Secure Deployment Guide
GFK-2830Y
Jan 2020

PACSystems™ RXi, RX3i and RSTi-EP Controller Secure Deployment Guide

EMERSON.

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.

Contents

Table of Figures

Section 1: About this Guide

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

Secure deployment information is provided in this manual for the following PACSystems products:

Family	Catalog Number
RXi Controller	ICRXICTL000
RX3i CPU with embedded Ethernet Interface	IC695CPE302
	IC695CPE305
	IC695CPE310
	IC695CPE330
	IC695CPE400
	IC695CPL410
RX3i CPU	IC695CPU310
	IC695CPU315
	IC695CPU320
	IC695NIU001
	IC695NIU001+ versions –AAAA and later
RX3i Redundancy CPU	IC695CRU320
RX3i Ethernet Interface	IC695ETM001
	IC695EDS001
	IC695EIS001
RX3i PROFINET® Controller	IC695PNC001
RX3i IEC 61850 Ethernet Communication Module	IC695ECM850
RSTi-EP CPU with embedded Ethernet Interface	EPSCPE100
RSTi-EP CPU with embedded Ethernet Interface	EPSCPE115

1.1 Revisions in this Manual

Note: A given feature may not be implemented on all PACSystems Ethernet interfaces. To determine whether a feature is available on a given model and firmware version, please refer to the *Important Product Information* (IPI) document provided with the product.

Rev	Date	Description
Y	Feb 2020	Updates for CPE100/115 security capabilities, SNTP, and network bandwidth limiting.
X	Nov 2019	Updated to include DNP3 Protocol Support on CPE400/CPL410 and CPE115.
W	Aug 2019	Added ETM001-Kxxx and OPC UA Security Added Serial Protocols Support and Updated Security Capabilities of RSTi-EP Controllers.
V	Jul 2018	Added CPL410 Rackless CPU w/Linux
U	Apr 2018	Added CPE115 module
T	Feb 2018	Added CPE302, CPE400 Serial I/O support, and CPE330 / CPE400 firmware update password management.
S	Dec 2017	Added notes for IC695PNC001 versions -Ax and -Bxxx (Rx3i PROFINET IO Controller module).
R	Oct 2017	Updated to include CPE400 and Hot Standby Redundancy with PROFINET IO.
P	Aug 2017	Updated to include MRP support for RSTi-EP CPE100.
N	May 2017	Updated to include references to the RSTi-EP Standalone controller CPE100.
M	Apr 2017	Updated *Ethernet Protocols* to include SNTP for CPE305, CPE310, CPE330, and CPE400
L	Dec 2016	Updated multiple sections to include references to the CPE400.
K	Jun 2016	Updated section *PROFINET Controller Duplicate IP* to include IC695PNC001 in discussion.

Rev	Date	Description
J	May 2016	*Updated the table* *Supported Ethernet Protocols RXi and RX3i Modules for the IC695CPE330.* Added new sections: *OPC UA Server* *PROFINET Controller Duplicate IP* *MRP Ring Ethernet Traffic Storm Prevention*
H	Apr 2016	Added information for support of the IC695EDS001 and IC695EIS001 modules
G	Feb 2016	Updated password recommendations for Enhanced Security. Updated RX7i Modules table information
F	Dec 2015	Updated the information in the section *General Recommendations*.
E	Nov 2015	Added "OPC UA Server" as a supported protocol for some PACSystems CPUs. Encouraged the use of the Memory Protection Switch. Added recommendations for compensating controls when protocols are used with weak or no authentication. Added a reference equating the Reference Architecture to the Purdue Model. Added specific compensating controls for the RX7i ETM module and RXi.
D	Aug 2015	Updated information in the table, *Supported Ethernet Protocols RXi and RX3i Modules* for IC695CPE330 to include Ethernet Global Data.
C	Jun 2015	Updated information for IC695PNC001 and added second security-specific fault information.
B	Mar 2015	Added information for the support of the IC695CPE330 CPU.
A	Nov 2014	Added information for support of the IC695ECM850 module

Section 2: Introduction

This section introduces the fundamentals of security and secure deployment.

2.1 What is 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://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 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

The following security practices should be followed when using Emerson products and solutions.

The controllers and supervisory level computers covered in this document were 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. Additional routers and firewalls (such as those illustrated in Section 6.1, *Reference Architecture*) that have been configured with access rules customized to the site's specific needs must be used to access devices described in this document from outside the local control networks. If a control system requires external

- 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 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 PACSystems 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. (Refer to Section 3:Communication Requirements.)
4. Revise the network as needed to ensure appropriate partitioning, adding firewalls or other network security devices as appropriate. Update the network diagram. (Refer to Section 5.5 *DNP3 Outstation)*.
5. This section provides information to use when hardening the configuration of a DNP3 Outstation Protocol. Weigh these settings against the system’s requirements.
6. Configure firewalls and other network security devices. (Refer to Section 3.7, Ethernet Firewall Configuration and Section 5.5 *DNP3 Outstation).*
7. Enable and/or configure the appropriate security features on each PACSystems module. (Refer to Section 4: Security Capabilities.)
8. On each PACSystems module, change every supported password to something other than its default value. (Refer to Section 4.4: Password Management.)
9. Harden the configuration of each PACSystems module, disabling unneeded features, protocols and ports. (Refer to Section 5: Configuration Hardening.)
10. Test/qualify the system.
11. 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, refer to Section 7.5: *Additional Guidance*.

2.6 Related Documentation

Doc #	Title
GFK-2904	PROFINET I/O Devices Secure Deployment Guide
GFK-2993	Field Agents User Guide (with Secure Deployment information)
GFK-2222	PACSystems RX3i and RSTi-EP CPU Reference Manual
GFK-2223	PACSystems Installation Manual
GFK-2224	PACSystems RX3i and RSTi-EP TCP/IP Ethernet Communications User Manual
GFK-2225	PACSystems TCP/IP Ethernet Communications Station Manager User Manual
GFK-2571	PACSystems RX3i PROFINET Controller Manual
GFK-2572	PACSystems RX3i PROFINET Controller Command Line Interface Manual
GFK–2849	PACSystems RX3i IEC 61850 Ethernet Communication Module
GFK-2911	PACSystems RX3i DNP3 Outstation Module User's Manual
GFK-2314	PACSystems RX3i System Manual
GFK-2949	PACSystems RX3i IEC 104 Server Module IC695EIS001 User's Manual
GFK-2439	PACSystems RX3i Ethernet Network Interface Unit User's Manual
GFK-2950	PACSystems RX3i and RSTi-EP CPU Programmer's Reference Manual
GFK-2958	RSTi-EP User Manual
GFK-2816	PACSystems RXi Distributed I/O Controller User Manual
GFK-2849	PACSystems RX3i IEC 61850 Ethernet Communication Module User Manual
GFK-3002	PACSystems RX3i IC695CPE400 1.2GHz 64MB Rackless CPU w/Field Agent Quick Start Guide
GFK-3053	PACSystems RX3i IC695CPL410 1.2GHz 64MB Rackless CPU w/Linux Quick Start Guide
GFK-3055	PACSystems Controllers with Linux Secure Deployment Guide

Note that users of IC695CPL410 will need to consult the *PACSystems Controllers with Linux Secure Deployment Guide*, GFK-3055, as well as this guide.

In addition to these manuals, datasheets and Important Product Information documents describe individual modules and product revisions. The most recent PACSystems documentation is available online on the Support website. Please see the support link provided at the end of this document.

Section 3: Communication Requirements

Communication between different parts of a control system is, and must be, supported. However, the security of a control system can 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 isn't needed on a particular device (refer to Section 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.

We recommend 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 with PACSystems 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. (For example, in order to support SRTP communication between two nodes, the network must also support TCP, IP, and ARP in both directions between the nodes.)

Note that on a PACSystems node such as the RX3i, support for these protocols may be provided by a peripheral module (for example, IC695ETM001, IC695PNC001, or IC695ECM850) or by an interface that is embedded in the CPU/NIU module.

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 Protocols Supported

3.1.1 Ethernet Protocols

This section indicates which Ethernet protocols are supported, and by which PACSystems 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.

3.1.1.1 Supported Ethernet Protocols RXi and RX3i Modules

	Protocol	RXi	RX3i										
		ICRX ICTL000	IC695 CPE302	IC695 CPE305	IC695 CPE310	IC695 CPE330	IC695 CPE400	IC695 CPL410	IC695 ETM001	IC695 EDS001	IC695 EIS001	IC695 PNC001	IC695 ECM850
Link	ARP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	LLDP	✓				✓	✓	✓				✓	
Internet	IPv4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	ICMP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	IGMP	✓							✓	✓	✓		
Trans	TCP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	UDP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application Layer	BOOTP Client								✓[1]	✓	✓		
	DCE/RPC Client	✓				✓	✓	✓				✓	
	DNS Client								✓[1]	✓	✓		
	Ethernet Global Data		✓	✓	✓	✓	✓	✓	✓	✓	✓		
	FTP Server								✓[1]	✓	✓		
	HTTP Server	✓				✓	✓	✓					
	HTTPS Server					✓	✓	✓					
	Modbus® TCP Master	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
	Modbus TCP Slave	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
	OPC UA Server	✓	✓	✓	✓	✓	✓	✓					
	PROFINET DCP Client	✓				✓	✓	✓				✓	
	PROFINET DCP Server	✓				✓	✓	✓				✓	
	PROFINET I/O	✓				✓	✓	✓				✓	

[1] Not supported by IC695ETM001-Kxxx.

