GE

Intelligent Platforms

GFK-2830C

PACSystems* RXi, RX3i, and RX7i Controller

Secure Deployment Guide

June 2015

For public disclosure

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 GE 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 GE 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 GE products referenced herein.

This document is approved for public disclosure.

GE 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.

GE 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.

For further assistance or technical information, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

Revised: June 2015
Issued: Aug 2014

Copyright © 2014-2015 General Electric Company, All rights reserved.

*** Indicates a trademark of General Electric Company and/or its subsidiaries.
All other trademarks are the property of their respective owners.**

Refer to the section, *Contact Information* for support on this product.

Please send documentation comments or suggestions to *controls.doc@ge.com*

Document Updates

Revision	Location	Description
Rev C / June 2015	The sections, *Ethernet Protocols* and *Logging and Auditing*	Updated information IC695-PNC001 and added second security-specific fault information.
Rev B / Mar 2015	Throughout document	Added information for the support of the IC695CPE330 CPU
Rev A / Nov 2014	Throughout document	Added information for support of the IC695ECM850 module

Related Documents

Doc #	Title
GFK-2904	PROFINET I/O Devices Secure Deployment Guide
GFK-2816	PACSystems RXi Distributed I/O Controller User's Manual
GFK-2222	PACSystems CPU Reference Manual
GFK 2314	PACSystems RX3i System Manual
GFK 2223	PACSystems RX7i Installation Manual
GFK-2224	TCP/IP Ethernet Communications for PACSystems User's Manual
GFK-2225	TCP/IP Ethernet Communications for PACSystems Station Manager 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

Contact Information

If you purchased this product through an Authorized Channel Partner, then contact the seller directly.

General Contact Information

Online technical support and GlobalCare	http://support.ge-ip.com
Additional information	http://www.ge-ip.com/
Solution Provider	solutionprovider.ip@ge.com

Technical Support

If you have technical problems that cannot be resolved with the information in this manual, please contact us by telephone or email, or on the web at http://support.ge-ip.com

Americas

Online Technical Support	http://support.ge-ip.com
Phone	1-800-433-2682
International Americas Direct Dial	1-780-420-2010 (if toll free 800 option is unavailable)
Technical Support Email	support.ip@ge.com
Customer Care Email	customercare.ip@ge.com
Primary language of support	English

Europe, the Middle East, and Africa

Online Technical Support	http://support.ge-ip.com
Phone	+ 800-1-433-2682
EMEA Direct Dial	+ 420-23-901-5850 (if toll free 800 option is unavailable or dialing from a mobile telephone)
Technical Support Email	support.emea.ip@ge.com
Customer Care Email	customercare.emea.ip@ge.com
Primary languages of support	English, French, German, Italian, Czech, Spanish

Asia Pacific

Online Technical Support	http://support.ge-ip.com
Phone	+ 86-400-820-8208
	+ 86-21-3217-4826 (India, Indonesia, and Pakistan)
Technical Support Email	support.cn.ip@ge.com (China)
	support.jp.ip@ge.com (Japan)
	support.in.ip@ge.com (remaining Asia customers)
Customer Care Email	customercare.apo.ip@ge.com
	customercare.cn.ip@ge.com (China)

