Secure Deployment Guide
GFK-3166A
April 2020

PACMotion VFD

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 VFD. It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring the PACMotion VFD.

Secure deployment information is provided in this manual for the PACMotion VFD product family. An example catalog number is shown below for reference. Refer to *PACMotion Variable Speed Drives User Manual*, GFK-3042 for the PACMotion VFD Product Matrix and for further product details.

Example: IC866-0015-4B1-2P		
Product name	IC866	PACMotion VFD
Recommended motor power	0015	0015 = 1.5 kW
Connection voltage	4	2 = 200 – 240 V 4 = 380 – 480 V 6 = 500 – 600 V
Interference suppression on the input	B	0 = None A = Class C2 B = Class C1
Connection type	1	1 = 1-phase 3 = 3-phase
Design	2	2 = Standard IP20 housing 5 = IP55/NEMA-12K housing 6 = IP66/NEMA-4X housing
Option Card	P	P = Profinet RT (Standard) 0 = Empty (Purchase separately)
Country-specific variant	(60 Hz)	60 Hz design
Emerson HW/FW revision	- XXYY	XX = Hardware Revision YY = Firmware Revision

1.1 Revisions in this Manual

Rev	Date	Description
A	April 2020	• Initial Publication. Rebranded under Emerson guidelines. Replaces GFK-3029A.

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
PACSystems RX3i & RSTi-EP PROFINET I/O Controller Manual	GFK-2571

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 VFD Manuals

PACMotion Variable Frequency Drives User Guide	GFK-3111
PACMotion Variable Frequency Drives Advanced User Guide	GFK-3112

1.2.4 Secure Deployment Guides

PROFINET I/O Devices Secure Deployment Guide	GFK-2904
PACSystems RXi,RX3i,RX7i 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=emerson%20product%20security%20advisoriess [emerson-mas.force.com]

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

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 VFD.

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. (Parameters P2-40, P6-30).
5. Configure firewalls and other network security devices
6. Only utilize the Bluetooth Parameter Module during commissioning and/or when making parameter changes. Do not leave device plugged into VFD once these activities complete.
7. On each PACMOTION VFD, change all Extended Parameter Access Code Definition to something other than its default value. (Parameters P2-40, P6-30).
8. Only utilize the HMS tool “IP Config” with the PACMotion VFD Network card connected to the PC running the tool only. When using PROFINET, it is recommended to use the Proficy Machine Edition (PME) tool “PROFINET DCP” to assign device names and IP-addresses (if

required). The tool is accessed via the “Utilities” menu within PME. Reference user documentation for more information.

9. On each PACMotion VFD, lock parameter changes by setting Parameter P2-39 to “1:Locked” when placing a drive into service.
10. Save the drive parameters to a file via VFD Studio and archive this file as a backup.
11. Test / qualify the system.
12. 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 0,

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 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 (refer to chapter 5, Configuration Hardening), and by using appropriately configured and deployed network security devices (for example, firewalls and routers) to block every protocol (whether disabled or not) that doesn't need to pass 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 doing this requires knowing which protocol is needed for each system-level interaction.

This section describes how the supported serial and Ethernet application protocols are used and 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 help 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

This section indicates which Ethernet protocols are supported, and by which PACMotion VFD network adapter. 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.

	Protocol	PACMotion VFD	
		PROFINET Option: IC866-OC-P	Modbus TCP Option: IC866-OC-M
Link	ARP	✓	✓
	LLDP	✓	✓
Internet	IPv4	✓	✓
	ICMP	✓	✓
Trans	TCP	✓	✓
	UDP	✓	✓
Application Layer	DCE/RPC Client	✓	
	DCE/RPC Server	✓	
	PROFINET DCP Client		
	PROFINET DCP Server	✓	
	PROFINET I/O	✓	
	MRP	✓	
	SNMP v1 Server	✓	
	http	✓	
	Modbus TCP		✓

3.1.2 Serial Protocols

In addition to Ethernet, PACMotion VFD products also support communication over serial ports (RS-485). The information provided here should be used to help guide the specification of any external security controls required to restrict remote serial access, as well as the specification of any required physical security.

This section indicates which serial protocols are supported, and by which PACMotion VFD modules. 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.

Protocol	VFD Studio	Keypad: IC866-EKPD	Bluetooth Module: IC866-BLUE	Base VFD
RS-485	✓	✓	✓	✓
Modbus RTU				✓

3.2 PROFINET

This section describes the communication paths needed to support common operations on a PROFINET network.