	Protocol	RXi	RX3i										
		ICRX ICTL000	IC695 CPE302	IC695 CPE305	IC695 CPE310	IC695 CPE330	IC695 CPE400	IC695 CPL410	IC695 ETM001	IC695 EDS001	IC695 EIS001	IC695 PNC001	IC695 ECM850
	IEC 61850 Client												✓
	DNP3 Outstation						✓	✓		✓			
	IEC 60870-5-104 Server										✓		
	MRP	✓				✓	✓	✓				✓	
	Reliable Datagram Client								✓	✓	✓		
	Reliable Datagram Server								✓	✓	✓		
	Remote Station Mgr Client								✓	✓	✓		
	Remote Station Mgr Server	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
	Set Temporary IP Server					✓	✓	✓	✓[1]	✓	✓		
	SNMP v2c Server	✓				✓	✓	✓				✓	✓
	SNTP Client		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
	SRTP Client	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
	SRTP Server	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
	Telnet Server											✓[2]	
	HSB Redundancy Link						✓	✓					

[2] Supported by IC695PNC001-Ax only. Not supported by IC695PNC001-Bxxx.

3.1.1.2 Supported Ethernet Protocols RSTi-EP Modules

	Protocol	RSTi-EP	
		EPS CPE100	EPS CPE115
Link	ARP	✓	✓
	LLDP	✓	✓
Internet	IPv4	✓	✓
	ICMP	✓	✓
	IGMP		
Trans	TCP	✓	✓
	UDP	✓	✓
Application Layer	BOOTP Client		
	DCE/RPC Client	✓	✓
	DNS Client		
	Ethernet Global Data	✓	✓
	FTP Server		
	HTTP Server	✓	✓
	Modbus® TCP Master	✓	✓
	Modbus TCP Slave	✓	✓
	OPC UA Server	✓	✓
	PROFINET DCP Client	✓	✓
	PROFINET DCP Server	✓	✓
	PROFINET I/O	✓	✓
	IEC 61850 Client		
	DNP3 Outstation		✓
	IEC 60870-5-104 Server		
	MRP	✓	✓
	Reliable Datagram Client		
	Reliable Datagram Server		
	Remote Station Mgr Client		
	Remote Station Mgr Server	✓	✓
	Set Temporary IP Server		
	SNMP v2c Server	✓	✓
	SNTP Client		✓
	SRTP Client	✓	✓
	SRTP Server	✓	✓
	Telnet Server		

3.1.2 Serial Protocols

In addition to Ethernet, many PACSystems products[3] also support communication over serial ports (RS-232, RS-485, and/or USB). 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 PACSystems 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.

3.1.2.1 PACSystems RX3i Modules

Protocol	IC695 CPE 302	IC695 CPE 305	IC695 CPE 310	IC695 CPU 310	IC695 CPU 315	IC695 CPU 320	IC695 CRU 320	IC695 CPE 330	IC695 CPE 400	IC695 CPL 410	IC695 ETM 001	IC695 EDS 001	IC695 EIS 001	IC695 NIU 001	IC695 NIU 001+	IC695 PNC 001	IC695 ECM 850
Application -specific[4]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							
ASCII Terminal											✓[1]	✓	✓			✓[2]	✓
Modbus RTU Slave	✓	✓	✓	✓	✓	✓	✓							✓	✓		
SNP Slave	✓	✓	✓	✓	✓	✓	✓							✓	✓		

3.1.2.2 PACSystems RSTi-EP Modules

Protocol	EPSCPE100	EPSCPE115
Application- specific[4]	✓	✓
ASCII Terminal		
Modbus RTU Slave	✓	✓
SNP Slave		

[3] RSTi-EP Controllers supports serial communications from release 9.85 or later.

[4] Some modules can be configured so that one or more of their serial ports is controlled by the user application program that is executing on the controller. Such “Application-specific” protocols are outside of the scope of this document and will not be discussed further.

3.2 Service Requests

The PACSystems Service Request protocol is a proprietary, media-independent application protocol that provides access to all of the services supported by the PACSystems Controller. This is the primary protocol used by PAC Machine Edition: Logic Developer – PLC when communicating with a PACSystems CPU. It supports many different operations, including:

- Upload/Download the user application and configuration to the Controller
- Start/Stop the Controller
- Read, write, verify, or clear Flash/EEPROM memory
- Clear Controller memory
- Gather diagnostic info from a Controller
- Verify Equality
- View and, in some cases, set the target Controller's operating parameters: device information, memory usage, date and time, reference points/words, access levels, passwords and OEM key, and sweep information
- View and optionally clear a log of any faults that have occurred in the Controller

The Service Request protocol is transported over a specific media by encapsulating it within a media-specific protocol. Specifically, SRTP is used for transporting it over an Ethernet network and SNP is used for transporting it over a serial channel. Almost all SRTP and SNP transmissions contain at least a portion of a Service Request/Reply embedded within them.

Supporting communication between any two nodes using Service Requests requires that the system support communicating using either SRTP or SNP between those two nodes.

3.2.1 SRTP

SRTP is used to send Service Requests to a Controller through an Ethernet network, and to convey the results back to the client. PACSystems can be both an SRTP Server (processing service requests) and an SRTP Client (sending service requests).

3.2.1.1.1 SRTP Server

SRTP Server functionality is enabled at all times on the modules that support this protocol.

3.2.1.1.2 SRTP Channels

The SRTP Channels feature allows a PACSystems controller to behave as an SRTP Client, sending a limited selection of Service Requests to other SRTP Servers. The user application running on the controller dictates which requests to send (if any) and where to send them.

3.2.2 SNP

SNP is used to send Service Requests to a Controller through a serial connection, and to convey the results back to the client. Support for SNP Slave functionality is enabled whenever a PACSystems Controller's serial port is configured to support either SNP

Slave or Modbus RTU Slave. This is because the Controller's serial ports will auto-switch from Modbus RTU mode to SNP mode when an SNP packet is received.

3.2.2.1.1 Firmware Update

The SNP protocol is also used to support updating the firmware on the PACSystems Controller or on any installed module that supports having its firmware updated over the backplane. This is accomplished through the use of Service Requests that are only supported when received through a serial port. Firmware updates are not supported over Ethernet using the SRTP protocol.

Protocol	WinLoader.exe (Windows® OS)	PACSystems
SNP	Master	Slave

3.3 Server

This section summarizes the available communication-centric functionality, where the communication is initiated by some other device or computer.

Functionality		Required Application Protocols	Example Clients
Ethernet	Service Requests	SRTP	PAC Machine Edition HMI Other controllers
	EGD Consumption	Ethernet Global Data[5]	Other controllers
	Process EGD Commands	Reliable Datagram Svc	Other controllers
	Modbus TCP Slave	Modbus TCP	HMI Other controllers 3rd-party Masters
	Ethernet Station Manager	Remote Station Mgr	stamgr24.exe on computer Other Ethernet interface

[5] This is one-way communication, from client to server. No response is provided from the server back to the client. However, a single PACSystems controller can be both a client and a server.

Functionality		Required Application Protocols	Example Clients
	OPC UA Server	OPC UA	UaExpert
	PROFINET Controller command shell	Telnet	telnet.exe on computer
	DNP3 Outstation or Server	DNP3	DNP3 Master or Client
	IEC 60870-5-104 Server or Slave	IEC 60870-5-104	IEC 104 Master or Client
	Web Server	HTTP, HTTPS	Web browser
	Update Web Pages	FTP	ftp.exe on computer
	Network Management	SNMP v2c	SNMP client on computer
	Assign IP before configuring module	Set Temporary IP	PAC Machine Edition
Serial	Service Requests	SNP Slave	PAC Machine Edition HMI Other controllers
	Firmware Update	SNP Slave	WinLoader.exe on computer
	Modbus RTU Slave	Modbus RTU	HMI Other controllers 3rd-party Masters
	Serial Station Manager	ASCII Terminal	Terminal emulator on computer
	PROFINET Controller command shell	ASCII Terminal	Terminal emulator on computer
	ECM850 command shell	ASCII Terminal	Terminal emulator on computer

3.4 Client

This section summarizes the available communication-centric functionality, where the communication is initiated by the PACSystems controller. The servers involved in these communications are selected by the user application and/or configuration.

