GE's
Automation &
Controls

GFK-2904C

PROFINET I/O Devices
Secure Deployment Guide

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: February 2017
Issued: Mar 2014

*** 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 / Feb 2017	Throughout document	Updated for replacement IC695PNS001
Rev B / June 2016	Throughout document	Replaced “GE Intelligent Platforms” with “GE’s Automation & Controls” where used. This includes URLs.
	Section, Lower Level Protocol	Updated Internet Layer Protocols table to include IGMP
Rev A / July 2014	Section, *Genius Gateway*	Added new section
	Section, *Reference Architecture*	Updated diagram to include Genius Gateway

Safety Symbol Legend

Warning

Indicates a procedure, condition, or statement that, if not strictly observed, could result in personal injury or death.

Caution

Indicates a procedure, condition, or statement that, if not strictly observed, could result in damage to or destruction of equipment.

Attention

Indicates a procedure, condition, or statement that should be strictly followed to improve these applications.

Note Notes call attention to information that is especially significant to understanding and operating the equipment.

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)

Notes

Contents

1 About this Guide

This document provides information that can be used to help improve the cyber security of systems that include GE's Automation & Controls PROFINET I/O devices. It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring PROFINET I/O products.

Secure deployment information is provided in this manual for the following GE's Automation & Controls products.

Family	Catalog Number	Description
PACSystems RX3i	IC695PNS001	PROFINET Scanner module
PACSystems RX3i	IC695GCG001	Genius Communications Gateway

1.1 Related Documents

GFK-2816, PACSystems RXi Distributed I/O Controller User's Manual
GFK-2222, PACSystems CPU Reference Manual
GFK 2314, PACSystems RX3i System Manual
GFK-2571, PACSystems RX3i PROFINET Controller Manual
GFK-2737, PACSystems RX3i PROFINET Scanner Manual
GFK-2883, PACSystems RX3i CEP User's Manual
GFK-2892, PACSystems RX3i Genius Communications Gateway User's Manual

Notes

2 Introduction

This section introduces the fundamentals of security and secure deployment.

2.1 Security

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

- Confidentiality: Ensure only the people you want to see information can see it.
- Integrity: Ensure the data is what it is supposed to be.
- Availability: Ensure the system or data is available for use.

GE's Automation & Controls recognizes the importance of building and deploying products with these concepts in mind and encourages customers to take appropriate care in securing their GE's Automation & Controls products and solutions.

Note As GE's Automation & Controls 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. GE Product Security Advisories can be found at the following location:

https://digitalsupport.ge.com/communities/en_US/Article/GE-Intelligent-Platforms-Security-Advisories

---

2.2 Firewall

Firewalls and other network security products, including Data Diodes and Intrusion Prevention Devices, can be an important component of any security strategy. However, a strategy based solely on any single security mechanism will not be as resilient as one that includes multiple, independent layers of security.

Therefore, GE's Automation & Controls recommends taking a *Defense in Depth* approach to security.

2.3 Defense in Depth

Defense in Depth is the concept of using multiple, independent layers of security to raise the cost and complexity of a successful attack. To carry out a successful attack on a system, an attacker would need to find not just a single exploitable vulnerability, but would need to exploit vulnerabilities in each layer of defense that protects an asset.

For example, if a system is protected because it is on a network protected by a firewall, the attacker only needs to circumvent the firewall to gain unauthorized access. However, if there is an additional layer of defense, for example, 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's Automation & Controls products and solutions.

- The PROFINET I/O Devices 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 the section, 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 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 GE's Automation & Controls product security updates, SIMs, and other recommendations.
- Apply all of the latest operating system security patches to control systems computers.
- Use anti-virus software on control systems computers and keep the associated anti-virus signatures up-to-date.
- Use whitelisting software on control systems computers and keep the whitelist up-to-date.

2.5 Checklist

This section provides a sample checklist to help guide the process of securely deploying PROFINET I/O 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. (See 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. (See section 6, Network Architecture & Secure Deployment.)
5. Configure firewalls and other network security devices. (See section 3.6, Ethernet Firewall Configuration and section 6, Network Architecture & Secure Deployment.)
6. Enable and/or configure the appropriate security features on each PROFINET I/O Device. (See section 4, Security Capabilities.)
7. On each PROFINET I/O Device, change every supported password to something other than its default value. (See section 4.4, Password Management.)
8. Harden the configuration of each PROFINET I/O Device, disabling unneeded features, protocols and ports. (See 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, see section 7.3, Additional Guidance.