Contents

1 About this Guide 7

2 Introduction 9

2.1 What is Security? 9

2.2 I have a firewall. Isn't that enough? 9

2.3 What is Defense in Depth? 9

2.4 General recommendations 10

2.5 Checklist 10

3 Communication Requirements 11

3.1 Protocols Supported 11

3.1.1 Ethernet Protocols 11

3.1.2 Serial Protocols 13

3.2 Service Requests 14

3.2.1 SRTP 14

3.2.2 SNP 14

3.3 Server 15

3.4 Client 16

3.5 PROFINET 17

3.6 IEC 61850 19

3.7 Ethernet Firewall Configuration 19

3.7.1 Lower-level Protocols 20

3.7.2 Application Layer Protocols 21

4 Security Capabilities 23

4.1 Capabilities by Product 23

4.2 Access Control and Authorization 24

4.2.1 Authorization Framework 24

4.2.2 Specifying Access Rights 25

4.2.3 Enforcement 28

4.3 Authentication 29

4.3.1 Summary 29

4.3.2 Plaintext Login 31

4.3.3 Secure Login 31

4.3.4 Recommendations 31

4.4 Password Management 31

4.5 Confidentiality and Integrity 33

4.5.1 Communications Protocols 33

4.5.2 Firmware Signatures 34

4.5.3 Logging and Auditing 34

5 Configuration Hardening 35

5.1 Controller 35

5.1.1 Serial Port Protocols 35

5.1.2 Modbus TCP Server 36

5.2 Ethernet Interface 36

5.3 PROFINET Controller 37

For public disclosure

6 Network Architecture and Secure Deployment 39
6.1 Reference Architecture 39
6.2 Remote Access and Demilitarized Zones (DMZ) 41
6.3 Access to Process Control Networks........ 41
6.4 Access to PROFINET Networks........ 42
6.5 Access to IEC 61850 Networks 42
7 Other Considerations 43
7.1 Patch Management........ 43
7.2 Real-time Communication........ 43
7.3 Additional Guidance 44
7.3.1 Protocol-specific Guidance 44
7.3.2 Government Agencies and Standards Organizations........ 44

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	Description
RXi Controller	ICRXICTL000	1 GHz CPU w/Ethernet and PROFINET I/O Controller, 10 MB user memory
RX3i CPU with embedded Ethernet Interface	IC695CPE305	1.1GHz Atom CPU, 5 MB user memory
	IC695CPE310	1.1GHz Atom CPU, 10 MB user memory
	IC695CPE330	1GHz G-Series CPU, 64 MB user memory
RX3i CPU	IC695CPU310	300MHz Celeron CPU, 10 MB user memory
	IC695CPU315	1 GHz Celeron-M CPU, 20 MB user memory
	IC695CPU320	1 GHz Celeron-M CPU, 64 MB user memory
	IC695NIU001	300MHz Celeron NIU
	IC695NIU001+ versions –AAAA and later	1.1 GHz Atom 510 NIU
RX3i Redundancy CPU	IC695CRU320	1 GHz Celeron-M CPU, 64 MB user memory
RX3i Ethernet Interface	IC695ETM001	Ethernet peripheral PCI module
RX3i PROFINET Controller	IC695PNC001	PROFINET I/O Controller module
RX3i IEC 61850 Ethernet Communication Module	IC695ECM850	IEC 61850 Client Ethernet Communication module
RX7i CPU with embedded Ethernet Interface	IC698CPE010	300MHz, Celeron CPU, 10MB user memory
	IC698CPE020	700MHz, Pentium CPU, 10 MB user memory
	IC698CPE030	600MHz, Pentium-M CPU, 64MB user memory
	IC698CPE040	1800MHz, Pentium-M CPU, 64MB user memory
RX7i Redundancy CPU with embedded Ethernet Interface	IC698CRE020	700MHz, Pentium CPU, 10 MB user memory
	IC698CRE030	600MHz, Pentium-M CPU, 64MB user memory
	IC698CRE040	1800MHz, Pentium-M CPU, 64MB user memory
RX7i Ethernet Interface	IC698ETM001	Ethernet peripheral VME module

Notes

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.

GE Intelligent Platforms recognizes the importance of building and deploying products with these concepts in mind and encourages customers to take appropriate care in securing their GE Intelligent Platforms products and solutions.

Note As GEIP 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. GEIP Product Security Advisories can be found at the following location: *http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB14607*

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, GE Intelligent Platforms 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

Adopting the following security best practices should be considered when using GE Intelligent Platforms products and solutions.

- 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 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 6, *Network Architecture and Secure Deployment*.)
5. Configure firewalls and other network security devices. (Refer to section 3.6, *Ethernet Firewall Configuration* and section 6, *Network Architecture and Secure Deployment*.)
6. Enable and/or configure the appropriate security features on each PACSystems module. (Refer to section 4, *Security Capabilities*.)
7. On each PACSystems module, change every supported password to something other than its default value. (Refer to section 4.4, *Password Management*.)
8. Harden the configuration of each PACSystems module, disabling unneeded features, protocols and ports. (Refer to section 5, *Configuration Hardening*.)
9. Test/qualify the system.
10. Create an update/maintenance plan.