Functionality		Required Application Protocols	Example Servers
Ethernet	SRTP Channels	SRTP	Other controllers
	Modbus TCP Channels	Modbus TCP	3rd-party device Other controllers

Functionality		Required Application Protocols	Example Servers
	EGD Production	Ethernet Global Data[5]	Other controllers
	Send EGD Commands	Reliable Datagram Svc	Other controllers
	Ethernet Station Manager	Remote Station Mgr	Other Ethernet interface
	Time Synchronization	SNTP	SNTP server
	Assign IP addresses using a centralized database of addresses	BOOTP	BOOTP server
	Lookup IP addresses by Name	DNS	DNS server
	IEC 61850 Client	IEC 61850 Client	Other IEC 61850 Servers

3.5 PROFINET

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

3.5.1 Installing an I/O Device

Commissioning, adding, or replacing an I/O 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	PAC Machine Edition	I/O device
PROFINET DCP	Client	Server

Supporting this path will allow PAC Machine Edition to directly discover all of the PROFINET I/O devices that are connected to the same subnet as the computer. (Note that this protocol is not routable.) It can then be used to (re-) assign a unique name to the I/O device being installed.

Note: This protocol can also be used to make other modifications to the I/O device, such as assigning a new IP address or resetting it to factory defaults. However, those functions are not generally required when installing an I/O device.

3.5.2 Network Discovery & Device Identification

PAC 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 I/O controller	Remote I/O controllers
DCE/RPC	Client	Server
PROFINET DCP	Client	Server

Note that no mechanism is provided through this communication path for assigning a name to a new I/O device.

3.5.3 Using an I/O device

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

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

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

Protocol	I/O controller	I/O device
MRP	Bi-directional	Bi-directional

3.6 IEC 61850

This section describes the communication paths needed to support common operations on an IEC 61850 network.

IEC 61850 is a global standard for use in utility communication, in particular for the information exchange between IEDs (Intelligent Electronic Devices) in a power transmission or distribution substation.

3.6.1 Installing an IED –Intelligent Electronic Device (IEC 61850 Server)

Commissioning, adding, or replacing an IED requires that the device be available on the IEC 61850 network so that the Integrated IEC 61850 Configurator in PAC Machine Edition can directly read the IEC 61850 Object model from the remote device. Doing this requires supporting the following communication path:

Protocol	PAC Machine Edition	IED
IEC 61850 (MMS – Self Description)	Client	Server

Supporting this path allows PAC Machine Edition to directly discover or read the IEC 61850 object data model from an IED that is connected to the same subnet as the computer. The data model read is used by the configurator to select objects or variables for monitoring and control.

3.6.2 Using an IED

Using IED's objects as part of the control application requires that all of the following communication paths be supported throughout the life of the application.

Protocol	Local communication module (e.g. ECM850)	IED(s)
IEC 61850	Client	Server

3.7 Ethernet Firewall Configuration

Network-based and host-based firewalls should be configured to only allow expected and required network traffic. This section identifies the EtherTypes and the TCP/UDP ports used by the protocols supported on PACSystems products.

This information should be used to help configure network firewalls, in order to support only the required communications paths for any particular installation.

3.7.1 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 here.

3.7.1.1 Link Layer Protocols

Protocol	EtherType
ARP	0x0806
LLDP	0x88cc

3.7.1.2 Internet Layer Protocols

Protocol	EtherType	IP Protocol #
IPv4	0x0800	(n/a)
ICMP	0x0800	1
IGMP	0x0800	2

3.7.1.3 Transport Layer Protocols

Protocol	EtherType	IP Protocol #
TCP	0x0800	6
UDP	0x0800	17

Each of these lower-level protocols is required by one or more of the Application protocols supported on the PACSystems family of products.

3.7.2 Application Layer Protocols

PACSystems devices are capable of acting as a server, responding to requests sent through any of several different protocols. They are also capable of acting as a client, sending requests to other servers using any of several different protocols. The exact set of protocols that are enabled/used will depend on which modules are installed, how they are configured, and the details of the application program that is running on the CPU.

Protocol	Server TCP Port	Dest UDP Port	EtherType (non-IP protocol)
BOOTP		67 on server 68 on client	
DCE/RPC		34964 on server >1023 on client	
DNS	53	53 on server >1023 on client	
Ethernet Global Data		18246	
FTP	20, 21		
HTTP	80		
HTTPS	443		
Modbus TCP	502		
OPC UA	4840		
PROFINET DCP			0x8892
PROFINET I/O			0x8892
MRP			0x88e3
Reliable Datagram Svc		7937 on server >1023 on client	
Remote Station Mgr		18245	
SNMP v2c		161 on server >1023 on client	
SNTP		123	
SRTP	18245		

Protocol	Server TCP Port	Dest UDP Port	EtherType (non-IP protocol)
Telnet	23		
Set Temporary IP	1		
IEC 61850 Client	102		
DNP3 Outstation	20000[6]		
IEC 60870-5-104 Server	2404[7]		

[6] The Port number for DNP3 outstation by convention is 20000. For module IC695EDS001, If the SoE (Sequence of Event) feature is enabled in the configuration, then port number 20001 will also be opened for transmitting buffered event data to the Master. However, it should be noted that this port number can be configured to any number desired through a special COMMREQ block (say X), in which case the port number (X+1) will be opened for SOE connection if SOE is enabled in the configuration. Refer to the *PACSystems RX3i DNP3 Outstation Module User's Manual*, GFK-2911 for details of such configuration.

For Controller IC695CPE400/CPL410, the Port number for DNP3 outstation can be configured to any desired number through Hardware Configurator in the PAC Machine Edition. Note that the Controller uses the same Port number for both the SoE (Sequence of Events) & Most recent Event Report transfers.

[7] The Port number for IEC 60870-5-104 server by convention is 2404. In a typical case of Multiple Client configuration, there can be multiple connections with different port numbers opened as (2404+i), where i=0 to Number of Client connections configured-1. If the number of client connections is configured as 4, then the connections with port numbers 2404,2405,2406,2407 will be opened. However, it should be noted that this port number can be configured to any number desired through a special COMMREQ block (say X), in which case the port numbers (X to X+i where i = Number of Client connections-1) will be opened for Multiple Client configuration for a typical case. Refer to the *PACSystems RX3i IEC 104 Server Module IC695EIS001 User's Manual,* GFK-2949 for details of such configurations.

Section 4: Security Capabilities

This section describes the PACSystems capabilities and security features which 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 PACSystems module.

4.1.1 PACSystems RXi modules

Security Capability	ICRXICTL000
Predefined set of Subjects & Access Rights	✓
Plaintext Login	✓
Secure Login (SRP-6a)	✓
Access Control List	✓
Firmware Signatures	✓
Internal Firewall	✓

4.1.2 PACSystems RX3i Modules

Security Capability	IC695 CPE 302	IC695 CPE 305	IC695 CPE 310	IC695 CPU 310	IC695 CPU 315	IC695 CPU 320	IC695 CRU 320	IC695 CPE 330	IC695 CPE 400	IC695 CPL 410	IC695 ETM 001	IC695 EDS 001	IC695 EIS 001	IC695 NIU 001	IC695 NIU 001+	IC695 PNC 001	IC695 ECM 850
Predefined set of Subjects & Access Rights	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Plaintext Login	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓[2]	✓
Secure Login (SRP-6a)	✓	✓	✓		✓	✓	✓	✓	✓	✓					✓		
Access Control List	✓	✓	✓		✓	✓	✓	✓	✓	✓					✓		

Security Capability	IC695 CPE 302	IC695 CPE 305	IC695 CPE 310	IC695 CPU 310	IC695 CPU 315	IC695 CPU 320	IC695 CRU 320	IC695 CPE 330	IC695 CPE 400	IC695 CPL 410	IC695 ETM 001	IC695 EDS 001	IC695 EIS 001	IC695 NIU 001	IC695 NIU 001+	IC695 PNC 001	IC695 ECM 850
Firmware Signatures								✓	✓	✓	✓[8]					✓[9]	✓[10]
Secure Boot									✓	✓							
Internal Firewall								✓	✓	✓	✓[8]					✓[9]	

4.1.3 PACSystems RSTi-EP Modules

Security Capability	EPSCPE100	EPSCPE115
Predefined set of Subjects & Access Rights	✓	✓
Plaintext Login	✓	✓
Secure Login (SRP-6a)	✓	✓
Access Control List	✓	✓
Firmware Signatures	✓	✓
Secure Boot		
Verified Boot	✓	✓
Internal Firewall	✓	✓

[8] Supported by IC695ETM001-Kxxx only. Not supported by IC695ETM001-Jx.

[9] Supported by IC695PNC-Bxxx only. Not supported by IC695PNC001-Ax.

[10] Secure Firmware upgrade supported via RX3i Controllers using WinLoader.