Notes

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 chapter 5, *Configuration Hardening*), and by using appropriately configured and deployed network security devices (for example, firewalls and routers) to block every protocol (whether disabled or not) that doesn't need to pass from one network/segment to another.

GE's Automation & Controls 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.

To support PROFINET communication between two nodes, the network must also support UDP, IP, and ARP in both directions between the nodes.

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

Note On a PROFINET I/O device, support for these protocols may be provided by a peripheral module (for example, a PROFIBUS or Serial Communications 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 Supported Protocols

3.1.1 ETHERNET Protocols

This section indicates which Ethernet protocols are supported, and by which PROFINET I/O Devices. 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	RX3i		
		IC695PNS001-Axxx	**IC695PNS001-BAxx**	**IC695GCG001**
Link	ARP	✓	✓	✓
	LLDP	✓	✓	✓
Internet	IPv4	✓	✓	✓
	ICMP	✓	✓	✓
Trans	TCP		✓	✓
	UDP	✓	✓	✓
Application Layer	DCE/RPC Client	✓	✓	✓
	DCE/RPC Server	✓	✓	✓
	PROFINET DCP client			
	PROFINET DCP server	✓	✓	✓
	PROFINET I/O	✓	✓	✓
	HTTP Server		✓	
	HTTPS Server		✓	
	MRP	✓	✓	✓
	SNMP v1 server			✓
	SNMP v2c server			

3.1.2 Serial Protocols

In addition to Ethernet, PROFINET I/O Devices may also support communication over serial ports (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 PROFINET I/O Devices. Note that some of the supported protocols may not be required in a given system, since the installation may only be using a subset of the available protocols.

Protocol	**IC695PNS001-Axxx**
SNP Slave†	✓
† SNP functionality may be limited. For example, it may only provide Firmware Update Services.	

3.2 Service Requests

The GE's Automation & Controls Service Request protocol is a proprietary, media-independent application protocol that provides access to services of GE's Automation & Controls products. 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 & 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, SNP is used for transporting it over a serial channel. Almost all 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 a media-specific protocol such as SNP between those two nodes.

3.2.1 SNP

Firmware Update The SNP protocol is often used in GE's Automation & Controls PROFINET I/O Devices to support updating the firmware on products or on an installed module that supports having its firmware updated over the backplane. SNP is used to send Service Requests to a node via a serial connection, and to convey the results back to the client.

Protocol	WinLoader.exe (Windows® Computer)	I/O Device
SNP	Master	Slave

3.3 PROFINET

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

3.3.1 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	Proficy Machine Edition	I/O Device
PROFINET DCP	Client	Server

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.

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.) Proficy Machine Edition implements the Client functionality directly from the computer network adapter, so I/O devices must be local to the computer's network adapter. It can then be used to (re-)assign a unique name to the I/O device being installed.

3.3.2 Network Discovery and Device Identification

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

Protocol	Local I/O Controller	Remote I/O Controllers and I/O Devices
DCE/RPC	Client	Server
PROFINET DCP	Client	Server

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

3.3.3 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 ring physical topology) then the following application protocol must also be supported.

Protocol	I/O Controller	I/O Device
MRP	Bi-directional	Bi-directional

3.4 Ethernet Firewall Configuration

Refer to the section Reference Architecture for a diagram showing firewall placement.

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 PROFINET I/O Devices.

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

3.4.1 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	ETHERNET Type
ARP	0x0806
LLDP	0x88cc

Internet Layer Protocols

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

Transport Layer Protocols

Protocol	ETHERNET Type	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 PROFINET products.

3.4.2 Application Layer Protocols

PROFINET devices are capable of acting as a server, responding to requests sent via 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.