3.2.1 Installing an IO Device

Commissioning, adding, or replacing an IO device requires that the device be assigned a unique name to use on the PROFINET network. Doing this requires supporting the following communication path.

Protocol	Proficy Machine Edition	IO device
PROFINET DCP	Client	Server

Supporting this communication path allows Proficy Machine Edition to directly discover all of the PROFINET IO devices that are connected to the same subnet as the PC. (Note that this protocol is not routable.) It can then be used to (re-)assign a unique name to the IO device being installed.[1]

[1] This protocol can also be used to make other modifications to the IO device, such as assigning a new IP address or resetting it to factory defaults. However, those functions are not generally required when "Installing an IO device".

3.2.2 Network Discovery and Device Identification

Proficy Machine Edition can also request information about the devices on a PROFINET network from a PACSystems Controller, and then retrieve additional identification information about each device. This request is sent to the PACSystems Controller using the Service Request protocol (described elsewhere) embedded within the SRTP or SNP protocols. The PACSystems Controller satisfies those requests using the following communication paths.

Protocol	Local IO controller	Remote IO controllers and IO devices
DCE/RPC	Client	Server
PROFINET DCP	Client	Server

Note: No mechanism is provided via this communication path for assigning a name to a new IO device.

3.2.3 Using an IO Device

Using PROFINET IO as part of the control application requires that all of the following communication paths be supported throughout the life of the application.

Protocol	IO controller	IO devices
DCE/RPC	Client	Server
PROFINET DCP	Client	Server
PROFINET IO	Bi-directional	Bi-directional

In addition, if the PROFINET network is configured to support Media Redundancy (MRP), which requires a ring physical topology, then the following application protocol must also be supported.

Protocol	IO controller	IO device
MRP	Bi-directional	Bi-directional

3.3 Modbus TCP

This section describes the communication paths needed to support common operations on a Modbus TCP network.

3.3.1 Installing an IO Device

Commissioning, adding, or replacing an IO device requires that the device be assigned a unique Ethernet IP address. For Modbus/TCP, this is done via the HMS ipconfig tool. This requires the usage on the PC of port 3250. Additionally, due to the broadcast nature of this tool, it is recommended that the user have a direct Ethernet connection to the device when setting the Ethernet IP address.

Protocol	Proficy Machine Edition	IO device
ICHP	ICHP	ICHP

3.3.2 Using an IO Device

Using Modbus TCP as part of the control application requires that all of the following communication paths be supported throughout the life of the application.

Protocol	IO controller	IO devices
Modbus TCP	Modbus TCP Client	Modbus TCP Server

Section 4: Secure Capabilities

This section describes the capabilities of the PACMotion VFD 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 VFD Ethernet based communication module.

Security Capability	PROFINET Option: IC866-OC-P
Predefined set of Subjects and Access Rights	Parameters: P2-40, P6-30 – Define Drive Parameter Access. P2-39 – Locks Drive Parameter Change
Encoded Login	No
Secure Login (SRP-6a)	No
Access Control List	No
Firmware Signatures	Yes

4.2 Access Control and Authorization

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

This section describes the Access Control capabilities supported by PACMotion VFD network option cards, which includes its Authorization capabilities.

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.

4.2.2 VFD Faceplate and PACMotion VFD Studio Parameter Access

PACMotion VFD provides codes to define which parameters are accessible from either the drive faceplate or PACMotion VFD Studio. The user configures access to advanced drive parameters via parameter P2-40 and P6-30. The parameters allow the user to define a numerical code that must be entered to gain access to advanced drive parameters. Additionally, the user can lock out all drive parameter changes via P2-39. It is recommended that parameter P2-39 be set prior to placing the VFD into service. Reference the PACMotion VFD User manual for additional information regarding these parameters.

4.2.3 Modbus TCP Parameter Access

The Modbus TCP interface allows the user access to read/write any drive parameter. Thus, it is recommended to limit access to this network and backup drive parameters via the "save to file" function within VFD Studio.

4.3 Authentication

The PACMotion VFD product allows the user to configure Drive Parameters (P2-40 & P6-30) to restrict access to advanced drive parameters via PACMotion VFD Studio or the VFD faceplate while also preventing any Drive Parameter changes (P2-39).

The Modbus TCP interface does not support authentication and allows access to all drive parameters

NOTE: The drive ships with default access codes for P2-40 and P2-65. It is recommended that the user changes these default values during commissioning.

4.3.1 Summary

This section summarizes the authentication mechanisms supported by PACMotion VFD and the supported communications adapters.