4.2 Access Control and Authorization

The Access Control process can be divided into two phases:

Definition – Specifying the access rights for each subject (referred to as Authorization), and

Enforcement – Approving or rejecting access requests.

This section describes the Access Control capabilities supported by PACSystems, 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 most familiar way this is achieved is by assigning a unique User ID to each person who will access the system.

PACSystems, however, doesn't provide such a facility – there is no support for creating User IDs. In many cases, a User ID doesn't even have to be specified to authenticate. In such cases, authorization is based on the functionality being used and the password that is provided for authentication. Never-the-less, the authentication features supported on PACSystems implicitly define a fixed set of subjects, which are identified here.

The set of implicitly defined subjects will vary depending on the server protocols that are supported, which depends on what modules are installed and how they are configured. Each kind of server has its own set of predefined subjects – there are no subjects that apply across multiple servers (other than *anonymous*). Further, each instance of a server has its own instances of the predefined subjects – access rights for each subject must be separately managed for each instance of a given kind of server.

For example, each PACSystems controller acts as a Service Request server. Therefore, access rights for each PACSystems controller in the system must be independently managed. Similarly, each Ethernet Interface supports the Ethernet Station Manager server. Therefore, access rights for each Ethernet Interface must be individually managed – even when multiple Ethernet Interface modules are located in a single rack, providing service to a single PACSystems controller.

The subjects defined and supported by each server protocol are indicated in the following table.

Functionality		Application Protocol	Subjects Available
Ethernet	Service Requests	SRTP	Anonymous PRIV Level 1 user PRIV Level 2 user PRIV Level 3 user PRIV Level 4 user OEM user
	EGD Consumption	Ethernet Global Data	Anonymous
	Process EGD Commands	Reliable Datagram Svc	Anonymous
	Modbus TCP Slave	Modbus TCP	Anonymous
	Ethernet Station Manager	Remote Station Mgr	Anonymous STA Modify-level user
	OPC UA Server	OPC UA	Anonymous PRIV Level 2 user PRIV Level 3 user PRIV Level 4 user
	DNP3 Outstation or Server	DNP3	Anonymous
	IEC 60870-5-104 Server or Slave	IEC 60870-5-104	Anonymous
	PROFINET Controller command shell	Telnet [2]	Anonymous PNC admin
	Web Server	HTTP, HTTPS	Anonymous
	Update Web Pages	FTP	FTP user
	Network Management	SNMP v2c	Anonymous
	Assign IP before configuring module	Set Temporary IP	Anonymous
Serial	Service Requests	SNP Slave	Anonymous PRIV Level 1 user PRIV Level 2 user PRIV Level 3 user PRIV Level 4 user OEM user
	Firmware Update	SNP Slave	Anonymous
	Modbus RTU Slave	Modbus RTU	Anonymous
	Serial Station Manager	ASCII Terminal	Anonymous STA Modify-level user
	PROFINET Controller command shell	ASCII Terminal [2]	Anonymous PNC admin
	ECM850 command shell	ASCII Terminal	Anonymous admin

4.2.2 Specifying Access Rights

For each subject, PACSystems provides predefined access rights. In some cases, those access rights can be partially restricted, while in other cases they either cannot be changed at all, or can only be revoked by disabling the associated server/protocol.

4.2.2.1 Predefined Access Rights

The Access Rights to data on the PACSystems controller itself, regardless of the protocol being used, are the most complex. The services provided directly by other PACSystems modules have simple, well-documented access rights and so aren't discussed here further. These specifically include the PROFINET Controller command shell, Ethernet Station Manager, the SNMP server, the Web server, and the FTP server. See the user manuals for each of those services for more details.

While the *PACSystems RX3i and RSTi-EP CPU Reference Manual,* GFK-2222, includes a description of the features allowed at each of the Service Request authentication levels (refer to the *System Security* section of that manual), it does not present the information in the complete Access Control context. Therefore, a summary table has been provided here to explicitly show the access rights granted to each subject. Note that the access right granted to an Anonymous subject may vary based on the protocol being used to communicate with the PACSystems server.

4.2.2.2 Access Rights on PACSystems Controller

Subject	Application Configuration	Application Logic (while in STOP)	Application Logic (while in RUN)	Application Data	Application Data Overrides/Forces	Fault Tables	Controller Status (e.g. RUN/STOP)	PRIV Level Passwords	Module Firmware
OEM user	A	A	—	—	—	—	—	—	—
PRIV Level 4 user	RWD	RWD	RW	RWD	RWD	RD	RW	WD	W
PRIV Level 3 user	RWD	RWD	R	RWD	RWD	RD	RW	—	—
PRIV Level 2 user	R	R	R	RW	R	RD	RW	—	—
PRIV Level 1 user	R	R	R	R	R	R	R	—	—
Anonymous (SRTP, SNP)	Same as highest *PRIV Level user* that currently has no password.								

Subject	Application Configuration	Application Logic (while in STOP)	Application Logic (while in RUN)	Application Data	Application Data Overrides/Forces	Fault Tables	Controller Status (e.g. RUN/STOP)	PRIV Level Passwords	Module Firmware
Anonymous (EGD, Modbus TCP & RTU)	—	—	—	RW	RW	—	—	—	—

Key: A=access control, R=read, W=write, D=delete/clear

Since the set of subjects is fixed and the access rights for each subject are predefined, it is likely that there won't be a one-to-one mapping from the subjects identified here, to the people who act as those subjects. Multiple subjects may be mapped onto a single person, and/or multiple people may need to all share a single subject (in which case they will all need to know the same password).

The OEM user has the ability to prohibit any subject from reading or writing the Application configuration or logic. That subject does not have the ability to grant additional access rights to any of the subjects.

4.2.2.3 Physical Access

The PACSystems RX3i controllers support a configuration setting that can be used to require physical access to the controller in order to change the application configuration, application logic and/or overrides/forces of application data. This is controlled using the *Memory Protection Switch* setting in the hardware configuration that is downloaded to the controller. Emerson strongly recommends the use of the Memory Protection Switch in conjunction with passwords set at PRIV Levels 2, 3, and 4 whenever possible in order to prevent remote, unauthorized modifications to the PLC.

When the Memory Protection Switch setting is enabled and the RUN/STOP switch is physically in the RUN position, then the predefined Access Rights are changed to the following.

4.2.2.4 Access Rights with Memory Protection ENABLED and physical switch in RUN position

Subject	Application Configuration	Application Logic (while in STOP)	Application Logic (while in RUN)	Application Data	Application Data Overrides /Forces	Fault Tables	Controller Status (e.g. RUN/STOP)	PRIV Level Passwords	Module Firmware
OEM user	A	A	—	—	—	—	—	—	—
PRIV Level 4 user	R	R	R	RW	R	RD	RW	WD	W

Subject	Application Configuration	Application Logic (while in STOP)	Application Logic (while in RUN)	Application Data	Application Data Overrides /Forces	Fault Tables	Controller Status (e.g. RUN/STOP)	PRIV Level Passwords	Module Firmware
PRIV Level 3 user	R	R	R	RW	R	RD	RW	—	—
PRIV Level 2 user	R	R	R	RW	R	RD	RW	—	—
PRIV Level 1 user	R	R	R	R	R	R	R	—	—
Anonymous (SRTP, SNP)		Same as highest *PRIV Level user* that currently has no password.							
Anonymous (EGD, Modbus TCP & RTU)	—	—	—	RW	R	—	—	—	—
	Key: A=access control, R=read, W=write, D=delete/clear Since the set of subjects is fixed and the access rights for each subject are predefined, it is likely that there won't be a one-to-one mapping from the subjects identified here, to the people who act as those subjects. Multiple subjects may be mapped onto a single person, and/or multiple people may need to all share a single subject (in which case they will all need to know the same password).								

4.2.2.5 Modbus-specific Limitations

Access to Application Data through any of the Modbus servers (Modbus TCP, Modbus RTU) is limited to only those data items that have been mapped into the Modbus address space. For both Modbus TCP and RTU, this mapping is fixed and cannot be altered, but Modbus TCP and/or Modbus RTU can be disabled if they are not needed (refer to Section 5: *Configuration Hardening*).

For details on the default mapping between Modbus Registers and the Application Data in a PACSystems RXi Controller, refer to the *PACSystems RXi Distributed I/O Controller User Manual*, GFK-2816. For other PACSystems controllers, refer to the *PACSystems RX3i and RSTi-EP TCP/IP Ethernet Communications User Manual,* GFK-2224.

4.2.2.6 Access Control Lists

Some PACSystems controllers (refer to Section 4.1, *Capabilities by Product*) allow fine-grain control over the access rights to the *Application Data*. An Access Control List may optionally be defined to further restrict which application variables can be read and/or written by external clients, but cannot be used to grant additional access rights.

The Access Control List will restrict access from external clients communicating over one of the following protocols:

- Modbus TCP
- Reliable Datagram Svc (i.e. EGD Commands)

Access to the Application Data using other protocols is either unaffected by the Access Control List (Modbus RTU, EGD Exchanges) or is only affected with the cooperation of the client (SRTP and SNP), and so cannot be relied upon for data security.