Note Secure deployment is only one part of a robust security program. This document, including the checklist above, is limited to only providing secure deployment guidance. For more information about security programs in general, refer to section 7.3, *Additional Guidance*.

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.

GE Intelligent Platforms 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 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.

Supported Ethernet Protocols

	Protocol	RXi	RX3i						RX7i							
		ICR- XICT- L000	IC695- CPE 305	IC695- CPE 310	IC695- CPE 330	IC695- ETM 001	IC695- PNC 001	IC695- ECM 850	IC698- CPE 010	IC698- CPE 020	IC698- CPE 030	IC698- CPE 040	IC698- CRE 020	IC698- CRE 030	IC698- CRE 040	IC698- ETM 001
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	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓
	PROFINET DCP client	✓					✓									
	PROFINET DCP server	✓					✓									
	PROFINET I/O	✓					✓									
	IEC 61850 Client							✓								
	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 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.

PACSystems RX3i modules

Protocol	IC695-CP-E305	IC695-CP-E310	IC695-CP-U310	IC695-CP-U315	IC695-CP-U320	IC695-CR-U320	IC695-CP-E330	IC695-ET-M001	IC695-NI-U001	IC695-NI-U001+	IC695-PN-C001	IC695-EC-M850
Application-specific[2]	✓	✓	✓	✓	✓	✓	✓					
ASCII Terminal								✓			✓	✓
Modbus RTU Slave	✓	✓	✓	✓	✓	✓			✓	✓		
SNP Slave	✓	✓	✓	✓	✓	✓			✓	✓		

[2] 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 won’t be discussed further.

PACSystems RX7i modules

Protocol	IC698CP-E010	IC698CP-E020	IC698CP-E030	IC698CP-E040	IC698-CRE020	IC698-CRE030	IC698-CRE040	IC698ET-M001
Application-specific[2]	✓	✓	✓	✓	✓	✓	✓	
ASCII Terminal	✓	✓	✓	✓	✓	✓	✓	✓
Modbus RTU Slave	✓	✓	✓	✓	✓	✓	✓	
SNP Slave	✓	✓	✓	✓	✓	✓	✓	

[2] 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 won’t 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 Proficy 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).

SRTP Server

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

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.

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® computer)	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	Proficy Machine Edition HMI Other controllers
	EGD Consumption	Ethernet Global Data†	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
	PROFINET Controller command shell	Telnet	telnet.exe on computer
	Web Server	HTTP	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	Proficy Machine Edition
† 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
Serial	Service Requests	SNP Slave	Proficy 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
	EGD Production	Ethernet Global Data[†]	Other controllers
	Send EGD Commands	Reliable Datagram Svc	Other controllers
	Ethernet Station Manager	Remote Station Mgr	Other Ethernet interface
	Time Synchronization	SNTP	[t] 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

[†] 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.

3.5 PROFINET

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

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	Proficy Machine Edition	I/O device
PROFINET DCP	Client	Server

Supporting this path will allow Proficy 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*.

Network Discovery & 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 I/O controller	Remote I/O controllers and I/O devices
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.

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 ring physical 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 IED's (Intelligent Electronic Devices) in a power transmission or distribution substation.

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 Proficy Machine Edition can directly read the IEC 61850 Object model from the remote device. Doing this requires supporting the following communication path:

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

Supporting this path allows Proficy 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.

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.

Link Layer Protocols

Protocol	EtherType
ARP	0x0806
LLDP	0x88cc

Internet Layer Protocols

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

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.

Application Layer Protocols

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		
Modbus TCP	502		
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		
Telnet	23		
Set Temporary IP	1		
IEC 61850 Client	102		

Notes

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.