Application Layer Protocols

Protocol	Server TCP Port	Destination UDP Port	ETHERNET Type (non-IP protocol)
DCE/RPC		34964 on server >1023 on client	
HTTP	80		
HTTPS	443		
PROFINET DCP			0x8892
PROFINET I/O			0x8892
MRP			0x88e3
SNMP v1		161 on server >1023 on client	

4 Security Capabilities

This section describes the GE's Automation & Controls PROFINET I/O Device 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 PROFINET module.

Security Capability	IC695PNS001-AXXX	IC695PNS001-BAxx	IC695GCG001
Predefined set of Subjects and Access Rights	✓	✓	✓
Plaintext Login			
Access Control List			
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 GE's Automation & Controls PROFINET I/O Devices, 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.

GE's Automation & Controls PROFINET I/O Devices, however, don'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 on a particular protocol. In such cases, authorization is based on the functionality being used and the password that is provided for authentication. Nevertheless, the authentication features supported on PROFINET I/O Devices implicitly define a fixed set of subjects, which are identified here.

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

Subjects Available on GE's Automation & Controls PROFINET I/O Devices

Trans-port Medium	Functionality	Application Protocol	Subjects Available
Serial	Firmware Update	SNP Slave	Anonymous
Ethernet	Web Server	HTTP	Anonymous
	Web Server Firmware Update	HTTP	Firmware Updater
	Web Server Password Reset	HTTPS	Anonymous

4.2.2 Specifying Access Rights

For each subject, GE's Automation & Controls PROFINET I/O Devices provide predefined access rights.

4.2.2.1 Predefined Access Rights

Using the SNP Slave Application Protocol to update firmware on a PROFINET I/O Device, the Anonymous Subject is granted the same Service Request PRIV Level as the highest *PRIV Level user* that currently has no password. This equates to PRIV Level 4 user on PROFINET I/O Devices which allows Write Access to support the Firmware Update Functionality.

4.2.2.2 Physical Access

The Web Server Password Reset feature requires physical access to the PROFINET I/O Device to assign the Firmware Updater password.

4.2.3 Enforcement

Each of the PROFINET I/O Devices enforces the access rights for the data and services that it provides.

4.3 Authentication

GE's Automation & Controls PROFINET I/O Devices may provide 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 particularinstallation's security requirements.

Note The default configuration for all Server protocols except Web Server Firmware Update is for no authentication, or for authentication using well-known default values.

4.3.1 Server Protocols

This section summarizes the authentication mechanisms supported by PROFINET I/O Devices for each protocol. It is important to note that some PROFINET I/O Devices only support a subset of the options listed here. See section 4.1, Capabilities by Product for more details.

Authentication Available on Servers

Trans-port Medium	Functionality	Application Protocol	Subjects Available
Serial	Firmware Update	SNP Slave	None
Ethernet	Web Server	HTTP	None
	Web Server Firmware Update	HTTP	Firmware Updater

4.3.2 Authentication Supported by the PROFINET Protocol

The PROFINET I/O specification does not define an authentication mechanism and so none is supported on GE's Automation & Controls PROFINET I/O Device PROFINET communications.

4.3.3 Plaintext Login

Authentication for a protocol may involve sending a plaintext password to the Server. 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.

4.3.4 Recommendations

GE's Automation & Controls 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.

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

1. 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 in the section Reference Architecture 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.
2. 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.

3. 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.
4. 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.
5. 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.
6. To limit the impact of the compromise of any single user account, it is recommended to divide administrator privileges into several user accounts, each for its own operational function.
7. 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.
8. Carefully protect sources of and access to credentials (user names, passwords) for all ICS equipment, including switches, routers, firewalls, IDS, IPS, etc.
9. 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 the 4.2.1 Authorization framework section, 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.

Changing Passwords

Functionality	Authenticated Subjects	How Passwords are assigned
Firmware Update	PRIV Level 4 user	Static login and password
Web Server Firmware Update	Firmware Updater	Through Web Server Reset Password webpages. 8-16 characters At least one lower case At least one upper case At least one number (0-9) At least one special character: !"#%&'()*+,-./:;< = >?@[\]^_`{|}~

4.5 Confidentiality and Integrity

4.5.1 Communication 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, only the Web Page Reset Password HTTPS communications provides Encryption. None of other the communications protocols supported by PROFINET I/O Devices provide either of these features, as detailed in the table below. Therefore, compensating controls may be required to meet an installation's security requirements for protecting data in-flight.