For details on enabling and using an Access Control List with PACSystems, see the

PACSystems RXi and RX3i Security topic in the HELP for PAC Machine Edition.

4.2.2.7 Internal Firewall

Some PACSystems modules have a built-in firewall (refer to Section 4.1, *Capabilitiesby Product*). These firewalls do not support user-specific configuration, but limit the incoming traffic to supported protocols and rates of the particular module.

4.2.3 Enforcement

Each of the PACSystems modules enforces the access rights for the data and services that it provides. Thus, the PACSystems controller ensures that the Application Configuration can only be updated by a user with the access rights to write/delete the Application Configuration. Similarly, the PACSystems Ethernet Interface ensures that only the *STA Modify-level* user can execute Ethernet Station Manager commands that are capable of modifying the operation of the module.

4.2.4 Protecting User Logic

It is important to note that without setting PACSystems Controller passwords at PRIV Levels 2, 3, and 4, it may be possible for an attacker on the same network as the controller to attempt to modify the user application or application data. To mitigate this threat, Emerson recommends always setting PRIV Level 2, 3, and 4 passwords and enabling Enhanced Security as described in Section 4.3.

Controlling access to all application logic is a very important step in protecting the overall system. This is particularly important for applications with C blocks as they provide a very flexible way for customers to implement application logic, but also a very flexible method for attackers to manipulate the user application.

For this reason, customers must add controls to their application development and deployment processes to ensure that malicious user application code (including C applications) are not being accidentally included and downloaded by a legitimate user. These controls can include manual inspection of the application, static analysis of the codebase, and maintaining cryptographic hashes of the application to ensure modifications, accidental or otherwise, are noticed before a legitimate user downloads an application that has been maliciously tempered with on the computer running the programming software.

Users should not include C blocks or other logic blocks (including C code) from the Internet or other untrusted sources into user applications without manual inspection and static analysis of the code at a minimum.

4.3 Authentication

PACSystems provides password-based authentication for some, but not all, of its server protocols. For each unauthenticated protocol that is enabled, compensating controls may be needed to satisfy the security requirements of a particular installation.

Note: The default configuration for all Server protocols is for no authentication, or for authentication using well-known default values.

4.3.1 Summary

This section summarizes the authentication mechanisms supported by PACSystems for each protocol. It is important to note that some PACSystems controllers only support a subset of the authentication options listed here. Refer to Section 4.1: *Capabilities by Product* for more details.

4.3.1.1 Authentication Available on PACSystems Servers

Functionality		Application Protocol	Authentication Options
Ethernet	Service Requests	SRTP	Secure login (SRP-6a) Plaintext login Disabled

Functionality		Application Protocol	Authentication Options
	EGD Consumption	Ethernet Global Data	None
	Process EGD Commands	Reliable Datagram Svc	None
	Modbus TCP Slave	Modbus TCP	None
	Ethernet Station Manager	Remote Station Mgr	Plaintext login
	OPC UA Server	OPC UA	None Plaintext login Encrypted login
	DNP3 Outstation or Server	DNP3	None
	IEC 60870-5-104 Server or Slave	IEC 60870-5-104	None
	PROFINET Controller command shell	Telnet	Plaintext login
	Web Server	HTTP, HTTPS	None
	Update Web Pages	FTP	Plaintext login
	Web Server Firmware Update	HTTP	None[11]
	Network Management	SNMP v2c	None[12]
	Assign IP before configuring module	Set Temporary IP	None
Serial	Service Requests	SNP Slave	Secure Login (SRP-6a) Plaintext Login Disabled
	Firmware Update	SNP Slave	None – must be Disabled
	Modbus RTU Slave	Modbus RTU	None
	Serial Station Manager	ASCII Terminal	Plaintext login
	PROFINET Controller command shell	ASCII Terminal	Plaintext login
	ECM850 command shell	ASCII Terminal	Plaintext login

[11] Web Server Firmware Update on the RXi supports a plaintext User ID and password, but they are set to well-known, fixed values.

[12] SNMP v2c supports a plaintext *community string*. Refer to each PACSystems product manual for details on the community string settings and what SNMP features are accessible by the community string.

4.3.1.2 Authentication Supported by PACSystems Clients

Functionality		Required Application Protocols	Authentication Supported
Ethernet	SRTP Channels	SRTP	None
	EGD Production	Ethernet Global Data[5]	None
	Send EGD Commands	Reliable Datagram Svc	None
	Modbus TCP Channels	Modbus TCP	None
	Ethernet Station Manager	Remote Station Mgr	Plaintext login[1]
	Time Synchronization	SNTP	None
	Assign IP addresses using a centralized database of addresses	BOOTP	None
	Lookup IP addresses by Name	DNS	None

Note: Login is not supported by SRTP Channels, even though passwords may be enabled on the SRTP server. When using SRTP Channels, the SRTP server cannot have password protection enabled for PRIV level 2 if data writes are required.

4.3.1.3 Authentication Supported by the PROFINET Protocol

The PROFINET I/O specification does not define an authentication mechanism and so none is supported on PACSystems for any PROFINET communications.

4.3.2 Plaintext Login

Authentication for many of the supported protocols involves sending a plaintext password to the PACSystems controller. A plaintext password is sent over the network without any confidentiality protection, such as encryption. The consequence is that any network entity between the two endpoints exchanging authentication information could sniff the network traffic and observe the plaintext password. In some cases, these plaintext passwords cannot be more than seven (7) characters long. When such protocols are required, additional compensating controls may be needed to satisfy the security requirements of a particular installation.

4.3.3 Secure Login

Some models of PACSystems controllers support a cryptographically secure password login mechanism when using the SRTP or SNP protocols. The algorithm used is the Secure Remote Password protocol (SRP-6a). This feature is controlled by the *Enhanced Security* setting in PAC Machine Edition – the same setting that enables the use of an Access Control List.

For details on enabling the Secure Login feature, refer to the *PACSystems RXi and RX3i Security* topic in the HELP for *PAC Machine Edition*.

4.3.4 Recommendations

Emerson strongly recommends that authentication be used for every enabled protocol that supports authentication, that all default passwords be changed, and that access be appropriately restricted to any computer-based file that includes a plaintext password.

When a choice between a plaintext-based login and a Secure Login is available, Emerson strongly recommends that the Secure Login feature be used since it prevents network entities from sniffing plaintext passwords and increases the password maximum length to 31 characters.

Whenever protocols are used with no authentication mechanism, or when authentication is disabled or relies on sending credentials in plaintext across the network, it is critical to control physical and electronic access to the network to prevent unauthorized messages from being sent and acted upon.

Below are recommended actions to be taken to mitigate the risk of external or internal entities accessing an Industrial Control System (ICS) network and sending unauthorized messages.

4.3.4.1 Personnel Security Protection

All individuals with permission to physically access ICS systems should have background checks and be trained in the proper use and maintenance of ICS systems.

4.3.4.2 Physical Security Perimeter Protection

1. All ICS hardware should be placed in locked cabinets, with policies and procedures to restrict access to the key.
2. Network equipment such as switches, routers, firewalls, and Ethernet cabling should be physically protected in locked enclosures such as cabinets or closets with policies and procedures to restrict access to these enclosures.
3. Whenever possible, there should be no physical network path from an ICS network to the Internet. It should not be possible for an attacker to reach an ICS network from any Internet-facing computer.
4. Networks should always be physically segmented as suggested in the Reference Network Architecture diagram to avoid exposure to ICS networks.

5. Each ICS system asset should be visibly labeled by a unique identifier, with all expected asset identification compiled into an access-controlled list.

4.3.4.3 Electronic Security Perimeter Protection

1. All external access to an ICS network should be managed through a Virtual Private Network (VPN) or similar technology leveraging two-factor authentication. Next-Generation Firewalls should be properly configured and deployed at each conduit between physical networks that deny all but the specifically allowed protocol families, source addresses, and destination addresses, and specific application-level commands between the two adjacent networks. For example, a Next-Generation Firewall could prohibit write operations across networks while allowing read operations.
2. If one network node such as a PLC or HMI uses unauthenticated protocols to exchange information or commands with another network node on the same physical network, a Next-Generation Firewall could be deployed between the two network nodes. This Next-Generation Firewall should be configured to explicitly whitelist all expected messages between the two network nodes, and deny all other unexpected messages.
6. To detect and alert for unexpected, unauthenticated messages on a given network, an Intrusion Detection System (IDS) could be configured and deployed. Consider configuring the IDS to log all events to a Security Information and Event Management (SIEM) system that aggregates all security information on the ICS network.
7. To detect and actively prevent unexpected, unauthenticated messages on a given network from reaching a given network node, an Intrusion Prevention System (IPS) could be configured and deployed. Consider configuring the IPS to log all events to a Security Information and Event Management (SIEM) system that aggregates all security information on the ICS network.
8. To limit the impact of the compromise of any single user account, it is recommended to divide *administrators* privileges into several user accounts, each for its own operational function.
9. To limit the impact of the compromise of any single set of credentials (user name, password) for any ICS equipment, it is recommended to never re-use credentials for different tools or purposes.
10. Carefully protect sources of and access to credentials (user names, passwords) for all ICS equipment, including switches, routers, firewalls, IDS, IPS, etc.
11. Enforce a policy of rotating credentials for ICS equipment periodically and after personnel changes. Note that products with no support for enforcement of unique passwords over time should be compensated for with policies and procedures that require a history of unique passwords.