PACSystems RXi modules

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

PACSystems RX3i modules

Security Capability	IC695-CP-E305	IC695-CP-E310	IC695-CP-U310	IC695-CP-U315	IC695-CP-U320	IC695-CR-U320	IC695-CP-E330	IC695E-TM001	IC695-NIU001	IC695-NIU001+	IC695-PN-C001	IC695-EC-M850
Predefined set of Subjects & Access Rights	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Plaintext Login	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Secure Login (SRP-6a)	✓	✓		✓	✓	✓	✓			✓		
Access Control List	✓	✓		✓	✓	✓	✓			✓		
Firmware Signatures							✓					✓†

† Secure Firmware upgrade supported via RX3i Controllers using Winloader.

PACSystems RX7i modules

Security Capability	IC695CPE305	IC695CPE310	IC695CPU310	IC695CPU315	IC695CPU320	IC695CRU320	IC695ETM001	IC695NIU001
Predefined set of Subjects & Access Rights	✓	✓	✓	✓	✓	✓	✓	✓
Access Control List								
Secure Login (SRP-6a)								
Plaintext Login	✓	✓	✓	✓	✓	✓	✓	✓
Firmware Signatures								

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 table below.

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
	PROFINET Controller command shell	Telnet	Anonymous PNC admin
	Web Server	HTTP	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	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.

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 GFK-2222, *PACSystems CPU Reference Manual* includes a description of the features allowed at each of the Service Request authentication levels (refer to the section, *System Security* 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.

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.								
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.

Physical Access

The PACSystems RX3i and RX7i 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.

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.

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
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).									

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 GFK-2816. For other PACSystems controllers, refer to GFK-2224, *TCP/IP Ethernet Communications for PACSystems User's Manual*.

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 Proficy Machine Edition.

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.

4.3 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 a particular installation's security requirements.

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.

Authentication Available on PACSystems Servers

Functionality		Application Protocol	Authentication Options
Ethernet	Service Requests	SRTP	Secure login (SRP-6a) Plaintext login Disabled
	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
	PROFINET Controller command shell	Telnet	Plaintext login
	Web Server	HTTP	None
	Update Web Pages	FTP	Plaintext login
	Web Server Firmware Update	HTTP	None†
	Network Management	SNMP v2c	None††
	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

Functionality	Application Protocol	Authentication Options

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

[††]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.

Authentication Supported by PACSystems Clients

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

[†] 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.

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.

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 a particular installation's security requirements.

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 Proficy 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 *Proficy Machine Edition*.

4.3.4 Recommendations

GE Intelligent Platforms 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, GE Intelligent Platforms strongly recommends that the Secure Login feature be used since it prevents network entities from sniffing plaintext passwords.

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.

GE Intelligent Platforms strongly recommends the use of long (7 characters or more), complex passwords wherever passwords are used for authentication.

Functionality	Authenticated Subjects	How Passwords are assigned
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 *Proficy 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.
PROFINET Controller command shell	PNC admin	Changed directly on the PROFINET Controller command shell by running the following command: `loginCfg password` Max of 10 characters in password.
ECM command shell	admin	Changed directly on the ECM850 command shell by running the following command: `loginCfg password` Max of 10 characters in password.
Ethernet Station Manager	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
Update Web Pages	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.
Web Server Firmware Update	FW update user	Static login and password

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 or not it was malicious.

Currently, none 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.

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
	Modbus TCP	N	N
	PROFINET DCP	N	N
	PROFINET I/O	N	N
	IEC 61850 Client	N	N
	MRP	N	N
	RDS	N	N
	Remote Station Mgr	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 General Electric Company, 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. Proficy 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.

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.

GE Intelligent Platforms recommends disabling, on each PACSystems product, all ports, services and protocols that aren't required for the intended application.

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.

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.

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 or RX7i, 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.

Disabling Ethernet Services

Service	Parameter name	Value
BOOTP Client	Use BOOTP for IP Address	False
FTP Server	Max FTP Server Connections	0
IP Routing	Gateway IP Address	0.0.0.0
DNS Client	Name Server IP Address	0.0.0.0
SNTP Client	Network Time Sync	None
Web Server	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 GFK-2224, *TCP/IP Ethernet Communications for PACSystems User's Manual*.