Protocol-provided Security Capabilities

Transport Medium	Protocol	Data Encryption	Message Authentication Codes
ETHERNET	DCE/RPC	N	N
	HTTP	N	N
	HTTPS	Y	N
	PROFINET DCP	N	N
	PROFINET I/O	N	N
	MRP	N	N
Serial	SNP Slave	N	N

4.5.2 Firmware Signatures

Some GE's Automation & Controls PROFINET I/O Devices may have digitally signed firmware images to provide cryptographic assurance of the firmware's integrity. For PROFINET I/O Devices that support this feature, a digital signature is used to verify that any firmware being loaded onto the module 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

GE's Automation & Controls PROFINET I/O Devices do not provide a dedicated security log embedded within the module, nor do they integrate with an external Security Information and Event Management (SIEM) system.

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 PROFINET I/O Devices 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's Automation & Controls recommends disabling, on each PROFINET I/O Device, all ports, services, and protocols that aren't required for the intended application.

5.1 Scanner

This section provides information to use when hardening the configuration of a PROFINET I/O Device Scanner or it's DAP (Device Access Point). These options should be considered when configuring any PROFINET I/O Device that supports them.

Service	How to Disable
IP Routing	Set *Gateway IP Address* to 0.0.0.0 in the hardware configuration and download to the PROFINET I/O controller.
Ethernet Port Enable	Set Port Speed of Port submodule to Disabled in the hardware configuration and download to the PROFINET I/O controller. This will prevent the port from powering up and establishing a link. This setting is retained over a power cycle.
SD Card Identity	Set the name of the Device using a DCP Client with the SD Card inserted. Remove SD Card and enable the physical Write-Protect feature on the SD Card. Re-insert the SD Card in the Scanner. This will prevent future attempts to rename the Scanner from persisting over a power cycle.
Front Panel Ethernet Port	Set IP Address, Subnet Mask, and Gateway IP Address to 0.0.0.0 in the hardware configuration and download to the PROFINET I/O Controller. No Web Server access or firmware update functionality will be available through the front panel Ethernet port.
Firmware Update During RUN Mode	Clear the IC695PNS001-BAxx control bit to disable firmware updates while the unit is connected to a PROFINET IO Controller that is in RUN mode.

5.2 Genius Gateway

This section provides information to use when hardening the configuration of and access to a Genius Communications Gateway.