Recommendations on password complexity and management can be found in NIST 800-118, Guide to Enterprise Password Management.

4.4 Password Management

As described in Section 4.2.1 *Authorization Framework*, each instance of a server has its own instances of the predefined subjects. As a result, passwords for each subject must be separately managed for each instance of a given kind of server.

For example, each PACSystems controller acts as a Service Request server. Therefore, the passwords for each PACSystems controller in the system must be independently managed. Similarly, each Ethernet Interface supports the Ethernet Station Manager server. Therefore, the passwords for each Ethernet Interface must be independently managed – even when multiple Ethernet Interface modules are located in a single rack, providing service to a single PACSystems controller.

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 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.

Emerson strongly recommends that any default password be changed before deployment of the device. The table below identifies services that contain a default password.

Functionality	Authenticated Subjects	How Passwords are assigned	Default Provided
Service Requests	PRIV Level 1 user PRIV Level 2 user PRIV Level 3 user PRIV Level 4 user OEM user	All of these passwords are controlled by the PRIV Level 4 user. Refer to the *PACSystems RXi and RX3i Security* topic in the HELP for *PAC Machine Edition* for details on how to specify these passwords. Max of 31 characters in password when Secure Login is enabled. Max of 7 characters otherwise.	No
OPC UA	PRIV Level 2 user PRIV Level 3 user PRIV Level 4 user	All of these passwords are controlled by the PRIV Level 4 user. See above.	No
PROFINET Controller command shell [2]	PNC admin	Changed directly on the PROFINET Controller command shell by running the following command: `loginCfg password` Max of 10 characters in password.	Yes

Functionality	Authenticated Subjects	How Passwords are assigned	Default Provided
ECM command shell	admin	Changed directly on the ECM850 command shell by running the following command: loginCfg password Max of 10 characters in password.	Yes
Ethernet Station Manager[1]	STA Modify-level user	Included in plaintext in an AUP file that must be imported into the Ethernet Configuration and downloaded to the PACSystems controller. stpasswd=<newpass> Max of 7 characters in password	No
Update Web Pages[1]	FTP user	Included in plaintext in an AUP file that must be imported into the Ethernet Configuration and downloaded to the PACSystems controller. tpasswd=<newpass> Max of 7 characters in password.	Yes
Web Server Firmware Update	FW update user	Changed using web portal. Password must have 8-16 characters, use both uppercase and lowercase letters, and include at least one number and special character. To reset your password. Go to the "Administrator" menu found on the web portal homepage.	Yes

For more detailed information on assigning these passwords, see the User's Manual for the appropriate product.

4.5 Confidentiality and Integrity

4.5.1 Communications Protocols

Some communications protocols provide features that help protect data while it is *in flight*– actively moving through a network. The most common of these features include:

- Encryption – Protects the confidentiality of the data being transmitted.
- Message Authentication Codes – Ensures message authenticity and integrity by cryptographically detecting message tampering or forgery. This ensures the data originated from the expected source and was not altered since it was transmitted, regardless of whether it was malicious or not.

Currently, few of the communications protocols supported by PACSystems provide either of these features, as detailed in the following table. Therefore, compensating controls may be required to meet an installation’s security requirements for protecting data in-flight.

4.5.1.1 Protocol-Provided Security Capabilities

Protocol		Data Encryption	Message Authentication Codes
Ethernet	BOOTP	N	N
	DCE/RPC	N	N
	DNS	N	N
	Ethernet Global Data	N	N
	FTP	N	N
	HTTP	N	N
	HTTPS	Y	N
	Modbus TCP	N	N
	OPC UA Server	Y	Y
	DNP3 Outstation or Server	N	N
	IEC 60870-5-104 Server or Slave	N	N

Protocol		Data Encryption	Message Authentication Codes
	PROFINET DCP	N	N
	PROFINET I/O	N	N
	IEC 61850 Client	N	N
	MRP	N	N
	RDS	N	N
	Remote Station Manager	N	N
	SNMP v2c	N	N
	SNTP	N	N
	SRTP	N	N
	Telnet	N	N
	Set Temporary IP	N	N
Serial	ASCII Terminal	N	N
	Modbus RTU Slave	N	N
	SNP Slave	N	N

4.5.2 Firmware Signatures

Some PACSystems controllers have digitally signed firmware images to provide cryptographic assurance of the firmware's integrity. For controllers that support this feature, a digital signature is used to verify that any firmware being loaded onto the controller was supplied by the Intelligent Platforms LLC and has not been modified. If the digital signature validation fails, the new firmware will not be installed onto the device.

4.5.3 Logging and Auditing

The PACSystems controller doesn't provide a dedicated security log embedded within the controller, nor does it integrate with an external Security Information and Event Management (SIEM) system. However, the PACSystems controller does log operational events into two small (64 entry) fault tables. Each fault entry includes the time & date that the fault was logged, using the date/time maintained on the Controller.

These fault tables can be read by remote clients as well as by the user application running on the controller. Thus, logged events could be communicated to an external system for persistent storage and auditing, if required by an installation's security policy. PAC Machine Edition can be used to export the fault tables to an XML file or print them. The fault tables can also be remotely retrieved using the PACSAnalyzer tool and stored in a text file.

Most of the events that are logged in the PACSystems fault tables represent functional issues, such as hardware failures and unexpected firmware operation. While those are not specific to security, they may still provide information that is useful during a security audit. There are two security-specific faults that can be logged.

1. When an attempt to authenticate using the Service Request protocol fails, a specific fault is logged in the Controller Fault Table and a system variable (#BAD_PWD) is set to signal that a login attempt has failed. The fault text is "Password Access Failure", and the fault extra data encodes information specific to the event.
2. When an attempt to use an access-controlled feature fails due to insufficient privileges, a specific fault is logged in the Controller Fault Table. The fault text is "Access Control List violation detected", and the fault extra data encodes information specific to the event.

Section 5: Configuration Hardening

This section is intended to assist in reducing the potential attack surface by providing information that can be used to harden the configuration of the PACSystems products that are present in a particular installation. Configuration Hardening should be considered in addition to enabling and using security features such as Authentication, Access Control and Authorization.

On each PACSystems product, all ports, services and protocols that are not required for the intended application, should be disabled.

5.1 Controller

This section provides information to use when hardening the configuration of a PACSystems controller. These options should be considered when configuring any PACSystems controller that supports them.

These settings are specified within the hardware configuration that is downloaded to the PACSystems controller.

5.1.1 Serial Port Protocols

The hardware configuration for the PACSystems controller includes the ability to modify the operation of the serial ports embedded on the controller, including which server protocols will be supported. This selection is controlled by the Port Mode setting, which must be individually specified for each serial port. The protocols that will be supported for each option are summarized here.

5.1.1.1 Serial Port Configuration

Port Mode	Supported Protocols
RTU Slave	Modbus RTU Slave SNP Slave
SNP Slave	SNP Slave
Serial I/O Message Mode	Application-defined
Available	(none)

To reduce the potential attack surface, configure each serial port using the most restrictive option that still supports the required protocol(s). Setting the *Port Mode* to *Available* will disable all protocols for a given serial port, but very low-level handling of data received on that port will still occur.

5.1.2 Modbus TCP Server

The hardware configuration for the PACSystems controller can be used to disable Modbus TCP server access to data on the controller. This is managed using the *Modbus Address Space Mapping Type* setting.

5.1.2.1 Modbus TCP configuration

Modbus Address Space Mapping Type	Modbus TCP Data Access
Standard Modbus Addressing	Allowed
Disabled	Not allowed

Note: This setting affects all the Ethernet Interfaces for the controller. Even when using a modular PACSystems platform such as the RX3i , there is no way to enable Modbus TCP server on one Ethernet Interface while having it disabled on another.

5.2 Ethernet Interface

This section provides information to use when hardening the configuration of a PACSystems Ethernet Interface. These settings should be considered when configuring any PACSystems Ethernet Interface.

The Ethernet Interface can be configured to disable a number of services. The table below lists those services and indicates the configuration value that will disable each. Note that some of these settings will not entirely close the TCP/UDP port, but they will still reduce the attack surface.