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 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`

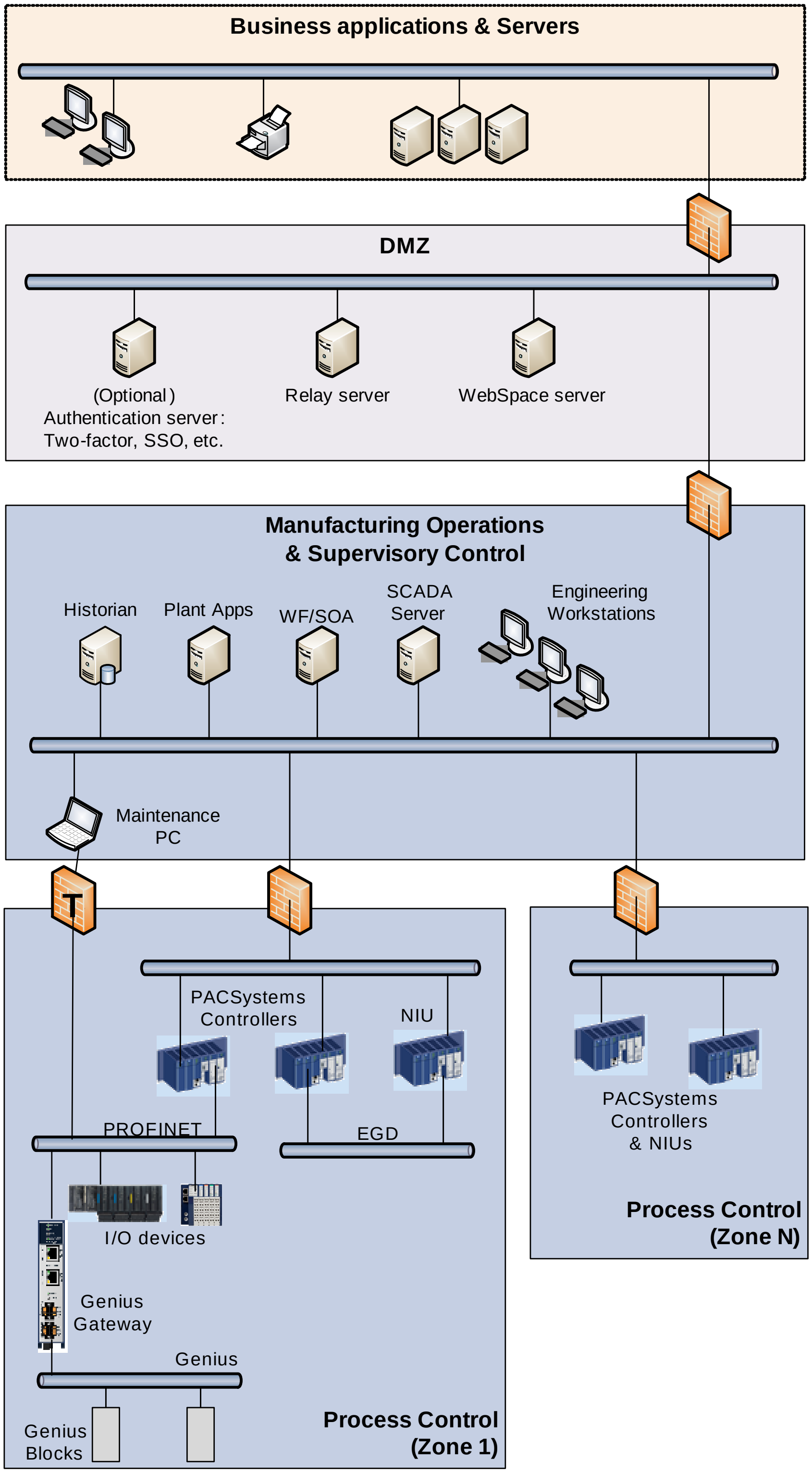
Notes

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

The following figure shows a reference deployment of PACSystems components.



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 Proficy 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 doesn't 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 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 aren't 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 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 Proficy 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 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 aren't needed for performing maintenance functions.

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 Additional Guidance

7.3.1 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

7.3.2 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 cybersecurity 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 & operating a cyber-security program, including recommended technologies for industrial automation and control systems.

GE Intelligent Platforms

1-800-433-2682
1-434-978-5100
www.ge-ip.com