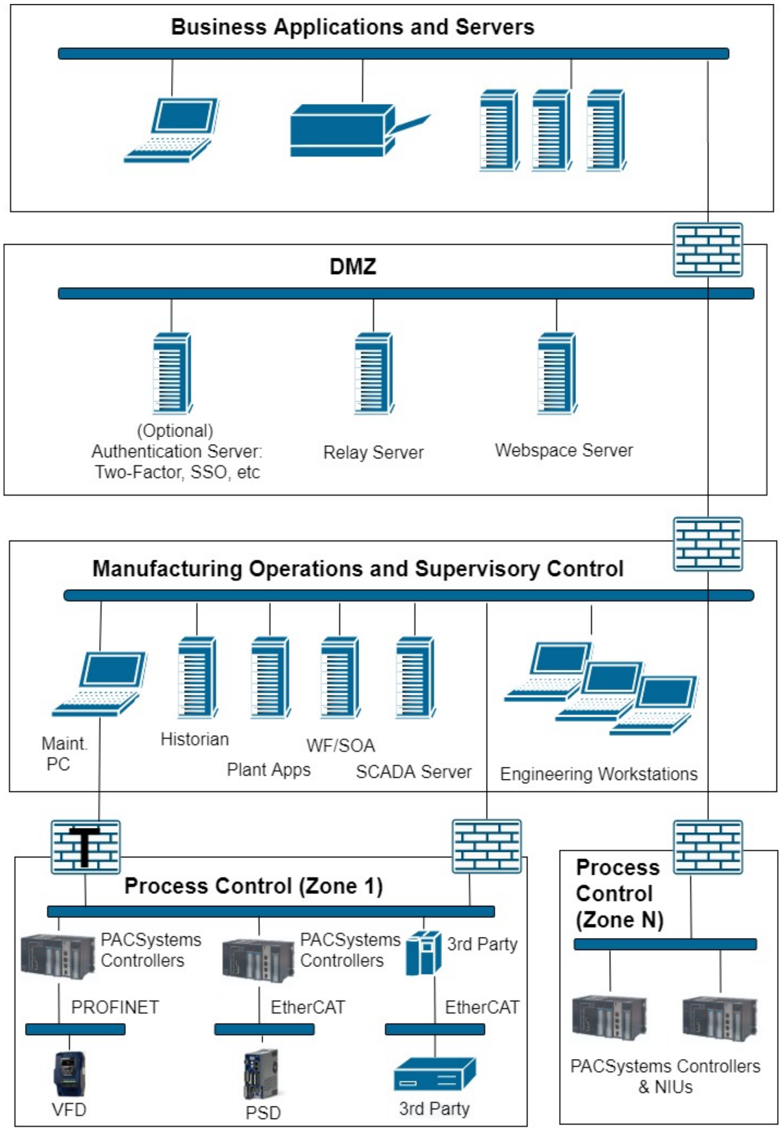
Section 5: Network Architecture and Secure Deployment

This section provides security recommendations for deploying PACMotion Servo products in the context of a larger network.

5.1 Reference Architecture

The following figure displays a reference deployment of PACMotion Servo products.

Figure 1: Network Architecture



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, as well as from other Process Control networks.

5.2 Remote Access and Demilitarized Zones (DMZ)

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 to a control network is required from the business network or from the internet, carefully control, 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 just 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.

5.3 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 does not need to be used between those regions, then the firewall should be configured to block that protocol. If, in addition to that, a controller does not have some other reason it needs to use that 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 of 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. Since communication to PACMotion PSD Service Port can occur from a PC on the “untrusted” side of the Process Control network firewall, protecting a Process Control network using a NAT firewall may cause additional communication challenges. Before deploying NAT, carefully consider its impact on the required communications paths.

Section 6: Other Considerations

6.1 Patch Management

A strategy for applying security fixes, including patches, firmware updates, and configuration changes, should be included in a facility's security plan. Applying these updates will require that an affected PACMotion PSD be temporarily taken out of service.

Finally, some installations require extensive qualification be performed before changes are deployed to the production environment. While this requirement is independent of security, ensuring the ability to promptly apply security fixes while minimizing downtime may drive the need for additional infrastructure to help with this qualification.

6.2 Real-Time Communication

When designing the network architecture, it is important to understand what impact the network protection devices (such as firewalls) will have on the real-time characteristics of the communications traffic that must pass through them. In particular, the EtherCAT network is expected to be on a separate network with no network traffic beyond EtherCAT contained within this network.

6.3 Denial-of-Service (DoS) due to Fuzzing

Fuzzing is a technique where an attacker sends invalid packet length, header values, invalid sequencing and data/payload to the device, which can cause the device to fail and preventing legitimate users from accessing or using the application.

It is recommended to use the firewall to protect the device from unauthorized access in general. The Service port is an Ethernet-based port and is recommended to not be connected to a network. For EtherCAT Networks, it is strongly recommended to only have EtherCAT devices connected to the network. In the PACMotion Servo system application the devices should be limited to the PMM345 and PACMotion PSD only.

6.4 Denial-of-Service (DoS) due to Storm

Storms determine the maximum rate at which the device can process packets, and also the device behavior after a DoS condition is reached. Attackers can storm the interface to a point that causes the device to fail; preventing legitimate users from accessing or using the application.

Most mid-range to high-end firewalls today have the capability to detect storms which originate from devices in a less-trusted security zone/network, and should be used to mitigate the effects of DoS attacks due to storms in general. The Service port is an Ethernet-based port and is recommended to not be connected to a network. For EtherCAT Networks, it is strongly recommended to only have

EtherCAT devices connected to the network. In the PACMotion Servo system application the devices should be limited to the PMM345 and PACMotion PSD only.

6.5 Additional Guidance

6.5.1 Protocol-Specific Guidance

Protocol standards bodies may publish guidance on how to securely deploy and use their protocols. Such documentation, when available, should be considered in addition to this document.

6.5.2 Government Agencies and Standards Organizations

Government agencies and international standards organizations may provide guidance on creating and maintaining a robust security program, including how to securely deploy and use Control Systems. For example, the U.S. Department of Homeland Security has published guidance on Secure Architecture Design and on Recommended Practices for cyber security with Control Systems. Such documentation, when appropriate, should be considered in addition to this document. Similarly, the International Society of Automation publishes the ISA-99 specifications to provide guidance on establishing and operating a cyber-security program, including recommended technologies for industrial automation and control systems.

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.

EMERSON™