5.2.1.1 Disabling Ethernet Services

Service	Parameter Name	Value
BOOTP Client[1]	Use BOOTP for IP Address	False
FTP Server[1]	Max FTP Server Connections	0
IP Routing	Gateway IP Address	0.0.0.0
DNS Client[1]	Name Server IP Address	0.0.0.0
SNTP Client	Network Time Sync	None
Web Server[1]	Max Web Server Connections	0

These settings are specified within the hardware configuration that is downloaded to the PACSystems controller. For more information on these parameters, refer to the *TCP/IP Ethernet Communications for PACSystems User's Manual*, GFK-2224.

5.3 PROFINET Controller

This section provides information to use when hardening the configuration of a PACSystems PROFINET Controller. These settings should be considered when configuring any PACSystems PROFINET Controller.

Service	How to Disable
IP Routing	Set *Gateway IP Address* to 0.0.0.0 in the hardware configuration and download to the PACSystems controller.
Telnet Server	Login to the PROFINET Controller[2] Command Line Interface as *admin*. Run the following command: no telnet ***Note:*** Telnet server is disabled by default. The current state of the telnet server can be confirmed by running: show telnetd

5.4 OPC UA

This section shows those OPC UA parameter settings that provide the maximum hardening. Weigh these settings against the system's requirements.

Parameters	How to Harden
Server Enabled	Set this parameter to **False** if the OPC UA protocol will not be used. This will eliminate all OPC UA attack surfaces from the controller.
Certificate Expiration Date Checking	Set this parameter to **Strict** to force the controller to check for valid dates on all installed security certificates. Please be aware that if this parameter is **Strict**, when a previously installed certificate expires, all communication with the associated OPC UA client will cease. A new, valid certificate must be installed to allow communication to resume.
Certificate Debug Commands	Set this parameter to **Disabled**. This will prevent anyone from looking at the contents of the controller's certificate stores with the OPC UA Station Manager command.

5.5 DNP3 Outstation

This section provides information to use when hardening the configuration of a DNP3 Outstation Protocol. Weigh these settings against the system's requirements.

Parameters	How to Harden
DNP3 Outstation Protocol	Set this parameter to **Disabled** if the DNP3 Outstation protocol will not be used. This will eliminate all DNP3 Outstation attack surfaces from the controller.

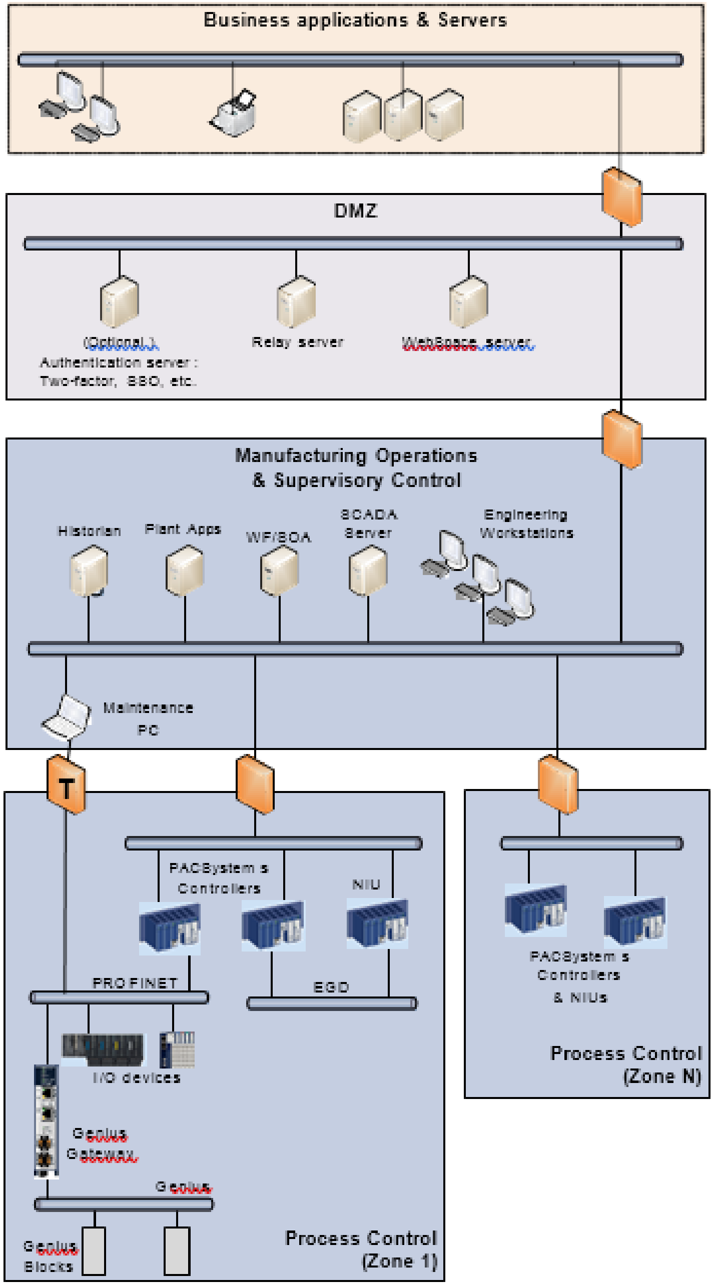
Section 6: Network Architecture and Secure Deployment

This section provides security recommendations for deploying PACSystems controllers in the context of a larger network.

6.1 Reference Architecture

Figure 1 shows a reference deployment of PACSystems components using the logical segmentation of the Purdue Enterprise Reference Architecture, otherwise known as the Purdue Model.

Figure 1: PACSystems Deployed in Purdue Model



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 a 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.

6.2 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 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.

6.3 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. For example, since PAC Machine Edition uses SRTP to download the application to the PACSystems controllers and NIUs, then SRTP traffic must be allowed through the firewall. However, 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. If, in addition to that, a controller has no other need for that protocol, then – in addition to blocking it at the firewall – the controller itself should be configured to disable support for the protocol itself.

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 PACSystems controllers will typically be initiated from a computer 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.

6.4 Access to PROFINET Networks

Commissioning and maintaining the devices on the PROFINET network requires the ability to communicate from a computer to the I/O devices on that network. For example, if a PROFINET I/O device fails and needs to be replaced, the replacement I/O device will need to be assigned a name. As described in Section 3.5, *PROFINET*, this is done using the PROFINET DCP protocol. However, to help ensure that the Maintenance computer cannot be used to launch attacks on the I/O devices using other protocols, the firewall it connects through should block all protocols that are not needed for performing the maintenance functions.

Note: Since the PROFINET DCP protocol is not routable, the firewall used will most likely need to be configured so it operates in *Transparent* mode (This is noted by the use of a "T" on the firewall in the Reference Architecture diagram.). This will allow the Maintenance computer to be part of the same subnet as the PROFINET I/O devices, as required by the PROFINET DCP protocol.

6.5 Hot Standby CPU Redundancy with PROFINET IO

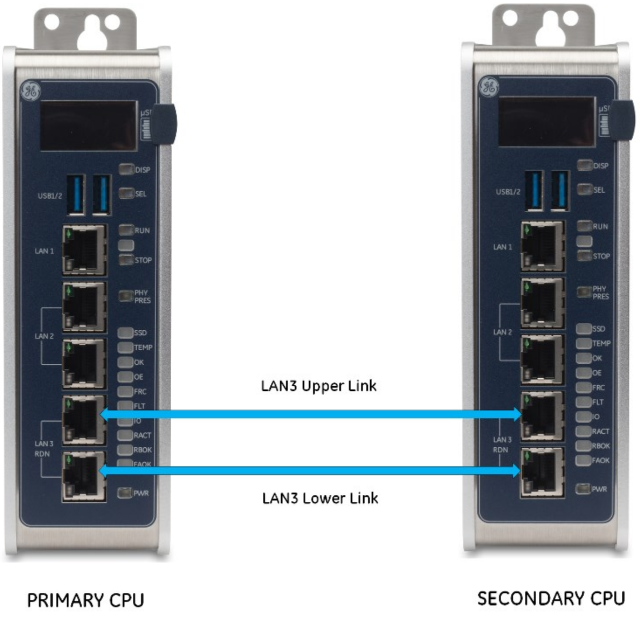
Hot Standby CPU Redundancy allows a critical application or process to continue operating if a failure occurs in any single component. A Hot Standby system employs two CPUs:

- an Active unit that is actively controlling the process at a given moment, and
- a Backup unit that is synchronized with the Active unit and can take over the process in a bumpless fashion, should that become necessary.

The two units are synchronized when both are in Run Mode, the Backup unit has received the latest status and synchronization information from the Active unit via a redundancy link, and both are running their logic solutions in parallel.

In the case of CPE400 or CPL410, LAN3 is utilized as the high-speed data synchronization link between the redundant CPUs. This is a dedicated Ethernet link connecting the two LAN3 ports on the Active CPU to the equivalent ports on the Backup CPU, as shown in Figure 2. The upper port of the Primary is connected to the upper port of the Secondary, and the lower port to the lower port. No crossing is permitted.