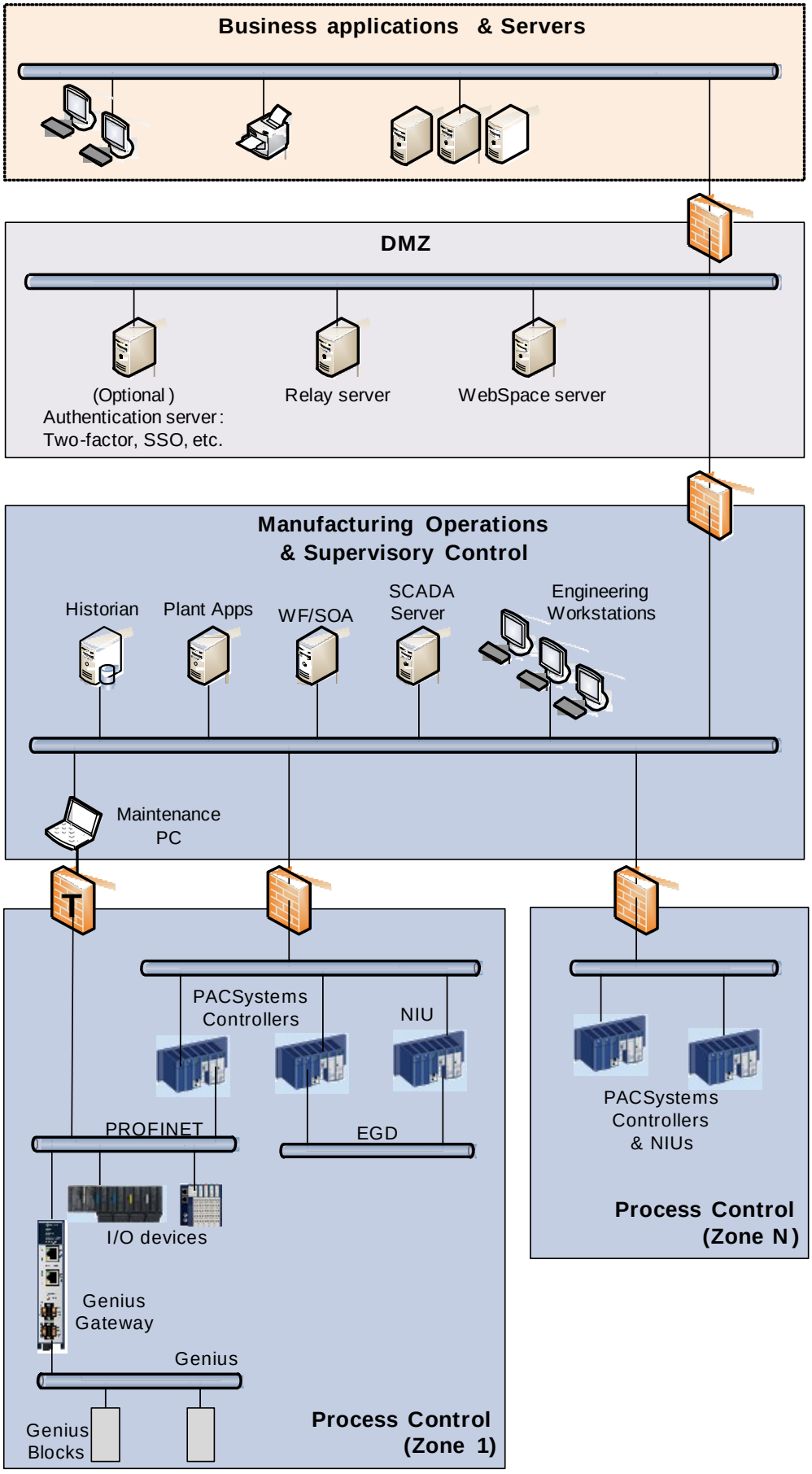
Service	How to Disable
IP Routing	Set *Gateway IP Address* to 0.0.0.0 in the hardware configuration and download to the PROFINET I/O controller.
SD Card Identity	Set the name of the Device using a DCP Client with the SD Card inserted. Remove SD Card and enable the physical Write-protect feature on the SD Card. Re-insert the SD Card in the Gateway. This will prevent future attempts to rename the Scanner from persisting over a power cycle.
Physical Access	Restrict physical access to the rear of the Gateway. Consider the use of secure screws when mounting the Gateway. This will prevent future attempts to perform an unauthorized firmware upgrade by restricting access to the SD card and the firmware upgrade pushbutton.

6 Network Architecture and Secure Deployment

This section provides security recommendations for deploying GE's Automation & Controls PROFINET I/O Devices in the context of a larger network.

6.1 Reference Architecture

The following figure shows a reference deployment of GE's Automation & Controls components.


Business applications & Servers
DMZ
(Optional)
Authentication server:
Two-factor, SSO, etc.
Relay server
WebSpace server
Manufacturing Operations
& Supervisory Control
Historian
Plant Apps
WF/SOA
SCADA
Server
Engineering
Workstations
Maintenance
PC
PACSystems
Controllers
NIU
PROFINET
EGD
I/O devices
Genius
Gateway
Genius
Genius
Blocks
Process Control
(Zone 1)
PACSystems
Controllers
& NIUs
Process Control
(Zone N)

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

A Demilitarized Zone (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 and 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 and 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 3.5 PROFINET, this can be 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 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.

Transparent mode is noted by the use of a T on the firewall in the Reference Architecture diagram.

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 PROFINET I/O Device be temporarily taken out of service.

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 protocol is generally expected to operate with small, known, worst-case bounds on its 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 and operating a cybersecurity program, including recommended technologies for industrial automation and control systems.

Notes

Automation & Controls from GE

1-800-433-2682
1-434-978-5100
www.geautomation.com