Mode	Functionality	Application Protocol	Subjects Available
RS-485	Firmware Update	Serial RS-485	Access to RS-485 Network
	Parameter Update	Serial RS-485	With parameters locked (P2-39) physical access to Drive required to unlock parameters

Mode	Functionality	Application Protocol	Subjects Available
Bluetooth	Firmware Update	Bluetooth	Access to Bluetooth Network Physical Access to Bluetooth Parameter Module required to Unlock Bluetooth Module.
	Parameter Update	Bluetooth	Access to Bluetooth Network Physical Access to Bluetooth Parameter Module required to Unlock Bluetooth Module. With parameters locked (P2-39) physical access to Drive required to unlock parameters.

4.4 Password Management

Emerson strongly recommends the use of long (12 characters or more), complex passwords wherever passwords are used for authentication. Whenever using a password scheme with a fixed maximum character length for passwords, Emerson recommends setting passwords to utilize the full character length available whenever possible in order to make it more difficult for attackers to crack passwords. Recommendations on password complexity and management can be found in the Guide to Enterprise Password Management, NIST 800-118.

PACMotion VFD currently only supports numerical codes for Extended Parameter Access. Thus, it is strongly recommended, when putting a drive into service, that parameter changes are locked out via the Parameter Access Lock (parameter P2-39). Unlocking this requires physical access to the drive or to the Modbus TCP network if utilized.

Access Mechanism/Utility	Authenticated Subjects	How Passwords are assigned
PACMotion VFD	Extended Parameter Access Code Definition (P2-40, P6-30)	During setup change from default

4.5 Confidentiality and Integrity

PACMotion VFD firmware updates are encrypted and validated when loaded into the VFD drive.

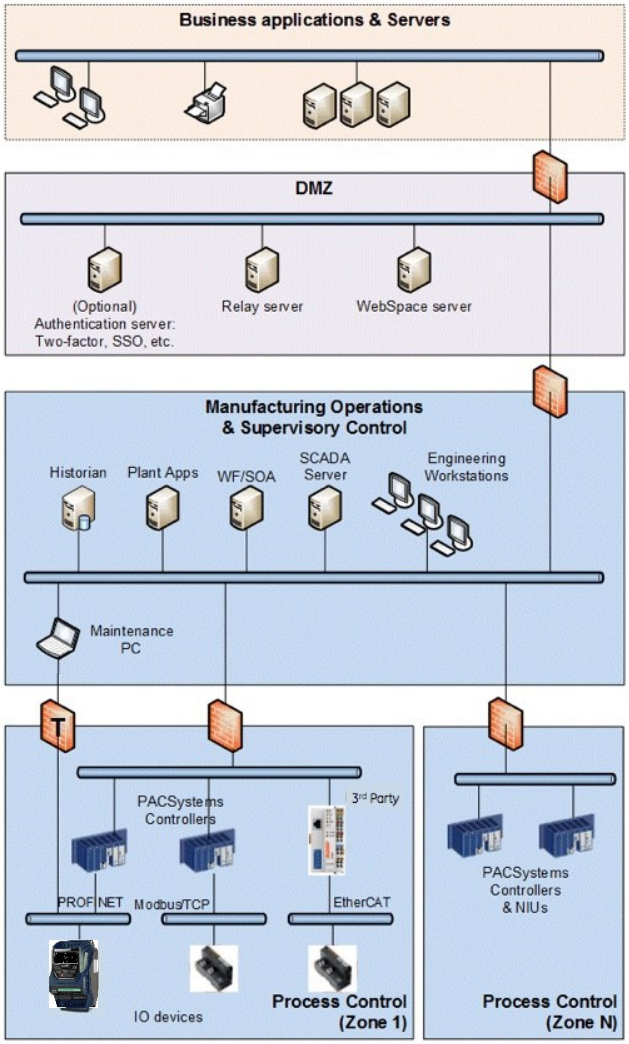
Section 5: Network Architecture and Secure Deployment

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

5.1 Reference Architecture

The following figure displays a reference deployment of PACMotion VFD.

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 (such as Modbus TCP) 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 VFD network adapters will typically be initiated 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 often require that an affected PACMotion VFD 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 PROFINET IO and Reliable Datagram Service protocols are generally expected to operate with small, known, worst-case bounds on their communications latency and jitter. As a result, network architectures that require real-time communications to pass through such devices may limit the applications that can be successfully deployed.

6.3 Denial of Service due to Fuzzing – PROFINET protocols

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.

6.4 Denial of Service due to Storm – PROFINET protocols

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 Denial of service attacks due to storms.

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