Figure 2: CPE400/CPL410 LAN3 Connections for Hot Standby Redundancy



Note that CPE400/CPL410 LAN3 is used as a dedicated link, solely for CPU data synchronization in Hot Standby Redundancy Systems. Although the underlying network is a standard Ethernet network, no other Ethernet devices are permitted, except the two matched LAN3 ports on the Primary and Secondary CPUs. Failure to observe this restriction will invalidate the configuration.

The system is completely functional with only one Ethernet link operating on LAN3, but both links should nevertheless be connected to provide for communications redundancy on the link itself. Refer to the *PACSystems RX3i IC695CPE400 1.2GHz 64MB Rackless CPU w/Field Agent Quick Start Guide*, GFK 3002A or later for Hot Standby Redundancy set up. For CPL410, refer to the *PACSystems RX3i IC695CPL410 1.2GHz 64MB Rackless CPU w/Linux Quick Start Guide*, GFK-3053.

From a security perspective, the Ethernet network features of LAN3 are subject to the same security requirements as any Ethernet network. However, since no other devices may be attached, and the link is hard-wired, there is nothing additional that the user needs to consider.

A second aspect of implementing Hot Standby CPU Redundancy with RX3i CPE400/ CPL410 is its total reliance on PROFINET IO. Most other rack-based CPU systems employ rack-based or Genius I/O, but these are not compatible with the CPE400/CPL410. From a security perspective, the PROFINET features of LAN1 and LAN2 are subject to the same security requirements as any PROFINET network.

6.6 Access to IEC 61850 Networks

Commissioning and maintaining the devices on an IEC 61850 network requires the ability to communicate from a Maintenance PC in the Manufacturing Operations & Supervisory Control network to remote devices like Intelligent Electronic Devices (IED) on the IEC 61850 network, which typically implement an IEC 61850 server. For example, the integrated IEC 61850 configurator in PAC Machine Edition can connect to a remote IED and directly read its IEC 61850 object model over the IEC 61850 protocol. This is described in Section 3.6: *IEC 61850*. Refer to the *PACSystems RX3i IEC 61850 Ethernet Communication Module User Manual*, GFK-2849, for more details. However, to mitigate attacks launched from the Maintenance PC using other protocols, the firewall between the Maintenance PC and the IEC 61850 network should block all protocols that are not needed for performing maintenance functions.

6.7 Hot Standby CPU Redundancy with DNP3 Outstation

Hot Standby CPU Redundancy allows a critical application or process to continue operating if a failure occurs in any single component. A Hot Standby system employs two CPUs:

- an Active unit that is actively controlling the process at a given moment while storing the Event Reports (SOE / Most Recent), and
- a Backup unit that is synchronized with the Active unit including the Event Reports.

The two units are synchronized when both are in Run Mode, the Backup unit has received the latest status and synchronization information such as Event Reports from the Active unit via a redundancy link, and both are running their logic solutions in parallel. For more information, please refer GFK-3103(PACSystems DNP3 Outstation user Manual)

Section 7: Other Considerations

7.1 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 PACSystems controller be temporarily taken out of service.

If temporarily taking a controller out of service in order to apply security fixes is expected to cause an unacceptable disruption to the system's availability, then consider designing the control system to use redundancy. PACSystems supports Hot-Standby CPU Redundancy which will allow many, if not all, security fixes to be applied to the redundant controllers while continuing to control the process.

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.

7.2 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 I/O, Ethernet Global Data, 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.

7.3 RXi Compensating Controls

7.3.1 Network Bandwidth Limiting

The RXi Controller's Ethernet interfaces are not capable of sustaining Ethernet communications above a speed of 8 Mbps over the SRTP Server's TCP port (18245/TCP) and 10 Mbps in general. Above these thresholds, ARP, IMCP, UDP, and TCP services may become unavailable. Care must be taken to design and implement the network to prevent excessive traffic to RXi Controller Ethernet interfaces.

In order to reduce the likelihood of intentional or accidental network flooding that could cause a loss of availability in RXi Controller Ethernet interfaces. Please follow the relevant recommendations in Section 4.3.4. To further mitigate the loss of availability for a particularly critical asset, a switch or firewall configured for ingress and egress rate-limiting can be placed directly between the RXi Controller and the rest of the network. In the event of a network storm, the switch or firewall will selectively drop traffic to limit the rate of traffic that reaches a given RXi Controller. Additionally, it is recommended to leave the OPC UA Server in its default disabled state unless the application leverages OPC UA.

7.4 RSTi-EP Compensating Controls

7.4.1 Network Bandwidth Limiting

The RSTi-EP CPE100/CPE115 Controller's Ethernet interfaces are not capable of sustaining Ethernet communications above a speed of 5 Mbps over the SRTP Server's TCP port (18245/TCP) and 10 Mbps in general. Above these thresholds, ARP, IMCP, UDP, and TCP services may become unavailable. Care must be taken to design and implement the network to prevent excessive traffic to RSTi-EP CPE100/CPE115 Controller Ethernet interfaces.

To reduce the likelihood of intentional or accidental network flooding that could cause a loss of availability in RSTi-EP CPE100/CPE115 Controller Ethernet interfaces. Please follow the relevant recommendations in Section 4.3.4. To further mitigate the loss of availability for a particularly critical asset, a switch or firewall configured for ingress and egress rate-limiting can be placed directly between the RSTi-EP CPE100/CPE115 Controller and the rest of the network. In the event of a network storm, the switch or firewall will selectively drop traffic to limit the rate of traffic that reaches a given RSTi-EP Controller. Additionally, it is recommended to leave the OPC UA Server in its default disabled state unless the application leverages OPC UA.

7.5 Additional Guidance

7.5.1 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. This includes, but is not limited to the following document:

- PROFINET Security Guideline (TC3-04-0004a) by PROFIBUS INTERNATIONAL

7.5.2 OPC UA Server

When running an OPC UA Server with a *Limited Communications Window*, the server can process enough requests to use the entire window, which will add that time to your PLC Logic sweep. For example, a 100 ms *Limited Backplane Communications Window* could add the full 100 ms to your PLC Logic Sweep. Caution should be taken to ensure the Communication Window is configured within the tolerances of the system.

7.5.3 PROFINET Controller Duplicate IP

The duplicate IP address handling for the RX3i PROFINET Controller (IC695PNC001 firmware revision 2.26 and above) and the Embedded PROFINET Controller on the RX3i CPE330, CPE400, CPL410 and RSTi-EP CPE100/CPE115 behaves as follows.

In each case, the system has an active PROFINET network with a PROFINET Controller connected to at least one PROFINET Device.

1. If a second PROFINET Controller with an identical IP address to the active PROFINET Controller is added to the network, the second Controller will not

enter the network and will log a fault to indicate *Duplicate IP Detected*. The first Controller will maintain all device connections.

2. If a device with an identical IP address to an active PROFINET Controller is added to the network, the Controller will log a *Duplicate IP Detected* fault and maintain all device connections.
3. If a device with an identical IP address to an active PROFINET Device is added to the network, the Controller will log a *Duplicate IP Detected* fault and maintain all device connections.

7.5.4 MRP Ring Ethernet Traffic Storm Prevention

The RX3i CPE330, CPE400, CPL410 and RSTi-EP CPE100/CPE115 LAN 2 and the RX3i PNC001 can all be configured as an MRP Ring Manager (MRM). However, none of these defaults to be an MRM.

To prevent an Ethernet Traffic Storm, the physical ring must not be completely connected until the MRM configuration is stored to an Ethernet node on the ring. Failure to have an active MRM configured in an Ethernet ring configuration will result in an Ethernet Traffic Storm caused by the ring's network loop topology. An Ethernet Traffic Storm will prevent communication to all Ethernet nodes connected to the ring until the ring is physically broken or an MRM is configured.

Before clearing and power cycling the configuration of a CPE330 that is configured as an MRM in a ring topology, it is recommended that either (a) the ring be broken by physically disconnecting an Ethernet port on any network node in the ring, or (b) some other network node in the ring be configured as a MRM.

To prevent storms in a ring where a PROFINET Controller is configured as an MRM, the controller will maintain that functionality even after a clear and power cycle, and will continue to do so until a different configuration is stored to that controller, providing the new configuration prevents the controller from operating as an MRM. It is still recommended that the ring be broken by physically disconnecting an Ethernet port on any network node in the ring until a single MRM is configured for the ring.

7.5.5 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 Industrial Control Systems. For example, the U.S. Department of Homeland Security has published guidance on Secure Architecture Design and on Recommended Practices for cybersecurity with Industrial Control Systems. Similarly, the International Society of Automation publishes the ISA-99 specifications to provide guidance on establishing & operating a cyber-security program, including recommended technologies for industrial automation and control systems. Such documentation, when appropriate, should be considered in addition to this document.

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™